Unable to locate subtitle

AWS Snowball Edge Guía para desarrolladores

AWS Snowball Edge Guía para desarrolladores: ***Unable to locate subtitle***

Table of Contents

¿Qué es AWS Snowball Edge?

AWS Snowball Edge es un tipo de dispositivo Snowball con capacidad de cómputo y almacenamiento integrados para determinadas funciones. AWS Snowball Edge puede procesar datos localmente y ejecutar cargas de trabajo de computación perimetral, además de transferir datos entre su entorno local y el Nube de AWS entorno local. Nube de AWS

Cada uno de los dispositivos Snowball Edge puede transportar datos a velocidades superiores a las de Internet. Para transportar los datos, estos se envían en los dispositivos a través de un transportista regional. Los dispositivos son resistentes e incluyen etiquetas de envío de tinta electrónica.

Los dispositivos Snowball Edge tienen tres opciones de configuración: optimizados para almacenamiento, optimizados para cómputo y optimizados para cómputo con GPU. Cuando en esta guía se mencionen los dispositivos Snowball Edge, se estará haciendo referencia a todas las opciones del dispositivo. Siempre que una determinada información se aplique exclusivamente a una o varias configuraciones opcionales de los dispositivos (por ejemplo, cómo los dispositivos Snowball Edge con GPU tienen una GPU incorporada), se indicará expresamente. Para obtener más información, consulte Configuraciones de dispositivos Snowball Edge.

Temas

AWS Snowball Características de Edge

Los dispositivos Snowball Edge tienen las siguientes características:

- Grandes cantidades de capacidad de almacenamiento o funcionalidad de computación para los dispositivos. Esto depende de las opciones que elija al crear el trabajo.
- Adaptadores de red con una velocidad de transferencia de hasta 100 Gbits por segundo.
- Se aplica el cifrado, con el que se protegen los datos en reposo y en tránsito físico.
- Puede importar o exportar datos entre los entornos locales y Amazon S3. Los datos se transportan físicamente a través de uno o varios dispositivos sin necesidad de usar Internet.
- Los dispositivos Snowball Edge actúan como contenedores resistentes. La pantalla de tinta electrónica integrada cambia para mostrar la etiqueta de envío cuando el dispositivo está listo para enviarse.
- Los dispositivos Snowball Edge tienen una pantalla LCD integrada que se puede usar para administrar las conexiones de red y obtener información sobre el estado del servicio.
- Los dispositivos Snowball Edge se pueden agrupar en clústeres de entre tres y 16 dispositivos distintos para que los trabajos de computación y almacenamiento locales obtengan una gran durabilidad de los datos, así como para ampliar o reducir el almacenamiento local a petición.
- Puede usar Amazon EKS Anywhere en dispositivos Snowball Edge para las cargas de trabajo de Kubernetes.
- Los dispositivos Snowball Edge disponen de puntos de conexión compatibles con Amazon S3 y Amazon EC2, lo que permite realizar casos de uso mediante programación.
- Los dispositivos Snowball Edge admiten los nuevos tipos de instancia `sbe1`, `sbe-c` y `sbe-g`, que puede utilizar para ejecutar instancias de computación en el dispositivo a través de imágenes de máquina de Amazon (AMI).
- Snowball Edge admite los siguientes protocolos de transferencia de datos para la migración de datos:
  - NFSv3
  - NFSv4
  - NFSv4.1
  - Amazon S3 a través de HTTP o HTTPS (mediante una API compatible con la versión 1.16.14 y anteriores de AWS CLI)

Servicios relacionados con Edge AWS Snowball

Puede utilizar un AWS Snowball Edge dispositivo con los siguientes AWS servicios relacionados:

- Adaptador Amazon S3: se utiliza para la transferencia programática de datos de entrada y salida AWS mediante la API de Amazon S3 para Snowball Edge, que admite un subconjunto de operaciones de la API de Amazon S3. En esta función, los datos se transfieren al dispositivo Snow AWS en tu nombre y el dispositivo se te envía (para un trabajo de exportación), o te AWS envía un dispositivo Snow vacío y tú transfieres los datos de tus fuentes locales al dispositivo y los devuelves a AWS (para un trabajo de importación)»
- Almacenamiento compatible con Amazon S3 en dispositivos Snow Family: utilícelo para satisfacer las necesidades de datos de servicios de computación como Amazon EC2, Amazon EKS Anywhere para Snow y otros. Esta función está disponible en los dispositivos Snowball Edge y proporciona un conjunto ampliado de API de Amazon S3 y funciones como una mayor resiliencia con una configuración de clústeres flexible para 3 a 16 nodos, administración de buckets locales y notificaciones locales.
- Amazon EC2: ejecute instancias de computación en un dispositivo Snowball Edge mediante el punto de conexión compatible con Amazon EC2, que admite un subconjunto de operaciones de la API de Amazon EC2. Para obtener más información acerca del uso de Amazon EC2 en AWS, consulte Introducción a las instancias de Linux de Amazon EC2.
- Amazon EKS Anywhere para Snow: cree y utilice clústeres de Kubernetes en dispositivos Snow Family. Consulte Uso de Amazon EKS Anywhere on AWS Snow.
- AWS Lambda impulsado por AWS IoT Greengrass: invoque funciones Lambda basadas en el almacenamiento compatible con Amazon S3 en dispositivos de la familia Snow, acciones de almacenamiento realizadas en AWS Snowball Edge un dispositivo. Para obtener más información acerca del uso de Lambda, consulte Uso AWS Lambda con un AWS Snowball borde y la Guía para desarrolladores de AWS Lambda.
- Amazon Elastic Block Store (Amazon EBS): proporcione volúmenes de almacenamiento de nivel de bloque para su uso con instancias compatibles con EC2. Para obtener más información, consulte Amazon Elastic Block Store (Amazon EBS).
- AWS Identity and Access Management (IAM): utilice este servicio para controlar de forma segura el acceso a los recursos. AWS Para obtener más información, consulte ¿Qué es IAM?
- AWS Security Token Service (AWS STS): solicite credenciales temporales con privilegios limitados para los usuarios de IAM o para los usuarios que autentique (usuarios federados). Para más información, consulte Credenciales de seguridad temporales en IAM.
- Amazon EC2 Systems Manager: utilice este servicio para ver y controlar su infraestructura en AWS. Para obtener más información, consulte ¿Qué es AWS Systems Manager?

Acceder al servicio Snow Family

Puede usar la API de administración de trabajos Consola de administración de la familia de productos Snow de AWSo la API de administración de trabajos para crear y administrar trabajos. Para obtener más información acerca del uso de Consola de administración de la familia de productos Snow de AWS, consulte Introducción. Para obtener más información sobre la API de administración de trabajos, consulte la Referencia de la API de administración de trabajos de AWS Snowball.

Acceso a un dispositivo AWS Snowball Edge

Una vez instalado el dispositivo Snowball Edge, puede configurarlo con una dirección IP desde la pantalla LCD y, a continuación, desbloquear el dispositivo mediante el cliente de Snowball Edge o AWS OpsHub for Snow Family. Después, puede realizar tareas de transferencia de datos o de computación periférica. Para obtener más información, consulte Uso de un dispositivo AWS Snowball Edge.

Precios de AWS Snowball Edge

Para obtener información sobre los precios y las tarifas del servicio y sus dispositivos, consulte Precios de AWS Snowball Edge.

Supervisión de dispositivos

AWS supervisará el dispositivo Snow y podrá recopilar métricas e información de uso cuando el dispositivo Snow esté conectado a un Región de AWS. Si el dispositivo Snow no está conectado al Región de AWS, no supervisará el dispositivo Snow. AWS

Si AWS detecta un problema irreparable y es necesario sustituir el equipo físico, AWS se lo comunicaremos. A continuación, podrá realizar un trabajo de reemplazo que le enviaremos a sus instalaciones. Esto no conlleva ningún cargo adicional, ya que el monitoreo de los dispositivos Snow está incluido como parte de la tarifa de servicio del dispositivo Snow.

Recursos para usuarios primerizos AWS Snowball

Si es la primera vez que utiliza el servicio AWS Snow Family, le recomendamos que lea las siguientes secciones en orden:

1. Para obtener más información sobre las opciones y los tipos de dispositivos, consulte AWS Snowball Información sobre el hardware del dispositivo perimetral.
2. Para obtener más información sobre los tipos de trabajos, consulte Descripción de AWS Snowball Edge Jobs.
3. Para obtener end-to-end información general sobre cómo usar un AWS Snowball Edge dispositivo, consulteCómo funciona AWS Snowball Edge.
4. Cuando esté listo para empezar, consulte Introducción.
5. Para obtener información acerca del uso de instancias de computación en un dispositivo, consulte Uso de instancias de computación compatibles con Amazon EC2.

AWS Snowball Información sobre el hardware del dispositivo perimetral

Todos los dispositivos Snowball Edge comparten características físicas, como el tamaño y el peso, pero contienen diferentes tipos de hardware para adaptarse al uso previsto. Los dispositivos diseñados para la transferencia de datos se configuran con más capacidad de almacenamiento y los dispositivos diseñados para la informática se configuran con más CPU y memoria virtuales. En esta sección se proporciona información sobre las características físicas de los dispositivos Snowball Edge y sus especificaciones de procesamiento y almacenamiento.

Temas

Configuraciones de dispositivos Snowball Edge

Los dispositivos Snowball Edge cuentan con las siguientes opciones de configuración:

- Optimizado para el almacenamiento de Snowball Edge (para la transferencia de datos): esta opción de dispositivo Snowball Edge tiene 80 TB de capacidad de almacenamiento utilizable.
- 210 TB con almacenamiento optimizado para Snowball Edge: esta opción de dispositivo Snowball Edge tiene 210 TB de capacidad de almacenamiento utilizable.

- Optimizado para el almacenamiento de Snowball Edge (con funcionalidad de procesamiento compatible con EC2): esta opción de dispositivo Snowball Edge tiene hasta 80 TB de capacidad de almacenamiento utilizable, 40 vCPU y 80 GB de memoria para la funcionalidad de procesamiento. También incluye 1 TB de capacidad de almacenamiento SSD adicional para los volúmenes de bloques conectados a las AMI compatibles con Amazon EC2.
- Snowball Edge optimizado para computación: este dispositivo Snowball Edge (con un procesador AMD EPYC Gen2) es el que tiene la mayor funcionalidad de computación, con hasta 104 CPU virtuales, 416 GB de memoria y 28 TB de SSD NVMe dedicado para instancias de computación.

  Snowball Edge, optimizado para computación (con AMD EPYC Gen1), tiene hasta 52 vCPU, 208 GB de memoria, 39,5 TB de capacidad de almacenamiento utilizable y 7,68 TB de SSD NVMe dedicado para instancias de cómputo.
- Snowball Edge optimizado para computación con GPU: esta opción de dispositivo Snowball Edge es idéntica a la opción optimizada para computación (con un procesador AMD EPYC Gen1) e incluye una unidad de procesamiento de gráficos (GPU) instalada. La GPU es equivalente a la disponible en el tipo de instancia P3 compatible con Amazon EC2.

> **Note**
>
> Al utilizar el almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow en estos dispositivos, el almacenamiento utilizable variará. Consulte Uso de almacenamiento compatible con Amazon S3 en dispositivos de la familia Snow en dispositivos de la familia Snow para conocer la capacidad de almacenamiento con almacenamiento compatible con Amazon S3 en dispositivos de la familia Snow.

Para obtener más información acerca de la funcionalidad de computación de estas tres opciones, consulte Uso de instancias de computación compatibles con Amazon EC2. Aquí se describen las diferencias en cuanto a la creación de trabajos y la capacidad del disco en terabytes.

> **Note**
>
> Cuando hablamos de dispositivos Snowball Edge, esto incluye todas las variantes opcionales del dispositivo. Siempre que una determinada información se aplique exclusivamente a una o varias configuraciones opcionales de los dispositivos (por ejemplo, si la opción

Snowball Edge optimizado para computación con GPU tiene un dispositivo periférico de GPU integrado), se indicará expresamente.

En la siguiente tabla, se resumen las diferencias entre las distintas opciones de dispositivos. Para obtener información acerca de las especificaciones de hardware, consulte AWS Snowball Especificaciones de los dispositivos Edge.

	Snowball Edge optimizado para almacenamiento (para la transferencia de datos)	Snowball Edge optimizado para almacenamiento con 210 TB	Snowball Edge optimizado para almacenamiento (con funcionalidad de computación de EC2)	Snowball Edge optimizado para computación con un procesador AMD EPYC Gen2 y NVME	Snowball Edge optimizado para computación con un procesador AMD EPYC Gen1, HDD y 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
vCPU	40	104	40	104	52
Memoria utilizable	80 GB	416 GB	80 GB	416 GB	208 GB
Tarjeta de seguridad	Sí	Sí	Sí	Sí	Sí
GPU (opcional)	Ninguna	Ninguna	Ninguna	Ninguna	NVidia V100
SSD	SATA de 1 TB	NVMe de 210 TB	SATA de 1 TB	NVMe de 28 TB	NVMe de 7,68 TB

	Snowball Edge optimizado para almacenamiento (para la transferencia de datos)	Snowball Edge optimizado para almacenamiento con 210 TB	Snowball Edge optimizado para almacenamiento (con funcionalidad de computación de EC2)	Snowball Edge optimizado para computación con un procesador AMD EPYC Gen2 y NVME	Snowball Edge optimizado para computación con un procesador AMD EPYC Gen1, HDD y GPU opcional
HDD utilizable	80 TB	No aplicable	80 TB	No aplicable	39,5 TB utilizables
Interfaces de red	• 2 x 10 Gbit: RJ45 (uno utilizable) • 1x 25 Gbit — SFP28 • 1x 100 Gbit — QSFP28	• 2 x 10 Gbit: RJ45 (uno utilizable) • 1x 25 Gbit — SFP28 • 1x 100 Gbit — QSFP28	• 2 x 10 Gbit: RJ45 (uno utilizable) • 1x 25 Gbit — SFP28 • 1x 100 Gbit — QSFP28	• 2 x 10 Gbit: RJ45 (uno utilizable) • 1x 25 Gbit — SFP28 • 1x 100 Gbit — QSFP28	• 2 x 10 Gbit: RJ45 (uno utilizable) • 1x 25 Gbit — SFP28 • 1x 100 Gbit — QSFP28

	Snowball Edge optimizado para almacenamiento (para la transferencia de datos)	Snowball Edge optimizado para almacenamiento con 210 TB	Snowball Edge optimizado para almacenamiento (con funcionalidad de computación de EC2)	Snowball Edge optimizado para computación con un procesador AMD EPYC Gen2 y NVME	Snowball Edge optimizado para computación con un procesador AMD EPYC Gen1, HDD y GPU opcional
Características de seguridad física	• Tornillos magnéticos ocultos • Conmutadores de intrusión • Etiquetas NFC • Elementos antimanipulación • Aplicación Android para detección de manipulaciones • GPS y celular • Revestimiento conformado	• Tornillos magnéticos ocultos • Conmutadores de intrusión • Etiquetas NFC • Elementos antimanipulación • Aplicación Android para detección de manipulaciones • Revestimiento conformado	• Tornillos magnéticos ocultos • Conmutadores de intrusión • Etiquetas NFC • Elementos antimanipulación • Aplicación Android para detección de manipulaciones • GPS y celular • Revestimiento conformado	• Tornillos magnéticos ocultos • Conmutadores de intrusión • Etiquetas NFC • Elementos antimanipulación • Aplicación Android para detección de manipulaciones • Revestimiento conformado	• Tornillos magnéticos ocultos • Conmutadores de intrusión • Etiquetas NFC • Elementos antimanipulación • Aplicación Android para detección de manipulaciones • Revestimiento conformado

Casos de uso de dispositivos

En la siguiente tabla se muestran los casos de uso de los diferentes AWS Snow Family devices.

Caso de uso	Snowball Edge	AWS Snowcone	
Importación de datos a Amazon S3	✓	✓	
Exportación desde Amazon S3	✓		
Almacenamiento local duradero	✓		
Computación local con AWS Lambda	✓	✓	
Instancias de computación locales	✓	✓	
Almacenamiento de Amazon S3 de larga duración en un clúster de dispositivos	✓		
Uso con AWS IoT Greengrass (IoT)	✓	✓	
Transferencia de archivos mediante NFS con una GUI	✓	✓	
Cargas de trabajo de GPU	✓		

> **Note**
>
> Las cargas de trabajo que necesitan compatibilidad con una GPU requieren la opción Snowball Edge optimizado para computación con GPU.
> Los 210 TB optimizados para el almacenamiento de Snowball Edge admiten la transferencia de datos a través de NFS, un adaptador S3 y un almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow.

AWS Snowball Especificaciones de los dispositivos Edge

En esta sección, encontrará las especificaciones de los tipos de dispositivos AWS Snowball Edge y del hardware.

Temas

Especificaciones de los dispositivos Snowball Edge optimizados para almacenamiento (para transferencia de datos)

La siguiente tabla contiene las especificaciones de hardware de los dispositivos Snowball Edge optimizados para almacenamiento.

Elemento	Especificaciones de los dispositivos Snowball Edge optimizados para almacenamiento (para transferencia de datos)
Especificaciones de almacenamiento	
Capacidad de almacenamiento en HDD	80 TB de capacidad utilizable
Especificaciones de la fuente de alimentación	

Elemento	Especificaciones de los dispositivos Snowball Edge optimizados para almacenamiento (para transferencia de datos)
Alimentación	Regiones de AWS En EE. UU.: NEMA 5—15p 100—220 voltios. En todas las regiones de AWS se incluye un cable de alimentación
Consumo eléctrico	304 vatios para un caso de uso medio, aunque la fuente de alimentación tiene una capacidad nominal de 1200 vatios.
Voltaje	100 – 240 V CA
Frecuencia	47/63 Hz
Conexiones de datos y de red	2 x 10 Gbit: RJ45 (uno utilizable) 1x 25 Gbit — SFP28 1x 100 Gbit — QSFP28
Cables	Cada AWS Snowball Edge dispositivo envía cables de alimentación específicos para cada país. No se incluye ningún otro cable ni conector óptico. Para obtener más información, consulte Hardware de red compatible.
Requisitos térmicos	AWS Snowball Los dispositivos Edge están diseñados para operaciones de oficina y son ideales para operaciones de centros de datos.
Salida de decibelios	En promedio, un AWS Snowball Edge dispositivo produce 68 decibelios de sonido, normalmente más silencioso que el de una aspiradora o la música del salón.
Especificaciones de dimensiones y peso	

Elemento	Especificaciones de los dispositivos Snowball Edge optimizados para almacenamiento (para transferencia de datos)
Peso	49,7 libras (22,54 kg)
Altura	15,5 pulgadas (394 mm)
Ancho	10,6 pulgadas (265 mm)
Longitud	28,3 pulgadas (718 mm)
Especificaciones ambientales	
Vibración	Uso no operativo equivalente a la norma ASTM D4169 para camiones de nivel I: 0,73 GRMS
Choque	Uso operativo equivalente a 70 G (MIL-S-901) Uso no operativo equivalente a 50 G (ISTA-3A)
Altitud	Uso operativo equivalente a entre 0 y 3000 metros (0 a 10 000 pies) Uso no operativo equivalente a entre 0 y 12 000 metros
Intervalo de temperatura	0 – 45° C (operativo)

Especificaciones de los dispositivos Snowball Edge optimizados para almacenamiento de 210 TB

La siguiente tabla contiene las especificaciones de hardware de los dispositivos Snowball Edge optimizados para almacenamiento de 210 TB.

Elemento	Especificaciones de los dispositivos Snowball Edge optimizados para almacenamiento de 210 TB
Especificaciones de computación y memoria	
CPU	104 vCPU
RAM	416 GB
Especificaciones de almacenamiento	
Capacidad de almacenamiento de NVME	210 TB utilizables (para transferencia de datos NFS y de objetos)
Capacidad de almacenamiento en SSD	Ninguna
Especificaciones de la fuente de alimentación	
Alimentación	Regiones de AWS En EE. UU.: NEMA 5—15p, 100—220 voltios. En todas las regiones de AWS se incluye un cable de alimentación
Consumo eléctrico	304 vatios para un caso de uso medio, aunque la fuente de alimentación tiene una capacidad nominal de 1200 vatios
Voltaje	100 – 240 V CA
Frecuencia	47/63 Hz
Conexiones de datos y de red	2 x 10 Gbit: RJ45 (uno utilizable) 1x 25 Gbit — SFP28

Elemento	Especificaciones de los dispositivos Snowball Edge optimizados para almacenamiento de 210 TB
	1x 100 Gbit — QSFP28
Cables	Cada AWS Snowball Edge dispositivo envía cables de alimentación específicos para cada país. No se incluye ningún otro cable ni conector óptico. Para obtener más información, consulte Hardware de red compatible.
Requisitos térmicos	AWS Snowball Edge los dispositivos están diseñados para operaciones de oficina y son ideales para operaciones de centros de datos.
Salida de decibelios	De media, un AWS Snowball Edge dispositivo produce 68 decibelios de sonido, normalmente más silencioso que el de una aspiradora o la música del salón.
Especificaciones de dimensiones y peso	
Peso	49,7 libras (22,54 kg)
Altura	15,5 pulgadas (394 mm)
Ancho	10,6 pulgadas (265 mm)
Longitud	28,3 pulgadas (718 mm)
Especificaciones ambientales	
Vibración	Uso no operativo equivalente a la norma ASTM D4169 para camiones de nivel I: 0,73 GRMS
Choque	Uso operativo equivalente a 70 G (MIL-S-901) Uso no operativo equivalente a 50 G (ISTA-3A)
Altitud	Uso operativo equivalente a entre 0 y 3000 metros (0 a 10 000 pies) Uso no operativo equivalente a entre 0 y 12 000 metros

Elemento	Especificaciones de los dispositivos Snowball Edge optimizados para almacenamiento de 210 TB
Intervalo de temperatura	0 – 30° C (operativo)

Especificaciones de los dispositivos Snowball Edge optimizados para almacenamiento (con EC2)

La siguiente tabla contiene las especificaciones de hardware de los dispositivos Snowball Edge optimizados para almacenamiento (con EC2).

Elemento	Especificaciones de los dispositivos Snowball Edge optimizados para almacenamiento (con EC2)
Especificaciones de computación y memoria	
CPU	40 vCPU
RAM	80 GiB
Especificaciones de almacenamiento	
Capacidad de almacenamiento en HDD	80 TB utilizables (para almacenamiento de objetos y bloques)
Capacidad de almacenamiento en SSD	1 TB de almacenamiento SSD SATA utilizable (para almacenamiento en bloque)
Especificaciones de la fuente de alimentación	

Elemento	Especificaciones de los dispositivos Snowball Edge optimizados para almacenamiento (con EC2)
Alimentación	Regiones de AWS En EE. UU.: NEMA 5—15p, 100—220 voltios. En todas las regiones de AWS se incluye un cable de alimentación
Consumo eléctrico	304 vatios para un caso de uso medio, aunque la fuente de alimentación tiene una capacidad nominal de 1200 vatios
Voltaje	100 – 240 V CA
Frecuencia	47/63 Hz
Conexiones de datos y de red	2 x 10 Gbit: RJ45 (uno utilizable) 1x 25 Gbit — SFP28 1x 100 Gbit — QSFP28
Cables	Cada AWS Snowball Edge dispositivo envía cables de alimentación específicos para cada país. No se incluye ningún otro cable ni conector óptico. Para obtener más información, consulte Hardware de red compatible.
Requisitos térmicos	AWS Snowball Edge los dispositivos están diseñados para operaciones de oficina y son ideales para operaciones de centros de datos.
Salida de decibelios	De media, un AWS Snowball Edge dispositivo produce 68 decibelios de sonido, normalmente más silencioso que el de una aspiradora o la música del salón.
Especificaciones de dimensiones y peso	
Peso	49,7 libras (22,54 kg)
Altura	15,5 pulgadas (394 mm)
Ancho	10,6 pulgadas (265 mm)

Elemento	Especificaciones de los dispositivos Snowball Edge optimizados para almacenamiento (con EC2)
Longitud	28,3 pulgadas (718 mm)
Especificaciones ambientales	
Vibración	Uso no operativo equivalente a la norma ASTM D4169 para camiones de nivel I: 0,73 GRMS
Choque	Uso operativo equivalente a 70 G (MIL-S-901) Uso no operativo equivalente a 50 G (ISTA-3A)
Altitud	Uso operativo equivalente a entre 0 y 3000 metros (0 a 10 000 pies) Uso no operativo equivalente a entre 0 y 12 000 metros
Intervalo de temperatura	0 – 45° C (operativo)

Especificaciones de los dispositivos Snowball Edge optimizados para computación

Elemento	Especificaciones de los dispositivos Snowball Edge optimizados para computación
Especificaciones de computación y memoria	
CPU	Hasta 104 vCPU (disponibles en configuraciones de 52 o 104 vCPU)
RAM	512 GB de RAM (hasta 416 GB de RAM, utilizables por el cliente)
GPU	nVidia V100 (disponible en la configuración Optimizado para computación con GPU; solo se ofrece con 52 vCPU)

Elemento	Especificaciones de los dispositivos Snowball Edge optimizados para computación
Especificaciones de almacenamiento	
Capacidad de almacenamiento en SSD	SSD NVMe de 28 TB o disco duro de 42 TB (39,5 TB utilizables)
Especificaciones de la fuente de alimentación	
Alimentación	Regiones de AWS En EE. UU.: NEMA 5—15p, 100—220 voltios. En todas las regiones de AWS se incluye un cable de alimentación
Consumo eléctrico	304 vatios para un caso de uso medio, aunque la fuente de alimentación tiene una capacidad nominal de 1200 vatios
Voltaje	100 – 240 V CA
Frecuencia	47/63 Hz
Conexiones de datos y de red	2 x 10 Gbit: RJ45 (uno utilizable) 1x 25 Gbit — SFP28 1x 100 Gbit — QSFP28
Cables	Cada AWS Snowball Edge dispositivo envía cables de alimentación específicos para cada país. No se incluye ningún otro cable ni conector óptico. Para obtener más información, consulte Hardware de red compatible.
Requisitos térmicos	AWS Snowball Edge los dispositivos están diseñados para operaciones de oficina y son ideales para operacion es de centros de datos.

Elemento	Especificaciones de los dispositivos Snowball Edge optimizados para computación
Salida de decibelios	De media, un AWS Snowball Edge dispositivo produce 68 decibelios de sonido, normalmente más silencioso que el de una aspiradora o la música del salón.
Especificaciones de dimensiones y peso	
Peso	49,7 libras (22,54 kg)
Altura	15,5 pulgadas (394 mm)
Ancho	10,6 pulgadas (265 mm)
Longitud	28,3 pulgadas (718 mm)
Especificaciones ambientales	
Vibración	Uso no operativo equivalente a la norma ASTM D4169 para camiones de nivel I: 0,73 GRMS
Choque	Uso operativo equivalente a 70 G (MIL-S-901) Uso no operativo equivalente a 50 G (ISTA-3A)
Altitud	Uso operativo equivalente a entre 0 y 3000 metros (0 a 10 000 pies) Uso no operativo equivalente a entre 0 y 12 000 metros
Intervalo de temperatura	0 – 45° C (operativo)

Hardware de red compatible

Para utilizar el AWS Snowball Edge dispositivo, necesitará sus propios cables de red. Para los cables RJ45, no hay recomendaciones específicas. Los cables SFP+ y QSFP+ y los módulos de Mellanox y Finisar están homologados como compatibles con el dispositivo.

Después de abrir el panel posterior del AWS Snowball Edge dispositivo, verá los puertos de red similares a los puertos que se muestran en la siguiente captura de pantalla.

Solo se puede utilizar una interfaz de red del AWS Snowball Edge dispositivo a la vez. Por lo tanto, puede utilizar cualquiera de los puertos para el siguiente hardware de red.

SFP

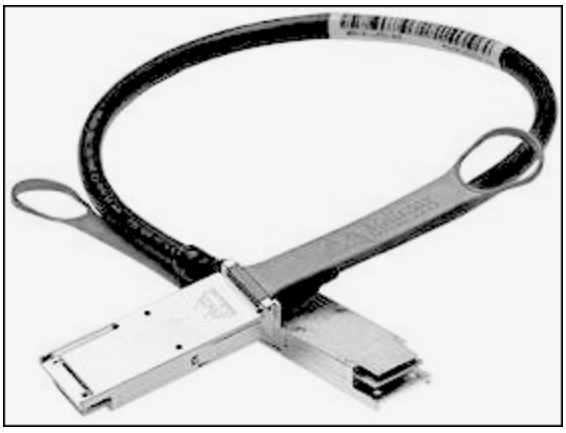
Este puerto proporciona una interfaz 10G/25G SFP28 compatible con los módulos transceptores SFP28 y SFP, y los cables de cobre de conexión directa (DAC). Debe proporcionar sus propios transceptores o cables DAC.

- Para el funcionamiento 10G, puede utilizar cualquier opción SFP+. Entre los ejemplos se incluyen:
  - Transceptor 10Gbase-LR (fibra monomodo)
  - Transceptor 10Gbase-SR (fibra multimodo)
  - Cable DAC SFP+
- Para el funcionamiento 25G, puede utilizar cualquier opción SFP28. Entre los ejemplos se incluyen:
  - Transceptor 25Gbase-LR (fibra monomodo)
  - Transceptor 25Gbase-SR (fibra multimodo)
  - Cable DAC SFP28

QSFP

Este puerto proporciona una interfaz QSFP+ de 40G en dispositivos optimizados para almacenamiento y una interfaz QSFP+ de 40/50/100G en dispositivos optimizados para computación. Los dos son compatibles con los módulos transceptores QSFP+y los cables DAC. Debe proporcionar sus propios transceptores o cables DAC. Algunos ejemplos son los siguientes:

- Transceptor 40Gbase-LR4 (fibra monomodo)
- Transceptor 40Gbase-SR4 (fibra multimodo)
- QSFP+ DAC

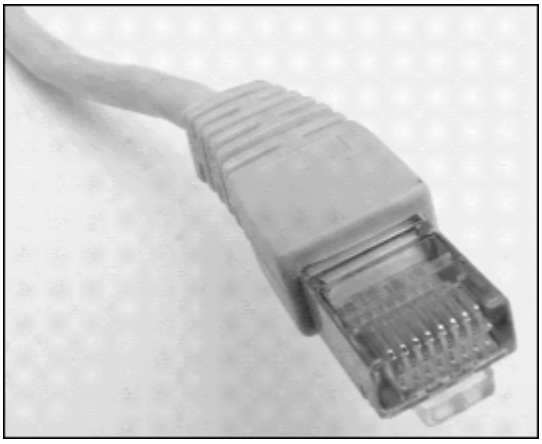


RJ45

Este puerto proporciona funcionamiento 1Gbase-TX/10Gbase-TX. Se conecta mediante cable UTP terminado con un conector RJ45. Los dispositivos Snowball Edge tienen dos puertos RJ45. Elija el puerto que desee utilizar.

El funcionamiento 1G se indica mediante una luz ámbar parpadeante. El funcionamiento 1G no se recomienda para las transferencias de datos a gran escala al dispositivo Snowball Edge, ya que aumenta drásticamente el tiempo necesario para transferir los datos.

El funcionamiento 10G se indica mediante una luz verde parpadeante. Requiere un cable UTP Cat6A con una distancia operativa máxima de 55 metros (180 pies).



Requisitos previos para usar dispositivos Snow Family

Antes de empezar a utilizar un dispositivo de la familia Snow, debes crear una AWS cuenta si no la tienes. También te recomendamos que aprendas a configurar tus instancias de datos e informática para usarlas con los dispositivos de la familia Snow.

AWS Snowball Edge es un servicio específico para cada región. Por lo tanto, antes de planificar su trabajo, asegúrese de que el servicio esté disponible en su Región de AWS. Asegúrese de que su ubicación y su depósito de Amazon S3 estén en el mismo país Región de AWS o en el mismo país, ya que esto afectará a su capacidad de pedir el dispositivo.

Si desea utilizar almacenamiento compatible con Amazon S3 en dispositivos Snow Family con dispositivos optimizados para computación a fin de realizar trabajos locales de almacenamiento y computación de periferia, debe aprovisionar la capacidad de S3 en el dispositivo o los dispositivos en el momento de realizar el pedido. El almacenamiento compatible con Amazon S3 en dispositivos Snow Family permite administrar buckets locales, por lo que puede crear buckets de S3 en el dispositivo o el clúster una vez que haya recibido el dispositivo o los dispositivos.

Como parte del proceso de pedido, debe crear un rol AWS Identity and Access Management (IAM) y una clave AWS Key Management Service (AWS KMS). La clave de KMS se utiliza para cifrar el código de desbloqueo del trabajo. Para obtener más información sobre la creación de funciones de IAM y claves de KMS, consulte Crear una tarea para solicitar un dispositivo de la familia Snow.

> **Note**
>
> En Asia Pacífico (Bombay), Amazon presta el Región de AWS servicio a través de Internet Services Private Limited (AISPL). Para obtener información sobre cómo suscribirse a Amazon Web Services en Asia Pacífico (Bombay) Región de AWS, consulte Suscripción a AISPL.

Temas

Inscríbase en una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirse a una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea una. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Signing in as the root user en la Guía del usuario de AWS Sign-In .
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .
2. En IAM Identity Center, conceda acceso administrativo a un usuario.

Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Iniciar sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

   Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .
2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

Preguntas frecuentes sobre el entorno local

Comprender su conjunto de datos y cómo está configurado el entorno local le ayudará a realizar la transferencia de datos. Tenga en cuenta lo siguiente antes de realizar el pedido.

¿Qué datos va a transferir?

La transferencia de una gran cantidad de archivos pequeños no funciona bien con AWS Snowball Edge. Esto se debe a que Snowball Edge cifra cada objeto individual. Se consideran archivos pequeños aquellos cuyo tamaño es inferior a 1 MB. Le recomendamos que las cierre con cremallera antes de transferirlas al dispositivo AWS Snowball Edge. También se recomienda no tener más de 500 000 archivos o directorios en cada directorio.

¿Se tendrá acceso a los datos durante la transferencia?

Es importante tener un conjunto de datos estático (es decir, que ningún usuario o sistema tenga acceso a los datos durante la transferencia). De lo contrario, se puede producir un error en la transferencia de archivos debido a una discordancia en la suma de comprobación. En ese caso, los archivos no se transferirán y se marcarán como `Failed`.

Para evitar que tus datos se dañen, no desconectes un dispositivo AWS Snowball Edge ni cambies su configuración de red durante la transferencia de datos. Los archivos deben encontrarse en un estado estático mientras se escriben en el dispositivo. La modificación de archivos mientras se están escribiendo en el dispositivo puede dar lugar a conflictos de lectura/escritura.

¿La red admitirá la transferencia AWS Snowball de datos?

Snowball Edge es compatible con los adaptadores de red RJ45, SFP+ o QSFP+. Compruebe que el conmutador es un conmutador gigabit. Según la marca del conmutador, puede presentar el texto gigabit o 10/100/1000. Los dispositivos Snowball Edge no admiten un conmutador de megabits ni de 10/100.

Trabajo con nombres de archivo que contienen caracteres especiales

Es importante destacar que si los nombres de los objetos contienen caracteres especiales, es posible que se produzcan errores. Aunque Amazon S3 permite caracteres especiales, le recomendamos encarecidamente que evite los siguientes caracteres:

- Barra diagonal invertida ("\")
- Llave de apertura ("{")
- Llave de cierre ("}")
- Corchete de apertura ("[")
- Corchete de cierre ("]")
- Símbolo menor que ("<")
- Símbolo mayor que (">")
- Caracteres ASCII no imprimibles (caracteres decimales 128-255)
- Acento circunflejo ("^")
- Carácter de porcentaje ("%")

- Acento grave ("`")
- Comillas
- Tilde ("~")
- Almohadilla ("#")
- Barra vertical ("|")

Si sus archivos tienen uno o más de estos caracteres en los nombres de los objetos, cambie el nombre de los objetos antes de copiarlos en el dispositivo AWS Snowball Edge. Los usuarios de Windows cuyos nombres de archivo contengan espacios deben tener cuidado al copiar objetos individuales o ejecutar un comando recursivo. En los comandos, escriba entre comillas los nombres de los objetos que incluyan espacios. A continuación se muestran ejemplos de este tipo de archivos.

Sistema operativo	Nombre de archivo: test file.txt
Windows	`“C:\Users\<username>\desktop\test file.txt”`
iOS	`/Users/<username>/test\ file.txt`
Linux	`/home/<username>/test\ file.txt`

> **Note**
>
> Los únicos metadatos de objeto que se transfieren son el nombre y el tamaño del objeto.

Cifrado Amazon S3 con AWS KMS

Puede usar las claves de cifrado AWS administradas por defecto o administradas por el cliente para proteger sus datos al importarlos o exportarlos.

Uso del cifrado de buckets predeterminado de Amazon S3 con claves AWS KMS administradas

Para habilitar el cifrado AWS administrado con AWS KMS

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.

2. Elija el bucket de Amazon S3 que desea cifrar.
3. En el asistente que aparece a la derecha, seleccione Propiedades.
4. En el cuadro Cifrado predeterminado, elija Desactivado (esta opción aparece atenuada) para activar el cifrado predeterminado.
5. Elija AWS-KMS como método de cifrado y, a continuación, elija la clave de KMS que desea usar. Esta clave se usa para cifrar los objetos que se colocan en el bucket mediante PUT.
6. Seleccione Guardar.

Una vez creado el trabajo de Snowball Edge y antes de importar los datos, agregue una declaración a la política de roles de IAM existente. Este es el rol que creó durante el proceso de pedido. Según el tipo de trabajo, el nombre del rol predeterminado es similar a `Snowball-import-s3-only-role` o `Snowball-export-s3-only-role`.

A continuación se muestran algunos ejemplos de este tipo de declaración.

Para importar datos

Si utiliza el cifrado del lado del servidor con claves AWS KMS administradas (SSE-KMS) para cifrar los buckets de Amazon S3 asociados a su trabajo de importación, también debe añadir la siguiente declaración a su función de IAM.

Example Ejemplo de rol de IAM de importación de Snowball

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

Para exportar datos

Si utiliza el cifrado del lado del servidor con claves AWS KMS administradas para cifrar los buckets de Amazon S3 asociados a su trabajo de exportación, también debe añadir la siguiente declaración a su función de IAM.

Example Rol de IAM de exportación de Snowball

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

Utiliza el cifrado por buckets predeterminado de S3 con las claves de los clientes AWS KMS

Puede utilizar el cifrado de bucket predeterminado de Amazon S3 con sus propias claves de KMS para proteger los datos que va a importar y exportar.

Para importar datos

Para habilitar el cifrado gestionado por el cliente con AWS KMS

1. Inicie sesión en la consola AWS Key Management Service (AWS KMS) AWS Management Console y ábrala en https://console.aws.amazon.com/kms.
2. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
3. En el panel de navegación, elija Claves administradas por el cliente y, a continuación, elija la clave de KMS asociada a los buckets que desea usar.
4. Expanda Política de claves si aún no está expandida.
5. En la sección Usuarios de claves, elija Agregar y busque el rol de IAM. Elija el rol de IAM y, a continuación, elija Agregar.
6. También puede elegir Cambiar a la vista de política para mostrar el documento de la política de claves y añadir una declaración a la política de claves. A continuación se muestra un ejemplo de la política.

Example de una política para la clave gestionada por el 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": "*"
}
```

Tras añadir esta política a la clave gestionada por el AWS KMS cliente, también es necesario actualizar el rol de IAM asociado al trabajo de Snowball. De forma predeterminada, el rol es `snowball-import-s3-only-role`.

Example del rol de IAM de importación de Snowball

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

Para obtener más información, consulte Uso de políticas basadas en la identidad (políticas de IAM) para AWS Snowball.

La clave de KMS que se usa tiene un aspecto similar al siguiente:

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

Para exportar datos

Example de una política para la clave gestionada por el 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": "*"
}
```

Tras añadir esta política a la clave gestionada por el AWS KMS cliente, también es necesario actualizar el rol de IAM asociado al trabajo de Snowball. De forma predeterminada, el rol es similar al siguiente:

`snowball-export-s3-only-role`

Example del rol de IAM de exportación de Snowball

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

Tras añadir esta política a la clave gestionada por el AWS KMS cliente, también es necesario actualizar el rol de IAM asociado al trabajo de Snowball. De forma predeterminada, el rol es `snowball-export-s3-only-role`.

Cifrado de Amazon S3 con cifrado del servidor

AWS Snowball admite el cifrado del lado del servidor con claves de cifrado gestionadas por Amazon S3 (SSE-S3). El cifrado del servidor se lleva a cabo para proteger los datos en reposo. SSE-S3 ofrece un cifrado sólido multifactor para proteger los datos en reposo en Amazon S3. Para obtener más información acerca de SSE-S3, consulte Uso del cifrado del servidor con claves administradas por Amazon S3 (SSE-S3) en la Guía del usuario de Amazon Simple Storage Service.

> **Note**
>
> Actualmente, AWS Snowball no admite el cifrado del lado del servidor con claves proporcionadas por el cliente (SSE-C). Sin embargo, es posible que desee utilizar ese tipo de SSE para proteger los datos que se han importado o incluso que ya lo utilice en los datos que desea exportar. En estos casos, tenga en cuenta lo siguiente:
>
> - Importación: si desea utilizar SSE-C para cifrar los objetos que ha importado a S3, cópielos a otro bucket en cuya política se haya definido el cifrado SSE-KMS o SSE-S3.
> - Exportación: si desea exportar objetos cifrados con SSE-C, cópielos primero a otro bucket que no tenga cifrado del servidor o que tenga una política en la cual se haya definido el cifrado SSE-KMS o SSE-S3.

Requisitos previos para usar el adaptador de Amazon S3 en dispositivos Snow Family para trabajos de importación y exportación

Puede usar el adaptador S3 en los dispositivos de la familia Snow cuando los utilice para mover datos de fuentes de datos locales a la nube o de la nube al almacenamiento de datos local. Para obtener más información, consulte Transferencia de archivos mediante el adaptador de Amazon S3 para la migración de datos.

El bucket de Amazon S3 asociado al trabajo debe usar la clase de almacenamiento estándar de Amazon S3. Antes de crear el primer trabajo, tenga en cuenta la siguiente información.

Para los trabajos que importan datos a Amazon S3, siga estos pasos:

- Asegúrese de que los nombres de los archivos y las carpetas que va a transferir se ajustan a lo indicado en las directrices de nomenclatura de claves de objeto de Amazon S3. No se importará a Amazon S3 ningún archivo ni carpeta cuyo nombre no cumpla estas directrices.
- Planee qué datos desea importar a Amazon S3. Para obtener más información, consulte Planificación de transferencias grandes.

Antes de exportar datos desde Amazon S3, siga estos pasos:

- Sepa qué datos se van a exportar al crear el trabajo. Para obtener más información, consulte Uso de los rangos de exportación.

- A todos los archivos cuyo nombre contenga un signo de dos puntos (`:`), cámbieles el nombre en Amazon S3 antes de crear el trabajo de exportación para obtener estos archivos. Los archivos cuyo nombre contiene un signo de dos puntos no se exportan a Microsoft Windows Server.

Requisitos previos para utilizar el almacenamiento compatible con Amazon S3 en los dispositivos Snow Family

Utiliza el almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow cuando almacena datos en el dispositivo en su ubicación perimetral y los utiliza para operaciones informáticas locales. Los datos utilizados para las operaciones informáticas locales no se importarán a Amazon S3 cuando se devuelva el dispositivo.

Cuando solicite un dispositivo Snow para computación y almacenamiento locales con almacenamiento compatible con Amazon S3, tenga en cuenta lo siguiente.

- Cuando solicite el dispositivo, aprovisionará capacidad de almacenamiento de Amazon S3. Por lo tanto, tenga en cuenta sus necesidades de almacenamiento antes de pedir un dispositivo.
- Puede crear buckets de Amazon S3 en el dispositivo después de recibirlo, en lugar de hacerlo al solicitar un dispositivo Snow Family.
- Deberá descargar la última versión del cliente Snowball Edge AWS CLI (v2.11.15 o superior) o AWS OpsHub instalarlo en su ordenador para utilizar el almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow.
- Tras recibir el dispositivo, configure, inicie y utilice el almacenamiento compatible con Amazon S3 en los dispositivos Snow Family de acuerdo con lo expuesto en la sección Uso del almacenamiento compatible con Amazon S3 en los dispositivos Snow Family de esta guía.

Requisitos previos para usar instancias de computación en dispositivos Snow Family

Puede ejecutar instancias informáticas compatibles con Amazon EC2 alojadas en un AWS Snowball Edge con los tipos de `sbe-g` instancia `sbe1``sbe-c`, y:

- El tipo de instancia `sbe1` funciona en dispositivos que tienen la opción Snowball Edge optimizado para almacenamiento.
- El tipo de instancia `sbe-c` funciona en dispositivos que tienen la opción Snowball Edge optimizado para computación.

- Los tipos de instancia `sbe-c` y `sbe-g` funcionan en dispositivos que tienen la opción Snowball Edge optimizado para computación con GPU.

Todos los tipos de instancia de computación que se pueden utilizar con las diferentes opciones de dispositivos Snowball Edge son exclusivos de los dispositivos AWS Snowball Edge. Al igual que ocurre con sus homólogas basadas en la nube, estas instancias requieren el lanzamiento de imágenes de máquina de Amazon (AMI). Antes de crear el trabajo de Snowball Edge tiene que elegir la AMI de una instancia.

Para usar una instancia de cómputo en un Snowball Edge, cree un trabajo para solicitar un dispositivo de la familia Snow y especifique sus AMI. Puede hacerlo mediante la consola AWS Snowball de administración, el AWS Command Line Interface (AWS CLI) o uno de los AWS SDK. Normalmente, para poder utilizar las instancias, hay algunos requisitos organizativos previos que debe cumplir antes de crear el trabajo.

En el caso de los trabajos que utilizan instancias de computación, antes de poder añadir cualquier AMI a su trabajo, debe tener una AMI en su Cuenta de AWS y debe ser un tipo de imagen compatible. Actualmente, las AMI compatibles se basan en los siguientes sistemas operativos:

- Amazon Linux 2
- CentOS 7 (x86_64) - with Updates 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: las imágenes Xenial (HVM) ya no se admiten en los dispositivos Snowball Edge a través de Amazon EC2 VM Import/Export AWS Marketplace, pero se siguen utilizando en dispositivos Snowball Edge a través de Amazon EC2 VM Import/Export y se ejecutan localmente en las AMI.

Puede obtener estas imágenes en AWS Marketplace.

Si usa SSH para conectarse a las instancias que se ejecutan en un dispositivo Snowball Edge, puede utilizar su propio par de claves o puede crear uno en el dispositivo Snowball Edge. AWS OpsHub Para crear un key pair en el dispositivo, consulteTrabajo con pares de claves. Para usar el AWS CLI para crear un key pair en el dispositivo, consulte `create-key-pair`Lista de comandos de la AWS CLI compatibles con Amazon EC2 admitidos en un dispositivo Snowball Edge. Para obtener más información sobre los pares de claves y Amazon Linux 2, consulte los pares de claves de Amazon EC2 y las instancias de Linux en la Guía del usuario de Amazon EC2.

Para obtener información concreta acerca del uso de instancias de computación en un dispositivo, consulte Uso de instancias de computación compatibles con Amazon EC2.

Cómo funciona AWS Snowball Edge

AWS Snowball Los dispositivos Edge son propiedad AWS de su ubicación local y residen en ella mientras están en uso.

Hay tres tipos de trabajo que puede utilizar con un AWS Snowball Edge dispositivo. Aunque los casos de uso de los tipos de trabajo varían, cada uno de ellos presenta el mismo proceso de solicitud, recepción y devolución de dispositivos. Independientemente del tipo de trabajo que se utilice, una vez finalizado cada trabajo este se borra según la norma 800-88 del Instituto Nacional de Normalización y Tecnología (NIST).

Flujo de trabajo compartido

1. Creación del trabajo: cada trabajo se crea en la Consola de administración de la familia de productos Snow de AWS o en la API de administración de trabajos mediante programación. Se puede realizar un seguimiento del estado de un trabajo en la consola o mediante la API.
2. Preparación del dispositivo para el trabajo: preparamos un dispositivo AWS Snowball Edge para su trabajo y el estado de este último pasa a ser Preparing Snowball para indicar que se está preparando Snowball.
3. Envío de un dispositivo a través del transportista de la región: el transportista se hace cargo a partir de este punto; el estado del trabajo es ahora En tránsito hacia usted. Encontrará el número de seguimiento y un enlace al sitio web de seguimiento en la consola o a través de la API de administración de trabajos. Para obtener información acerca del transportista de su región, consulte Consideraciones sobre el envío para los dispositivos Snow Family.
4. Recibe el dispositivo: unos días después, el operador de tu región entrega el AWS Snowball Edge dispositivo a la dirección que indicaste al crear el trabajo y el estado del trabajo cambia a Entregado a ti. Observará que el dispositivo no se entrega en una caja, ya que él mismo es el propio contenedor de transporte.
5. Obtención de credenciales y descarga del cliente de Snowball Edge: para poder comenzar a transferir datos, debe obtener sus credenciales, el manifiesto del trabajo y el código de desbloqueo del manifiesto y, a continuación descargar el cliente de Snowball Edge.
   - El cliente de Snowball Edge es la herramienta que utilizará para administrar el flujo de datos entre el dispositivo y el destino de los datos en las instalaciones.

     Puede descargar e instalar el cliente de Snowball Edge desde la página AWS Snowball resources.

Debe descargar el cliente de Snowball Edge desde la página AWS Snowball Edge Resources e instalarlo en una estación de trabajo potente de su propiedad.

- El manifiesto se utiliza para autenticar el acceso al dispositivo; está cifrado para que solo el código de desbloqueo pueda descifrarlo. Puede obtener el manifiesto en la consola o mediante la API de administración de trabajos una vez que el dispositivo se encuentre en sus instalaciones.
- El código de desbloqueo es un código de 29 caracteres que se utiliza para descifrar el manifiesto. Puede obtener el código de desbloqueo en la consola o mediante la API de administración de trabajos. Le recomendamos guardar el código de desbloqueo en algún lugar separado del manifiesto para impedir el acceso no autorizado al dispositivo mientras este se encuentra en sus instalaciones.

6. Colocación del hardware: lleve el dispositivo al centro de datos y ábralo siguiendo las instrucciones de la carcasa. Conecte el dispositivo a la alimentación eléctrica y a la red local.
7. Encendido el dispositivo: a continuación, encienda el dispositivo pulsando el botón de encendido situado encima de la pantalla LCD. Espere unos minutos y aparecerá la pantalla Ready.
8. Obtención de la dirección IP del dispositivo: la pantalla LCD contiene la pestaña CONNECTION. Pulsa esta pestaña y obtén la dirección IP del AWS Snowball Edge dispositivo.
9. Utilice el cliente Snowball Edge para desbloquear el dispositivo: cuando utilice el cliente Snowball Edge para desbloquear el AWS Snowball Edge dispositivo, introduzca la dirección IP del dispositivo, la ruta a su manifiesto y el código de desbloqueo. El cliente de Snowball Edge descifrará el manifiesto y lo utilizará para autenticar su acceso al dispositivo.
10. Uso del dispositivo: el dispositivo ya está encendido y listo para su uso. Puede utilizarlo para transferir datos con el adaptador de Amazon S3 o el punto de montaje de Network File System (NFS) o para fines de computación y almacenamiento locales con un almacenamiento compatible con Amazon S3 en los dispositivos Snow Family.
11. Prepare el dispositivo para el viaje de vuelta: cuando haya terminado de colocar el dispositivo en su ubicación local, pulse el botón de encendido situado sobre la pantalla LCD. El dispositivo tarda unos 20 segundos en apagarse. Desenchufe el dispositivo y guarde sus cables de alimentación eléctrica en el soporte situado en la parte superior. A continuación, cierre las tres puertas del dispositivo. El dispositivo está listo para su devolución.
12. El operador de tu región devuelve el dispositivo AWS: cuando el operador tiene el AWS Snowball Edge dispositivo, el estado del trabajo pasa a ser En tránsito a AWS.

> **Note**
>
> Se deben seguir unos pasos adicionales para los trabajos de exportación y de clúster. Para obtener más información, consulte Cómo funcionan los trabajos de exportación y Funcionamiento de los trabajos locales de computación y almacenamiento en clúster.

Temas

Cómo funcionan los trabajos de importación

Cada trabajo de importación utiliza un único dispositivo Snowball. Tras crear un trabajo para solicitar un dispositivo de la familia Snow en la API de gestión de trabajos Consola de administración de la familia de productos Snow de AWS o en la misma, le enviaremos un Snowball. Cuando lo reciba pasados unos días, debe conectar el dispositivo Snowball Edge a su red y transferir al dispositivo los datos que desee importar a Amazon S3. Cuando haya terminado de transferir los datos, devuelva el Snowball a AWS Amazon S3 e importaremos sus datos a Amazon S3.

Cómo funcionan los trabajos de exportación

Cada trabajo de exportación puede utilizar cualquier número de dispositivos AWS Snowball Edge. Si la lista contiene más datos de los que caben en un solo dispositivo, se le proporcionarán varios dispositivos. Cada parte del trabajo lleva asociado un único dispositivo. Una vez creadas las partes del trabajo, la primera de ellas adquiere el estado Preparing Snowball.

> **Note**
>
> La operación de listado para dividir el trabajo en partes es una función de Amazon S3, lo que significa que se le facturará igual que cualquier otra operación de Amazon S3.

Poco después, comenzaremos a exportar sus datos a un dispositivo. El tiempo necesario para exportar los datos variará en función de la naturaleza del conjunto de datos. Por ejemplo, la exportación de muchos archivos pequeños (menos de 10 MB) tarda mucho más tiempo. Cuando finalice la exportación, AWS preparará el dispositivo para que lo recoja el operador de su región. Cuando llega, conectas el AWS AWS Snowball Edge dispositivo a tu red y transfieres los datos del dispositivo al almacenamiento de tu red.

Cuando termines de transferir los datos, devuelve el dispositivo a AWS. Cuando recibimos un dispositivo correspondiente a una parte de un trabajo de exportación, lo borramos íntegramente. Esta operación de borrado se ajusta a los estándares 800-88 del Instituto Nacional de Normalización y Tecnología (NIST). Con este paso finaliza la parte del trabajo de que se trate.

- Para la lista de claves

  Antes de exportar los objetos del bucket de S3, escaneamos el bucket. Si el bucket se modifica después del escaneo, el trabajo podría sufrir demoras porque escaneamos objetos que faltan o que se han alterado.
- S3 Glacier Flexible Retrieval

  Es importante tener en cuenta que AWS Snowball no se pueden exportar objetos que pertenezcan a la clase de almacenamiento S3 Glacier. Estos objetos deben restaurarse antes de que AWS Snowball pueda exportar correctamente los objetos del bucket.

Funcionamiento de los trabajos locales de computación y almacenamiento

Puede utilizar la funcionalidad de procesamiento y almacenamiento local de un AWS Snowball Edge dispositivo ejecutando instancias informáticas AWS compatibles con EC2 o contenedores de Kubernetes en Amazon EKS Anywhere on Snow. En el caso de la funcionalidad de computación, el almacenamiento de datos lo proporciona el almacenamiento compatible con Amazon S3 en dispositivos Snow Family.

Puede crear depósitos de Amazon S3 en los dispositivos Snowball Edge para almacenar y recuperar objetos de forma local para aplicaciones que requieren acceso a datos locales, procesamiento local de datos y residencia de datos. El almacenamiento compatible con S3 en dispositivos Snow Family proporciona una nueva clase de almacenamiento, `SN0W`, que utiliza las API de Amazon S3 y está diseñada para almacenar datos de manera duradera y redundante en múltiples dispositivos Snowball

Edge. Puede usar las mismas API y características en los buckets de Snowball Edge que en Amazon S3, como políticas de ciclo de vida, cifrado y etiquetado. Cuando se devuelven el dispositivo o los dispositivos AWS, se borran todos los datos creados o almacenados en el almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow. Para obtener más información, consulte Trabajos exclusivos de computación y almacenamiento locales.

Para obtener más información, consulte Trabajos de computación y almacenamiento local.

Funcionamiento de los trabajos locales de computación y almacenamiento en clúster

Un trabajo de clúster es un tipo de trabajo especial para el almacenamiento y la computación locales únicamente. Está pensado para las cargas de trabajo que requieren mayor durabilidad de los datos y capacidad de almacenamiento. Para obtener más información, consulte Opción de clúster local.

> **Note**
>
> Al igual que sucede con los trabajos de computación y almacenamiento locales independientes, los datos almacenados en un clúster no pueden importarse a Amazon S3 sin pedir dispositivos adicionales como parte de trabajos de importación independientes. Si pide estos dispositivos, puede transferirles los datos del clúster e importar los datos cuando devuelva los dispositivos de los trabajos de importación.

Los clústeres tienen de 3 a 16 dispositivos AWS Snowball Edge, denominados nodos. Cuando reciba los nodos de su transportista regional, conecte todos los nodos a la red y a la fuente de suministro eléctrico para obtener sus direcciones IP. Con estas direcciones IP, podrá desbloquear todos los nodos del clúster a la vez con un solo comando de desbloqueo y con la dirección IP de uno de los nodos. Para obtener más información, consulte Uso de los comandos del cliente Snowball Edge.

Puede escribir datos en un clúster desbloqueado si utiliza almacenamiento compatible con Amazon S3 en los dispositivos Snow Family y distribuye los datos entre los demás nodos.

Cuando haya terminado con el clúster, devuelva todos los nodos a AWS. Al recibir cada uno de los nodos de clúster, efectuaremos un borrado íntegro del dispositivo Snowball. Esta operación de borrado se ajusta a los estándares 800-88 del Instituto Nacional de Normalización y Tecnología (NIST).

Vídeos y blogs de Snowball Edge

- Migración de archivos de varios tamaños con los snow-transfer-tool dispositivos AWS Snowball Edge
- AWS Snowball Migración de datos de Edge
- AWS OpsHub for Snow Family
- Novetta proporciona IoT y Machine Learning en la periferia para la respuesta ante desastres
- Habilite las migraciones de bases de datos a gran escala con DMS y AWS Snowball
- Mejores prácticas de migración de datos con AWS Snowball Edge
- AWS Snowball resources
- Los dispositivos optimizados para almacenamiento en AWS Snowball Edge Compute compatibles con Amazon S3 ya están disponibles de forma general
- Introducción al almacenamiento compatible con Amazon S3 en dispositivos de la familia Snow en dispositivos AWS Snowball Edge

Precios a largo plazo para los dispositivos Snowball Edge

Al pedir un dispositivo Snowball Edge, puede elegir la opción de precio que mejor se adapte a su caso de uso. Hay dos tipos de precios: bajo demanda por cada día que tenga el dispositivo o precios a largo plazo con prepago, que pueden ser mensuales o de uno o tres años, según el tipo de dispositivo. Puede renovar automáticamente la opción de precios a largo plazo por períodos de uno o tres años, de modo que un nuevo período de prepago comience cuando finalice el período anterior y así evitar la interrupción del uso del dispositivo. La opción de precio mensual a largo plazo se renovará automáticamente mientras tenga el dispositivo en su poder. Para obtener más información sobre cómo solicitar un dispositivo, consulte Crear un trabajo para pedir un dispositivo de la familia Snow en esta guía.

Además de la comodidad presupuestaria que suponen, los precios a largo plazo le permiten cambiar los dispositivos Snowball Edge durante el período de precios elegido cuando cambien sus requisitos operativos. Por ejemplo, puede solicitar el cambio de dispositivos para que el nuevo dispositivo incluya una nueva AMI o nuevos datos de Amazon S3, o para reemplazar un dispositivo defectuoso. Consulte Cambio de dispositivos durante el período de precios a largo plazo.

> **Note**
>
> Si solicita el cambio o la sustitución de un dispositivo Snowball Edge con arreglo a un plan de precios de compromiso de 1 o 3 años por cualquier motivo que no sea un problema de hardware o software atribuido al servicio de AWS Snow, se le cobrará una tarifa por uso del dispositivo. Esta tarifa de cambio de dispositivo se determina como la tarifa mensual (para Snowball Edge optimizado para computación) o como una tarifa de trabajo bajo demanda para su configuración.

Para obtener más información sobre los precios a largo plazo, consulte Optimizing cost with long-term pricing options for AWS Snowball. Para ver AWS Snowball los precios para su empresa Región de AWS, consulte los AWS Snowball precios.

Cambio de dispositivos durante el período de precios a largo plazo

El cambio de dispositivos Snowball Edge durante el período de precios a largo plazo implica pedir un dispositivo nuevo y devolver inmediatamente el dispositivo actual.

1. Cree un nuevo trabajo para el dispositivo Snowball Edge de reemplazo. El dispositivo de reemplazo debe ser para el mismo tipo de trabajo y tener las mismas opciones de computación y almacenamiento que el dispositivo que tiene actualmente. Consulte Crear un trabajo para solicitar un dispositivo de la familia Snow en esta guía.
2. Devuelva inmediatamente el dispositivo que tiene actualmente. Consulte Apagado del dispositivo Snowball Edge yDevolución del dispositivo Snowball Edge. AWS gestionará la logística de sustitución del dispositivo y, por este cambio, se cobrará una tasa por el reciclaje del dispositivo.

Consideraciones sobre el envío para los dispositivos Snow Family

Al crear un trabajo para solicitar un dispositivo de la familia Snow, proporciona una dirección de envío y elige la velocidad de envío. Tenga en cuenta que la velocidad de envío no indica cuántos días transcurrirán desde que cree el trabajo hasta que reciba el dispositivo . Más bien, indica el tiempo que el dispositivo está en tránsito entre AWS y tu dirección de envío. Antes de que se envíe el dispositivo, lo AWS procesa para el trabajo. El tiempo necesario para procesar el trabajo depende de factores como el tipo y el tamaño del trabajo. Además, las empresas de transporte generalmente solo recogen los dispositivos salientes de la familia Snow una vez al día y los transportistas no recogen los dispositivos salientes los fines de semana. Así pues, el procesamiento antes del envío puede durar un día o más. Mientras AWS preparas tu dispositivo para el envío y cuando lo reciba después de que lo devuelvas, puedes controlar el estado de tu trabajo a través del Consola de administración de la familia de productos Snow de AWS. Para obtener más información, consulte Estados de los trabajos.

> **Note**
>
> La velocidad de envío que elijas se aplicará AWS cuando te envíes el dispositivo y cuando lo devuelvas a AWS.
> Los dispositivos Snowball Edge solo se pueden usar para importar o exportar datos dentro de la AWS región en la que se solicitaron los dispositivos.

Para obtener más información sobre cómo elegir la velocidad de envío y cómo introducir su dirección de envío al crear un pedido de un dispositivo de la familia Snow, consultePaso 4: elija las preferencias de seguridad, envío y notificación. Para obtener más información sobre cómo devolver un dispositivo de la familia Snow a AWS, consulteDevolución del dispositivo Snowball Edge.

Para obtener más información sobre los cargos de envío, consulte Precios de AWS Snowball Edge.

Restricciones de envío en función de la región

Antes de crear un trabajo para solicitar un dispositivo de la familia Snow, debe iniciar sesión en la consola desde los Región de AWS mismos datos de Amazon S3. AWS no envía dispositivos de la

familia Snow entre países del mismo Región de AWS país, por ejemplo, de Asia Pacífico (India) a Asia Pacífico (Australia).

Una excepción al envío entre distintos países es entre los países miembros de la Unión Europea (UE). Para las transferencias de datos en las AWS regiones europeas, solo enviamos dispositivos a los países miembros de la UE que se indican a continuación:

Alemania, Austria, Bélgica, Bulgaria, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Portugal, República Checa, República de Chipre, Rumanía y Suecia.

Los dispositivos de la familia Snow solo se pueden devolver a la misma AWS región en la que se solicitaron.

Se permiten los envíos nacionales dentro del mismo país. Ejemplos:

- Para las transferencias de datos en la región de Reino Unido, hacemos envíos internos de los dispositivos dentro del Reino Unido.
- Para las transferencias de datos en Asia-Pacífico (Bombay), solo enviamos dispositivos dentro de la India.

> **Note**
>
> AWS no envía los dispositivos de la familia Snow a apartados de correos.

Introducción

Con un AWS Snowball Edge dispositivo, puede acceder a la potencia de almacenamiento y cómputo Nube de AWS local y rentable en lugares donde la conexión a Internet podría no ser una opción. Además, puede transferir cientos de terabytes o petabytes de datos entre sus centros de datos en las instalaciones y Amazon Simple Storage Service (Amazon S3).

A continuación, encontrará instrucciones generales sobre cómo crear y realizar su primer trabajo para un dispositivo AWS Snowball Edge en la Consola de administración de la familia de productos Snow de AWS. La consola presenta los flujos de trabajo más comunes, separados en tipos de trabajos. Encontrará más información sobre los componentes específicos del dispositivo AWS Snowball Edge más adelante en esta documentación. Para obtener información general sobre el servicio, consulte Cómo funciona AWS Snowball Edge.

En los ejercicios de introducción se parte del Consola de administración de la familia de productos Snow de AWS supuesto de que utiliza la interfaz AWS OpsHub for Snow Family para crear su AWS Snowball Edge trabajo, la interfaz Amazon S3 para leer y escribir datos. Si prefiere crear el trabajo mediante programación y disponer de más opciones, puede utilizar la API de administración de trabajos. Para obtener más información, consulte Referencia de la API de AWS Snowball.

Antes de empezar, debe crear un usuario Cuenta de AWS y un usuario administrador en AWS Identity and Access Management (IAM). Para obtener más información, consulte Requisitos previos para usar dispositivos Snow Family.

Temas

- Devolución del dispositivo Snowball Edge
- Devolución de dispositivos Snow Family
- Monitorización del estado de la importación
- Obtener el informe y los registros de finalización del trabajo

Crear un trabajo para pedir un dispositivo de la familia Snow

Para solicitar un dispositivo de la familia Snow, debe crear un trabajo para solicitar un dispositivo de la familia Snow en el Consola de administración de la familia de productos Snow de AWS. Un trabajo es un término que se AWS utiliza para describir el ciclo de vida del uso de un dispositivo de la familia Snow por parte de un cliente. Un trabajo comienza cuando pides un dispositivo, continúa cuando lo AWS preparas y te lo envías y lo usas, y se completa después de AWS recibir y procesar el dispositivo una vez que lo devuelves. Los trabajos se clasifican por tipo: exportación, importación e informática y almacenamiento locales. Para obtener más información, consulte Descripción de los trabajos de AWS Snowball Edge.

Después de crear el trabajo para solicitar un dispositivo, puede usarlo Consola de administración de la familia de productos Snow de AWS para ver el estado del trabajo y supervisar el progreso del dispositivo que ha pedido mientras AWS se prepara para su envío y después de su devolución. Para obtener más información, consulte Estados de los trabajos. Una vez que el dispositivo haya sido devuelto y procesado por AWS, podrá acceder a un informe de finalización del trabajo y a los registros a través del Consola de administración de la familia de productos Snow de AWS. Para obtener más información, consulte Obtener el informe y los registros de finalización del trabajo en la consola.

También se pueden crear y administrar trabajos mediante la API de administración de trabajos. Para obtener más información, consulte la Referencia de la API de AWS Snowball.

Temas

- Paso 1: elija un tipo de trabajo
- Paso 2: elija las opciones de computación y almacenamiento
- Paso 3: elija las características y opciones que desee
- Paso 4: elija las preferencias de seguridad, envío y notificación
- Paso 5: revise el resumen del trabajo y cree el trabajo
- Descarga AWS OpsHub

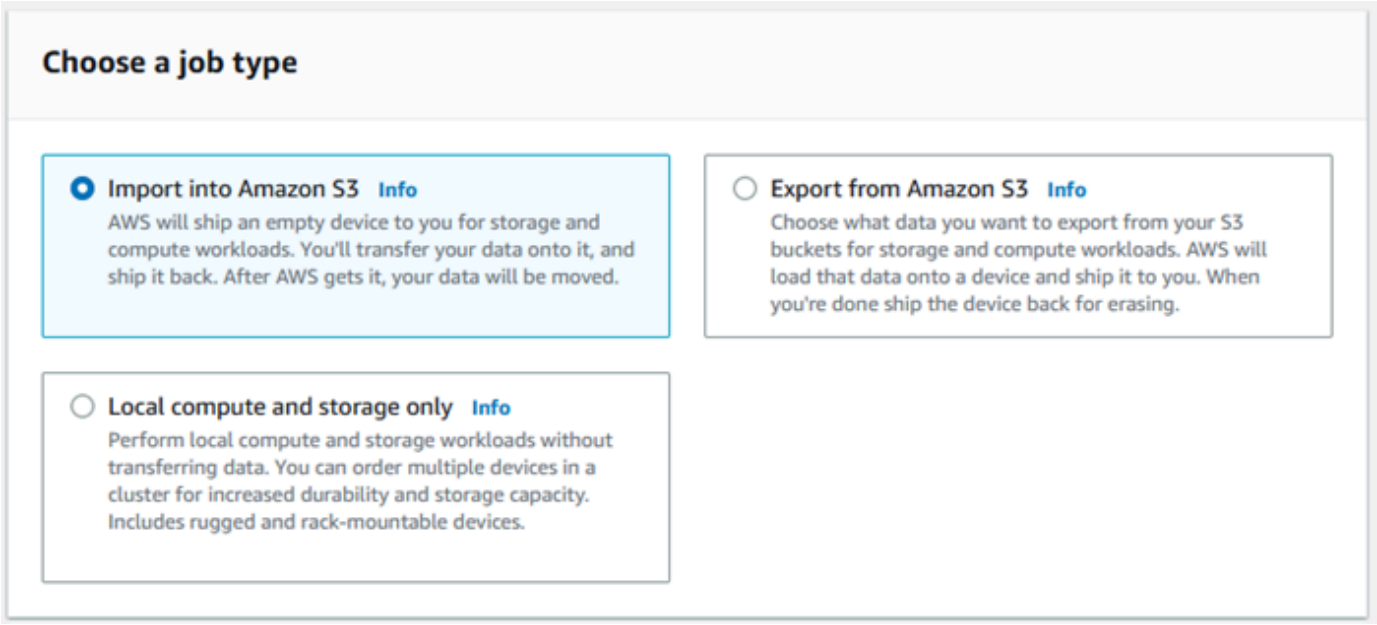
Paso 1: elija un tipo de trabajo

El primer paso para crear un trabajo consiste en determinar el tipo de trabajo que necesita y empezar a planificarlo mediante la Consola de administración de la familia de productos Snow de AWS.

Para elegir el tipo de trabajo

1. Inicie sesión en AWS Management Console y abra el Consola de administración de la familia de productos Snow de AWS. Si es la primera vez que crea un trabajo aquí Región de AWS, verá la página de la familia AWS Snow. De lo contrario, verá la lista de trabajos existentes.
2. Si es tu primer trabajo, selecciona Pedir un dispositivo de AWS la familia Snow. Si espera tener varios trabajos de migración de más de 500 TB de datos, elija Create your large data migration plan greater than 500 TB. De lo contrario, elija Crear trabajo en la barra de navegación izquierda. Seleccione Paso siguiente para abrir la página Planificar el trabajo.
3. En la sección Nombre del trabajo, proporcione un nombre para el trabajo en el cuadro Nombre del trabajo.
4. En función de sus necesidades, elija uno de los siguientes tipos de trabajo:

   - Importar a Amazon S3: elija esta opción para que le AWS envíen un dispositivo Snowball Edge vacío. Conecte el dispositivo a la red local y ejecute el cliente de Snowball Edge. Los datos se copian en el dispositivo mediante un recurso compartido de NFS o el adaptador S3, se devuelven al AWS dispositivo y se cargan los datos en él. AWS
   - Export from Amazon S3: elija esta opción para exportar datos de su bucket de Amazon S3 al dispositivo. AWS carga sus datos en el dispositivo y se lo devuelve. Conecte el dispositivo a la red local y ejecute el cliente de Snowball Edge. Copie los datos del dispositivo a sus servidores. Cuando termines, envía el dispositivo al AWS dispositivo y tus datos se borran del dispositivo.
   - Solo informático y almacenamiento locales: ejecute cargas de trabajo de computación y almacenamiento en el dispositivo sin transferir datos.



5. Elija Siguiente para continuar.

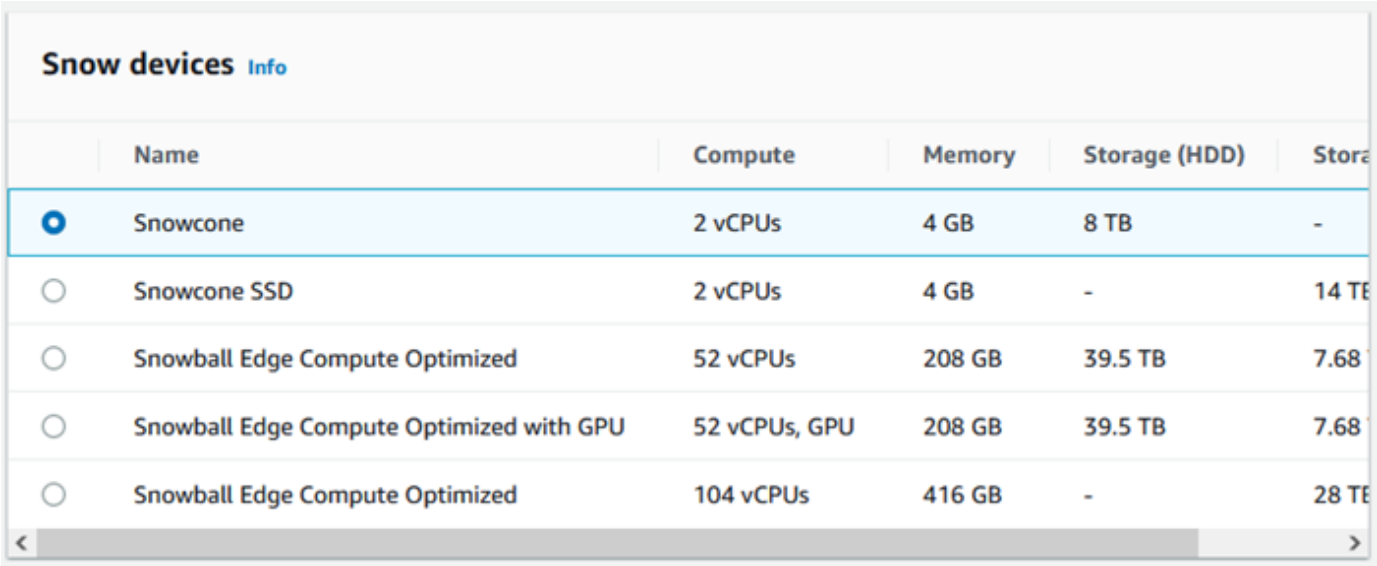
Paso 2: elija las opciones de computación y almacenamiento

Elija las especificaciones de hardware de su dispositivo Snow Family, qué instancias compatibles con Amazon EC2 desea incluir en él, cómo se almacenarán los datos y los precios.

Para elegir las opciones de computación y almacenamiento de su dispositivo

1. En la sección Dispositivos Snow, seleccione el dispositivo Snow Family que desea pedir.

> **Note**
>
> Es posible que algunos dispositivos de la familia Snow no estén disponibles según el lugar desde el Región de AWS que realice el pedido y el tipo de trabajo que elija.



2. En la sección Elija la opción de precios, en el menú Elija la opción de precios, elija el tipo de precio que desea aplicar a este trabajo. Si selecciona el precio de pago por adelantado con compromiso de 1 o 3 años, en Renovación automática, seleccione Activado para renovar automáticamente el precio cuando finalice el período actual o Desactivado si no desea renovarlo automáticamente. Para obtener más información sobre las opciones de precios a largo plazo de los dispositivos Snowball Edge, consulte los precios a largo plazo de los dispositivos Snowball Edge en esta guía. Para ver los precios de sus dispositivos Región de AWS, consulte AWS Snowball los precios.
3. En la sección Seleccionar el tipo de almacenamiento, elija la opción que mejor se adapte a sus necesidades:

   - S3 Adapter: utilice el adaptador de S3 para transferir datos mediante programación hacia y desde dispositivos Snow Family usando acciones de la API de REST de Amazon S3.
   - Amazon S3 compatible storage: utilice el almacenamiento compatible con Amazon S3 para implementar un almacenamiento de objetos escalable y duradero compatible con S3 en un único dispositivo Snowball Edge o en un clúster de varios dispositivos.
   - Transferencia de datos basada en NFS: utilice la transferencia de datos basada en el Sistema de archivos de red (NFS) para arrastrar y soltar archivos desde su equipo hasta los buckets de Amazon S3 de los dispositivos Snow Family.

> **Warning**
>
> La transferencia de datos basada en NFS no es compatible con el adaptador de S3. Si continúa con la transferencia de datos basada en NFS, debe montar el recurso compartido NFS para transferir objetos. No se podrá utilizar AWS CLI para transferir objetos.
> Consulte Uso de NFS para la transferencia de datos sin conexión en la Guía para desarrolladores de AWS Snowball Edge para obtener más información.

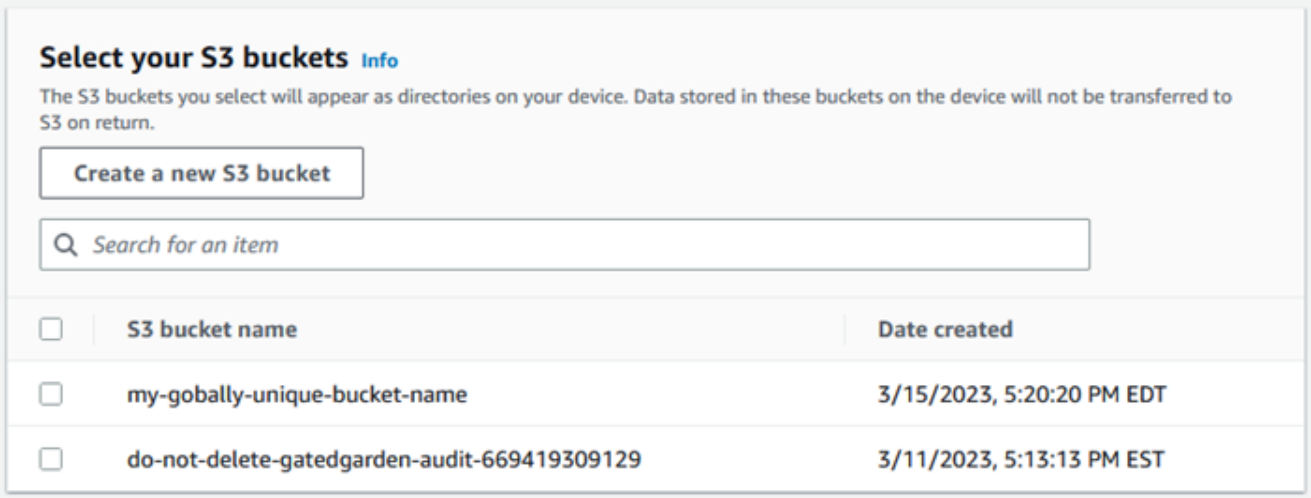
> **Note**
>
> Las opciones de tipo de almacenamiento disponibles dependen del tipo de trabajo y del dispositivo Snow que haya elegido.

4. Si seleccionó S3 Adapter como tipo de almacenamiento o si seleccionó un dispositivo que admite el almacenamiento en bloques, haga lo siguiente para seleccionar uno o más buckets de S3 que desea incluir en el dispositivo:

   - En la sección Select your S3 buckets, realice una o varias de las siguientes acciones para seleccionar uno o más buckets de S3:

     1. En la lista S3 bucket name, seleccione el nombre del bucket de S3 que desea usar.
     2. En el campo Buscar un elemento, introduzca el nombre completo de un bucket o parte de él para filtrar la lista de buckets disponibles y, a continuación, elija el bucket.
     3. Para crear un nuevo bucket de S3, elija Create a new S3 bucket. El nombre del nuevo bucket aparece en la lista Nombre del bucket. Elíjalo.

     Puede incluir uno o más buckets de S3. Estos buckets aparecen en el dispositivo como buckets de S3 locales.

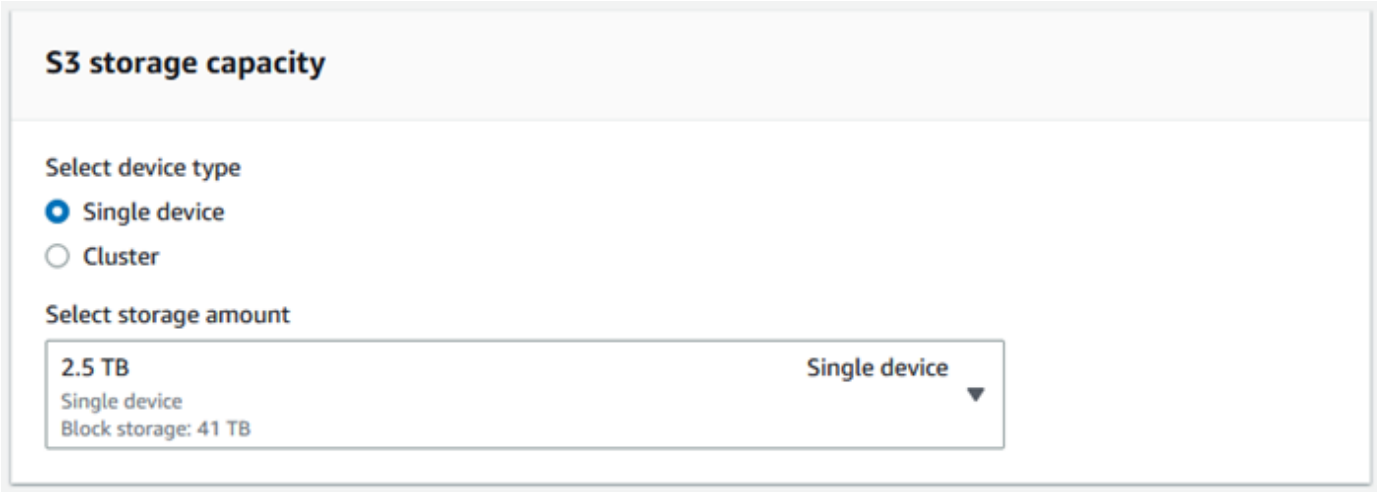


5. Si seleccionó Amazon S3 compatible storage como tipo de almacenamiento, en la sección S3 storage capacity, haga lo siguiente:

   a. Seleccione utilizar el almacenamiento compatible con Amazon S3 en los dispositivos Snow Family en un solo dispositivo o en un clúster de dispositivos. Consulte Uso de un AWS Snowball Edge clúster en esta guía.

   b. Seleccione la cantidad de almacenamiento del dispositivo que se utilizará para el almacenamiento compatible con Amazon S3 en los dispositivos Snow Family.

> **Note**
>
> Cuando se utiliza almacenamiento compatible con Amazon S3 en dispositivos Snow Family, puede administrar y crear buckets de Amazon S3 una vez que haya recibido el dispositivo, por lo que no es necesario elegirlos al realizar el pedido. Consulte Almacenamiento compatible con Amazon S3 en dispositivos Snow Family en esta guía.



6. Si seleccionó Transferencia de datos basada en NFS como tipo de almacenamiento, en la sección Select your S3 buckets, realice una o varias de las siguientes acciones para seleccionar uno o más buckets de S3:

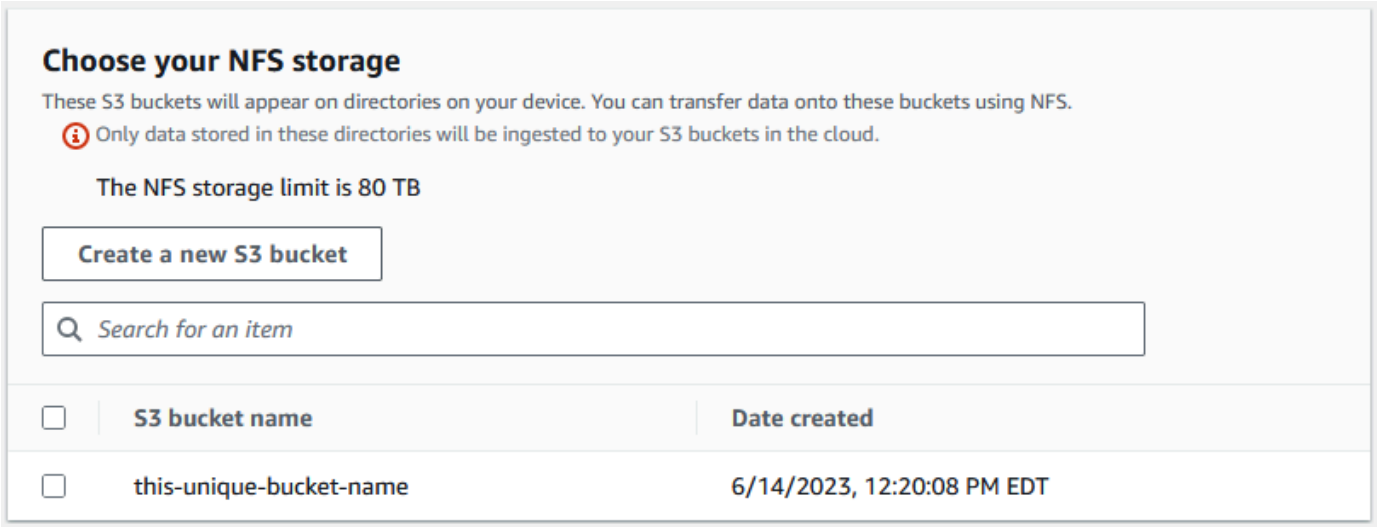
   a. En la lista S3 bucket name, seleccione el nombre del bucket de S3 que desea usar.

   b. En el campo Buscar un elemento, introduzca el nombre completo de un bucket o parte de él para filtrar la lista de buckets disponibles y, a continuación, elija el bucket.

   c. Para crear un nuevo bucket de S3, elija Create a new S3 bucket. El nombre del nuevo bucket aparece en la lista Nombre del bucket. Elíjalo.

   d. Después de elegir los buckets de S3 que va a usar con la transferencia de datos NFS, elija también un bucket de S3 como almacenamiento en bloques para las AMI. Consulte los pasos para elegir un bucket de S3.

   Puede incluir uno o más buckets de S3. Estos buckets aparecen en el dispositivo como buckets de S3 locales.



7. En la sección Compute using EC2-compatible instances - optional, elija las AMI compatibles con Amazon EC2 de su cuenta que desea incluir en el dispositivo. O bien, en el campo de búsqueda, introduzca el nombre completo de una AMI o parte de él para filtrar la lista de AMI disponibles y, a continuación, seleccione la AMI.

   Para obtener más información, consulte Añadir una AMI al pedir un dispositivo en esta guía.

   Esta característica conlleva cargos adicionales. Para más información, consulte Precios de AWS Snowball Edge.
8. Elija el botón Siguiente.

Paso 3: elija las características y opciones que desee

Elija las funciones y opciones que desee incluir en su trabajo con los dispositivos de la familia AWS Snow, como Amazon EKS Anywhere for Snow, una AWS IoT Greengrass instancia y la capacidad de administración remota de dispositivos.

Para elegir las características y opciones

1. En la sección Amazon EKS Anywhere on AWS Snow, para incluir Amazon EKS Anywhere on AWS Snow, selecciona Incluir Amazon EKS Anywhere on Snow y, a continuación, haz lo siguiente.

> **Note**
>
> Le recomendamos que cree su clúster de Kubernetes con la última versión de Kubernetes disponible compatible con Amazon EKS Anywhere. Para obtener más información, consulte Amazon EKS-Anywhere Versioning. Si su aplicación requiere una versión específica de Kubernetes, utilice cualquier versión de Kubernetes que Amazon EKS ofrezca como soporte estándar o extendido. Tenga en cuenta las fechas de lanzamiento y soporte de las versiones de Kubernetes al planificar el ciclo de vida de su implementación. Esto le ayudará a evitar la posible pérdida de soporte para la versión de Kubernetes que vaya a utilizar. Para obtener más información, consulte el calendario de versiones de Amazon EKS Kubernetes.

a. En la sección Crear una AMI propia, elija las AMI que ha creado para Amazon EKS Anywhere. Consulte Acciones que se deben realizar antes de pedir un dispositivo Snowball Edge para Amazon EKS Anywhere on Snow AWS.

b. En la sección Alta disponibilidad, para utilizar clústeres de Amazon EKS Anywhere en varios dispositivos Snowball Edge, elija el número de dispositivos que desea incluir en el pedido.

2. En la sección AWS IoT Greengrass on Snow, para incluir una AMI validada para las cargas de trabajo de IoT, seleccione Instalar una AMI AWS IoT Greengrass validada en mi dispositivo Snow.
3. Para habilitar la gestión remota de su dispositivo de la familia Snow mediante el cliente Snowball Edge, seleccione Gestionar el dispositivo Snow de forma remota con AWS OpsHub o el cliente AWS OpsHub Snowball.
4. Seleccione el botón Siguiente.

Paso 4: elija las preferencias de seguridad, envío y notificación

Temas

- Elección de las preferencias de seguridad
- Elección de sus preferencias de envío
- Selección de las preferencias de notificación

Elección de las preferencias de seguridad

Al configurar la seguridad, se añaden los permisos y la configuración de cifrado necesarios para proteger los datos de sus dispositivos AWS Snow Family mientras están en tránsito.

Para configurar la seguridad del trabajo

1. En la sección Cifrado, elija la Clave de KMS que desea usar.
   - Si quiere usar la clave predeterminada AWS Key Management Service (AWS KMS), elija AWS/importexport (predeterminada). Esta es la clave predeterminada que protege sus trabajos de importación y exportación cuando no se ha definido ninguna otra clave.
   - Si desea proporcionar su propia AWS KMS clave, elija Introducir un ARN clave, introduzca el nombre del recurso de Amazon (ARN) en el cuadro ARN de la clave y elija Usar esta clave de KMS. El ARN de clave se agregará a la lista.
2. En la sección Elegir el tipo de acceso al servicio, realice una de las siguientes acciones:
   - La consola Choose Snow creará y utilizará un rol vinculado al servicio para acceder AWS a los recursos en su nombre. para conceder a AWS Snow Family permisos para utilizar Amazon S3 y Amazon Simple Notification Service (Amazon SNS) en su nombre. El rol otorga la AssumeRole confianza del AWS Security Token Service (AWS STS) al servicio Snow
   - Elija Add an existing service role to use para especificar el ARN del rol que desea o bien puede usar el rol predeterminado.
3. Elija Siguiente.

Elección de sus preferencias de envío

La recepción y devolución de un dispositivo Snow Family implica el envío y la devolución del dispositivo, por lo que es importante que proporcione información de envío exacta.

Para proporcionar detalles de envío

1. En la sección Dirección de envío, seleccione una dirección existente o agregue una nueva.
   - Si elige Usar dirección reciente, se muestran las direcciones que tenemos en nuestros archivos. Elija con cuidado la dirección que desea de la lista.

- Si elige Agregar una nueva dirección, proporcione la información de la dirección solicitada. Consola de administración de la familia de productos Snow de AWS Guarda tu nueva información de envío.

> **Note**
>
> El país que proporcione en la dirección debe coincidir con el país de destino del dispositivo, que debe ser válido para ese país.

2. En la sección Rapidez de envío, elija una velocidad de envío para el trabajo. Esta velocidad muestra la rapidez de envío del dispositivo entre los destinos y no refleja la rapidez con la que llegará a partir de hoy. Puede elegir entre las siguientes velocidades de envío:

   - One-Day Shipping (1 business day)
   - Two-Day Shipping (2 business days)
   - Consulte Empresas de transporte.

Selección de las preferencias de notificación

Las notificaciones lo actualizan sobre el estado más reciente de los trabajos de sus dispositivos de la familia AWS Snow. Cree un tema de SNS y recibirá correos electrónicos de Amazon Simple Notification Service (Amazon SNS) a medida que cambie el estado de su trabajo.

Para configurar las notificaciones

- En la sección Establecer notificaciones, realice una de las siguientes acciones:
  - Si desea utilizar un tema de SNS existente, elija Usar un tema de SNS existente y después elija el tema Nombre de recurso de Amazon (ARN) de la lista.
  - Si desea crear un tema de SNS nuevo, elija Crear un nuevo tema de SNS. Introduzca un nombre para el tema y especifique una dirección de correo electrónico.

> **Note**
>
> Los dispositivos Snow creados en las regiones EE.UU. Oeste (Norte de California) y EE.UU. Oeste (Oregón) se envían a través de la región EE.UU. Este (Norte de Virginia). Debido a esto, las llamadas de servicio como Amazon SNS también se dirigen a través de EE. UU. Este (Norte de Virginia). Recomendamos crear nuevos

temas de SNS en la región EE.UU. Este (Virginia del Norte) para disfrutar de la mejor experiencia.

Las notificaciones se referirán a uno de los siguientes estados de su trabajo:

- Trabajo creado
- Preparando el dispositivo
- Preparando el envío
- En tránsito hacia usted
- Entregado a usted
- En tránsito a AWS
- En las instalaciones de clasificación
- En AWS
- Importando
- Completado
- Cancelado

Para obtener más información sobre las notificaciones de cambio de estado de trabajo y los temas de redes sociales cifradas, consulte las notificaciones para los dispositivos de la familia Snow en esta guía.

Seleccione Siguiente.

Paso 5: revise el resumen del trabajo y cree el trabajo

Después de proporcionar toda la información necesaria para el trabajo de su dispositivo de la familia AWS Snow, revise el trabajo y créelo. Tras crear el trabajo, AWS empezará a preparar el dispositivo de la familia Snow para su envío.

Los trabajos están sujetos a las leyes de control de exportación de determinados países y pueden requerir una licencia de exportación. También se aplican las leyes de exportación y reexportación de EE. UU. Está prohibido desviarse de las leyes y los reglamentos del país y de EE. UU.

1. En la página de resumen del trabajo, revise todas las secciones antes de crear el trabajo. Si desea realizar cambios, elija Editar en la sección correspondiente y edite la información.

2. Cuando haya terminado con la revisión y la edición, elija Crear trabajo.

> **Note**
>
> Después de crear un trabajo para pedir un dispositivo de la familia Snow, puede cancelarlo mientras esté en el estado Trabajo creado sin incurrir en ningún cargo. Para obtener más información, consulte Cancelar un trabajo a través del. Consola de administración de la familia de productos Snow de AWS

Una vez creado el trabajo, puede ver su estado en la sección Estado del trabajo. Para obtener información detallada sobre los estados de los trabajos, consulte Job Statuses.

Descarga AWS OpsHub

Los dispositivos de la familia AWS Snow ofrecen una herramienta fácil de usar que puede utilizar para administrar sus dispositivos y su entorno local Servicios de AWS. AWS OpsHub for Snow Family

Una AWS OpsHub vez instalado en su ordenador cliente, puede realizar tareas como las siguientes:

- Desbloquear y configurar dispositivos individuales o agrupados
- Transferir archivos
- Lanzar y administrar instancias que se ejecutan en dispositivos Snow Family.

Para obtener más información, consulte Uso AWS OpsHub for Snow Family para administrar dispositivos.

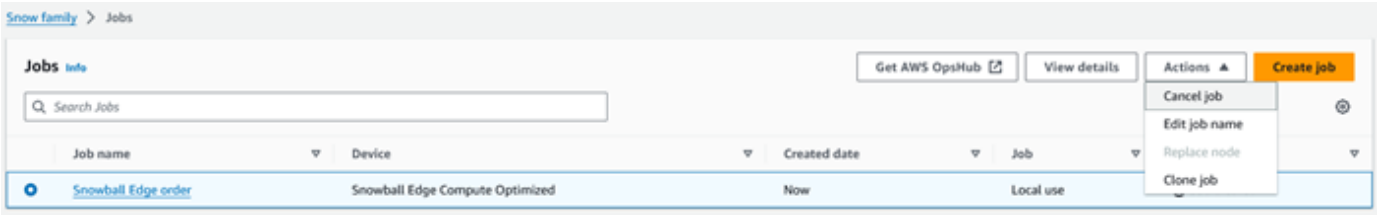
Para descargar e instalar AWS OpsHub for Snow Family

1. En los AWS Snowball recursos, haga clic en AWS OpsHub. En la AWS OpsHub sección con los enlaces de descarga, elija el enlace de descarga adecuado AWS OpsHub para instalarlo en su sistema operativo.
2. En la sección AWS OpsHub, seleccione Download en la línea correspondiente a su sistema operativo y siga los pasos de instalación. Cuando haya terminado, elija Next.

Cancelar un trabajo a través del Consola de administración de la familia de productos Snow de AWS

Después de crear un trabajo para solicitar un dispositivo de la familia Snow, puede cancelar el trabajo a través del Consola de administración de la familia de productos Snow de AWS. Si cancelas el trabajo, no recibirás el dispositivo que has pedido. Solo puede cancelar el trabajo mientras el estado del trabajo sea Trabajo creado. Una vez que el trabajo supere este estado, no podrá cancelarlo. Para obtener más información, consulte Estados de los trabajos.

1. Inicie sesión en la Consola de administración de la familia de productos Snow de AWS.
2. Elija el trabajo que desee cancelar.
3. Elija Actions. En el menú que aparece, selecciona Cancelar trabajo.



4. Aparece la ventana Cancelar trabajo. Para confirmar la cancelación del trabajo, introduzca **`job name`** y seleccione Cancelar trabajo. En la lista de trabajos, aparece Cancelado en la columna Estado.

Recepción del dispositivo Snowball Edge

Cuando recibas el AWS Snowball Edge dispositivo, es posible que notes que no viene en una caja. El dispositivo va integrado en su propio contenedor de transporte compacto y robusto. Al recibir el

dispositivo, inspecciónelo para ver si ha sufrido daños o alteraciones evidentes. Si observa cualquier indicio sospechoso en el dispositivo , no lo conecte a la red interna. Contacte con AWS Support e informe a nuestros profesionales sobre el problema para que le envíen otro dispositivo.

> **Important**
>
> El AWS Snowball Edge dispositivo es propiedad de AWS. La manipulación de un AWS Snowball Edge dispositivo constituye una infracción de la Política de uso AWS aceptable. Para obtener más información, consulte la Política de uso aceptable de AWS.

El dispositivo tiene un aspecto parecido al que se muestra en la imagen siguiente.

Si está listo para conectar el dispositivo a la red interna, consulte la siguiente sección.

Siguiente: Conexión a la red local

Conexión a la red local

Utilice el siguiente procedimiento para conectar el AWS Snowball Edge dispositivo a la red local. No es preciso conectar el dispositivo a Internet. El dispositivo tiene tres puertas: una delantera, otra posterior y una superior.

Conexión del dispositivo a la red

1. Abra las puertas delantera y posterior; y deslícelas en las ranuras del dispositivo reservadas para tal fin. Esto le permite obtener acceso a la pantalla LCD táctil integrada en la parte delantera del dispositivo, así como a los puertos de alimentación eléctrica y de red de la parte posterior.

   > **Note**
   >
   > No cierre las puertas delantera y posterior mientras utiliza el dispositivo Snowball Edge. Las puertas abiertas permiten que el aire enfríe el dispositivo. El cierre de las puertas mientras se utiliza el dispositivo puede hacer que el dispositivo se apague para evitar el sobrecalentamiento.

2. Abra la puerta superior, retire el cable de alimentación eléctrica suministrado de su soporte y conecte el dispositivo a la alimentación eléctrica.
3. Elija uno de sus propios cables de red RJ45, SFP+ o QSFP+ y conecte el dispositivo a la red local. Los puertos de red se encuentran en la parte posterior del dispositivo.
4. Encienda el AWS Snowball Edge dispositivo pulsando el botón de encendido situado sobre la pantalla LCD.
5. Cuando el dispositivo está listo, la pantalla LCD muestra un vídeo breve mientras el dispositivo se prepara para comenzar. Transcurridos unos 10 minutos, el dispositivo queda listo para desbloquearlo.
6. (Opcional) Puede cambiar la configuración de red predeterminada desde la pantalla LCD; para ello, elija CONNECTION.

   Puede cambiar la dirección IP por otra dirección estática, que proporcionará siguiendo este procedimiento.

Para solucionar problemas de arranque, consulte Solución de problemas de arranque.

Para cambiar la dirección IP de un AWS Snowball Edge dispositivo

1. En la pantalla LCD, seleccione CONNECTION.

Aparecerá una pantalla que muestra la configuración de red actual del dispositivo AWS Snowball Edge . La dirección IP que aparece debajo del cuadro desplegable se actualiza automáticamente para reflejar la dirección DHCP que solicitó el AWS Snowball Edge dispositivo.

2. (Opcional) Cambie la dirección IP por una dirección IP estática. También puede dejarla como está.

Ahora, el dispositivo está conectado a la red.

> **Important**
>
> Para evitar que tus datos se dañen, no desconectes el AWS Snowball Edge dispositivo ni cambies su configuración de conexión mientras esté en uso.

Siguiente: Obtener credenciales para acceder a un dispositivo de la familia Snow

Obtener credenciales para acceder a un dispositivo de la familia Snow

Cada trabajo tiene un conjunto de credenciales que debe obtener de la API de administración de trabajos Consola de administración de la familia de productos Snow de AWS o de la API de administración de trabajos para autenticar su acceso al dispositivo Snow Family. Estas credenciales son un archivo de manifiesto cifrado y un código de desbloqueo asociado. El archivo de manifiesto contiene información importante sobre el trabajo y los permisos asociados a él.

> **Note**
>
> Obtendrá las credenciales durante el transporte del dispositivo hacia sus instalaciones. Puede ver el estado del trabajo en la Consola de administración de la familia de productos Snow de AWS. Para obtener más información, consulte Estados de los trabajos.

Obtención de las credenciales mediante la consola

1. Inicie sesión en AWS Management Console y abra el Consola de administración de la familia de productos Snow de AWS.

2. En la consola, busque en la tabla el trabajo concreto cuyo manifiesto desea descargar y seleccione ese trabajo.
3. Amplíe el panel de estado del trabajo y elija Ver detalles del trabajo.
4. En el panel de detalles que aparece, expanda Credenciales y, a continuación, haga lo siguiente:

   - Anota el código de desbloqueo (incluidos los guiones), ya que tendrás que introducir los 29 caracteres para desbloquear el dispositivo.
   - Elija Descargar manifiesto en el cuadro de diálogo y, a continuación, siga las instrucciones para descargar el archivo de manifiesto del trabajo en el equipo. El nombre del archivo de manifiesto incluye el valor de ID del trabajo.

> **Note**
>
> Te recomendamos que no guardes una copia del código de desbloqueo en la misma ubicación del ordenador que el manifiesto para esa tarea. Para obtener más información, consulte Prácticas recomendadas para utilizar el dispositivo Snowball Edge.

Ahora que tiene sus credenciales, el siguiente paso es descargar el cliente de Snowball Edge, que se utiliza para desbloquear el AWS Snowball Edge dispositivo.

Siguiente: Descarga e instalación del cliente de Snowball Edge

Descarga e instalación del cliente de Snowball Edge

Puede descargar e instalar el cliente de Snowball Edge desde Recursos de AWS Snowball Edge. En esa página encontrará el paquete de instalación para su sistema operativo. Siga las instrucciones para instalar el cliente de Snowball Edge. Si el cliente de Snowball Edge se ejecuta desde un terminal de la estación de trabajo, puede que sea necesario usar una ruta específica, en función del sistema operativo:

- Microsoft Windows: una vez que el cliente se ha instalado, puede ejecutarlo desde cualquier directorio sin necesidad de preparación adicional.
- Linux: el cliente de Snowball Edge debe ejecutarse desde el directorio `~/snowball-client-linux-build_number/bin/`. El cliente de Snowball Edge solo se admite en distribuciones Linux de 64 bits.

- macOS: el script `install.sh` copia carpetas del archivo .tar del cliente de Snowball Edge al directorio `/usr/local/bin/snowball`. Si ejecuta este script, podrá ejecutar el cliente de Snowball Edge desde cualquier directorio si `/usr/local/bin` es una ruta en su `bash_profile`. Para verificar la ruta, use el comando `echo $PATH`.

Para obtener más información sobre los comandos del cliente Snowball Edge, consulte. Uso de los comandos del cliente Snowball Edge

Siguiente: Desbloquear el dispositivo de la familia Snow

Desbloquear el dispositivo de la familia Snow

En esta sección se describe el desbloqueo del dispositivo de la familia Snow mediante la CLI de Snowball Edge. Para desbloquear el dispositivo mediante AWS OpsHub una herramienta de interfaz gráfica de usuario (GUI) para los dispositivos de la familia Snow, consulte Desbloquear un dispositivo un dispositivo.

Antes de utilizar un dispositivo de la familia Snow para transferir datos o realizar tareas de computación perimetral, debe desbloquear el dispositivo. Al desbloquear el dispositivo, debe autenticar su capacidad de acceso proporcionando dos tipos de credenciales: un código de desbloqueo de 29 dígitos y un archivo de manifiesto. Tras desbloquear el dispositivo, podrá configurarlo con más detalle, transferir datos hacia o desde él, configurar y utilizar instancias compatibles con Amazon EC2 y mucho más.

Antes de desbloquear un dispositivo, el dispositivo debe estar conectado a la alimentación y a la red, encendido y tener asignada una dirección IP. Consulte las Conexión a la red local Necesitará la siguiente información sobre los dispositivos de la familia Snow:

- Descarga e instalación del cliente de Snowball Edge. Para obtener más información, consulte Descarga e instalación del cliente de Snowball Edge.
- Obtenga las credenciales del Consola de administración de la familia de productos Snow de AWS. Para uno o más dispositivos independientes, los códigos de desbloqueo y el archivo de manifiesto de cada dispositivo de la familia Snow. Para un clúster de dispositivos Snowball Edge, un código de desbloqueo y un archivo de manifiesto para el clúster. Para obtener más información sobre la descarga de credenciales, consulteObtener credenciales para acceder a un dispositivo de la familia Snow.
- Encienda cada dispositivo y conéctelo a la red. Para obtener más información, consulte Conexión a la red local.

Para desbloquear un dispositivo independiente con el cliente Snowball Edge

1. Busque la dirección IP del AWS Snowball Edge dispositivo en la pantalla LCD del AWS Snowball Edge dispositivo, en la pestaña Conexiones. Anote la dirección IP.
2. Utilice el `unlock-device` comando para autenticar su acceso al dispositivo de la familia Snow con la dirección IP del dispositivo de la familia Snow y sus credenciales, de la siguiente manera.

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

   El dispositivo indica que se ha desbloqueado correctamente con el siguiente mensaje.

```
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.
```

   Si el comando vuelve a aparecer`connection refused`, consulteSolución de problemas al desbloquear un dispositivo de la familia Snow.

   Example del **`unlock-device`** comando

   En este ejemplo, la dirección IP del dispositivo es`192.0.2.0`, el nombre del archivo de manifiesto es `JID2EXAMPLE-0c40-49a7-9f53-916aEXAMPLE81-manifest.bin` y el código de desbloqueo de 29 caracteres es. `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 un clúster de dispositivos Snowball Edge con el cliente Snowball Edge

1. Busque la dirección IP de cada uno de los dispositivos del clúster en la pantalla LCD de cada AWS Snowball Edge dispositivo, en la pestaña Conexiones. Tome nota de las direcciones IP.

2. Utilice el `snowballEdge unlock-cluster` comando para autenticar su acceso al clúster de AWS Snowball Edge dispositivos con la dirección IP de uno de los dispositivos del clúster, sus credenciales y las direcciones IP de todos los dispositivos del clúster de la siguiente manera.

```
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
```

El clúster de dispositivos indica que se desbloqueó correctamente con el siguiente mensaje.

```
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.
```

Si el comando vuelve a aparecer`connection refused`, consulte[Solución de problemas al desbloquear un dispositivo de la familia Snow](#).

Example del **`unlock-cluster`** comando

En este ejemplo, para un clúster de cinco dispositivos, la dirección IP de uno de los dispositivos del clúster es`192.0.2.0`, el nombre del archivo de manifiesto es `JID2EXAMPLE-0c40-49a7-9f53-916aEXAMPLE81-manifest.bin` y el código de desbloqueo de 29 caracteres es. `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
```

Solución de problemas al desbloquear un dispositivo de la familia Snow

Si el `unlock-device` comando vuelve a `connection refused` aparecer, es posible que haya escrito mal la sintaxis del comando o que la configuración de su ordenador o red esté impidiendo que el comando llegue al dispositivo Snow. Realice las siguientes acciones para resolver la situación:

1. Asegúrese de que el comando se haya introducido correctamente.
   a. Utilice la pantalla LCD del dispositivo para comprobar que la dirección IP utilizada en el comando es correcta.
   b. Asegúrese de que la ruta al archivo de manifiesto utilizado en el comando sea correcta, incluido el nombre del archivo.
   c. Utilice el Consola de administración de la familia de productos Snow de AWSpara comprobar que el código de desbloqueo utilizado en el comando es correcto.
2. Asegúrese de que el ordenador que está utilizando esté en la misma red y subred que el dispositivo Snow.
3. Asegúrese de que el ordenador que está utilizando y la red estén configurados para permitir el acceso al dispositivo Snow. Utilice el `ping` comando de su sistema operativo para determinar si el ordenador puede acceder al dispositivo Snow a través de la red. Compruebe las configuraciones del software antivirus, la configuración del firewall, la red privada virtual (VPN) u otras configuraciones del ordenador y la red.

Ahora puede empezar a utilizar el dispositivo de la familia Snow.

Siguiente: Configuración de usuarios locales

Configuración de usuarios locales

A continuación, se indican los pasos para configurar un administrador local en el AWS Snowball Edge dispositivo.

1. Recupere las credenciales de usuario raíz

Utilice `snowballEdge list-access-keys` y `snowballEdge get-secret-access-key` para obtener sus credenciales locales. Para obtener más información, consulte Obtención de credenciales.

2. Configure la credencial de usuario raíz con **`aws configure`**

   Proporcione los valores de `AWS Access Key ID`, `AWS Secret Access Key` y `Default region name`. El nombre de la región debe ser `snow`. Si lo desea, proporcione un `Default output format`. Para obtener más información sobre la configuración del AWS CLI, consulte Configuración del AWS CLI en la Guía del AWS Command Line Interface usuario.

3. Cree uno o más usuarios locales en el dispositivo

   Utilice el comando `create-user` para añadir usuarios al dispositivo.

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

   Después de añadir usuarios según sus necesidades empresariales, puede almacenar sus credenciales raíz de AWS en un lugar seguro y usarlas solo para tareas de administración de cuentas y servicios. Para obtener más información sobre cómo crear usuarios de IAM, consulte Creación de un usuario de IAM en la Cuenta de AWS en la Guía del usuario de IAM.

4. Cree una clave de acceso para su usuario

   > **Warning**
   >
   > En este escenario, se requieren usuarios de IAM con acceso programático y credenciales de larga duración, lo que supone un riesgo de seguridad. Para ayudar a mitigar este riesgo, le recomendamos que brinde a estos usuarios únicamente los permisos que necesitan para realizar la tarea y que los elimine cuando ya no los necesiten. Las claves de acceso se pueden actualizar si es necesario. Para obtener más información, consulte Actualización de claves de acceso en la Guía de usuario de IAM.

   Utilice el comando `create-access-key` para crear una clave de acceso para su usuario.

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

Guarde la información de clave de acceso en un archivo y distribúyalo a los usuarios.

5. Cree una política de acceso

   Quizás desee que diferentes usuarios tengan distintos niveles de acceso a la funcionalidad en el dispositivo. En el ejemplo siguiente se crea un documento de política denominado `s3-only-policy` y se asocia a un usuario.

```
{
  "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. Asocie la política a su usuario

   Utilice `attach-user-policy` para asociar la política s3-only-policy a un usuario.

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

Para obtener más información acerca del uso local de IAM, consulte Uso local de IAM.

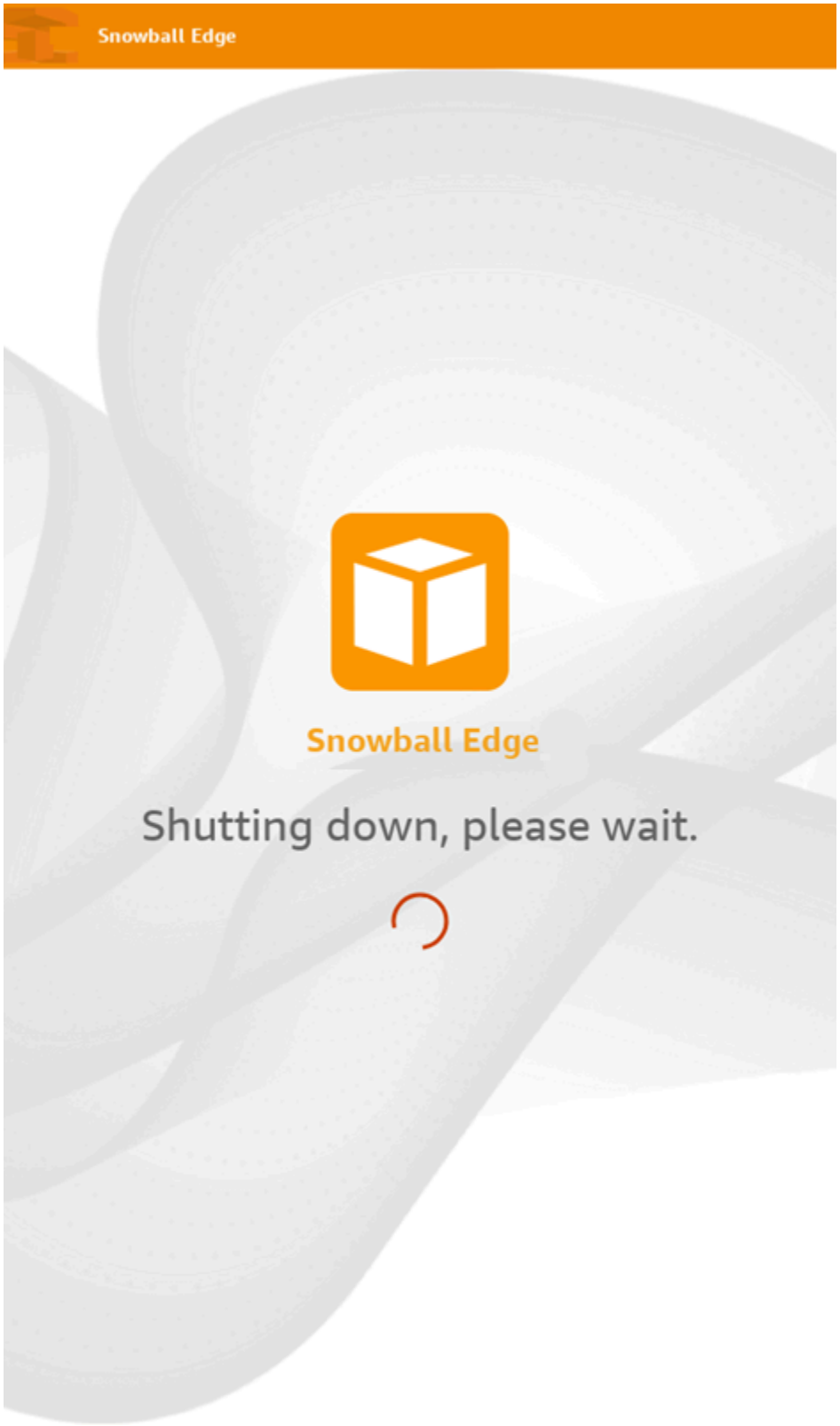
Siguiente: Uso de un dispositivo AWS Snowball Edge

Reinicio del dispositivo Snow Family

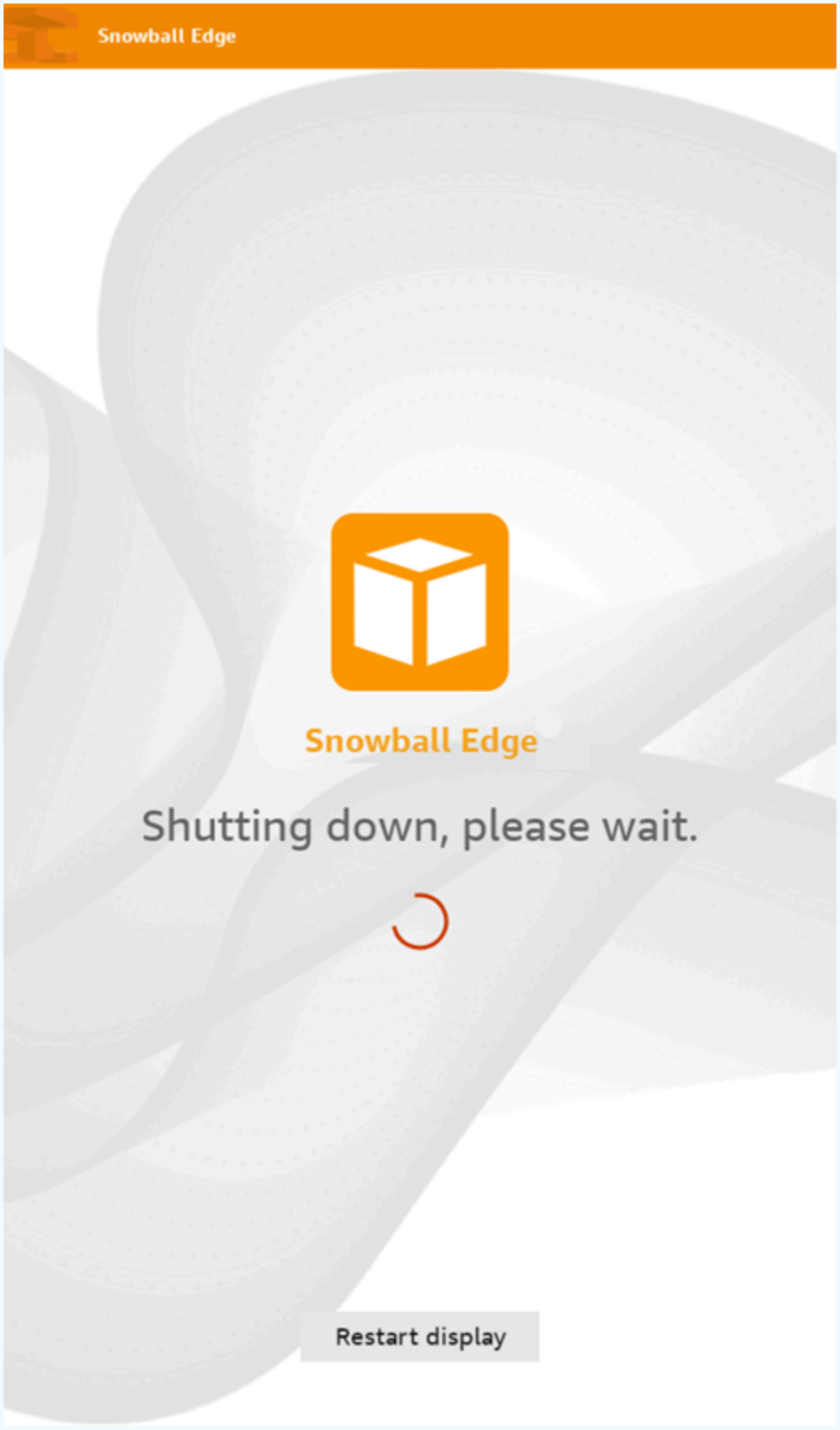
Antes de reiniciar un dispositivo Snow Family, asegúrese de que se hayan detenido todas las transferencias de datos al dispositivo.

Reinicio del dispositivo con el botón de encendido:

1. Cuando haya finalizado toda comunicación con el dispositivo, apáguelo pulsando el botón de encendido situado encima de la pantalla LCD. El dispositivo tarda unos 20 segundos en apagarse. Mientras el dispositivo se apaga, la pantalla LCD muestra un mensaje que indica que el dispositivo se está apagando.


Snowball Edge
Snowball Edge
Shutting down, please wait.

> **Note**
>
> Si la pantalla LCD muestra el mensaje de apagado cuando el dispositivo no se está apagando realmente, pulse el botón Restart display de la pantalla para que esta vuelva a funcionar normalmente.


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

2. Pulse el botón de encendido. Cuando el dispositivo está listo, la pantalla LCD muestra un vídeo breve mientras el dispositivo se prepara para comenzar. Transcurridos unos 10 minutos, el dispositivo queda listo para desbloquearlo.
3. Desbloquee el dispositivo. Consulte Desbloquear el dispositivo de la familia Snow.

Reinicio del dispositivo mediante el cliente de Snowball Edge:

1. Cuando haya finalizado toda comunicación con el dispositivo, utilice el comando `reboot-device` para reiniciarlo. Cuando el dispositivo está listo, la pantalla LCD muestra un vídeo breve mientras el dispositivo se prepara para comenzar. Transcurridos unos 10 minutos, el dispositivo queda listo para desbloquearlo.

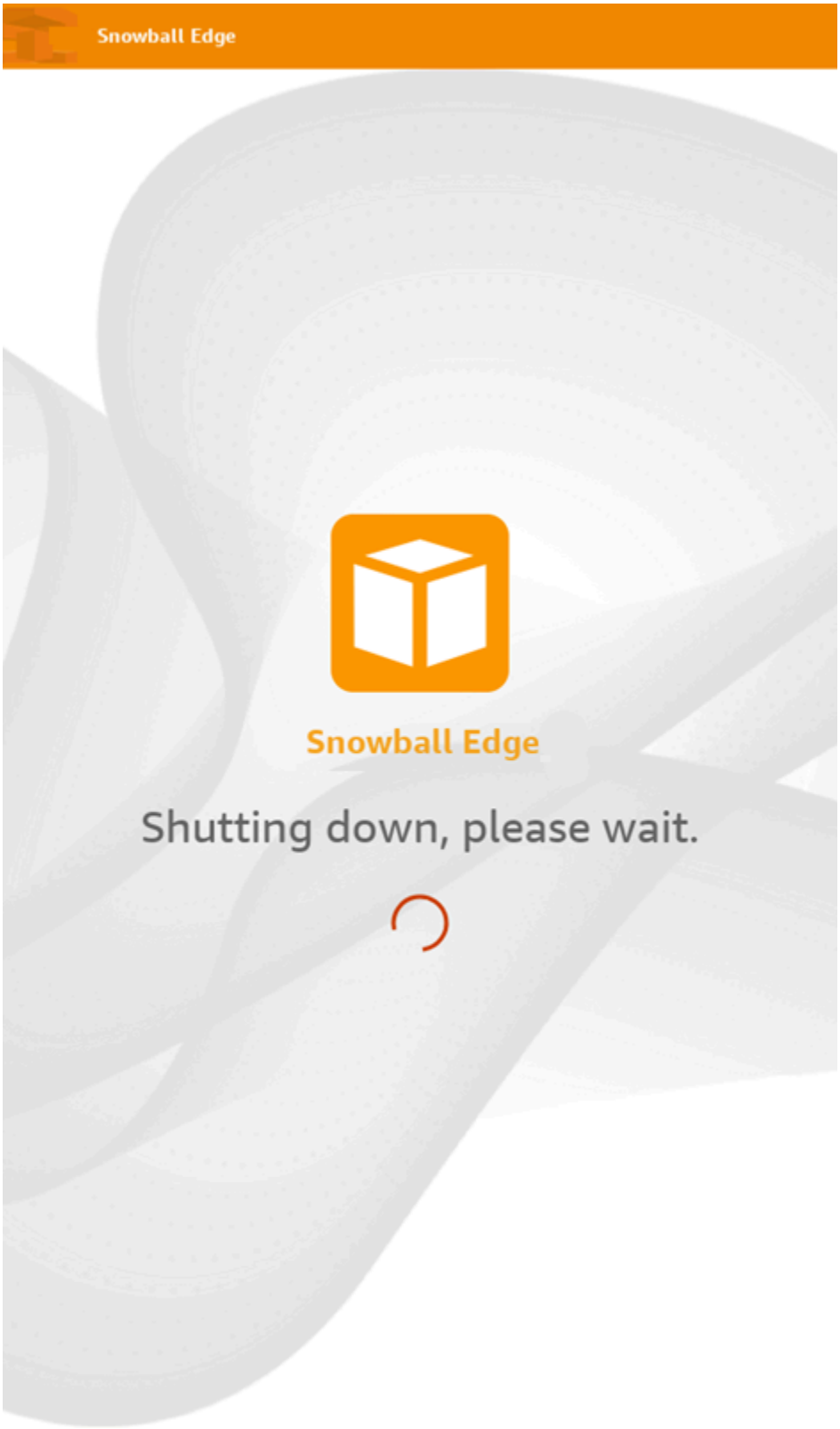
   ```
   snowballEdge reboot-device
   ```

2. Desbloquee el dispositivo. Consulte Desbloquear el dispositivo de la familia Snow.

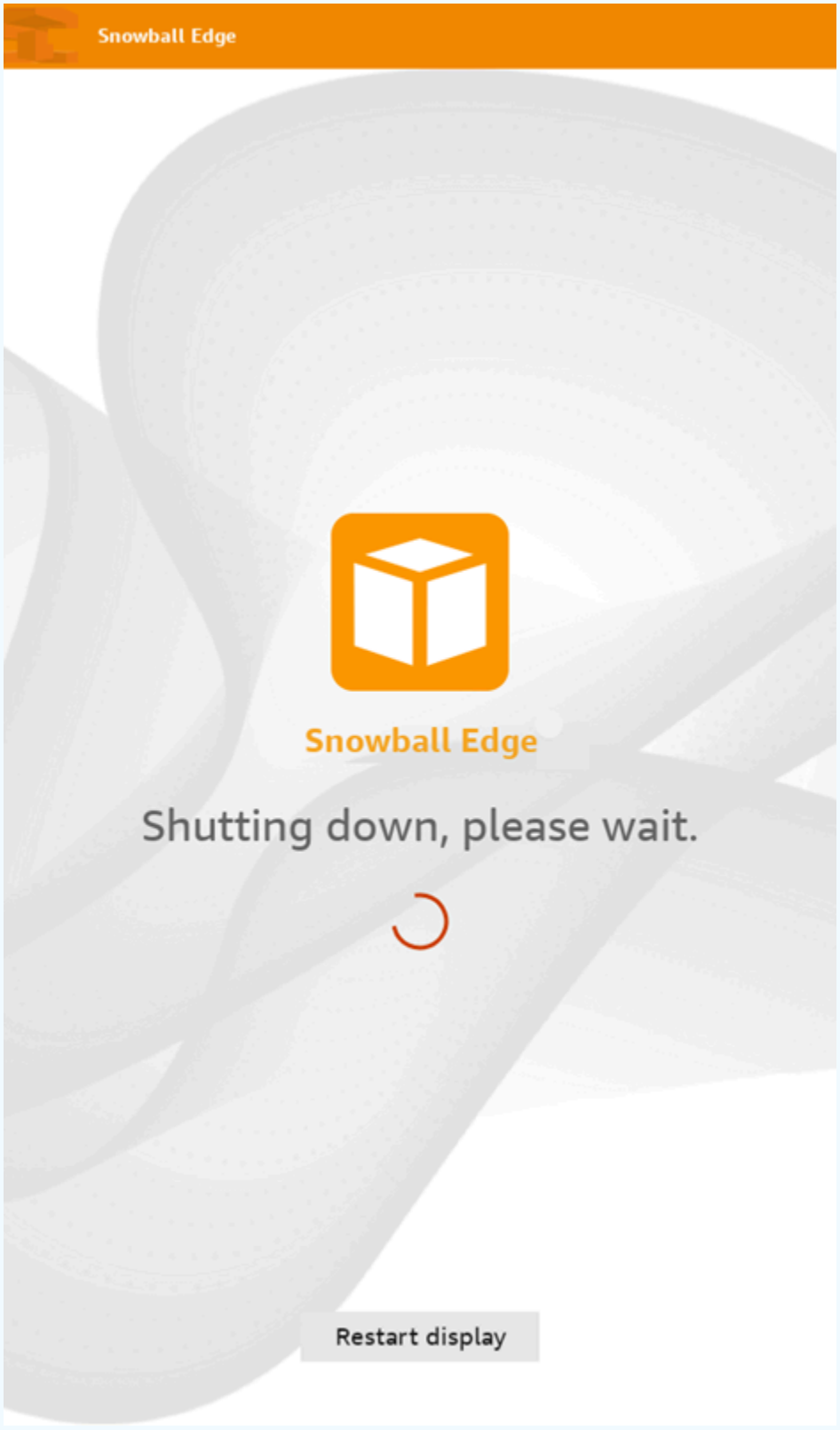
Apagado del dispositivo Snowball Edge

Cuando hayas terminado de transferir los datos al AWS Snowball Edge dispositivo, prepáralo para su viaje de regreso a AWS. Antes de continuar, asegúrese de que se hayan detenido todas las transferencias de datos al dispositivo. Si utilizabas la interfaz NFS para transferir datos, desactívala antes de apagar el dispositivo. Para obtener más información, consulte Administración de la interfaz NFS.

Cuando haya finalizado toda comunicación con el dispositivo, apáguelo pulsando el botón de encendido situado encima de la pantalla LCD. El dispositivo tarda unos 20 segundos en apagarse. Mientras el dispositivo se apaga, la pantalla LCD muestra un mensaje que indica que el dispositivo se está apagando.


Snowball Edge
Snowball Edge
Shutting down, please wait.

> **Note**
>
> Si la pantalla LCD muestra el mensaje de apagado cuando el dispositivo no se está apagando realmente, pulse el botón Restart display de la pantalla para que esta vuelva a funcionar normalmente.


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

Cuando el dispositivo se apague, la información de envío aparecerá en la pantalla de tinta electrónica. Si la información de envío de la devolución no aparece en la pantalla de tinta electrónica, póngase en contacto con nosotros AWS Support.

Siguiente: Devolución del dispositivo Snowball Edge

Devolución del dispositivo Snowball Edge

Cuando haya terminado de utilizar el Snowball Edge y lo haya apagado, una empresa de transporte se lo devolverá a. AWS El transportista proporciona automáticamente un número de seguimiento para el envío del dispositivo. El número de seguimiento aparece en el Consola de administración de la familia de productos Snow de AWS. Puede acceder al número de seguimiento y a un enlace al sitio web de seguimiento del transportista consultando los detalles del estado del trabajo en la consola. Para obtener más información, consulta el artículo Envío de devoluciones para los dispositivos de la familia Snow.

El transportista entrega el dispositivo a una instalación de AWS clasificación y lo envía al centro de AWS datos. En el centro de datos, AWS se asegurará de que el dispositivo no haya sido manipulado durante el envío y de que esté en buen estado. Si el dispositivo contiene datos para importarlos a Amazon S3, AWS empezará a importarlos. De lo contrario, los datos del dispositivo se borrarán de forma segura. Puede realizar un seguimiento de los cambios de estado a medida que AWS procesa el dispositivo en el Consola de administración de la familia de productos Snow de AWS. Recibirás notificaciones de Amazon SNS sobre los cambios de estado si seleccionaste esa opción al crear el trabajo para pedir el dispositivo. Para obtener más información, consulte Supervisión del estado de la importación.

Los valores de estado final incluyen cuándo se ha recibido el AWS Snowball Edge dispositivo AWS, cuándo comienza la importación de datos y cuándo se ha completado el trabajo.

> **Note**
>
> Si el dispositivo contiene datos que pretendía importar a Amazon S3 y no desea que se importen los datos del dispositivo, póngase en contacto con nosotros AWS Support para solicitar la cancelación del trabajo de Snow. Si cancela el trabajo, omitiremos la transferencia de datos y borraremos el dispositivo de forma segura siguiendo los procesos establecidos. No podemos almacenar en nuestras instalaciones ningún dispositivo que contenga sus datos debido a nuestros estrictos procedimientos operativos y de cadena de custodia.

Para preparar un AWS Snowball Edge dispositivo para el envío de devolución

1. Apague el dispositivo. Para obtener más información, consulte Apagado del dispositivo Snowball Edge.
2. Desconecte todos los cables de red conectados al dispositivo.
3. Desconecte el cable de alimentación. Guárdalo en el conector para cables situado en la parte superior del AWS Snowball Edge dispositivo.
4. Cierre las puertas de la parte posterior, superior y frontal del AWS Snowball Edge dispositivo. Presiona cada puerta hasta que oigas y sientas un clic.

Siguiente: Devolución de dispositivos Snow Family

Devolución de dispositivos Snow Family

El AWS Snowball Edge dispositivo se envía desde un centro de AWS datos y se entrega en él. La información de envío prepagada que aparece en la pantalla de tinta electrónica del dispositivo incluye la dirección para devolver el AWS Snowball Edge dispositivo. La velocidad de envío de la devolución coincide con la velocidad de envío original cuando recibió el dispositivo. Puede realizar un seguimiento de los cambios de estado desde la Consola de administración de la familia de productos Snow de AWS y hacer un seguimiento del progreso del paquete a través del transportista de su región.

Para obtener más información sobre cómo devolver el AWS Snowball Edge dispositivo, consulteTransportistas.

> **Important**
>
> A menos que se indique lo contrario AWS, nunca coloques una etiqueta de envío separada en el AWS Snowball Edge dispositivo. Utiliza siempre la información de envío que aparece en la pantalla de tinta electrónica del AWS Snowball Edge dispositivo.

Transportistas

Cuando crea un pedido para un dispositivo de la familia Snow, proporciona la dirección a la que se debe enviar el AWS Snowball Edge dispositivo. El transportista que opera en tu región se encarga

del envío de los dispositivos desde AWS y hacia ti AWS. Puede ver la información de envío saliente cuando su trabajo pase al estado Preparando el envío.

Hay un número de seguimiento para cada AWS Snowball Edge dispositivo que se envía. Encontrará el número de seguimiento y un enlace al sitio web de seguimiento en el panel de trabajos de Consola de administración de la familia de productos Snow de AWS o en la API de administración de trabajos.

Los dispositivos AWS Snowball Edge admiten los siguientes operadores:

- Para la India, el transportista es Blue Dart.
- En el caso de Corea, Japón, Australia e Indonesia, el transportista es Kuehne + Nagel.
- Para China y Hong Kong, el transportista es S.F. Express.
- En todas las demás regiones, el transportista es UPS.

Temas

AWS Snowball Edge UPS recoge en la UE, EE. UU., Reino Unido, Sudáfrica y Canadá

Con frecuencia, UPS puede recoger su dispositivo en la UE, EE. UU., Reino Unido, Sudáfrica y Canadá. A continuación presentamos algunas pautas útiles:

- Programa una recogida directamente con UPS o lleva el AWS Snowball Edge dispositivo a un centro de entrega de paquetes de UPS para su envío. AWS
- La etiqueta de envío prepagada de UPS que aparece en la pantalla de tinta electrónica contiene la dirección de devolución del AWS Snowball Edge dispositivo.

- El AWS Snowball Edge dispositivo se entrega a una instalación de AWS clasificación y se envía a un centro de AWS datos. UPS le proporciona un número de seguimiento.

> **Important**
>
> A menos que se indique lo contrario AWS, nunca coloque una etiqueta de envío separada en el AWS Snowball Edge dispositivo. Utilice siempre la información de envío que se muestra en la pantalla de tinta electrónica del dispositivo.

UPS envía dispositivos Snowball Edge a los siguientes países miembros de la UE: Alemania, Austria, Bélgica, Bulgaria, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Portugal, República Checa, República de Chipre, Rumanía y Suecia.

> **Note**
>
> Ahora, los pedidos entre el Reino Unido y los países de la Unión Europea se consideran internacionales y requieren la aprobación mediante un proceso internacional especial. Si necesita enviar un dispositivo entre el Reino Unido y la UE, envíenos un correo electrónico a <snowball-shipping@amazon.com> para solicitar una factura comercial antes de organizar la recogida o entrega con UPS.

Los servicios de UPS para los productos Snow Family son nacionales únicamente dentro de un país.

AWS Snowball Recogidas en el Reino Unido

En el Reino Unido, debe tener en cuenta la siguiente información relativa a la recogida de dispositivos Snowball Edge por parte de UPS:

- Puedes hacer los arreglos necesarios para que UPS recoja el AWS Snowball Edge dispositivo programando directamente la recogida con UPS, o bien llevas el AWS Snowball Edge dispositivo a un centro de entrega de paquetes de UPS para que te lo envíen. AWS
- La etiqueta de envío prepagada de UPS que aparece en la pantalla de tinta electrónica contiene la dirección correcta para devolver el AWS Snowball Edge dispositivo.
- El AWS Snowball Edge dispositivo se entrega a una instalación de AWS clasificación y se envía al centro de AWS datos. UPS le notificará automáticamente el número de seguimiento del trabajo.

> **Important**
>
> A menos que se le indique lo contrario personalmente AWS, nunca coloque una etiqueta de envío separada en el AWS Snowball Edge dispositivo. Utilice siempre la información de envío que se muestra en la pantalla de tinta electrónica del dispositivo.

Los servicios de UPS para los productos Snow Family son nacionales únicamente dentro de un país.

> **Note**
>
> Desde enero de 2021, el Reino Unido ya no forma parte de la UE. Los pedidos entre el Reino Unido y otros países de la UE son pedidos internacionales, un proceso de disponibilidad no general que solo se aprueba mediante un proceso internacional especial. Si un cliente ha obtenido el visto bueno y va a devolver un dispositivo desde un país de la UE a LHR o desde el Reino Unido a un país de la UE, debe solicitar primero una devolución a `<snowball-shipping@amazon.com>` para que se le pueda proporcionar una factura comercial antes de organizar la recogida o la entrega con UPS.

AWS Snowball recogidas en Brasil

Estas son algunas pautas para la recogida de un dispositivo Snowball Edge en Brasil por parte de UPS:

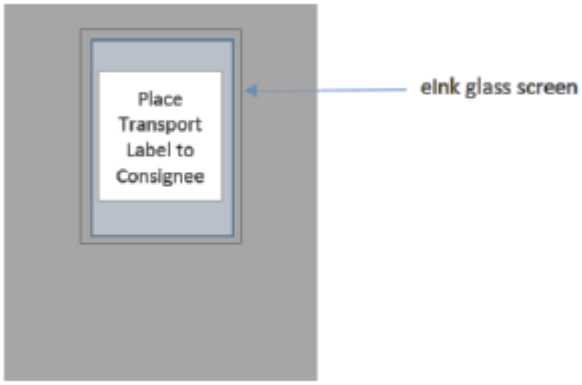
- Cuando esté preparado para devolver un dispositivo Snowball Edge, llame al 0800-770-9035 para concertar la recogida con UPS.
- Snowball Edge está disponible internamente en Brasil, incluidos 26 estados y el Distrito Federal.
- Si tiene un identificador fiscal del Cadastro Nacional de Pessoa Juridica (CNPJ), es importante que sepa cuál es antes de crear el trabajo.
- Debe emitir el documento adecuado para devolver el dispositivo Snowball Edge. Confirme con el departamento fiscal cuál de los documentos siguientes es necesario en su estado, en función de su registro de Imposto sobre Circulação de Mercadorias e Serviços (ICMS):
  - Dentro de São Paulo: suelen ser necesarias una declaración de ICMS negativa y una factura de impuestos electrónica (NF-e).
  - Fuera de São Paulo: se suele necesitar lo siguiente:
    - Una declaración no ICMS

- Una “nota fiscal avulsa”
- Una factura de impuestos electrónica (NF-e)

> **Note**
>
> En cuanto a la declaración tributaria ICMS negativa, le recomendamos que genere cuatro copias: una para sus registros y las otras tres para el transporte.

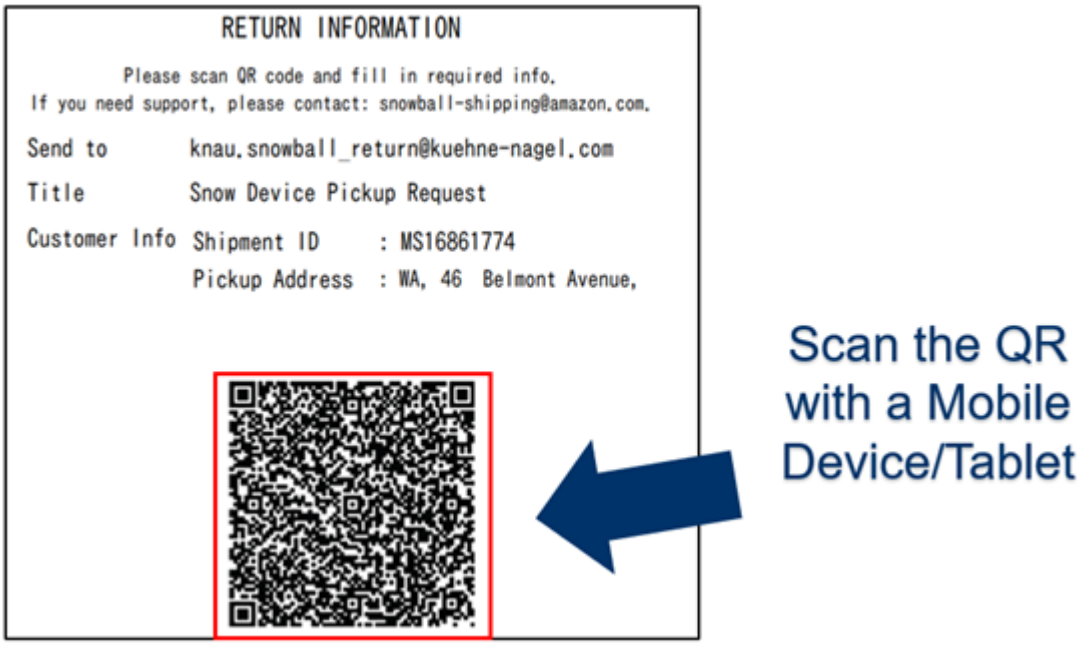
AWS Snowball camionetas en Australia

En Australia, si vas a devolver un AWS Snowball Edge dispositivo a AWS, coloca la etiqueta de transporte de devolución (que se encuentra en la bolsa que contiene estas instrucciones) sobre la etiqueta de tinta electrónica del dispositivo Snow.



> **Note**
>
> Si no recibió ninguna etiqueta de devolución con el dispositivo, envíe un correo electrónico a knau.snowball_return@kuehne-nagel.com e indique el número de serie del dispositivo o su número de referencia.

Para tramitar la devolución del dispositivo Snow Family, escanee con su dispositivo móvil el código QR que aparece en las instrucciones de devolución. En el dispositivo, aparece un hiperenlace a un mensaje de correo electrónico. El mensaje contiene información como la dirección de correo electrónico, el asunto y el número de control o el número de albarán. Rellene la fecha de recogida, el nombre y los detalles de contacto, o proporcione una nueva dirección de recogida si hay algún cambio.



AWS Snowball recogidas en la India

En la India, Blue Dart es quien recoge el dispositivo Snowball. Cuando esté listo para devolver el dispositivo Snowball, apáguelo y prepárelo para su devolución. Para programar la recogida, envíe un correo electrónico a snowball-pickup@amazon.com con el asunto Snowball Pickup Request. En el mensaje, incluya la siguiente información:

- ID de trabajo: el ID de trabajo asociado al Snowball al que desea que se devuelva. AWS
- Cuenta de AWS ID: el ID de la AWS cuenta que creó el trabajo.
- Earliest Pickup Time: la hora más temprana del día (en hora local) a la que se puede recoger el dispositivo Snowball.
- Latest Pickup Time: la hora más tardía del día (en hora local) a la que se puede recoger el dispositivo Snowball.
- Special Instructions (opcional): instrucciones especiales para recoger el dispositivo Snowball, incluidos los datos de contacto para coordinar la recogida.

El equipo de Snowball organizará la recogida con Blue Dart y le enviará un correo electrónico de confirmación. Blue Dart le proporcionará una etiqueta de envío de papel y recogerá el dispositivo Snowball.

> **Important**
>
> Al utilizar un dispositivo Snowball en India, recuerde presentar todos los documentos fiscales en su estado.

AWS Snowball Edge recoge en Corea

En Corea, Kuehne + Nagel gestiona las recogidas. Cuando esté listo para devolver su dispositivo, envíe un mensaje de correo electrónico a snowball-shipping@amazon.com con el asunto Snowball Pickup Request para que nos encarguemos de programar la recogida. En el cuerpo del mensaje, incluya la siguiente información:

- ID de trabajo: el ID de trabajo asociado al Snowball al que desea que se devuelva. AWS
- Pickup Address: la dirección donde se recogerá el dispositivo.
- Pickup Date: el primer día en el que le gustaría que se efectuara la recogida del dispositivo.
- Point of contact details: el nombre, la dirección de correo electrónico y el número de teléfono local que puede usar Kuehne + Nagel para comunicarse con usted si es necesario.

Pronto recibirá un correo electrónico de seguimiento del equipo de Snowball con información sobre la recogida en la dirección en la que se proporcionó el dispositivo. Apague el dispositivo y téngalo preparado para la recogida, normalmente entre las 13:00 y las 15:00 h.

AWS Snowball Edge recoge en Hong Kong

En Hong Kong, S.F. Express se encarga de las recogidas. Cuando esté listo para devolver el dispositivo, envíe un correo electrónico a snowball-shipping-ap-east -1@amazon.com con la solicitud de recogida de Snowball en el asunto para que podamos programar su recogida. En el cuerpo del mensaje, incluya la siguiente información:

- ID del trabajo
- Cuenta de AWS ID
- Nombre del contacto
- Número de teléfono del contacto
- Dirección de correo electrónico del contacto
- El día que desea que se recoja el dispositivo

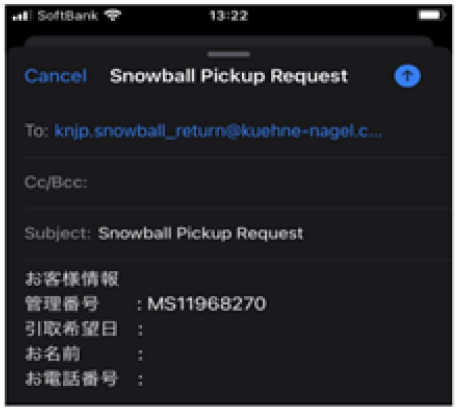
- La hora de recogida más temprana
- La hora de recogida más tardía
- Dirección de recogida

Una vez que haya concertado la fecha de recogida con S.F. Express, no podrá reprogramarla.

S.F. Express AWS entregará el dispositivo. El número de seguimiento de S.F. Express para el envío de devolución indica cuándo se entregó.

AWS Snowball Recogidas en Singapur, Japón e Indonesia

En Singapur, Japón e Indonesia, cuando esté listo para devolver el dispositivo, escanee con su teléfono móvil el código QR que aparece en la etiqueta de tinta electrónica de devolución. Esto le llevará directamente a una plantilla de correo electrónico. Rellene la fecha y la hora de recogida y los datos de contacto.



> **Note**
>
> Si su dirección de recogida es diferente a la dirección en la que se entregó el dispositivo, añada la nueva dirección en el cuerpo del correo electrónico para que se la comuniquemos al transportista designado.

> **Note**
>
> En Japón, la empresa de transporte cobra una tasa de envío de 120,00 $. En la descripción de la tasa se indica Snowball, pero la tasa se aplica al envío de todos los dispositivos Snow Family.

AWS Snowball recepción y devolución en Dubái (Emiratos Árabes Unidos)

Estas son algunas pautas que debe seguir a la hora de recibir o devolver un dispositivo AWS Snowball Edge en Dubái.

Recepción de un dispositivo Snowball Edge

Si va a recibir un dispositivo Snowball Edge en una zona franca, cuando UPS le notifique que el paquete está listo para su entrega, debe solicitar, obtener y compartir el pase de entrada para su zona franca.

Si se encuentra en una zona franca o en territorio continental, firme el comprobante de entrega (POD) cuando reciba el dispositivo.

Devolución de un dispositivo Snowball Edge

Si va a devolver un dispositivo Snowball Edge, programe una recogida con UPS directamente en el 600 544 743 o a través del sitio web de UPS. Asegúrese de que la información de envío de la devolución aparezca en la pantalla de tinta electrónica antes de la recogida del dispositivo. Consulte Devolución del dispositivo Snowball Edge. Si se trata de una zona franca, cuando se te notifique que se le ha asignado un conductor de UPS para recoger el dispositivo, debe solicitar, obtener y compartir el pase de entrada para la zona franca.

La etiqueta de envío a portes pagados de UPS que aparece en la pantalla de tinta electrónica contiene la dirección correcta a la que se devolver el dispositivo Snowball.

El dispositivo Snowball Edge se entrega a una instalación de AWS clasificación y se envía al centro de AWS datos. UPS le proporcionará automáticamente el número de seguimiento del trabajo.

> **Important**
>
> A menos que se indique lo contrario personalmente AWS, nunca coloque una etiqueta de envío independiente en el dispositivo Snowball Edge. Utilice siempre la etiqueta de envío que se muestra en la pantalla de tinta electrónica del dispositivo.

Los servicios de UPS para los productos Snow Family son nacionales únicamente dentro de un país.

Velocidades de envío

En cada país, las velocidades de envío disponibles varían. Estos plazos de envío se basan en el país al que envíes el dispositivo. AWS Snowball Edge Las velocidades de envío son las siguientes:

- Australia, Japón, Singapur, Indonesia y Corea del Sur: al realizar envíos dentro de estos países, tiene acceso a la velocidad de envío estándar de 1 a 3 días.
- Brasil: para los envíos dentro de Brasil, tiene a su disposición el envío UPS Domestic Express Saver, con entrega al cabo de dos días laborables en horario comercial. La velocidad de envío puede verse afectada por retrasos fronterizos interestatales.
- Unión Europea (UE): cuando se realizan envíos a cualquier país de la UE, es posible utilizar la modalidad urgente. Por lo general, AWS Snowball Edge los dispositivos que se envían exprés se entregan en aproximadamente un día. Además, la mayoría de los países de la UE pueden utilizar el envío estándar, que suele tardar menos de una semana, de ida o de vuelta.
- Hong Kong: cuando se realizan envíos dentro de Hong Kong, tiene acceso al envío urgente.
- India: cuando se realizan envíos dentro de la India, los dispositivos Snowball Edge se entregan en un plazo de siete días laborables desde que AWS recibe todos los documentos fiscales relacionados.
- Dubái, Emiratos Árabes Unidos: tiene acceso al envío Courier Express Saver.
- Reino Unido: si realiza envíos dentro del Reino Unido, tiene acceso al envío exprés. Normalmente, los dispositivos Snowball Edge que se envían con la modalidad urgente tardan alrededor de un día en entregarse. Además, puede utilizar el envío estándar, que suele tardar menos de una semana, de ida o de vuelta.
- Estados Unidos de América (EE. UU.) y Canadá: para los envíos en Estados Unidos o Canadá, dispone de opciones de envío en 24 o 48 horas.

Monitorización del estado de la importación

Para supervisar el estado de su trabajo de importación en la consola, inicie sesión Consola de administración de la familia de productos Snow de AWSen el Región de AWS lugar donde se creó el trabajo. Elija en la tabla el trabajo cuyo seguimiento desea realizar, o bien búsquelo utilizando los parámetros que prefiera en la barra de búsqueda situada encima de la tabla. Después de seleccionar el trabajo, aparece información detallada sobre él en la tabla, incluida una barra que muestra su estado en tiempo real.

> **Note**
>
> Si no podemos importar datos a nuestros centros de datos desde el dispositivo Snow debido a algún problema con los permisos de acceso que ha configurado, intentaremos notificárselo y tendrá 30 días a partir de la fecha en que le enviemos la notificación para resolver el problema. Si el problema no se resuelve, podemos cancelar tu AWS Snow Family trabajo y eliminar los datos del dispositivo.

Cuando el dispositivo llegue a su AWS destino, el estado de su trabajo cambiará de En tránsito AWS a En espera AWS. Por término medio, se tarda un día en iniciar la importación de los datos a Amazon S3. Cuando esta comienza, el estado del trabajo cambia a Importando. Se tardará aproximadamente el mismo tiempo en importar AWS los datos del dispositivo de la familia Snow que en moverlos al dispositivo de la familia Snow. Una vez importados los datos, el estado del trabajo cambia al estado Completado.

Ahora ha completado su primer trabajo de importación de datos a Amazon S3 con AWS Snowball Amazon S3. En la consola, puede obtener un informe sobre la transferencia de los datos. Para abrir este informe en la consola, seleccione el trabajo en la tabla y expándalo para mostrar la información detallada. Elija Obtener informe para descargar el informe de finalización del trabajo en un archivo PDF. Para obtener más información, consulte Obtener el informe y los registros de finalización del trabajo.

Siguiente: Obtener el informe y los registros de finalización del trabajo

Obtener el informe y los registros de finalización del trabajo

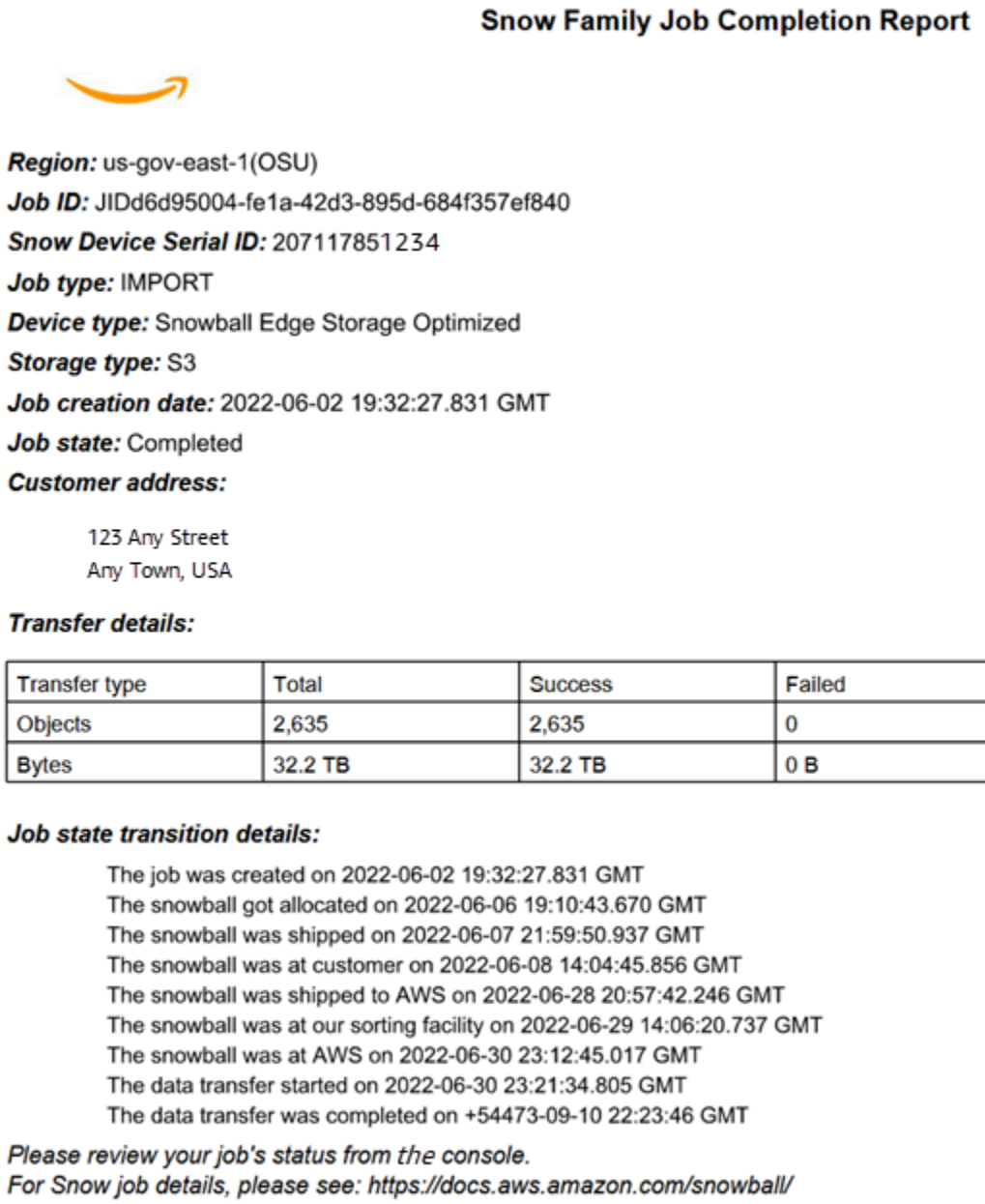
Cuando utiliza un dispositivo de la familia Snow para importar o exportar datos desde Amazon S3, obtiene un informe de trabajo en PDF descargable. Para los trabajos de importación, este informe

está disponible cuando finaliza el proceso de importación. En el caso de los trabajos de exportación, el informe de trabajo suele estar disponible mientras se le entrega el AWS Snowball Edge dispositivo correspondiente a la parte del trabajo. Los informes de finalización de trabajos no están disponibles solo para trabajos de computación y almacenamiento locales.

El informe del trabajo proporciona información sobre el estado de la transferencia de datos de Amazon S3. El informe incluye información acerca del trabajo o de la parte del trabajo para sus registros. El informe del trabajo también incluye una tabla con información general sobre el número total de objetos y bytes transferidos entre el dispositivo y Amazon S3.

Para obtener más información sobre el estado de los objetos transferidos, puede consultar los dos registros asociados: un registro de éxito y otro de errores. Los registros se guardan en formato de valores separados por comas (CSV); el nombre de cada registro incluye el ID del trabajo o la parte del trabajo que se describe en ese registro.

Puede descargar el informe y los registros desde la Consola de administración de la familia de productos Snow de AWS. A continuación se muestra un informe de ejemplo.



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/

Obtención del informe y los registros del trabajo

1. Inicie sesión en AWS Management Console y abra el Consola de administración de la familia de productos Snow de AWS.
2. Seleccione el trabajo o la parte del trabajo en la tabla y expanda el panel de estado.

Aparecen tres opciones para obtener el informe y los registros del trabajo: Get job report, Descargar registro de éxito y Descargar registro de errores.

3. Elija el registro que desea descargar.

En la siguiente lista se describen los valores posibles para el informe:

- Completado: la transferencia se ha completado correctamente. Encontrará más información detallada en el registro de éxito.
- Completado con errores: algunos o todos los datos no se han transferido. Encontrará más información detallada en el registro de errores.

Siguiente: Uso de un dispositivo AWS Snowball Edge

Migración de datos de gran tamaño con AWS Snow Family devices

La migración de datos de gran tamaño desde ubicaciones en las instalaciones requiere una planeación, una orquestación y una ejecución cuidadosas para garantizar que los datos se migren correctamente a AWS.

Le recomendamos que cuente con una estrategia de migración de datos antes de iniciar la migración para evitar la posibilidad de que se incumplan los plazos, se superen los presupuestos y se produzcan errores en la migración. AWS Los servicios de Snow le ayudan a organizar, ordenar y realizar un seguimiento de sus proyectos de migración de datos de gran tamaño mediante la función de gestión de migración de datos de gran tamaño (LDMM) de la Consola de administración de la familia de productos Snow de AWS familia Snow.

En los temas Planificación de transferencias grandes y Calibración de una transferencia grande se describe un proceso manual de migración de datos. Puede simplificar los pasos manuales mediante el plan de migración de LDMM de Snow Family.

Temas

Planificación de transferencias grandes

Le recomendamos que planifique y calibre las grandes transferencias de datos entre los dispositivos AWS Snowball Edge que tiene in situ y sus servidores según las instrucciones que se indican en las próximas secciones.

Temas

Paso 1: analice los datos que va a trasladar a la nube

Antes de crear su primer trabajo con el Consola de administración de la familia de productos Snow de AWS, asegúrese de evaluar el volumen de datos que necesita transferir, dónde están almacenados actualmente y el destino al que desea transferirlos. En las transferencias de datos a escala de uno o varios petabytes, estas tareas administrativas serán mucho más sencillas cuando reciba los dispositivos Snow Family.

Si va a migrar datos al Nube de AWS por primera vez, le recomendamos que diseñe un modelo de migración a la nube. La migración a la nube no se produce de la noche a la mañana. Requiere un proceso de planificación cuidadoso para garantizar que todos los sistemas funcionen según lo esperado.

Cuando haya terminado este paso, debería saber la cantidad total de datos que va a mover a la nube.

Paso 2: calcule la velocidad de transferencia objetivo

Es importante calcular la rapidez con la que puede transferir datos a los dispositivos Snow Family conectados a cada uno de los servidores. Esta velocidad estimada en MB/s determina la rapidez con la que puede transferir los datos desde su origen de datos a los dispositivos Snowball Edge mediante la infraestructura de red local.

> **Note**
>
> Para las transferencias de datos de gran tamaño, le recomendamos que utilice Amazon S3. Debe seleccionar esta opción cuando pida los dispositivos en la Consola de administración de la familia de productos Snow de AWS.

Para determinar una velocidad de transferencia de referencia, transfiera un pequeño subconjunto de los datos al dispositivo Snowball Edge o transfiera un archivo de muestra de 10 GB y observe el rendimiento.

A la hora de determinar la velocidad de transferencia objetivo, tenga en cuenta que es posible mejorar el rendimiento ajustando el entorno, incluida la configuración de red, cambiando aspectos como la velocidad de la red, el tamaño de los archivos que se van a transferir y la velocidad de

lectura de datos en los servidores locales. El adaptador de Amazon S3 copia los datos a los dispositivos Snow Family tan rápido como lo permiten las condiciones existentes.

Paso 3: determine cuántos dispositivos Snow Family se necesitan

Determine cuántos dispositivos de la familia Snow necesita para la migración de datos a gran escala utilizando la cantidad total de datos que planea trasladar a la nube AWS, la velocidad de transferencia estimada y el número de días a los que desea transferir los datos. Según el tipo de dispositivo, los dispositivos Snowball Edge tienen aproximadamente 39,5 TB, 80 TB o 210 TB de espacio de almacenamiento utilizable. Por ejemplo, si quiere transferir 300 TB de datos a AWS más de 10 días y tiene una velocidad de transferencia de 250 MB/s, necesitará 4 dispositivos Snowball Edge. Si quedan menos de 40 TB de datos por transferir, se recomendarán AWS Snowcone dispositivos (con 14 TB de espacio útil).

> **Note**
>
> El AWS Snow Family devices LDMM incluye un asistente para estimar el número de dispositivos AWS Snow Family devices que se pueden admitir simultáneamente. Para obtener más información, consulte Creación de un plan de migración de datos de gran tamaño.

Paso 4: cree los trabajos

Una vez que sepa cuántos dispositivos Snow Family necesita, debe crear un trabajo de importación para cada dispositivo. La característica LDMM de Snow Family simplifica la creación de varios trabajos. Para obtener más información, consulte Pedido del siguiente trabajo.

> **Note**
>
> Puede realizar el siguiente pedido de trabajo y añadirlo de forma automática al plan directamente desde el Programa recomendado de pedido de trabajos. Para obtener más información, consulte Programa recomendado de pedido de trabajos.

Paso 5: separe los datos en segmentos de transferencia

Como práctica recomendada para las transferencias de datos de gran tamaño que afectan a varios trabajos, se recomienda dividir lógicamente los datos en conjuntos de datos más pequeños y más

manejables. Esto le permite transferir cada partición de una en una o varias particiones en paralelo. Al planificar las particiones, asegúrese de que los datos de las particiones combinadas quepan en los dispositivos Snow Family para el trabajo. Por ejemplo, puede separar la transferencia en particiones de cualquiera de las siguientes maneras:

- Puede crear 10 particiones de 8 TB cada una para un dispositivo Snowball Edge.
- En el caso de los archivos de gran tamaño, cada archivo puede ser una partición individual hasta el límite de tamaño de 5 TB de los objetos en Amazon S3.
- Cada partición puede tener tamaños distintos y cada partición individual puede estar formada por datos del mismo tipo (por ejemplo, los archivos pequeños en una partición, los comprimidos en otra, los archivos grandes en otra, etc.). Este enfoque le ayuda a determinar su velocidad de transferencia media para distintos tipos de archivos.

> **Note**
>
> En cada uno de los archivos transferidos se realizan operaciones de metadatos. La sobrecarga es la misma, independientemente del tamaño de los archivos. Por lo tanto, el desempeño será más rápido al comprimir archivos pequeños en una agrupación de mayor tamaño, agrupar los archivos por lotes o transferir archivos individuales más grandes.

La creación de estos segmentos de transferencia de datos puede facilitar la resolución de los problemas de transferencia, ya que intentar solucionar los problemas de una transferencia heterogénea de gran tamaño después haberse ejecutado durante un día o más puede resultar complejo.

Cuando haya terminado de planificar la transferencia de datos a escala de petabytes, se recomienda transferir algunos segmentos al dispositivo Snow Family desde el servidor para calibrar la velocidad y el tiempo de transferencia total.

Calibración de una transferencia grande

Puede calibrar el rendimiento de la transferencia transfiriendo un conjunto representativo de sus particiones de datos. Elija varias particiones que haya definido y transfiéralas a un dispositivo Snow Family. Lleve un registro de la velocidad de transferencia y del tiempo de transferencia total de cada operación. Si los resultados de la calibración son inferiores a la velocidad de transferencia objetivo,

podrá copiar varias partes de la transferencia de datos en paralelo a la vez. En este caso, repita la calibración con las particiones adicionales del conjunto de datos.

Siga agregando otras operaciones de copia paralelas durante la calibración hasta que observe una disminución en la suma de la velocidad de transferencia de todas las instancias que están transfiriendo datos en ese momento. Finalice la última instancia activa y anote la nueva velocidad de transferencia objetivo.

Puede transferir datos más rápido a los dispositivos Snow Family si transfiere datos en paralelo mediante uno de los siguientes escenarios:

- Usando varias sesiones del adaptador de S3 en una estación de trabajo en un único dispositivo Snow Family.
- Usando varias sesiones del adaptador de S3 en varias estaciones de trabajo en un único dispositivo Snow Family.
- Usando varias sesiones de la interfaz de S3 (utilizando una o varias estaciones de trabajo) en varios dispositivos Snow Family.

Cuando complete estos pasos, sabrá la rapidez con la que puede transferir datos a un dispositivo Snow Family.

Creación de un plan de migración de datos de gran tamaño

La función de plan de migración de datos de AWS Snow Family gran tamaño le permite planificar, realizar el seguimiento, supervisar y gestionar grandes migraciones de datos de 500 TB a varios petabytes mediante varios productos de servicio de la familia Snow.

Utilice la función de plan de migración de datos de gran tamaño para recopilar información sobre los objetivos de migración de datos, como el tamaño de los datos a los que se van a transferir AWS y la cantidad de dispositivos de la familia Snow necesarios para migrar los datos simultáneamente. Utilice el plan para crear un programa previsto para el proyecto de migración de datos y el programa recomendado de pedido de trabajos a fin de cumplir sus objetivos.

> **Note**
>
> Actualmente, el plan de migración de datos está disponible para trabajos de importación de más de 500 TB.

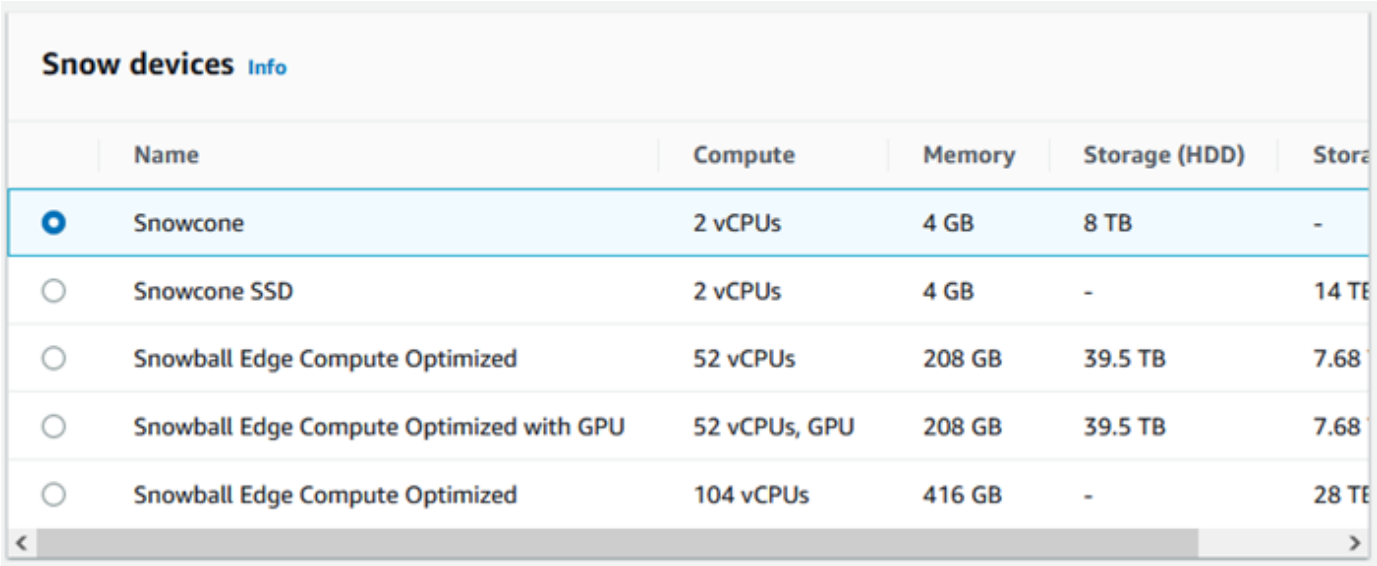
Temas

Paso 1: elija los detalles de la migración

> **Note**
>
> Hay disponible un plan de migración de datos de gran tamaño para las migraciones de datos de más de 500 TB. Cree pedidos de trabajo individualmente en dispositivos Snow Family para sus proyectos de transferencia de datos de menos de 500 TB. Para obtener más información, consulte Crear una tarea para solicitar un dispositivo de la familia Snow en esta guía.

1. Inicie sesión en la Consola de administración de la familia de productos Snow de AWS. Si es la primera vez que Consola de administración de la familia de productos Snow de AWS lo utilizas Región de AWS, verás la AWS Snow Family página. De lo contrario, verá la lista de trabajos existentes.
2. Si este es su primer plan de migración de datos, elija Crear nuevo plan de migración de datos grande en la página principal. De lo contrario, elija Planes de migración de datos grandes. Seleccione Crear plan de migración de datos para abrir el asistente de creación de planes.
3. En Asignar un nombre al plan de migración de datos, proporcione un Nombre del plan de migración de datos. El nombre del plan puede tener un máximo de 64 caracteres. Los caracteres válidos son A-Z, a-z, 0-9 y . - (guion). El nombre de un plan no debe empezar por **`aws:`**.
4. En Total de datos a migrar AWS, introduce la cantidad de datos a la que deseas migrar AWS.
5. En Dispositivos Snow, elija un dispositivo Snow Family.

   > **Note**
   >
   > Las opciones de dispositivo compatibles pueden variar según la disponibilidad de los dispositivos en algunas Regiones de AWS.



6. En Dispositivos simultáneos, introduzca el número de dispositivos Snow Family a los que puede copiar datos simultáneamente en su ubicación. Si no lo sabe con seguridad, pase a la siguiente sección para obtener información sobre cómo utilizar el asistente de estimación de dispositivos simultáneos para determinarlo.
7. Elija Siguiente.

Uso del asistente de estimación de dispositivos simultáneos

El asistente de estimación de dispositivos simultáneos le ayuda a determinar el número de dispositivos simultáneos que puede utilizar durante las migraciones de datos de gran tamaño.

Requisitos previos:

- Haber realizado una prueba de concepto para probar su metodología de transferencia de datos y haber medido el rendimiento con un dispositivo Snow Family en su entorno.
- Conocer la red y la conexión al almacenamiento de back-end.

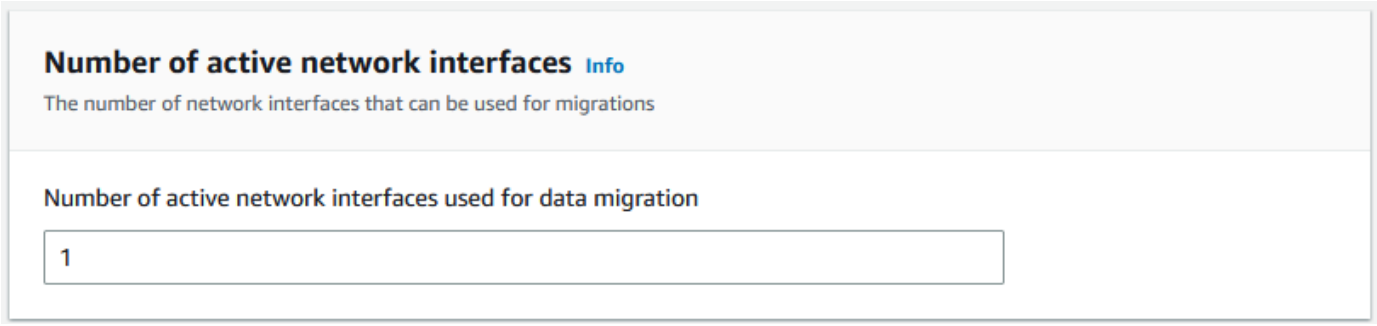
Paso 1: introduzca la información del origen de datos

En primer lugar, determine el rendimiento teórico máximo para copiar datos desde el origen de almacenamiento.

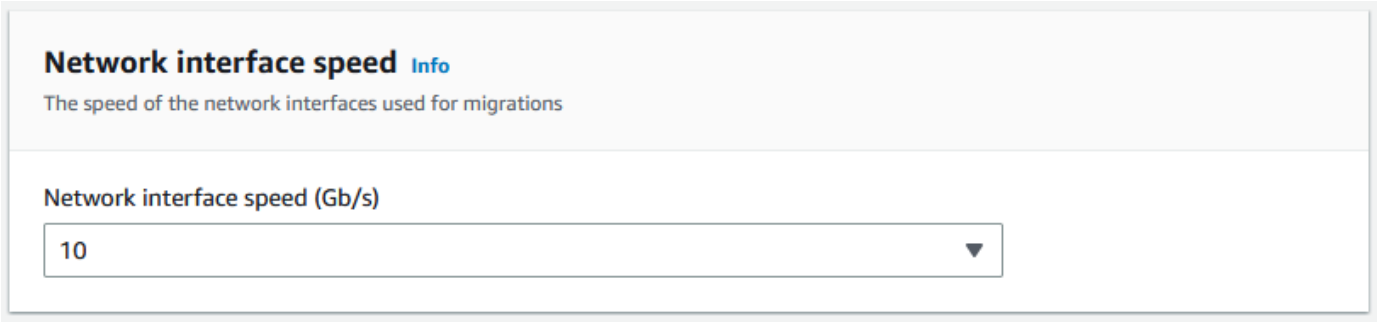
1. En Datos totales por migrar, introduzca la cantidad de datos que piensa migrar.

En Unidad, elija la unidad de medida (GB o TB) de la cantidad de datos que va a migrar.

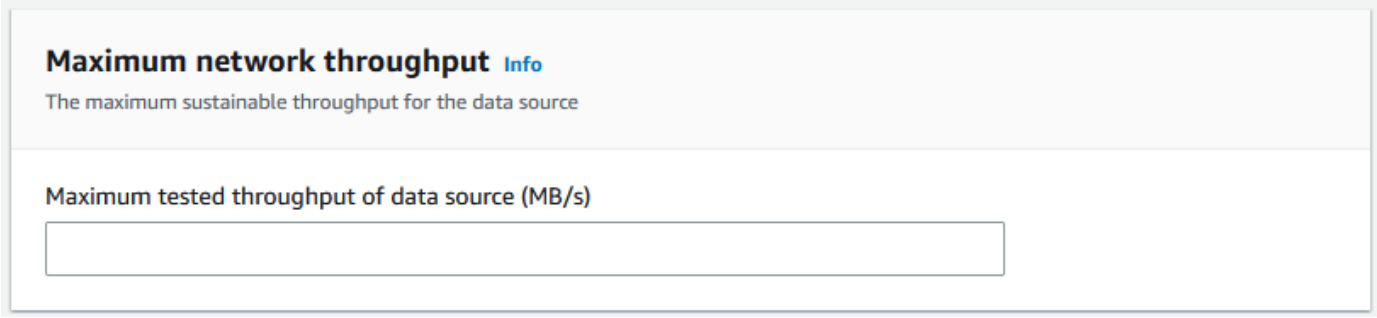
2. En Número de interfaces de red activas, indique el número de interfaces de red activas que tiene disponibles para la migración de datos desde el origen de almacenamiento.



3. En Velocidad de la interfaz de red, elija la velocidad de la interfaz de red para el origen de almacenamiento. Las velocidades de red se indican en Gb/s.



4. En Rendimiento máximo de red, introduzca el rendimiento máximo de red probado para su origen de almacenamiento que determinó durante la prueba de concepto. El rendimiento se indica en MB/s.

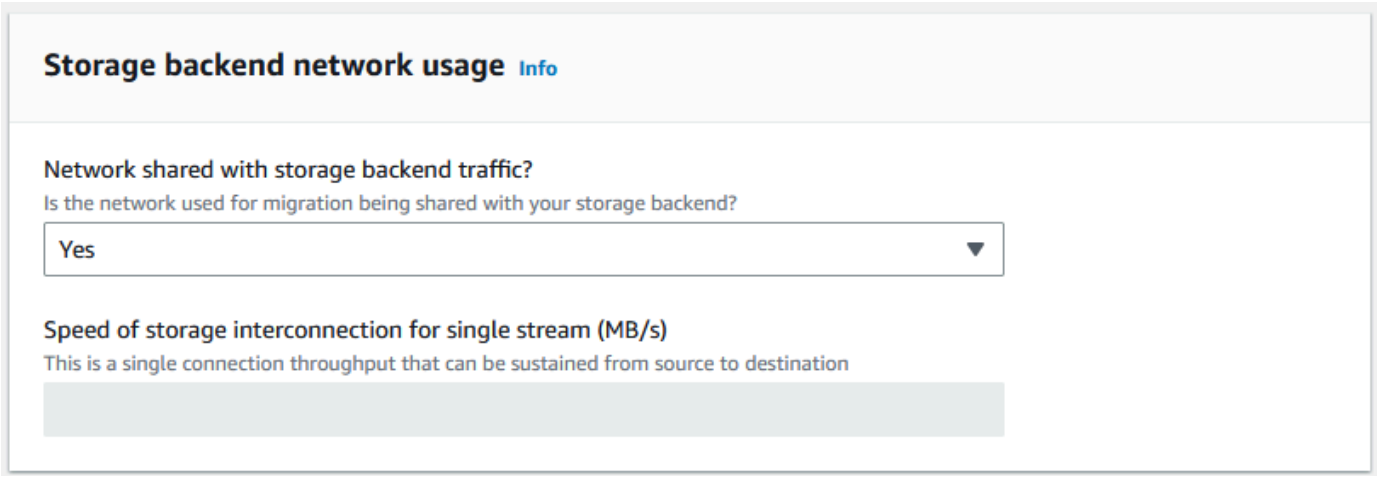


5. En Uso de la red backend de almacenamiento, indique si el origen de almacenamiento comparte una red con el almacenamiento de back-end.

   - Seleccione Sí si la red no se comparte. No es necesario que introduzca la velocidad de la interconexión de almacenamiento para un solo flujo.

- Elija No si la red se comparte. Introduzca la velocidad de interconexión de almacenamiento para un solo flujo en MB/s.

Según la opción que haya elegido, el asistente actualiza el valor de Rendimiento máximo de migración para el origen de datos (MB/s) que aparece en la parte inferior de la página.



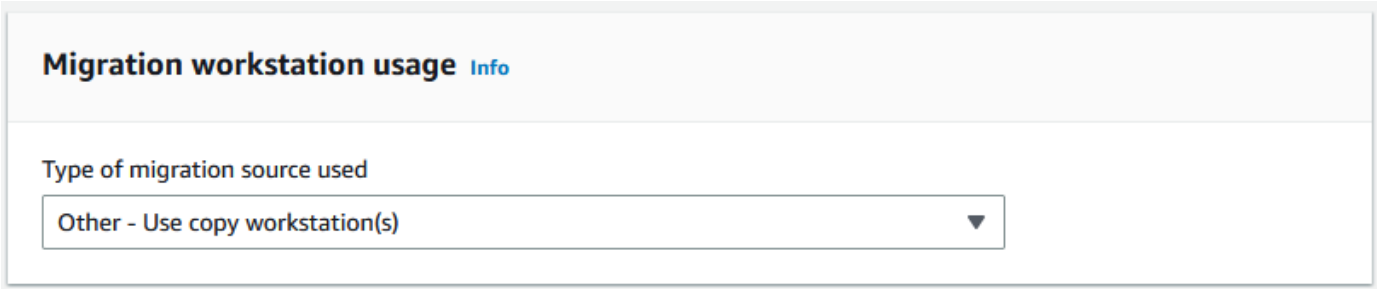
6. Elija Siguiente.

Paso 2: introduzca los parámetros de las estaciones de trabajo que usará para la migración

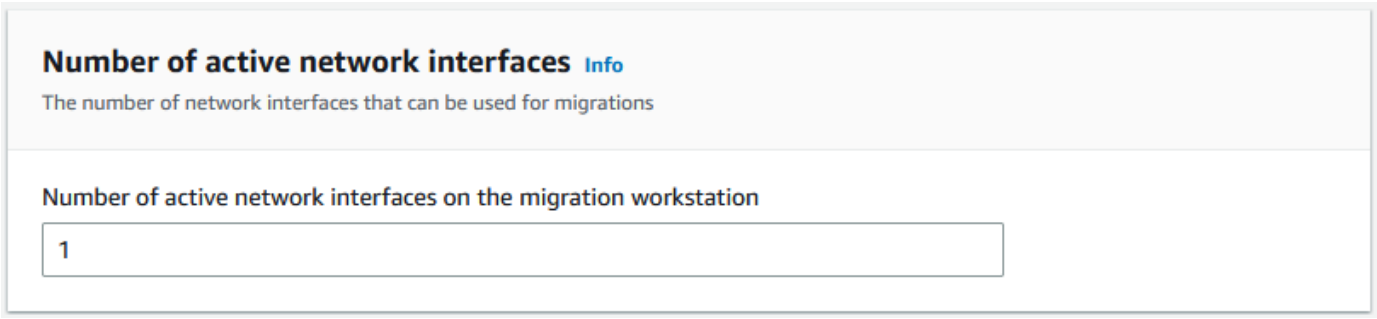
Puede conectar sus dispositivos Snow Family directamente a su origen de almacenamiento (un servidor Microsoft Windows, por ejemplo). En su lugar, puede optar por conectar los dispositivos Snow Family a una o más estaciones de trabajo para copiar los datos desde el origen de almacenamiento.

1. En Uso del puesto de trabajo de migración, indique la opción de uso de la estación de trabajo que prefiera.

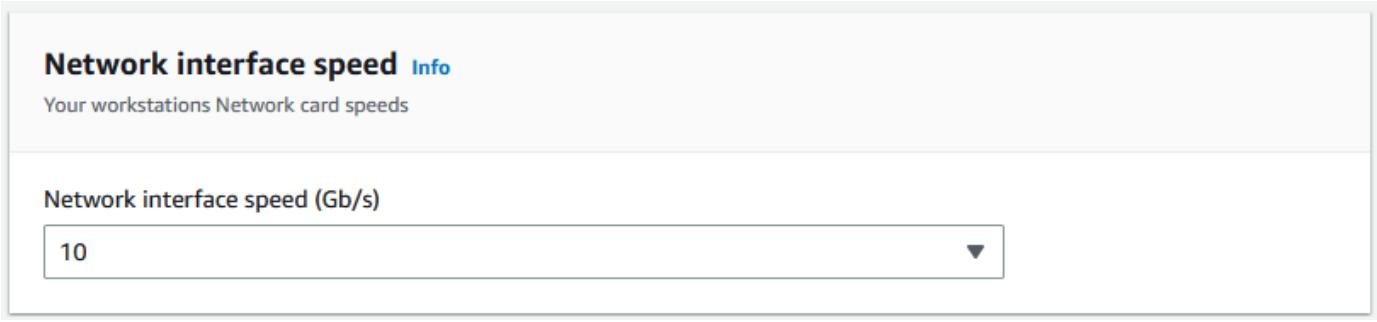
   - Elija Ninguno: utilice directamente el origen de datos para transferir datos directamente desde un origen de datos sin utilizar una estación de trabajo y, a continuación, seleccione Siguiente.
   - Elija Otro: utilice estaciones de trabajo de copia para utilizar una o más estaciones de trabajo para transferir datos.



2. En Número de interfaces de red activas, introduzca el número de puertos que se van a utilizar para la migración de datos.

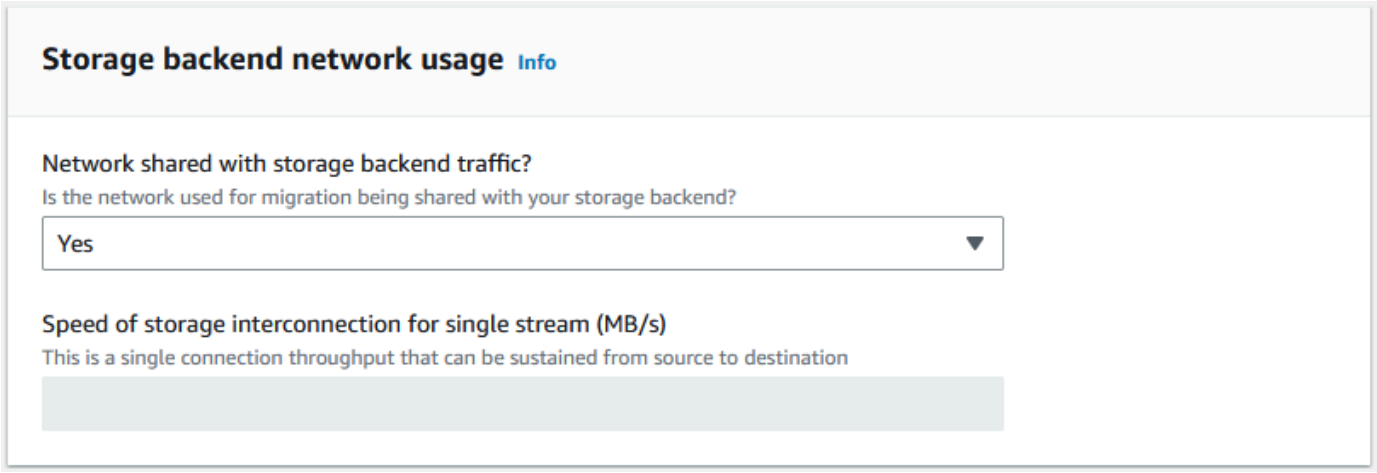


3. En Velocidad de las interfaces de red, elija la velocidad en Gb/s de las interfaces de red.

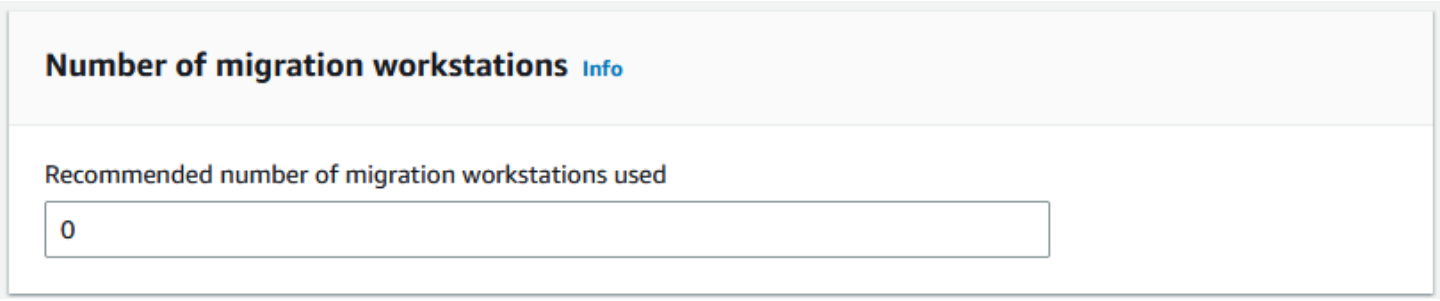


4. En Uso de la red backend de almacenamiento, indique si la red en la que se encuentran las estaciones de trabajo se comparte con el almacenamiento de back-end.

   - Seleccione Sí si se comparte.
   - Seleccione No si no se comparte. Introduzca la velocidad de interconexión de almacenamiento para un solo flujo en MB/s.

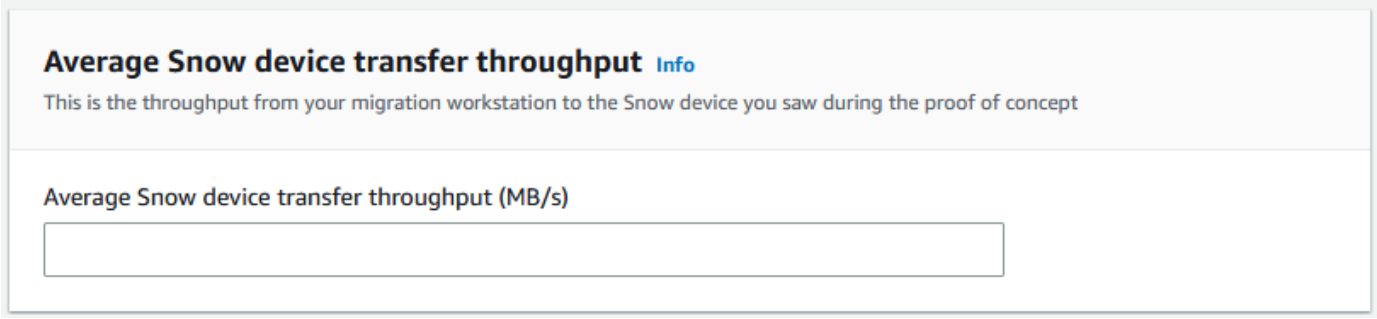


En función de sus datos, el asistente muestra una recomendación en Número de estaciones de trabajo de migración. Puede cambiar el número manualmente si no está de acuerdo con la recomendación. Este número aparecerá en Dispositivos simultáneos en el plan de migración de datos de gran tamaño.



Paso 3: introduzca el rendimiento medio de transferencia de los dispositivos Snow Family

1. En el campo Rendimiento medio de transferencia del dispositivo Snow, introduzca el rendimiento de transferencia en MB/s que vio durante la prueba de concepto.



En función del rendimiento medio, el asistente actualiza los valores de Cantidad recomendada de dispositivos Snow simultáneos y Cantidad máxima de dispositivos simultáneos en los detalles del plan de migración.

2. Elija Utilice este número para continuar y volver a elegir los detalles de la migración. Seleccione Siguiente y continúe con el siguiente paso (Paso 2: elija sus preferencias de envío, seguridad y notificación).

> **Note**
>
> Puede utilizar hasta 5 dispositivos Snow simultáneos.

Paso 2: elija sus preferencias de envío, seguridad y notificación

1. En la sección Dirección de envío, seleccione una dirección existente o cree una nueva.

   - > **Note**
     >
     > El país de la dirección debe coincidir con el país de destino del dispositivo y debe ser válido para ese país.

2. En Elegir el tipo de acceso al servicio, realice una de las siguientes acciones:

   - Permita que Snow Family cree un nuevo rol vinculado a un servicio para usted con todos los permisos necesarios para publicar CloudWatch métricas y notificaciones de Amazon SNS para sus trabajos de Snow Family.
   - Agregue un rol de servicio existente que tenga los permisos necesarios. Para ver un ejemplo de cómo configurar este rol, consulte Ejemplo 4: Permisos de rol esperados y política de confianza.

3. En Enviar notificaciones, elija si desea enviar notificaciones. Tenga en cuenta que si elige No enviar notificaciones sobre los planes de migración de datos no recibirá notificaciones de este plan, pero sí recibirá notificaciones de trabajos.
4. Para Establecer notificaciones,

   - elija Usar un tema de SNS existente
   - o Crear un nuevo tema de SNS.

Paso 3: revise y cree el plan

1. Revise la información de Detalles del plan y de las preferencias de envío, seguridad y notificación y modifíquela si es necesario.
2. Seleccione Crear plan de migración de datos para crear el plan.

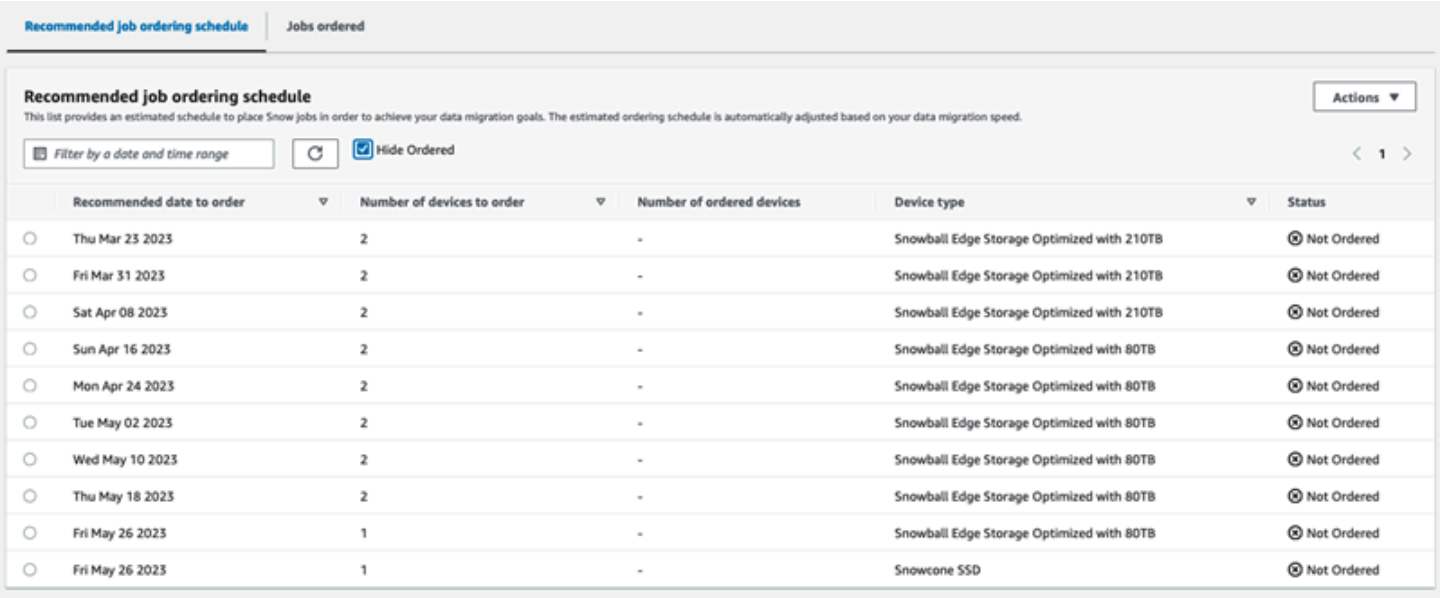
Uso del plan de migración de datos de gran tamaño

Tras crear el plan de migración de datos de gran tamaño, puede utilizar el programa y el panel resultantes como guía durante el resto del proceso de migración.

Programa recomendado de pedido de trabajos

Después de crear un plan de migración AWS Snow Family devices amplio, puede usar el programa de pedido de trabajos recomendado para crear nuevos trabajos.

> **Note**
>
> Las actualizaciones manuales que realice en el tamaño de los datos o en la cantidad de dispositivos simultáneos hacen que el programa se ajuste. El programa se ajusta automáticamente si un trabajo no se ha pedido antes de la fecha de pedido recomendada o si se ha pedido antes de la fecha de pedido recomendada. Si un trabajo se devuelve antes de la fecha de pedido recomendada, el programa se ajusta automáticamente.



Pedido del siguiente trabajo

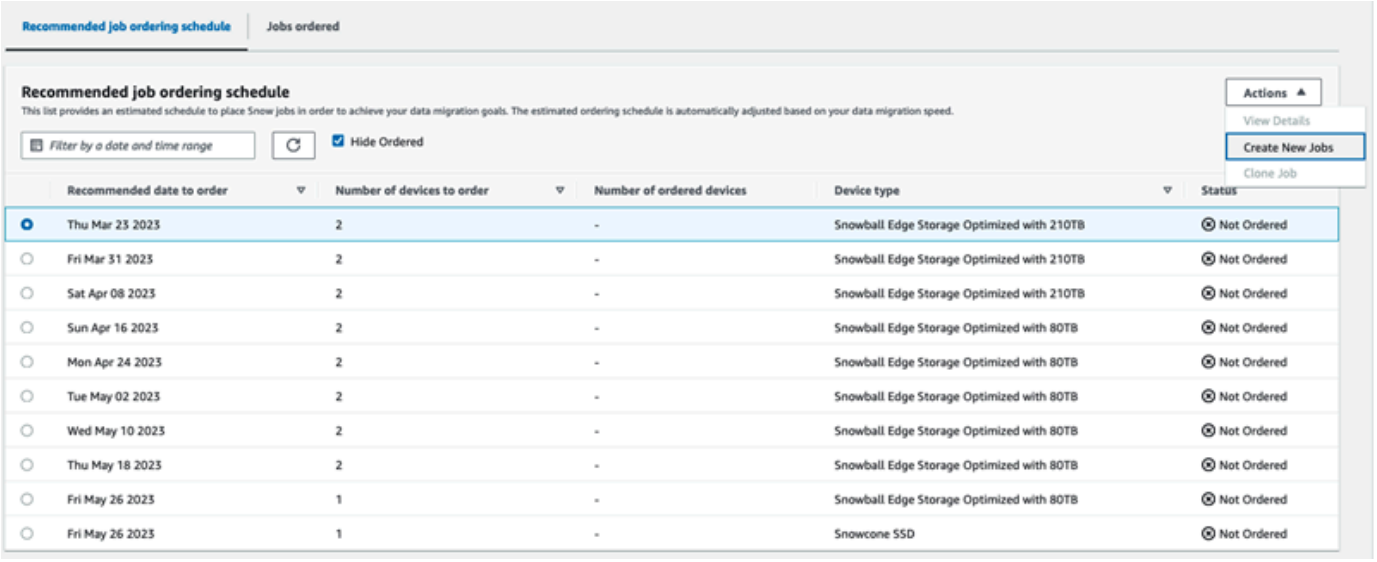
Para realizar el siguiente pedido, en lugar de crear manualmente un trabajo y añadirlo al plan, tiene la opción de clonar un trabajo que haya pedido anteriormente o crear uno rellenado previamente.

Clonación de un trabajo:

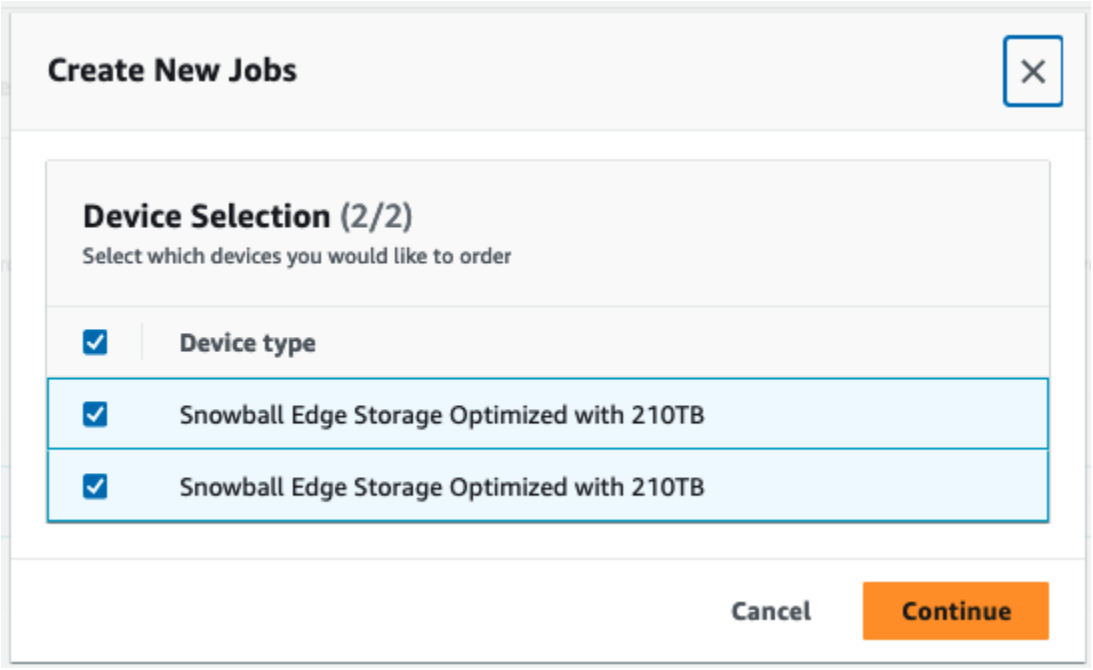
1. Elija el siguiente pedido (la primera recomendación que tiene el estado No pedido) del Programa recomendado de pedido de trabajos y, a continuación, seleccione Clonar trabajo en el menú Acciones. Aparece la ventana Clonar trabajo.
2. En la ventana Clonar trabajo, en la sección Trabajos pedidos, elija el trabajo que desea clonar.
3. En la sección Información de los nuevos trabajos, elija los dispositivos que desea pedir. Para cada dispositivo elegido, el Nombre del trabajo se rellenará automáticamente en función del trabajo elegido. Puede sobrescribir el nombre del trabajo.
4. Seleccione Confirmar para realizar el pedido de trabajos para los dispositivos elegidos. El sistema clona el trabajo para cada dispositivo.

Creación de nuevos trabajos:

1. Elija el siguiente pedido (la primera recomendación que tiene el estado No pedido) del Programa recomendado de pedido de trabajos y, a continuación, seleccione Crear nuevos trabajos en el menú Acciones. Aparece la ventana Crear nuevos trabajos.



2. En la sección Selección de dispositivos, elija los dispositivos que desea pedir. Elija Continuar.



3. Aparece la página Crear nuevo. La mayoría de los parámetros, como el tipo de trabajo, la dirección de envío y el tipo de dispositivo, se configuran en función del plan. El sistema crea el trabajo para cada dispositivo.

Puede ver si el trabajo o los trabajos se crearon correctamente o no. Los trabajos creados correctamente se añaden automáticamente al plan.

Lista de trabajos pedidos

Cada plan muestra una lista de trabajos pedidos. Al principio está vacío. Cuando empiece a pedir trabajos, podrá añadir trabajos al plan si selecciona Agregar trabajo en el menú Acciones. En el panel de supervisión se hace seguimiento de los trabajos que agregue aquí.

Del mismo modo, puede eliminar el trabajo de la lista de trabajos pedidos seleccionando Eliminar trabajo en el menú Acciones.

Le recomendamos que utilice el programa de pedido de trabajos que se proporciona en el plan para llevar a cabo una migración de datos fluida.

Panel de supervisión

Después de añadir los trabajos a su plan, podrá ver las métricas en el panel de control a medida que los trabajos vuelvan a AWS incorporarse. Estas métricas pueden ayudarle a realizar un seguimiento del progreso:

- Datos migrados a AWS: la cantidad de datos a los que se ha migrado hasta AWS ahora.
- Promedio de datos migrados por trabajo: cantidad media de datos por trabajo en terabytes.
- Total de trabajos de Snow: el número de trabajos de Snowball Edge pedidos en comparación con los trabajos restantes por pedir.
- Duración promedio de un trabajo de migración: la duración media de un trabajo en días.
- Estado de los trabajos de Snow: el número de trabajos que hay en cada estado.

Uso AWS OpsHub for Snow Family para administrar dispositivos

Los dispositivos de la familia Snow ahora ofrecen una herramienta fácil de usar que puede usar para administrar sus dispositivos y AWS servicios locales. AWS OpsHub for Snow Family Se utiliza AWS OpsHub en un ordenador cliente para realizar tareas como desbloquear y configurar dispositivos individuales o agrupados, transferir archivos y lanzar y gestionar instancias que se ejecutan en los dispositivos de la familia Snow. Se puede utilizar AWS OpsHub para gestionar los tipos de dispositivos Snow optimizados para almacenamiento y optimizados para cómputo. La AWS OpsHub aplicación está disponible sin coste adicional para usted.

AWS OpsHub toma todas las operaciones existentes disponibles en la API de Snowball y las presenta como una interfaz gráfica de usuario. Esta interfaz le ayuda a migrar rápidamente los datos a las aplicaciones de computación periférica Nube de AWS e implementarlas en los dispositivos de la familia Snow.

AWS OpsHub proporciona una visión unificada de los AWS servicios que se ejecutan en los dispositivos de la familia Snow y automatiza las tareas operativas mediante AWS Systems Manager ella. De este AWS OpsHub modo, los usuarios con diferentes niveles de experiencia técnica pueden gestionar una gran cantidad de dispositivos de la familia Snow. Con tan solo unos clics, puede desbloquear dispositivos, transferir archivos, administrar instancias compatibles con Amazon EC2 y monitorizar métricas de dispositivos.

Cuando el dispositivo Snow llegue, descargue, instale y lance la aplicación AWS OpsHub en un equipo cliente, como un portátil. Tras la instalación, puede desbloquear el dispositivo y empezar a gestionarlo y a utilizar AWS los servicios compatibles de forma local. AWS OpsHub proporciona un panel que resume las métricas clave, como la capacidad de almacenamiento y las instancias activas del dispositivo. También proporciona una selección de los servicios de AWS que se admiten en los dispositivos Snow Family. En cuestión de minutos, puede comenzar a transferir archivos al dispositivo.

Temas

- Administración de sus dispositivos
- Automatización de las tareas de administración
- Configuración de los servidores de tiempo NTP del dispositivo

Descarga AWS OpsHub para dispositivos de la familia Snow

Para descargar AWS OpsHub

1. Navegue hasta el sitio web de recursos de AWS Snowball.

2. En la AWS OpsHubsección, elija Descargar para su sistema operativo y siga los pasos de instalación.

Desbloqueo de un dispositivo

Cuando el dispositivo llegue a sus instalaciones, el primer paso consiste en conectarlo y desbloquearlo. AWS OpsHub le permite iniciar sesión, desbloquear y administrar dispositivos mediante los siguientes métodos:

- Localmente: para iniciar sesión en un dispositivo de forma local, debe encender el dispositivo y conectarlo a la red local. A continuación, proporcione un código de desbloqueo y un archivo de manifiesto.

- De forma remota: para iniciar sesión en un dispositivo de forma remota, debe encender el dispositivo y asegurarse de que puede conectarse a *device-order-region*.amazonaws.com a través de la red. A continuación, proporcione las credenciales AWS Identity and Access Management (IAM) (clave de acceso y clave secreta) del dispositivo Cuenta de AWS que está vinculado a su dispositivo.

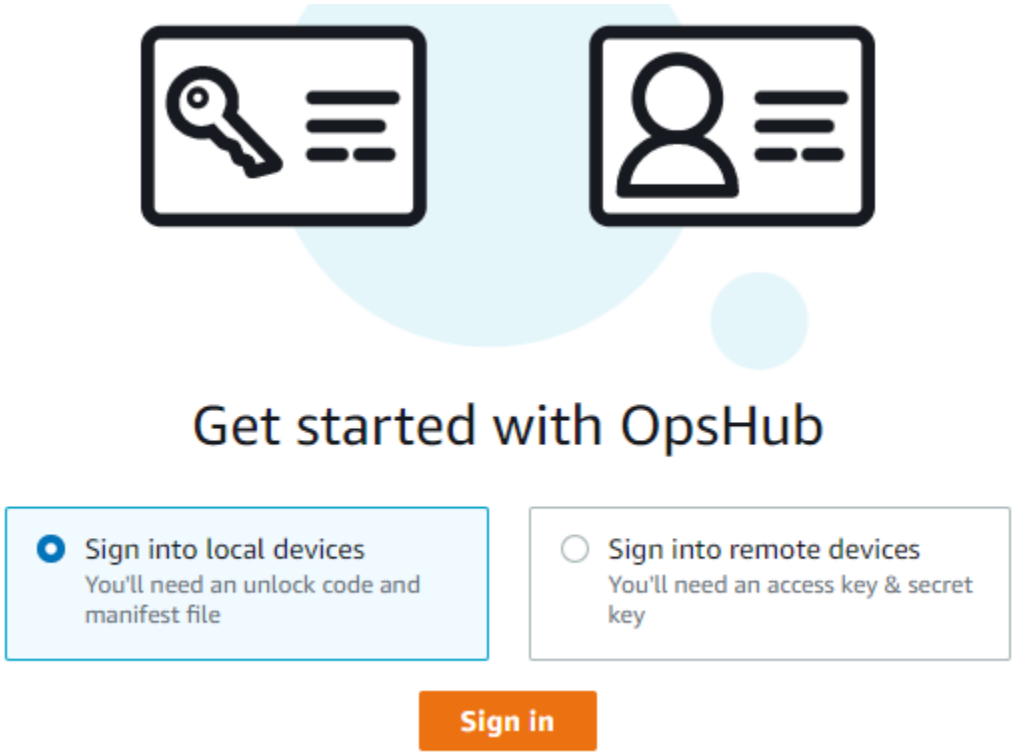
  Para obtener información sobre cómo habilitar la administración remota y crear una cuenta asociada, consulte Activación de Snow Device Management.

Temas

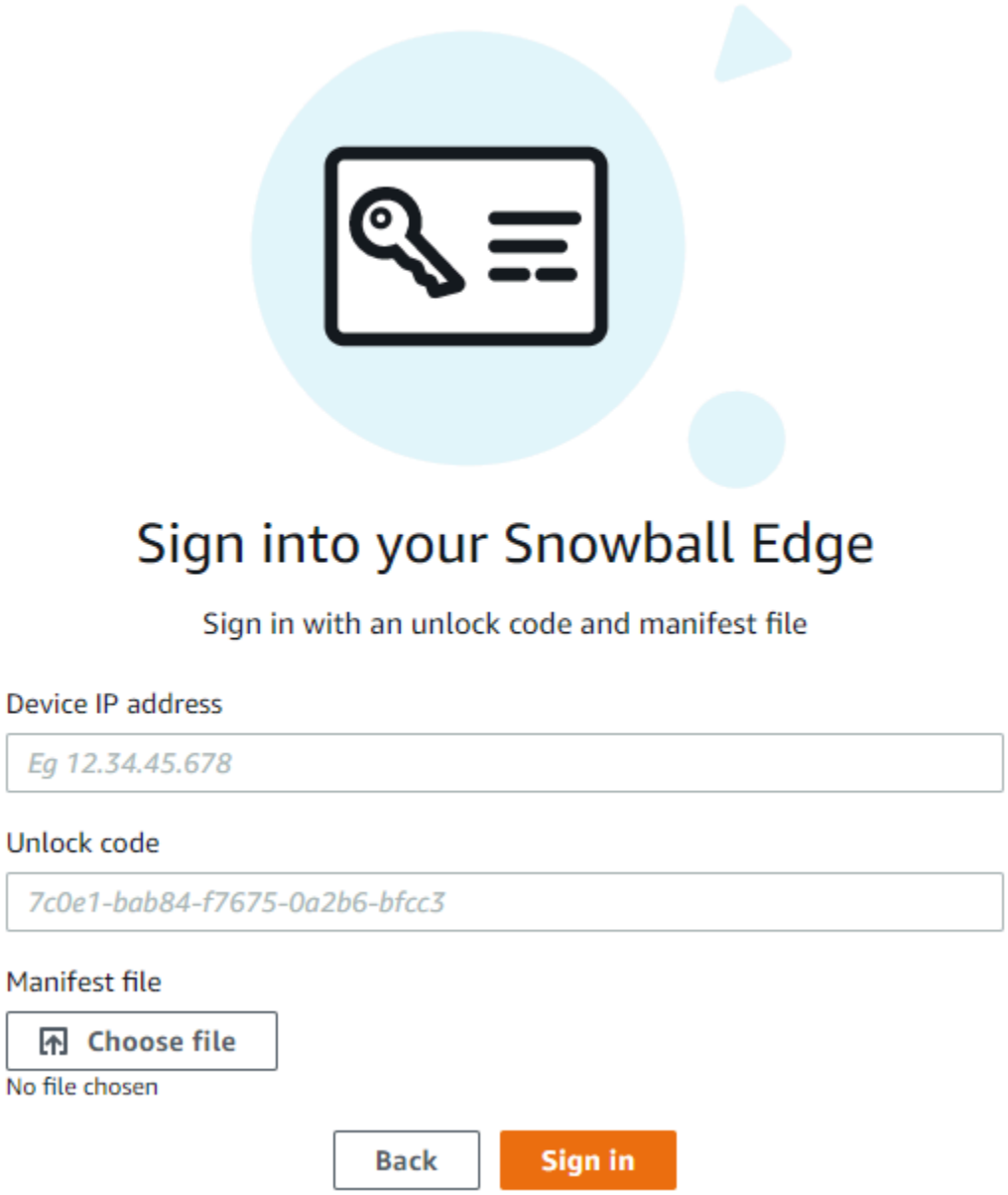
Desbloqueo de un dispositivo de forma local

Para conectar y desbloquear el dispositivo localmente

1. Abra la pestaña del dispositivo, localice el cable de alimentación y conecte el dispositivo a una fuente de alimentación.
2. Conecte el dispositivo a la red mediante un cable de red (normalmente un cable Ethernet RJ45), abra el panel frontal y encienda el dispositivo.
3. Abre la AWS OpsHub aplicación. Si es la primera vez que la utiliza, se le pedirá que seleccione un idioma. A continuación, elija Siguiente.
4. En la OpsHub página Comenzar con, selecciona Iniciar sesión en dispositivos locales y, a continuación, selecciona Iniciar sesión.



5. En la página Iniciar sesión en dispositivos locales, seleccione el tipo de dispositivo Snow Family y, a continuación, elija Iniciar sesión.
6. En la página Iniciar sesión, introduzca la Dirección IP del dispositivo y el Código de desbloqueo. Para seleccionar el manifiesto del dispositivo, seleccione Elegir archivo y, a continuación, elija Iniciar sesión.



7. (Opcional) Puede guardar las credenciales de su dispositivo como un perfil. Asigne un nombre al perfil y seleccione Guardar nombre de perfil. Para obtener más información sobre los perfiles, consulte Administración de perfiles.
8. En la pestaña Dispositivos locales, selecciona un dispositivo para ver sus detalles, como las interfaces de red y AWS los servicios que se ejecutan en el dispositivo. También puedes ver los detalles de los clústeres en esta pestaña o administrar tus dispositivos del mismo modo que lo haces con AWS Command Line Interface (AWS CLI). Para obtener más información, consulte Administrar AWS los servicios en tu dispositivo.

En el caso de los dispositivos que estén AWS Snow Device Management instalados, puedes seleccionar Habilitar la administración remota para activar la función. Para obtener más información, consulte Uso AWS Snow Device Management para administrar dispositivos.

Desbloqueo de un dispositivo de forma remota

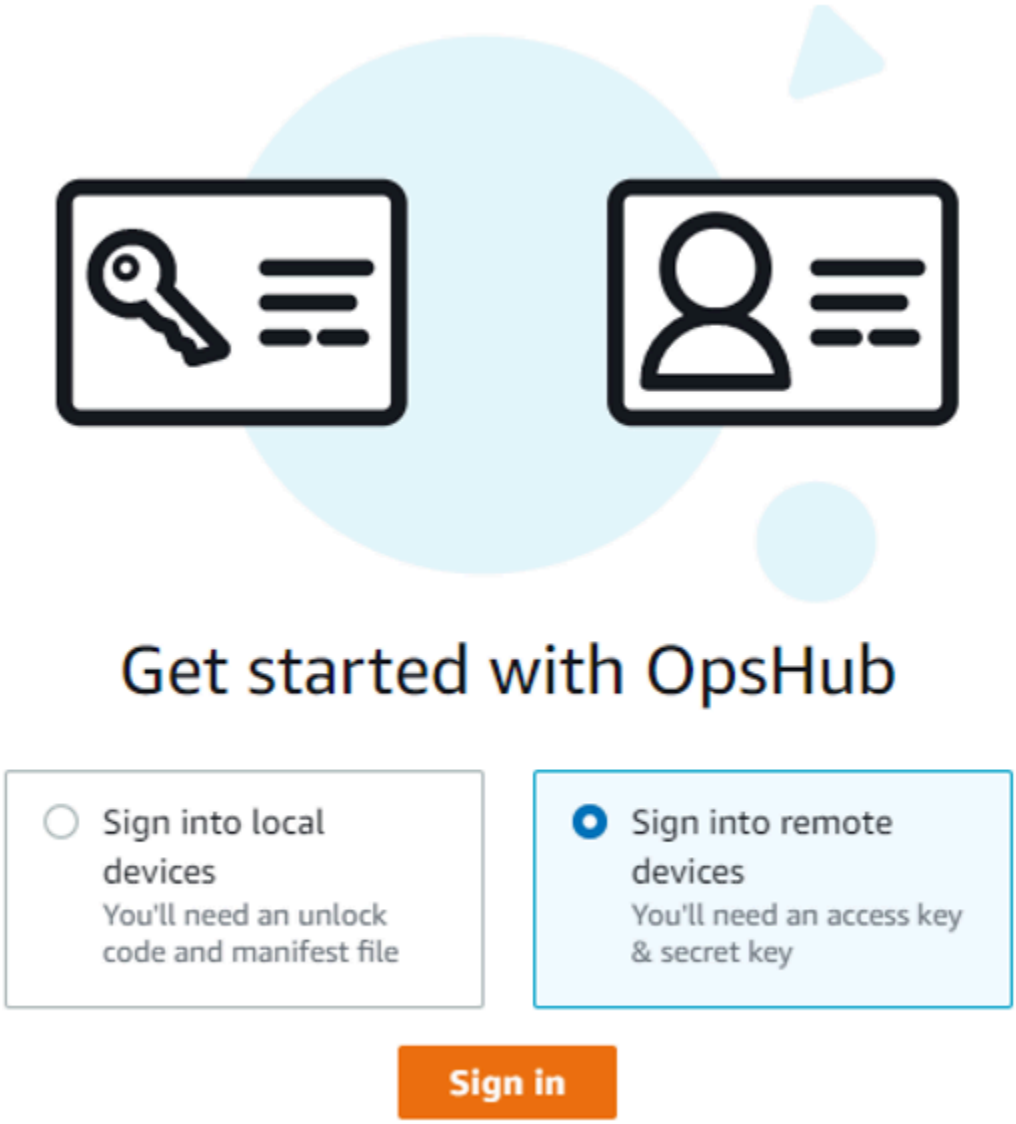
Para desbloquear un dispositivo de la familia Snow, no

Para conectar y desbloquear el dispositivo de forma remota

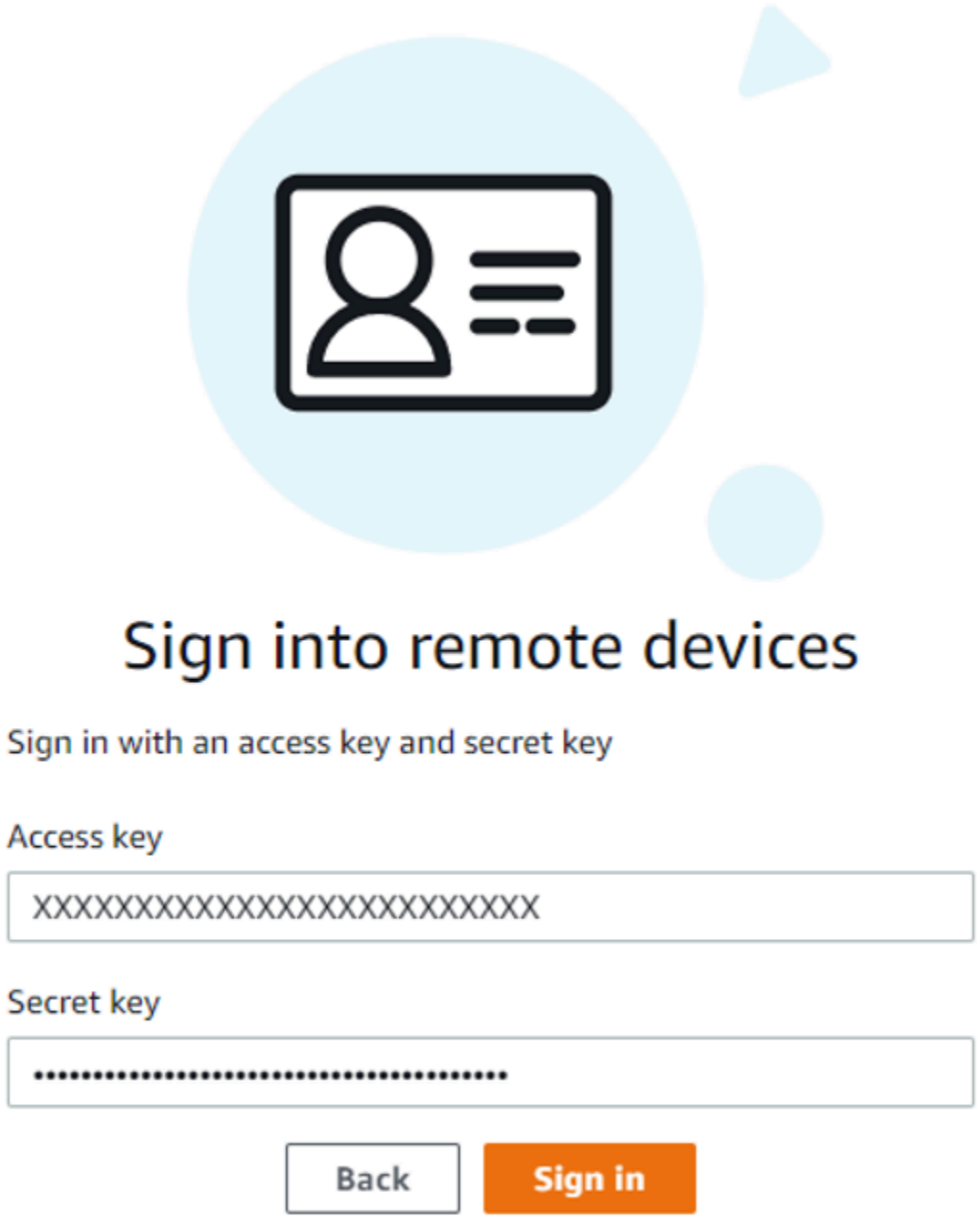
1. Abra la pestaña del dispositivo, localice el cable de alimentación y conecte el dispositivo a una fuente de alimentación.
2. Conecte el dispositivo a la red mediante un cable Ethernet (normalmente un cable RJ45), abra el panel delantero y encienda el dispositivo.

   > **Note**
   >
   > Para que el dispositivo se pueda desbloquear de forma remota, debe ser capaz de conectarse a *`device-order-region`*`.amazonaws.com`.

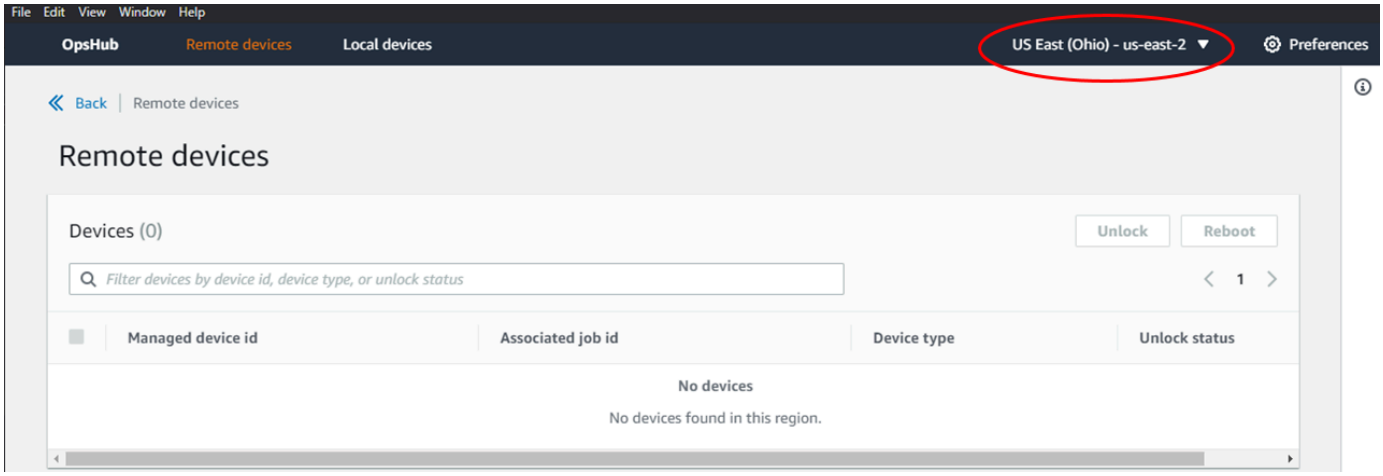
3. Abre la AWS OpsHub aplicación. Si es la primera vez que la utiliza, se le pedirá que seleccione un idioma. A continuación, elija Siguiente.
4. En la OpsHub página Comenzar con, selecciona Iniciar sesión en dispositivos remotos y, a continuación, selecciona Iniciar sesión.



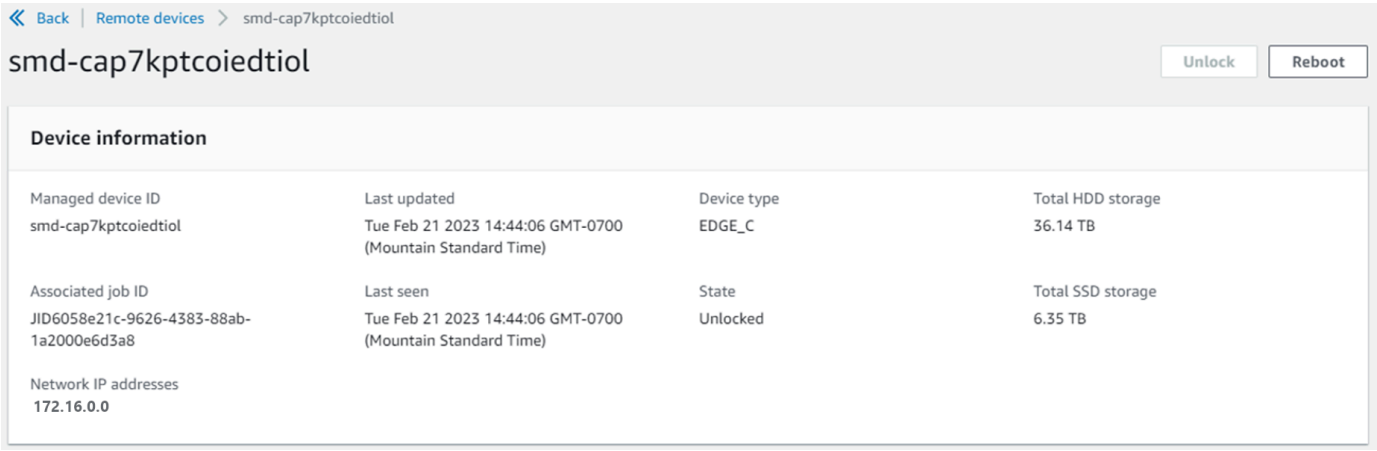
5. En la página Iniciar sesión en dispositivos remotos, introduzca las credenciales de AWS Identity and Access Management (IAM) (clave de acceso y clave secreta) de la Cuenta de AWS vinculada a su dispositivo y, a continuación, seleccione Iniciar sesión.



6. En la parte superior de la pestaña Dispositivos remotos, elija la región del dispositivo Snow que desea desbloquear de forma remota.



7. En la pestaña Dispositivos remotos, elija su dispositivo para ver sus detalles, como su estado y las interfaces de red. A continuación, seleccione Desbloquear para desbloquear el dispositivo.



Desde la página de detalles del dispositivo remoto, también puedes reiniciar tus dispositivos y gestionarlos del mismo modo que lo haces con AWS Command Line Interface (AWS CLI). Para ver los dispositivos remotos en otros dispositivos Regiones de AWS, selecciona la región actual en la barra de navegación y, a continuación, elige la región que deseas ver. Para obtener más información, consulte Administrar AWS los servicios en tu dispositivo.

Verificar la firma PGP de AWS OpsHub (opcional)

El paquete de instalación de la AWS OpsHub aplicación para el sistema operativo Linux está firmado criptográficamente. Puede utilizar una clave pública para verificar que el paquete del instalador sea original y que no se haya modificado. Si hay algún tipo de daño o alteración en los archivos, se produce un error en la verificación. Puede verificar la firma del paquete del instalador con GNU

Privacy Guard (GPG). Esta verificación es opcional. Si decide verificar la firma de la aplicación, puede hacerlo en cualquier momento.

Puede descargar el archivo SIGNATURE para el instalador del sistema operativo Linux desde AWS Snowcone Resources o Snowball Edge Resources.

Para comprobar si el paquete de AWS OpsHub instalación está activado para el sistema operativo Linux

1. Copie la siguiente clave pública, guárdela en un archivo y asigne un nombre al archivo. Por ejemplo, `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 la clave pública a su conjunto de claves y anote el valor de clave devuelto.

   GPG

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

Ejemplo de resultado

```
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 la huella digital. Asegúrese de sustituir *key-value* por el valor del paso anterior. Le recomendamos que utilice GPG para verificar la huella digital.

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

Este comando devuelve un resultado similar al siguiente.

```
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]
```

La huella digital debe coincidir con la siguiente:

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

Si la huella digital no coincide, no instales la AWS OpsHub aplicación. Póngase en contacto con AWS Support.

4. Verifique el paquete del instalador y descargue el archivo SIGNATURE según la arquitectura y el sistema operativo de su instancia si aún no lo ha hecho.
5. Verifique la firma del paquete del instalador. Asegúrese de reemplazar *signature-filename* y *OpsHub-download-filename* por los valores que especificó al descargar el archivo SIGNATURE y la aplicación AWS OpsHub .

GPG

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

Este comando devuelve un resultado similar al siguiente.

GPG

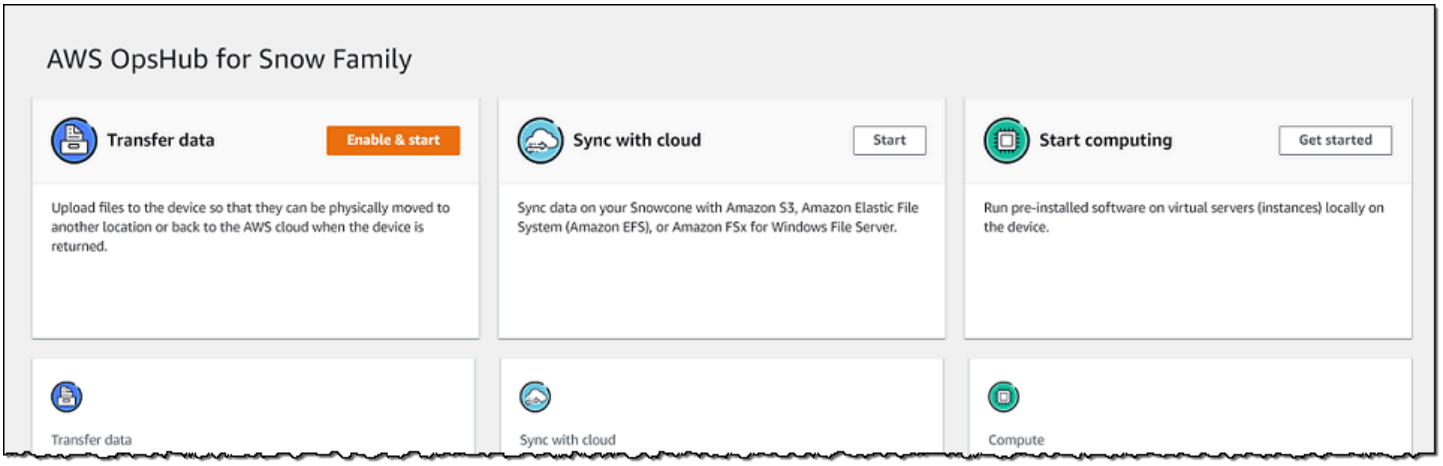
```
gpg: Signature made Mon Dec 21 13:44:47 2020 PST
gpg:                using RSA key 1655BBDE2B770256
gpg: Good signature from "AWS OpsHub for Snow Family <aws-opshub-
signer@amazon.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication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

Si se utiliza GPG y el resultado incluye la frase `BAD signature`, compruebe que ha realizado el procedimiento correctamente. Si sigue recibiendo esta respuesta, póngase en contacto con el agente AWS Support y no lo instale. El mensaje de advertencia sobre la confianza no significa que la firma no sea válida, sino que no se ha verificado la clave pública. Una clave solo es de confianza si la ha firmado usted o alguien en quien confíe.

Administrar AWS los servicios en tu dispositivo

Con AWS OpsHub, puede usar y administrar los AWS servicios en sus dispositivos de la familia Snow. Actualmente, AWS OpsHub es compatible con los siguientes recursos:

- Instancias de Amazon Elastic Compute Cloud (Amazon EC2): utilice instancias compatibles con Amazon EC2 para ejecutar software instalado en un servidor virtual sin enviarlo a la Nube de AWS para su procesamiento.
- Sistema de archivos de red (NFS): utilice recursos compartidos de archivos para mover datos a su dispositivo. Puede enviar el dispositivo para transferir sus datos AWS a esa ubicación o utilizarlo para transferirlos DataSync a otras Nube de AWS ubicaciones. Nube de AWS
- Almacenamiento compatible con Amazon S3 en dispositivos de la familia Snow: ofrece almacenamiento seguro de objetos con mayor resiliencia, escalabilidad y un conjunto de funciones de API de Amazon S3 ampliado para entornos robustos, móviles, periféricos y desconectados. Con el almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow, puede almacenar datos y ejecutar aplicaciones de alta disponibilidad en los dispositivos de la familia Snow para la computación perimetral.



Temas

- Uso local de instancias de computación compatibles con Amazon EC2
- Administración de un clúster de Amazon EC2
- Configuración del almacenamiento compatible con Amazon S3 en dispositivos Snow Family
- Administración del almacenamiento del adaptador de Amazon S3
- Administrar la interfaz NFS

Uso local de instancias de computación compatibles con Amazon EC2

Puede usarlo AWS OpsHub para ejecutar software preinstalado en servidores virtuales (instancias) de forma local en su dispositivo y también para administrar instancias de Amazon EC2 en su dispositivo.

Temas

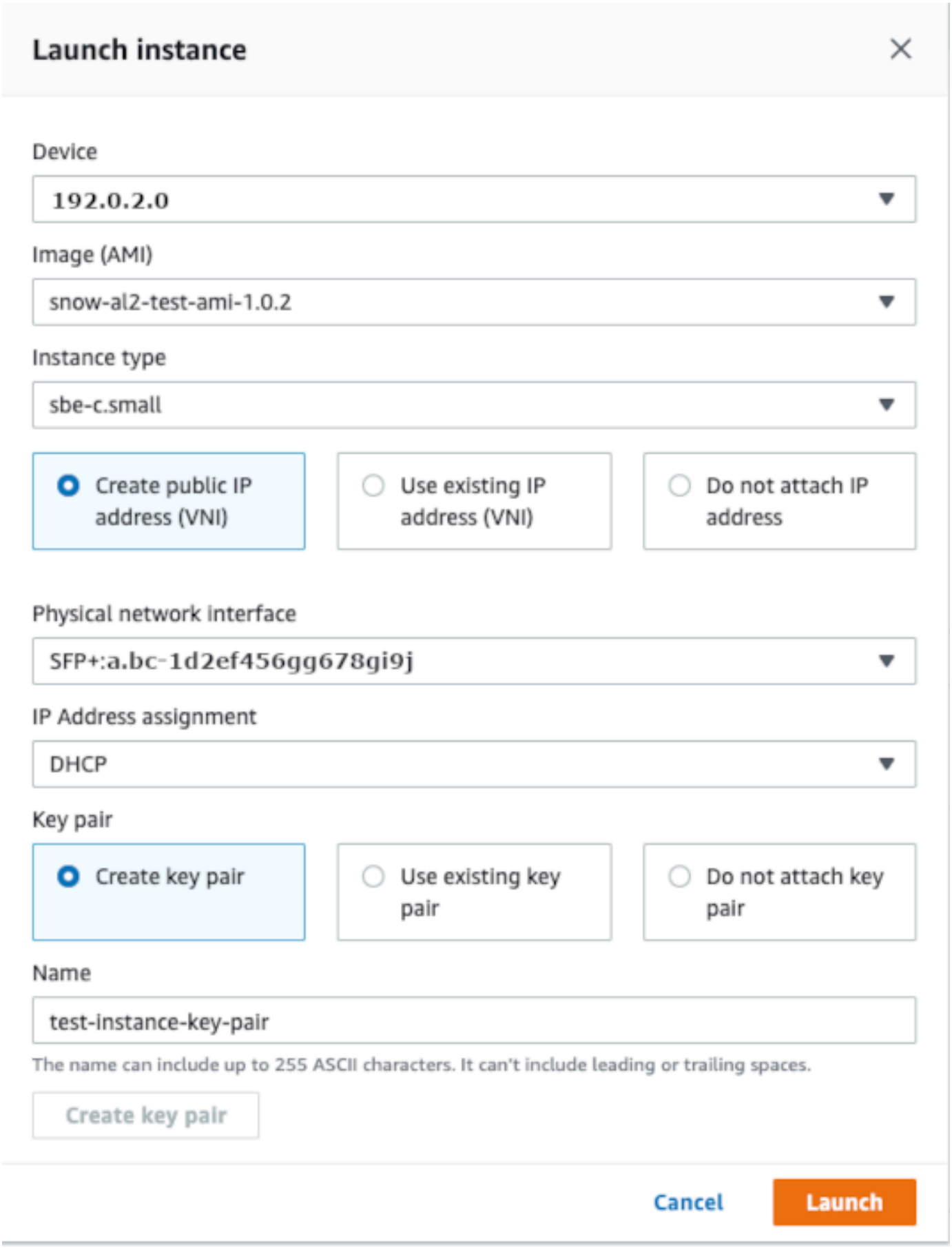
- Lanzamiento de una instancia compatible con Amazon EC2
- Detención de una instancia compatible con Amazon EC2
- Inicio de una instancia compatible con Amazon EC2
- Trabajo con pares de claves
- Terminación de una instancia compatible con Amazon EC2
- Uso local de volúmenes de almacenamiento
- Importación de una imagen a su dispositivo como una AMI compatible con Amazon EC2
- Eliminación de una instantánea
- Anulación del registro de una AMI

Lanzamiento de una instancia compatible con Amazon EC2

Siga estos pasos para lanzar una instancia compatible con Amazon EC2 mediante. AWS OpsHub

Para lanzar una instancia compatible con Amazon EC2

1. Abra la aplicación. AWS OpsHub
2. En la sección Iniciar computación del panel, seleccione Comenzar. O bien, seleccione el menú Servicios en la parte superior y, a continuación, seleccione Compute (EC2) para abrir la página Computación. Todos los recursos de computación aparecen en la sección Recursos.
3. Si tiene instancias compatibles con Amazon EC2 que se están ejecutando en el dispositivo, aparecen en la columna Nombre de instancia en Instancias. Puede ver los detalles de cada instancia en esta página.
4. Seleccione Lanzar instancia. Se abrirá el asistente de inicialización de instancias.
5. En Dispositivo, seleccione el dispositivo Snow en el que desea lanzar la instancia compatible con 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. En Imagen (AMI), seleccione una Imagen de máquina de Amazon (AMI) de la lista. Esta AMI se utiliza para lanzar la instancia.
7. En Tipo de instancia, seleccione uno de la lista.
8. Elija cómo desea asociar una dirección IP a la instancia. Dispone de las opciones siguientes:

   - Crear dirección IP pública (VNI): elija esta opción para crear una nueva dirección IP mediante una interfaz de red física. Seleccione una asignación de interfaz de red física y dirección IP.
   - Usar la dirección IP existente (VNI): elija esta opción para usar una dirección IP existente y, a continuación, usar interfaces de red virtuales existentes. Seleccione una interfaz de red física y una interfaz de red virtual.
   - No adjuntar dirección IP: elija esta opción si no desea adjuntar una dirección IP.
9. Seleccione cómo desea adjuntar un par de claves a la instancia. Dispone de las opciones siguientes:

   Crear par de claves: elija esta opción para crear un nuevo par de claves y lanzar la nueva instancia con este par de claves.

   Utilizar par de claves existente: elija esta opción para usar un par de claves existente para lanzar la instancia.

   No adjuntar dirección IP: elija esta opción si no desea adjuntar un par de claves. Debe reconocer que no podrá conectarse a esta instancia a menos que ya conozca la contraseña integrada en esta AMI.

   Para obtener más información, consulte Trabajo con pares de claves.
10. Elija Lanzar. Debería ver el lanzamiento de su instancia en la sección Instancias de computación. El Estado es Pendiente y, a continuación, cambia a En ejecución cuando termina.

Detención de una instancia compatible con Amazon EC2

Siga los siguientes pasos AWS OpsHub para detener una instancia compatible con Amazon EC2.

Para detener una instancia compatible con Amazon EC2

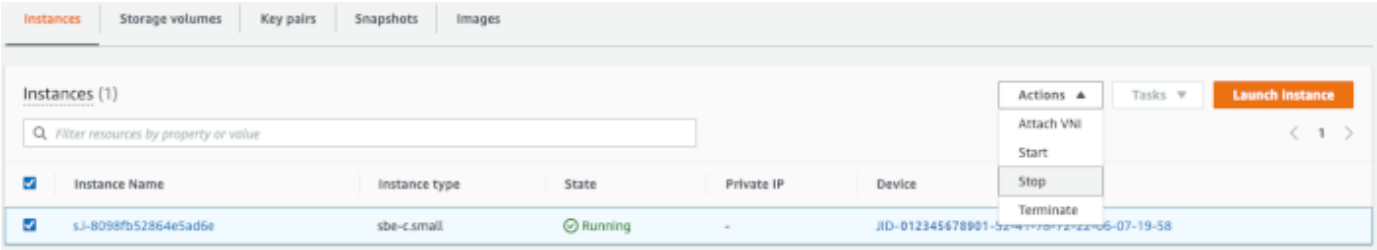
1. Abra la aplicación. AWS OpsHub

2. En la sección Iniciar computación del panel, seleccione Comenzar. O bien, seleccione el menú Servicios en la parte superior y, a continuación, seleccione Compute (EC2) para abrir la página Computación.

   Todos los recursos de computación aparecen en la sección Recursos.

3. Si tiene instancias compatibles con Amazon EC2 que se están ejecutando en el dispositivo, aparecen en la columna Nombre de instancia en Instancias.

4. Elija la instancia que desea detener, seleccione el menú Acciones y, a continuación, seleccione Detener. El Estado cambia a Deteniendo y, a continuación, a Detenido cuando termina.



Inicio de una instancia compatible con Amazon EC2

Siga estos pasos para iniciar una instancia compatible con Amazon EC2 mediante. AWS OpsHub

Para iniciar una instancia compatible con Amazon EC2

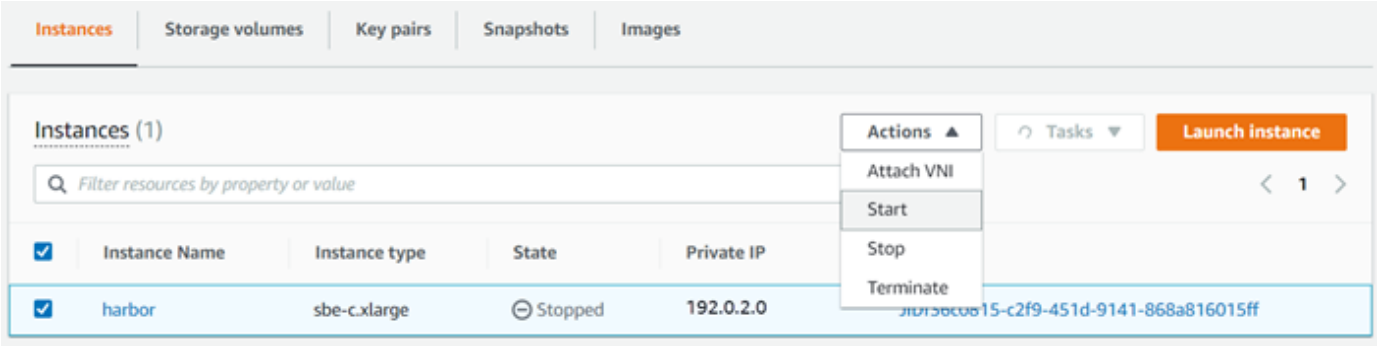
1. Abra la aplicación. AWS OpsHub

2. En la sección Iniciar computación del panel, seleccione Comenzar. O bien, seleccione el menú Servicios en la parte superior y, a continuación, seleccione Compute (EC2) para abrir la página Computación.

   Los recursos de computación aparecen en la sección Recursos.

3. En la columna Nombre de instancia en Instancias, busque la instancia que desea iniciar.

4. Seleccione la instancia y, a continuación, seleccione Iniciar. El Estado cambia a Pendiente y, a continuación, cambia a En ejecución cuando termina.



Trabajo con pares de claves

Cuando lanza una instancia compatible con Amazon EC2 y pretende conectarse a ella mediante SSH, debe proporcionar un par de claves. Puede utilizar Amazon EC2 para crear un nuevo par de claves o bien puede importar un par de claves existente o administrar sus pares de claves.

Para crear, importar o administrar pares de claves

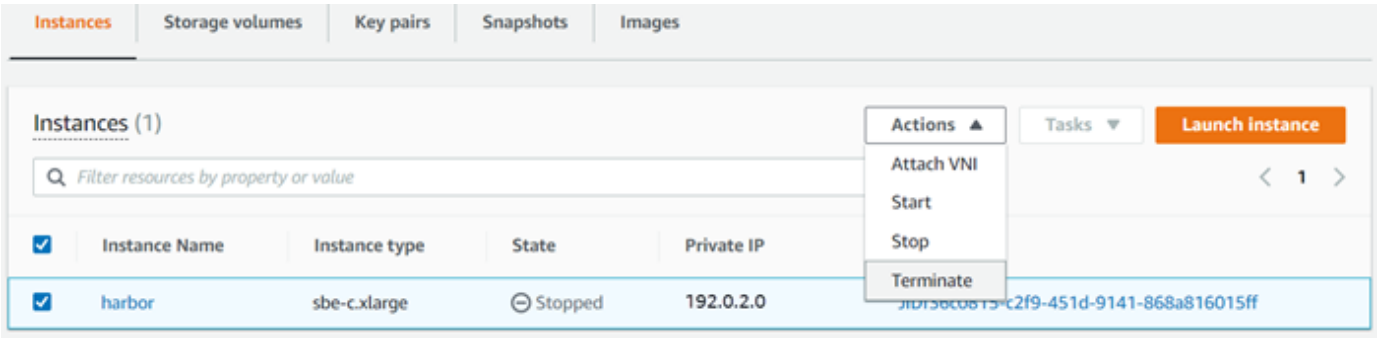
1. Abre Compute en el AWS OpsHub panel de control.
2. En el panel de navegación, elija la página Compute (EC2) y, a continuación, elija la pestaña Pares de claves. Se le redirigirá a la consola de Amazon EC2, donde podrá crear, importar o administrar sus pares de claves.
3. Para obtener instrucciones sobre cómo crear e importar pares de claves, consulte los pares de claves e instancias de Linux de Amazon EC2 en la Guía del usuario de Amazon EC2.

Terminación de una instancia compatible con Amazon EC2

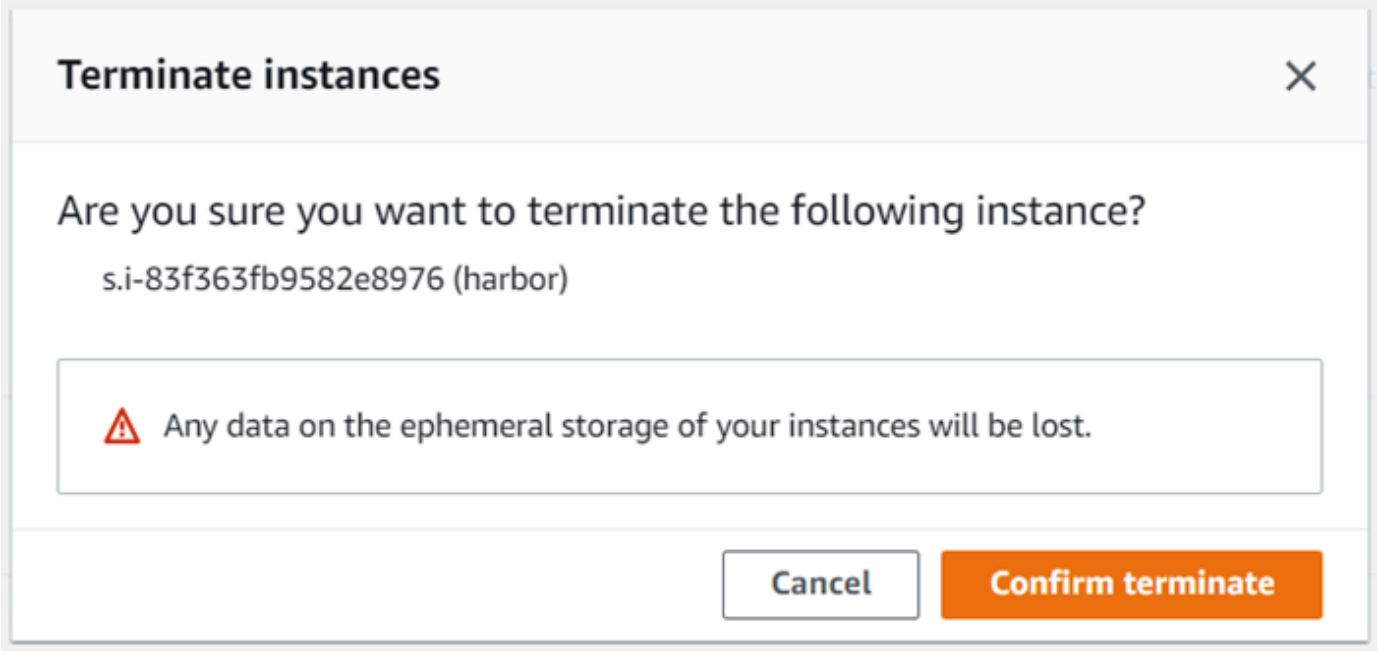
Después de terminar una instancia compatible con Amazon EC2, no puede reiniciarla.

Para terminar una instancia compatible con Amazon EC2

1. Abra la aplicación. AWS OpsHub
2. En la sección Iniciar computación del panel, seleccione Comenzar. O bien, seleccione el menú Servicios en la parte superior y, a continuación, seleccione Compute (EC2) para abrir la página Computación. Puede ver todos los recursos de computación en la sección Recursos.
3. En la columna Nombre de instancia en Instancias, busque la instancia que desea terminar.
4. Elija la instancia y elija el menú Acciones. En el menú Acciones, seleccione Terminar.



5. En la ventana Terminar instancias, seleccione Confirmar terminación.



> **Note**
>
> Una vez terminada la instancia, no puede reiniciarla.

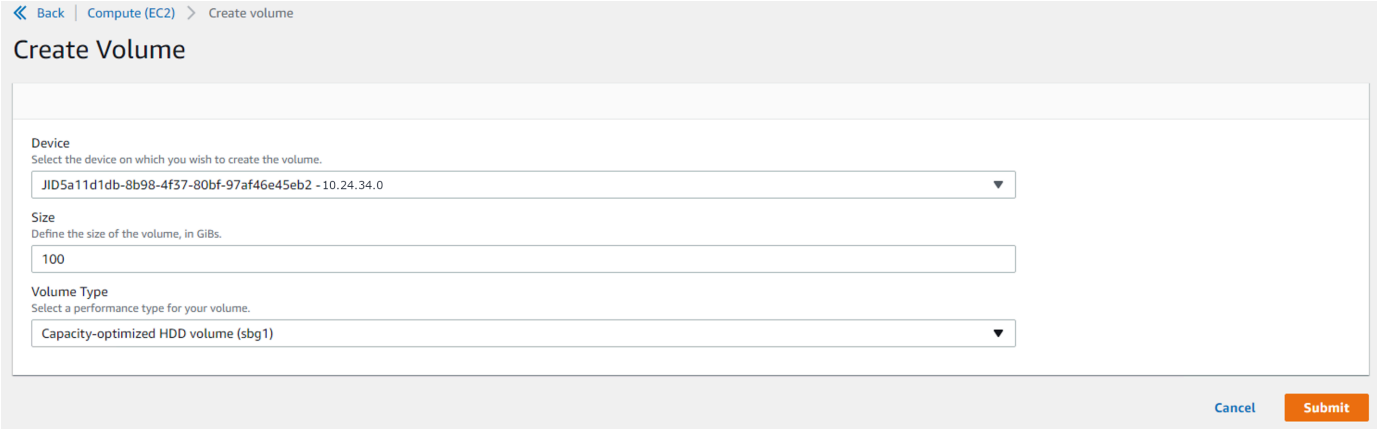
El Estado cambia a Terminando y, a continuación, cambia a Terminado cuando termina.

Uso local de volúmenes de almacenamiento

Las instancias compatibles con Amazon EC2 utilizan volúmenes de Amazon EBS para el almacenamiento. En este procedimiento, se crea un volumen de almacenamiento y se adjunta a la instancia mediante AWS OpsHub.

Para crear un volumen de almacenamiento

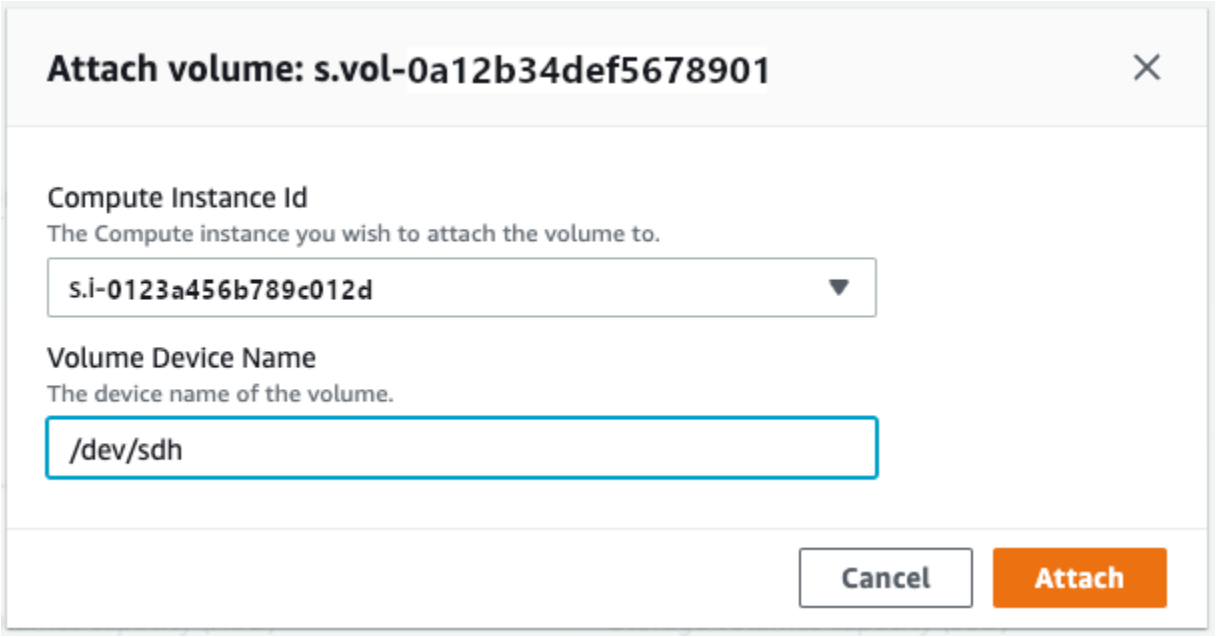
1. Abre la AWS OpsHub aplicación.
2. En la sección Iniciar computación del panel, seleccione Comenzar. O bien, seleccione el menú Servicios en la parte superior y, a continuación, seleccione Compute (EC2) para abrir la página Computación.
3. Seleccione la pestaña Volúmenes de almacenamiento. Si tiene volúmenes de almacenamiento en el dispositivo, los detalles sobre los volúmenes aparecen en Volúmenes de almacenamiento.
4. Seleccione Crear volumen para abrir la página Crear volumen.



5. Elija el dispositivo en el que desee crear el volumen, introduzca el tamaño (GiBspulgadas) que desee crear y elija el tipo de volumen.
6. Elija Enviar. El Estado es Creando y cambia a Disponible cuando termina. Puede ver su volumen y detalles del mismo en la pestaña Volúmenes.

Para adjuntar un volumen de almacenamiento a la instancia

1. Seleccione el volumen que ha creado y, a continuación, seleccione Adjuntar volumen.



2. En ID de instancia de informática, seleccione la instancia a la que desea adjuntar el volumen.
3. En Nombre del dispositivo de volumen, introduzca el nombre del dispositivo del volumen (por ejemplo, **`/dev/sdh`** o **`xvdh`**).
4. Elija Adjuntar.

Si ya no necesita el volumen, puede desasociarlo de la instancia y, a continuación, eliminarlo.

Importación de una imagen a su dispositivo como una AMI compatible con Amazon EC2

Puede importar una instantánea de la imagen a su dispositivo Snowball Edge y registrarla como una imagen de máquina de Amazon (AMI) compatible con Amazon EC2. Básicamente, una instantánea es una copia de un volumen de almacenamiento que puede utilizar para crear una AMI u otro volumen de almacenamiento. De este modo, puede llevar su propia imagen de un origen externo a su dispositivo y lanzarla como una instancia compatible con Amazon EC2.

Siga estos pasos para completar la importación de la imagen.

1. Cargue la instantánea en un bucket de Amazon S3 de su dispositivo.
2. Configure los permisos necesarios para conceder acceso a Amazon S3, Amazon EC2 y VM Import/Export, la característica que se utiliza para importar y exportar instantáneas.
3. Importe la instantánea del bucket de S3 a su dispositivo como una imagen.

4. Registre la imagen como una AMI compatible con Amazon EC2.
5. Lance la AMI como una instancia compatible con Amazon EC2.

> **Note**
>
> Tenga en cuenta las siguientes limitaciones al cargar instantáneas en dispositivos Snow Family.
>
> - Actualmente, los dispositivos Snow Family solo permiten importar instantáneas que tienen el formato de imagen RAW.
> - Actualmente, los dispositivos Snow Family solo permiten importar instantáneas cuyos tamaños oscilen entre 1 GB y 1 TB.

Paso 1: cargue una instantánea en un bucket de S3 de su dispositivo

Debe cargar la instantánea en Amazon S3 en su dispositivo antes de importarla. Esto se debe a que las instantáneas solo se pueden importar del almacenamiento de Amazon S3 que esté disponible en su dispositivo o clúster. Durante el proceso de importación, tiene que elegir el bucket de S3 de su dispositivo en el que desea almacenar la imagen.

Para cargar una instantánea en Amazon S3

- Para crear un bucket de S3, consulte Creación de almacenamiento de Amazon S3.

  Para cargar una instantánea en un bucket de S3, consulte Carga de archivos al almacenamiento de Amazon S3.

Paso 2: importe la instantánea desde un bucket de S3

Cuando la instantánea se cargue en Amazon S3, podrá importarla a su dispositivo. Todas las instantáneas que se han importado o están en proceso de importación se muestran en la pestaña Instantáneas.

Para importar la instantánea a su dispositivo

1. Abre la AWS OpsHub aplicación.

2. En la sección Iniciar computación del panel, seleccione Comenzar. O bien, seleccione el menú Servicios en la parte superior y, a continuación, seleccione Compute (EC2) para abrir la página Computación. Todos los recursos de computación aparecen en la sección Recursos.
3. Seleccione la pestaña Instantáneas para ver todas las instantáneas que se han importado a su dispositivo. El archivo de imagen de Amazon S3 es un archivo .raw que se importa al dispositivo como una instantánea. Puede filtrar por ID de instantánea o por el estado de la instantánea para buscar instantáneas específicas. Puede elegir un ID de instantánea para ver los detalles de esa instantánea.
4. Elija la instantánea que desea importar y seleccione Importar instantánea para abrir la página Importar instantánea.
5. En Dispositivo, elija la dirección IP del dispositivo Snow Family al que desea importar la instantánea.
6. En Descripción de la importación y Descripción de la instantánea, introduzca una descripción para cada una de ellas.
7. En la lista Rol, elija el rol que se utilizará para la importación. Los dispositivos de la familia Snow utilizan VM Import/Export para importar instantáneas. AWS asume esta función y la utiliza para importar la instantánea en su nombre. Si no tiene ningún rol configurado AWS Snowball Edge, abra el AWS Identity and Access Management (IAM) en el AWS OpsHub que podrá crear un rol de IAM local. El rol también necesita una política que tenga los permisos necesarios de VM Import/Export para realizar la importación. También tiene que asociar esta política al rol. Para obtener más información al respecto, consulte Uso local de IAM.

   A continuación, se muestra un ejemplo de la política.

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

Inicie sesión en la consola de IAM AWS Management Console y ábrala en https://console.aws.amazon.com/iam/.

El rol que cree debe tener permisos mínimos de acceso a Amazon S3. A continuación, se muestra un ejemplo de una 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. Elija Browse S3 y seleccione el bucket de S3 que contiene la instantánea que desea importar. Elija la instantánea y elija Enviar. La instantánea comienza a descargarse en su dispositivo. Puede elegir el ID de la instantánea para ver sus detalles. Puede cancelar el proceso de importación desde esta página.

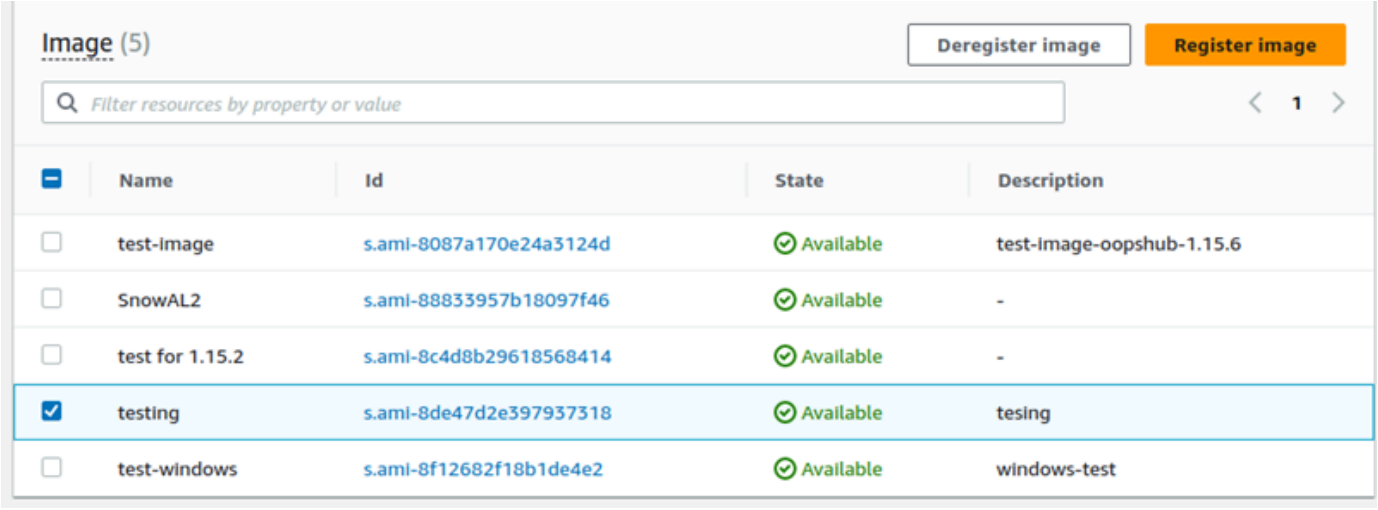
Paso 3: registre la instantánea como una AMI compatible con Amazon EC2

El proceso de creación de una AMI compatible con Amazon EC2 a partir de una imagen importada como instantánea se conoce como registro. Las imágenes que se importen a su dispositivo deben registrarse antes de poder lanzarse como instancias compatibles con Amazon EC2.

Para registrar una imagen importada como una instantánea

1. Abra la AWS OpsHub aplicación.

2. En la sección Iniciar computación del panel, seleccione Comenzar. O bien, seleccione el menú Servicios en la parte superior y, a continuación, seleccione Compute (EC2) para abrir la página Computación. Todos los recursos de computación aparecen en la sección Recursos.
3. Elija la pestaña Imágenes. Puede filtrar las imágenes por nombre, ID o estado para buscar una imagen específica.
4. Elija la imagen que desee registrar y seleccione Registrar imagen.



5. En la página Registrar imagen, proporcione un Nombre y una Descripción.
6. En Volumen raíz, especifique el nombre del dispositivo raíz.

   En la sección Dispositivo de bloques, puede cambiar el tamaño y el tipo de volumen.
7. Si desea que el volumen se elimine cuando se termine la instancia, elija Eliminar al terminar.
8. Si desea agregar más volúmenes, seleccione Agregar nuevo volumen.
9. Cuando haya terminado, elija Enviar.

Paso 4: lance la AMI compatible con Amazon EC2

- Para obtener más información, consulte Lanzamiento de una instancia compatible con Amazon EC2.

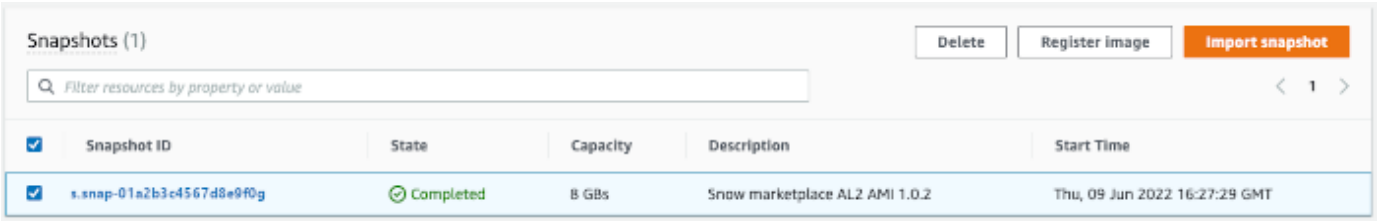
Eliminación de una instantánea

Si ya no necesita una instantánea, puede eliminarla del dispositivo. El archivo de imagen de Amazon S3 es un archivo .raw que se importa al dispositivo como una instantánea. Si una imagen está

usando la instantánea que va a eliminar, no se puede eliminar. Una vez terminada la importación, puede eliminar también el archivo .raw que cargó en Amazon S3 en su dispositivo.

Eliminar una instantánea

1. Abre la AWS OpsHub aplicación.
2. En la sección Iniciar computación del panel, seleccione Comenzar. O bien, seleccione el menú Servicios en la parte superior y, a continuación, seleccione Compute (EC2) para abrir la página Computación. Todos los recursos de computación aparecen en la sección Recursos.
3. Seleccione la pestaña Instantánea para ver todas las instantáneas que se han importado. Puede filtrar por ID de instantánea o por estado de la instantánea para buscar instantáneas específicas.
4. Elija las instantáneas que desea eliminar y después elija Eliminar. Puede elegir varias instantáneas.

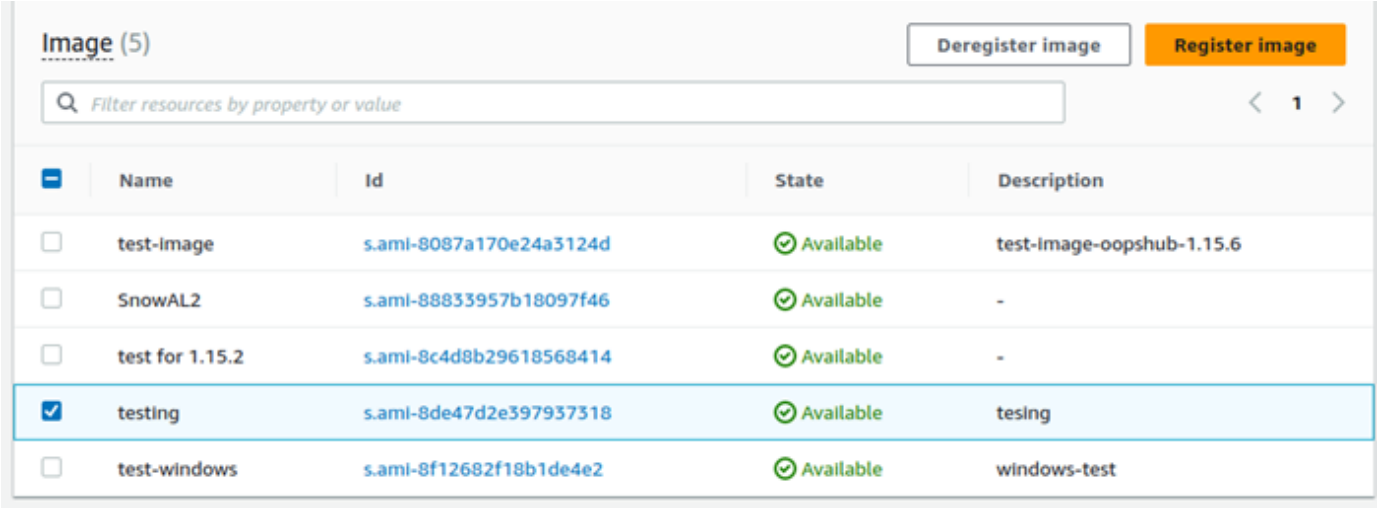


5. En el cuadro Confirmar la eliminación de la instantánea, seleccione Eliminar instantánea. Si la eliminación se realiza correctamente, la instantánea se elimina de la lista de la pestaña Instantáneas.

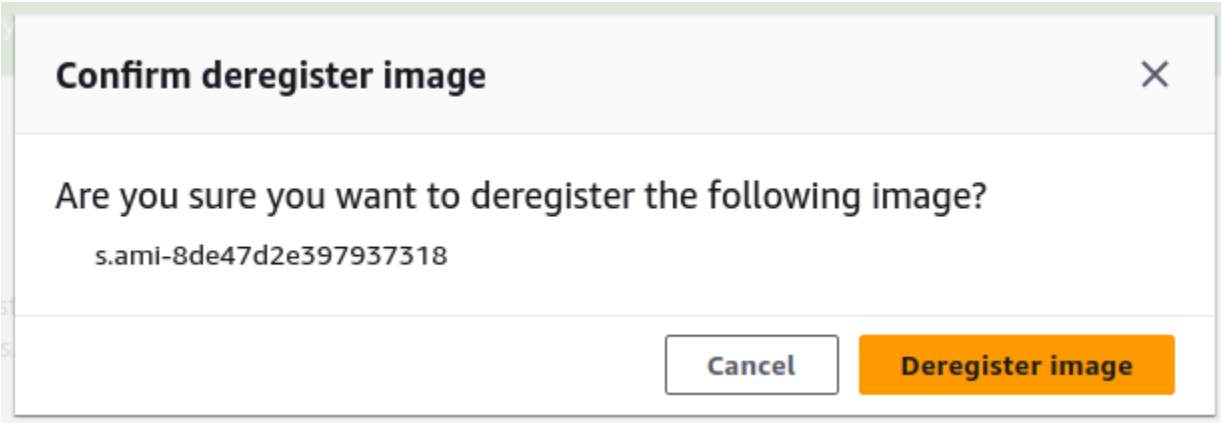
Anulación del registro de una AMI

Para anular el registro de una AMI

1. Abre la AWS OpsHub aplicación.
2. En la sección Iniciar computación del panel, seleccione Comenzar. O bien, seleccione el menú Servicios en la parte superior y, a continuación, seleccione Compute (EC2) para abrir la página Computación. Todos los recursos de computación aparecen en la sección Recursos.
3. Elija la pestaña Imágenes. Se muestra una lista de todas sus imágenes. Puede filtrar las imágenes por nombre, ID o estado para buscar una imagen específica.
4. Elija la imagen cuyo registro desea anular y seleccione Anular registro.



5. En la ventana Confirmar la anulación del registro de la imagen, confirme el ID de la imagen y seleccione Anular el registro de la imagen. Si la anulación del registro se realiza correctamente, la imagen se elimina de la lista de imágenes.



Administración de un clúster de Amazon EC2

Un clúster de Amazon EC2 es un grupo de dispositivos que se aprovisionan juntos como un clúster de dispositivos. Para usar un clúster, los AWS servicios del dispositivo deben estar ejecutándose en el punto final predeterminado. También debe elegir el dispositivo específico del clúster con el que desea hablar. Se utiliza un clúster por dispositivo.

Para crear un clúster de Amazon EC2

1. Conéctese e inicie sesión en su dispositivo Snow. Para obtener instrucciones sobre cómo iniciar sesión en el dispositivo, consulte Desbloqueo de un dispositivo.

2. En la página Choose device, seleccione Snowball Edge cluster y, a continuación, seleccione Next.
3. En la página Conéctese a su dispositivo, proporcione la dirección IP del dispositivo y las direcciones IP de otros dispositivos del clúster.
4. Seleccione Agregar otro dispositivo para agregar más dispositivos y, a continuación, seleccione Siguiente.
5. En la página Proporcione las claves, introduzca el código de desbloqueo del cliente del dispositivo, cargue el manifiesto del dispositivo y seleccione Desbloquear el dispositivo.

   Los dispositivos Snowball Edge utilizan un cifrado de 256 bits para garantizar la seguridad y la integridad de sus datos. chain-of-custody
6. (Opcional) Puede escribir un nombre para crear un perfil y, a continuación, elegir Guardar nombre de perfil. Se le dirigirá al panel, donde verá todos sus clústeres.

   Ahora puede empezar a utilizar los AWS servicios y a gestionar su clúster. Las instancias del clúster se administran de la misma manera que las instancias individuales. Para obtener instrucciones, consulte Administrar AWS los servicios en tu dispositivo o Administración de sus dispositivos.

Configuración del almacenamiento compatible con Amazon S3 en dispositivos Snow Family

El servicio de almacenamiento compatible con Amazon S3 en dispositivos Snow Family no está activo de forma predeterminada. Para iniciar el servicio en un dispositivo o un clúster, debe crear dos interfaces de red virtuales (VNIC) en cada dispositivo para conectarlas a los puntos de conexión `s3control` y `s3api`.

Temas

- Requisitos previos
- Mediante la opción de configuración Sencillo
- Uso de la opción de configuración avanzada
- Configuración del servicio de almacenamiento compatible con Amazon S3 en dispositivos Snow Family para que se inicie automáticamente
- Creación de un bucket en el almacenamiento compatible con Amazon S3 en dispositivos Snow Family

- Carga de archivos y carpetas en buckets de almacenamiento compatible con Amazon S3 en dispositivos Snow Family
- Eliminación de archivos y carpetas de buckets de almacenamiento compatible con Amazon S3 en dispositivos Snow Family
- Eliminación de buckets de almacenamiento compatible con Amazon S3 en dispositivos Snow Family

Requisitos previos

Antes de poder configurar su dispositivo o clúster utilizando AWS OpsHub for Snow Family, haga lo siguiente:

- Encienda el dispositivo Snowball Edge y conéctelo a la red.
- En el equipo local, descargue e instale la versión más reciente de AWS OpsHub. Conéctese al dispositivo o al clúster para desbloquearlo con un archivo de manifiesto. Para obtener más información, consulte Desbloqueo de un dispositivo.

Mediante la opción de configuración Sencillo

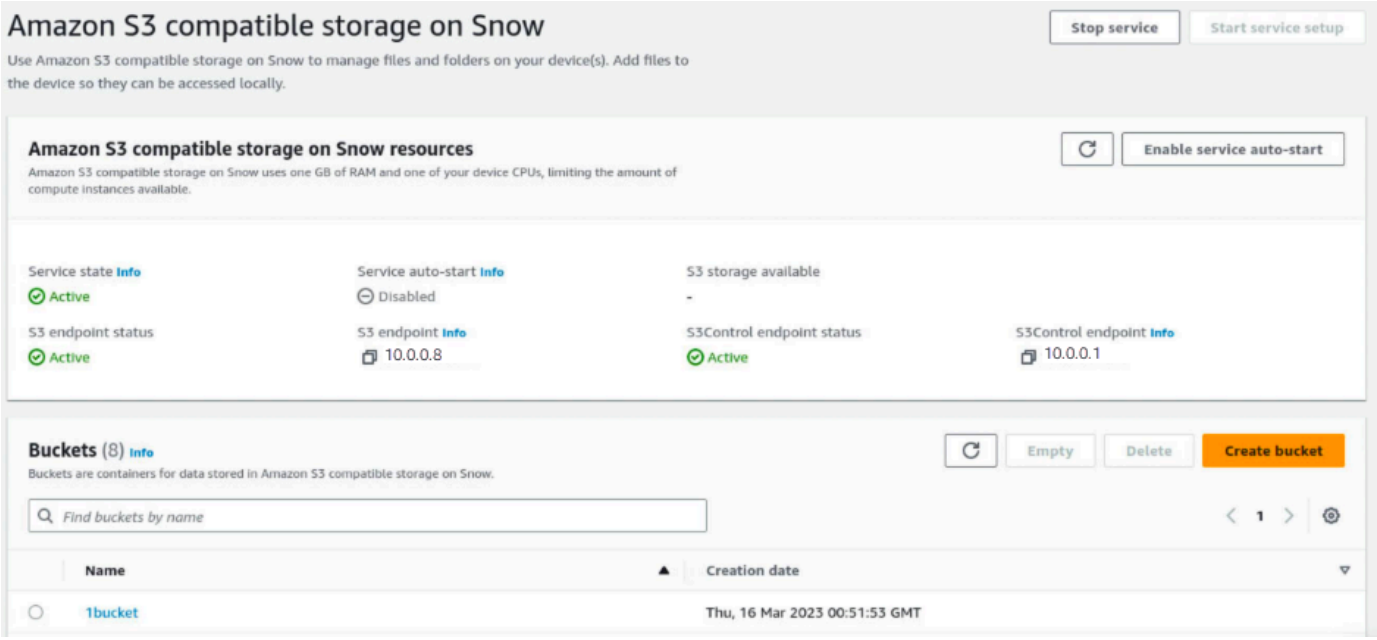
Si su red utiliza DHCP, use la opción de configuración Sencillo. Con esta opción, al iniciar el servicio se crean automáticamente las VNIC en cada dispositivo.

1. Inicia sesión en y AWS OpsHub, a continuación, selecciona Administrar almacenamiento.

   Esto le llevará a la página de inicio del almacenamiento compatible con Amazon S3 en dispositivos Snow Family.
2. En Tipo de configuración de inicio del servicio, seleccione Sencillo.
3. Seleccione Iniciar servicio.

   > **Note**
   >
   > Esta operación tarda unos minutos en completarse y depende de la cantidad de dispositivos que esté utilizando.

   Una vez iniciado el servicio, el estado del servicio es activo y hay puntos de conexión.



Uso de la opción de configuración avanzada

Utilice la opción de configuración avanzada si la red utiliza direcciones IP estáticas o si desea reutilizar VNI existentes. Con esta opción, puede crear manualmente VNIC para cada dispositivo.

1. Inicie sesión en y AWS OpsHub, a continuación, seleccione Administrar almacenamiento.

   Esto le llevará a la página de inicio del almacenamiento compatible con Amazon S3 en dispositivos Snow Family.
2. En Tipo de configuración de inicio del servicio, seleccione Avanzado.
3. Seleccione los dispositivos para los que necesita crear VNIC.

   En el caso de los clústeres, se necesita un cuórum mínimo de dispositivos para iniciar el servicio de almacenamiento compatible con Amazon S3 en dispositivos Snow Family. El cuórum es de dos para un clúster de tres nodos.

> **Note**
>
> Para el arranque inicial del servicio en una configuración de clúster, debe tener todos los dispositivos del clúster configurados y disponibles para que se inicie el servicio. Para los inicios posteriores, puede usar un subconjunto de los dispositivos si alcanza el cuórum, pero el servicio se iniciará en un estado degradado.

4. Para cada dispositivo, elija una VNIC existente o seleccione Crear interfaz de red virtual (VNI).

   Cada dispositivo necesita una VNIC para el punto de conexión S3 para las operaciones con objetos y otra para el punto de conexión S3Control para las operaciones de bucket.

5. Si va a crear una VNIC, elija una interfaz de red física e introduzca el estado, la dirección IP y la máscara de subred; a continuación, seleccione Crear interfaz de red virtual.

6. Una vez que haya creado las VNIC, elija Iniciar servicio.

> **Note**
>
> Esta operación tarda unos minutos en completarse y depende de la cantidad de dispositivos que esté utilizando.

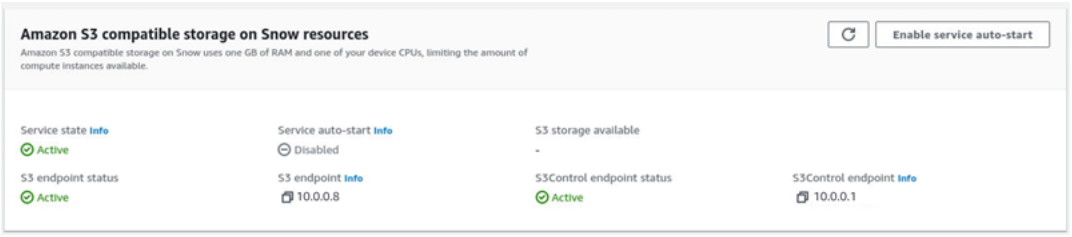
   Una vez iniciado el servicio, el estado del servicio es activo y hay puntos de conexión.

Configuración del servicio de almacenamiento compatible con Amazon S3 en dispositivos Snow Family para que se inicie automáticamente

1. Inicie sesión en y AWS OpsHub, a continuación, seleccione Administrar almacenamiento.

   Esto le llevará a la página de inicio del almacenamiento compatible con Amazon S3 en dispositivos Snow Family.

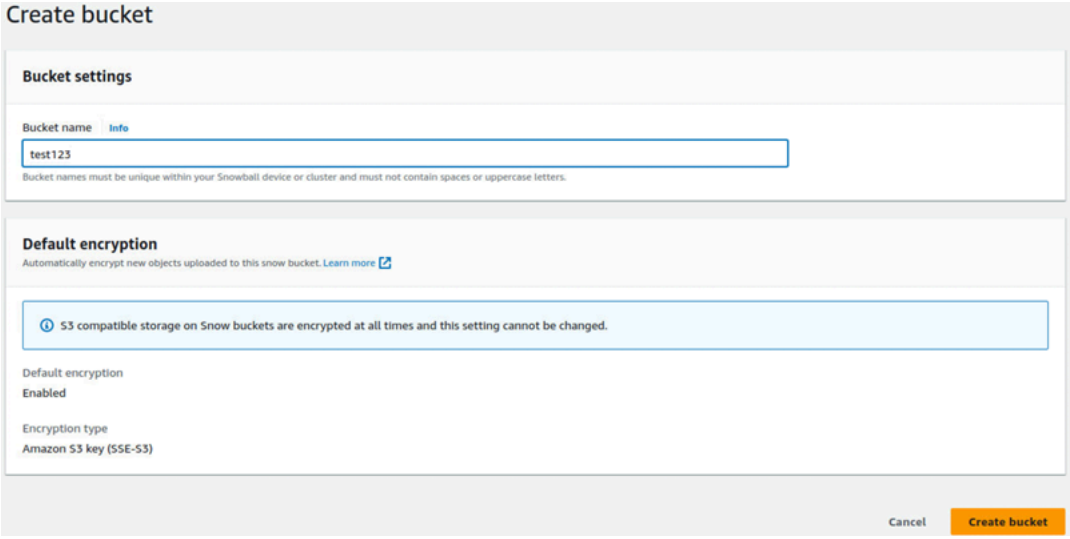
2. En Amazon S3 compatible storage on Snow resources, elija Enable service auto-start. El sistema configura el servicio para que se inicie automáticamente en el futuro.



Creación de un bucket en el almacenamiento compatible con Amazon S3 en dispositivos Snow Family

Utilice la AWS OpsHub interfaz para crear un bucket de Amazon S3 en su dispositivo de la familia Snow.

1. Abre AWS OpsHub.
2. En Administrar almacenamiento, seleccione Comenzar. Aparece la página Amazon S3 compatible storage on Snow.
3. En Buckets, seleccione Crear bucket. Aparece la pantalla Crear bucket.



4. En Nombre del bucket, escriba un nombre para el bucket.

> **Note**
>
> Los nombres de los buckets deben ser únicos en el dispositivo o clúster de Snowball y no deben contener espacios ni letras mayúsculas.

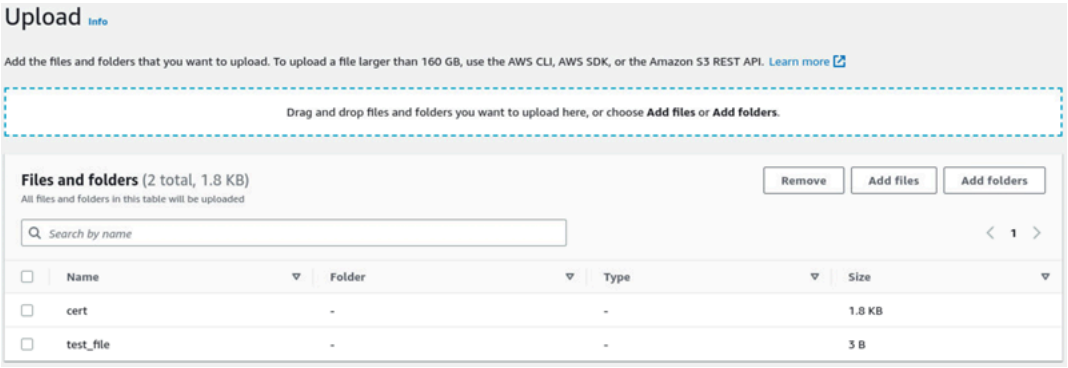
5. Elija Crear bucket. El sistema crea el bucket, que aparece en Buckets en la página Amazon S3 compatible storage on Snow.

Carga de archivos y carpetas en buckets de almacenamiento compatible con Amazon S3 en dispositivos Snow Family

Utilice la AWS OpsHub interfaz para cargar archivos y carpetas a un almacenamiento compatible con Amazon S3 en cubos de dispositivos de la familia Snow. Los archivos y las carpetas se pueden cargar por separado o juntos.

1. Abra AWS OpsHub
2. En Administrar almacenamiento, en Buckets, elija un bucket en el que desee cargar archivos. Aparece la página de ese bucket.

3. En la página del bucket, elija Cargar archivos. Aparece la página Cargar.



4. Cargue archivos o carpetas arrastrándolos desde el administrador de archivos del sistema operativo hasta la AWS OpsHub ventana o haga lo siguiente:

   a. Seleccione Agregar archivos o Agregar carpetas.

   b. Seleccione uno o varios archivos o carpetas que desea cargar. Seleccione Abrir.

   El sistema carga en el bucket del dispositivo las carpetas y los archivos seleccionados. Una vez finalizada la carga, los nombres de los archivos y carpetas aparecen en la lista Archivos y carpetas.

Eliminación de archivos y carpetas de buckets de almacenamiento compatible con Amazon S3 en dispositivos Snow Family

Utilice la AWS OpsHub interfaz para eliminar y eliminar permanentemente los archivos y carpetas de los depósitos del dispositivo de la familia Snow.

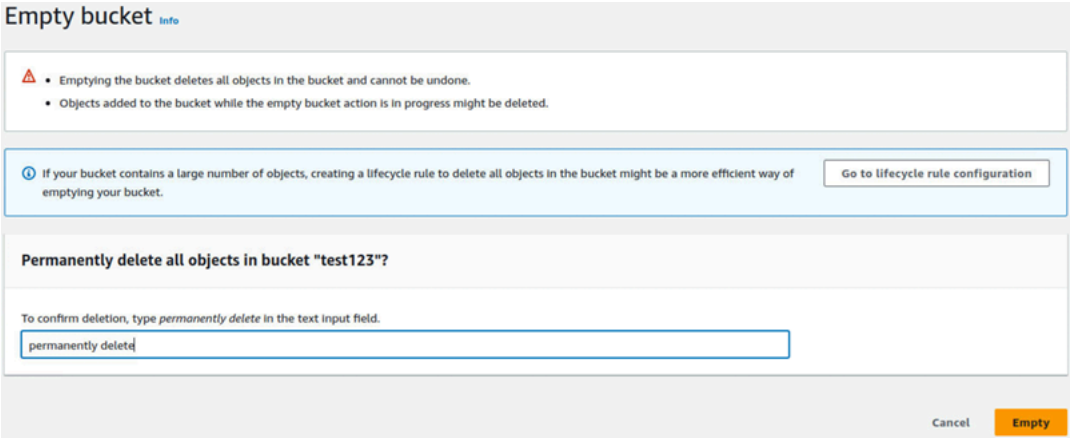
1. Abrir AWS OpsHub.
2. En Administrar almacenamiento, en Buckets, seleccione el nombre del bucket del que desea eliminar archivos y carpetas. Aparece la página de ese bucket.
3. En Archivos y carpetas, seleccione las casillas de verificación correspondientes a los archivos y carpetas que desea eliminar de forma permanente.
4. Seleccione Eliminar. El sistema elimina los archivos o carpetas del bucket del dispositivo.

Eliminación de buckets de almacenamiento compatible con Amazon S3 en dispositivos Snow Family

Para poder eliminar un bucket de un dispositivo, el bucket debe estar vacío. Puede eliminar archivos y carpetas desde el bucket o utilizar la herramienta Vaciar bucket. Para eliminar archivos y carpetas, consulte Eliminación de archivos y carpetas de buckets de almacenamiento compatible con Amazon S3 en dispositivos Snow Family.

Para usar la herramienta Vaciar bucket

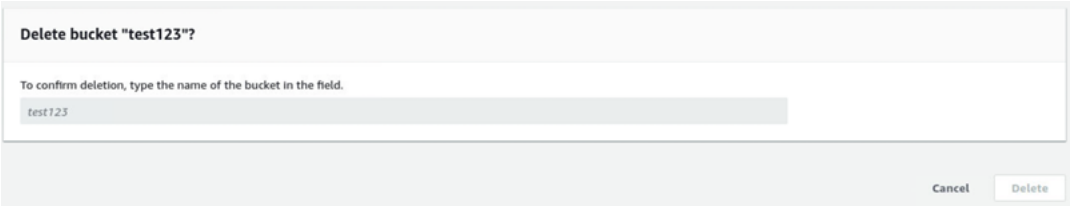
1. Abrir AWS OpsHub.
2. En Administrar almacenamiento, en Buckets, seleccione el botón de radio del bucket que desea vaciar.
3. Seleccione Vaciar. Aparece la página Vaciar bucket.



4. En el cuadro de texto de la página Vaciar bucket, escriba **`permanently delete`**.
5. Seleccione Vaciar. El sistema vacía el bucket.

Para eliminar un bucket vacío

1. En Administrar almacenamiento, en Buckets, seleccione el botón de radio del bucket que desea eliminar.
2. Seleccione Eliminar. Aparece la página Eliminar bucket.



3. En el cuadro de texto de la página Eliminar bucket, escriba el nombre del bucket.
4. Seleccione Eliminar. El sistema elimina el bucket del dispositivo.

Administración del almacenamiento del adaptador de Amazon S3

Puede utilizarlo AWS OpsHub para crear y gestionar el almacenamiento del Amazon Simple Storage Service (Amazon S3) en sus dispositivos de la familia Snow mediante el adaptador S3 para trabajos de importación y exportación.

Temas

Acceso al almacenamiento de Amazon S3

Puede cargar archivos en su dispositivo y obtener acceso a ellos localmente. Puede moverlos físicamente a otra ubicación del dispositivo o volver a importarlos a la ubicación Nube de AWS cuando devuelva el dispositivo.

Los dispositivos Snow Family utilizan buckets de Amazon S3 para almacenar y administrar archivos en su dispositivo.

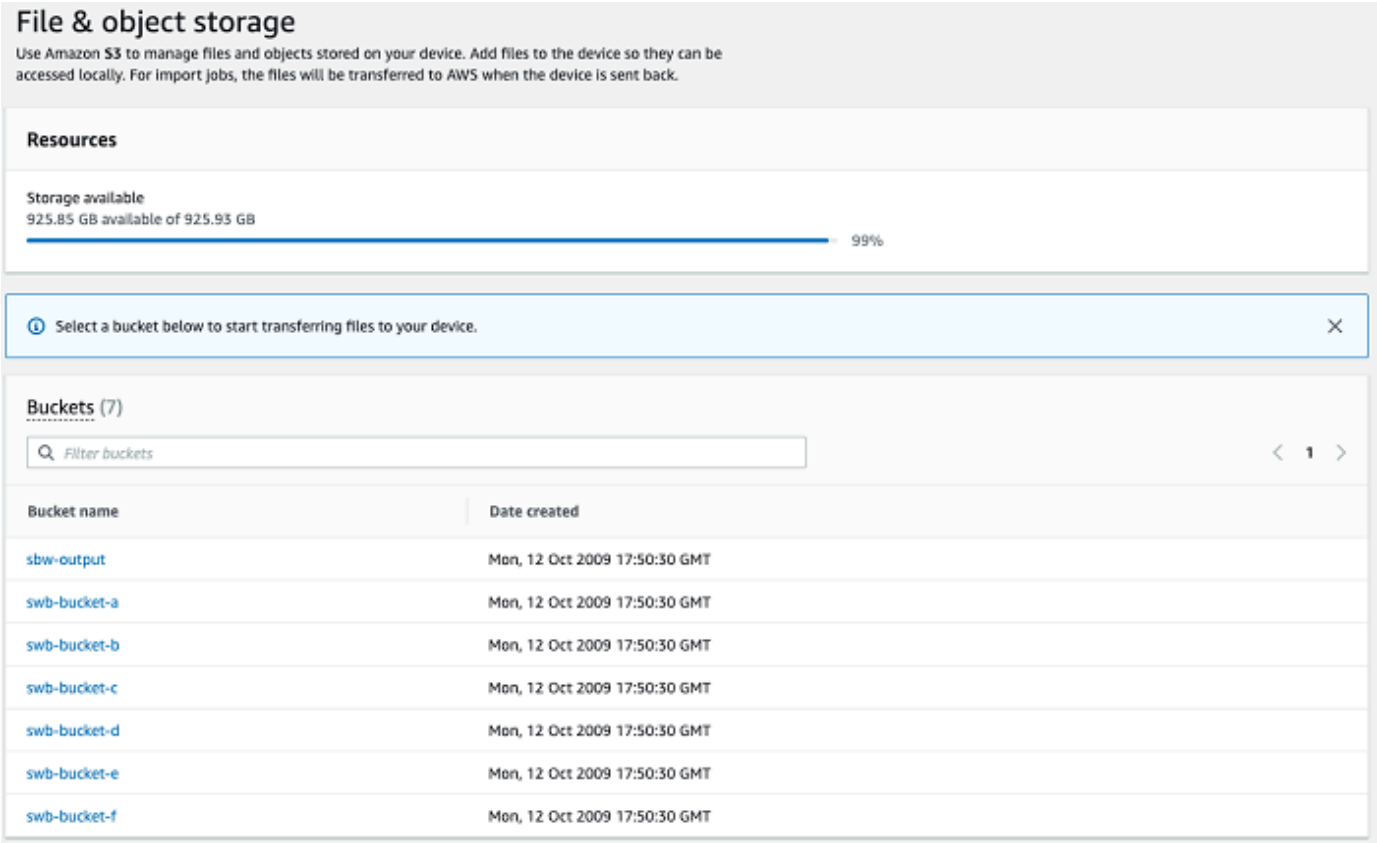
Para obtener acceso a un bucket de S3

1. Abre la AWS OpsHub aplicación.
2. En la sección Administrar el almacenamiento de archivos del panel, seleccione Comenzar.

   Si su dispositivo se ha pedido con el mecanismo de transferencia de Amazon S3, aparece en la sección Buckets de la página Almacenamiento de archivos y objetos. Puede ver los detalles de cada bucket en la página Almacenamiento de archivos y objetos.

   > **Note**
   >
   > Si el dispositivo se pidió con el mecanismo de transferencia NFS, el nombre del bucket aparecerá en la sección Puntos de montaje una vez configurado y activado el servicio

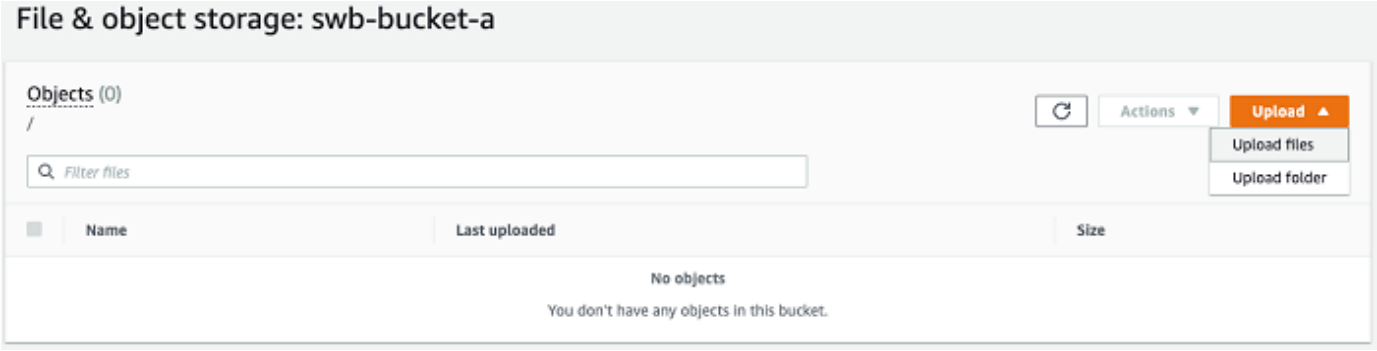
NFS. Para obtener más información acerca del uso de la interfaz de archivos, consulte Administrar la interfaz NFS.



Carga de archivos en el almacenamiento de Amazon S3

Para cargar un archivo

1. En la sección Administrar el almacenamiento de archivos del panel, seleccione Comenzar. Si tiene buckets de Amazon S3 en el dispositivo, aparecen en la sección Buckets de la página Almacenamiento de archivos. Puede ver los detalles de cada bucket en la página.
2. Seleccione el bucket en el que desea cargar archivos.
3. Seleccione Cargar y después Cargar archivos o bien arrastre y suelte los archivos en el bucket y elija Aceptar.

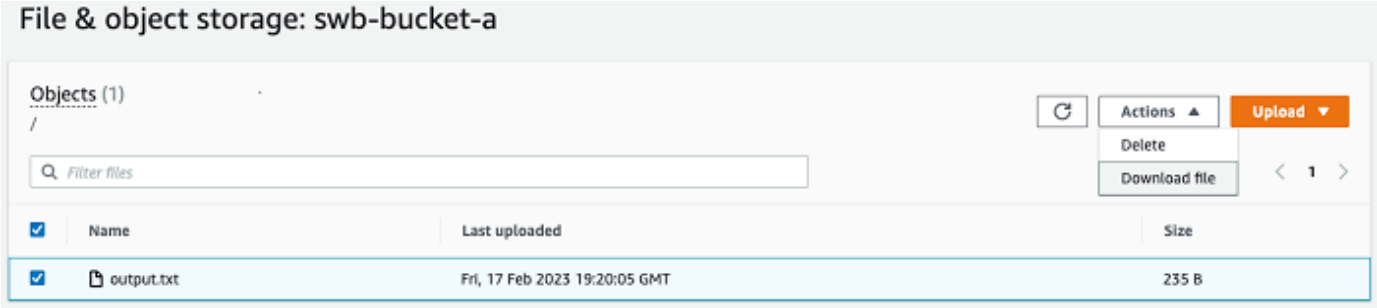


> **Note**
>
> Para cargar archivos más grandes, puede utilizar la característica de carga multiparte de Amazon S3 mediante la AWS CLI. Para obtener más información sobre la configuración de los ajustes de CLI de S3, consulte Configuración de CLI S3. Para obtener más información sobre la carga multiparte, consulte Descripción general de la carga multiparte en la Guía del usuario de Amazon Simple Storage Service.
> Se admite la carga de una carpeta desde un equipo local a Snowball Edge mediante AWS OpsHub el. Si el tamaño de la carpeta es muy grande, se tarda algún tiempo en leer la selección OpsHub de archivo/carpeta. Mientras OpsHub lee los archivos y las carpetas, no muestra un rastreador de progreso. Sin embargo, muestra un rastreador de progreso una vez que comienza el proceso de carga.

Descarga de archivos desde el almacenamiento de Amazon S3

Para descargar un archivo

1. En la sección Administrar el almacenamiento de archivos del panel, seleccione Comenzar. Si tiene buckets de Amazon S3 en el dispositivo, aparecen en la sección Buckets de la página Almacenamiento de archivos. Puede ver los detalles de cada bucket en la página.
2. Seleccione el bucket desde el que desea descargar archivos y desplácese hasta el archivo que desea descargar. Seleccione uno o más archivos.



3. En el menú Acciones, seleccione Descargar.
4. Seleccione una ubicación en la que descargar el archivo y seleccione Aceptar.

Eliminación de archivos del almacenamiento de Amazon S3

Si ya no necesita un archivo, puede eliminarlo de su bucket de Amazon S3.

Para eliminar un archivo

1. En la sección Administrar el almacenamiento de archivos del panel, seleccione Comenzar. Si tiene buckets de Amazon S3 en el dispositivo, aparecen en la sección Buckets de la página Almacenamiento de archivos. Puede ver los detalles de cada bucket en la página.
2. Seleccione el bucket del que desea eliminar archivos y desplácese hasta el archivo que desea eliminar.
3. En el menú Acciones, elija Eliminar.
4. En el cuadro de diálogo que aparece, seleccione Confirmar eliminación.

Administrar la interfaz NFS

Utilice la interfaz del sistema de archivos de red (NFS) para cargar archivos en el dispositivo de la familia Snow como si el dispositivo fuera el almacenamiento local de su sistema operativo. Esto permite un enfoque de transferencia de datos más fácil de usar, ya que puede utilizar funciones del sistema operativo, como copiar archivos, arrastrarlos y soltarlos, u otras funciones de la interfaz gráfica de usuario. Cada depósito S3 del dispositivo está disponible como terminal de interfaz NFS y se puede montar para copiar datos en él. La interfaz NFS está disponible para los trabajos de importación.

Puede utilizar la interfaz NFS si el dispositivo Snowball Edge se configuró para incluirla cuando se creó la tarea de pedido del dispositivo. Si el dispositivo no está configurado para incluir la interfaz

NFS, utilice el adaptador S3 o el almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow para transferir datos. Para obtener más información sobre el adaptador S3, consulteAdministración del almacenamiento del adaptador de Amazon S3. Para obtener más información sobre el almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow, consulteConfiguración del almacenamiento compatible con Amazon S3 en dispositivos Snow Family.

Cuando se inicia, la interfaz NFS utiliza 1 GB de memoria y 1 CPU. Esto puede limitar la cantidad de otros servicios que se ejecutan en el dispositivo de la familia Snow o la cantidad de instancias compatibles con EC2 que se pueden ejecutar.

Los datos transferidos a través de la interfaz NFS no se cifran durante el tránsito. Al configurar la interfaz NFS, puede proporcionar bloques CIDR y el dispositivo de la familia Snow restringirá el acceso a la interfaz NFS desde los ordenadores cliente con direcciones en esos bloques.

Los archivos del dispositivo se transferirán a Amazon S3 cuando se devuelva a Amazon S3 AWS. Para obtener más información, consulte Importación de trabajos a Amazon S3 .

Para obtener más información sobre el uso de NFS con el sistema operativo de su ordenador, consulte la documentación del sistema operativo.

Tenga en cuenta los siguientes detalles cuando utilice la interfaz NFS.

- Los nombres de archivo son claves de objeto que se encuentran en el bucket de S3 local del dispositivo Snow Family. El nombre de clave es una secuencia de caracteres Unicode cuya codificación UTF-8 tiene una longitud máxima de 1024 bytes. Recomendamos utilizar NFSv4.1 siempre que sea posible y codificar los nombres de los archivos con Unicode UTF-8 para garantizar una importación de datos correcta. Es posible que los nombres de archivo que no estén codificados con UTF-8 no se carguen en S3 o que se carguen en S3 con un nombre de archivo diferente, según la codificación NFS que se utilice.
- Asegúrese de que la longitud máxima de la ruta del archivo sea inferior a 1024 caracteres. Los dispositivos Snow Family no admiten rutas de archivos de más de 1024 caracteres. Si se supera esta longitud de ruta de archivo, se producirán errores en la importación de archivos.
- Para obtener más información, consulte Claves de objeto en la Guía del usuario de Amazon Simple Storage Service.
- Para las transferencias basadas en NFS, los metadatos de estilo POSIX estándar se añadirán a sus objetos a medida que se importen a Amazon S3 desde los dispositivos de la familia Snow. Además, verá los metadatos «x-amz-meta-user-agent aws-datasync» tal y como los utilizamos

actualmente AWS DataSync como parte del mecanismo de importación interna a Amazon S3 para la importación de dispositivos de la familia Snow con la opción NFS.

- Puede transferir hasta 40 millones de archivos con un único dispositivo Snowball Edge. Si necesita transferir más de 40 millones de archivos en un solo trabajo, agrupe los archivos para reducir el número de archivos por cada transferencia. Los archivos individuales pueden ser de cualquier tamaño, siendo el tamaño máximo de 5 TB para los dispositivos Snowball Edge con la interfaz NFS mejorada o la interfaz de S3.

También puede configurar y administrar la interfaz NFS con el cliente Snowball Edge, una herramienta de interfaz de línea de comandos (CLI). Para obtener más información, consulte Administración de la interfaz NFS.

Temas

Iniciar el servicio NFS en un sistema operativo Windows

Si el equipo cliente utiliza el sistema operativo Windows 10 Enterprise o Windows 7 Enterprise, inicie el servicio NFS en el equipo cliente antes de configurar NFS en la aplicación. AWS OpsHub

1. En el equipo cliente, abra Inicio, elija Panel de control y elija Programas.
2. Elija Activar o desactivar las características de Windows.

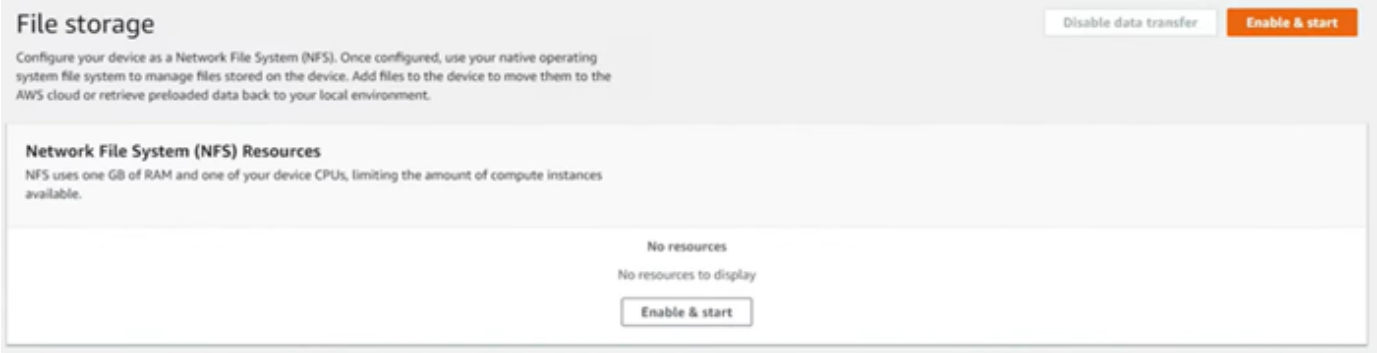
> **Note**
>
> Para activar las funciones de Windows, es posible que tenga que proporcionar un nombre de usuario y una contraseña de administrador para el equipo.

3. En Servicios para NFS, elija Cliente para NFS y elija Aceptar.

Configuración automática de la interfaz NFS

La interfaz NFS no se ejecuta en el dispositivo de la familia Snow de forma predeterminada, por lo que debe iniciarla para permitir la transferencia de datos en el dispositivo. Con unos pocos clics, su dispositivo de la familia Snow puede configurar rápida y automáticamente la interfaz NFS por usted. También puede configurar la interfaz NFS usted mismo. Para obtener más información, consulte Configuración manual de la interfaz NFS.

1. En la sección Transferir datos del panel, elija Habilitar e iniciar. Esta operación podría tardar un minuto o dos en completarse.



2. Cuando se inicia el servicio NFS, la dirección IP de la interfaz NFS aparece en el panel y la sección Transferencia de datos indica que el servicio está activo.
3. Seleccione Abrir en el explorador (si utiliza un sistema operativo Windows o Linux) para abrir el recurso compartido de archivos en el explorador de archivos de su sistema operativo y empezar a transferir archivos al dispositivo de la familia Snow. Puede copiar y pegar o arrastrar y soltar archivos desde el ordenador cliente al recurso compartido de archivos. En el sistema operativo Windows, el recurso compartido de archivos tiene el siguiente aspecto`buckets(\\12.123.45.679)(Z:)`.

> **Note**
>
> En los sistemas operativos Linux, el montaje de puntos finales NFS requiere permisos de root.

Configuración manual de la interfaz NFS

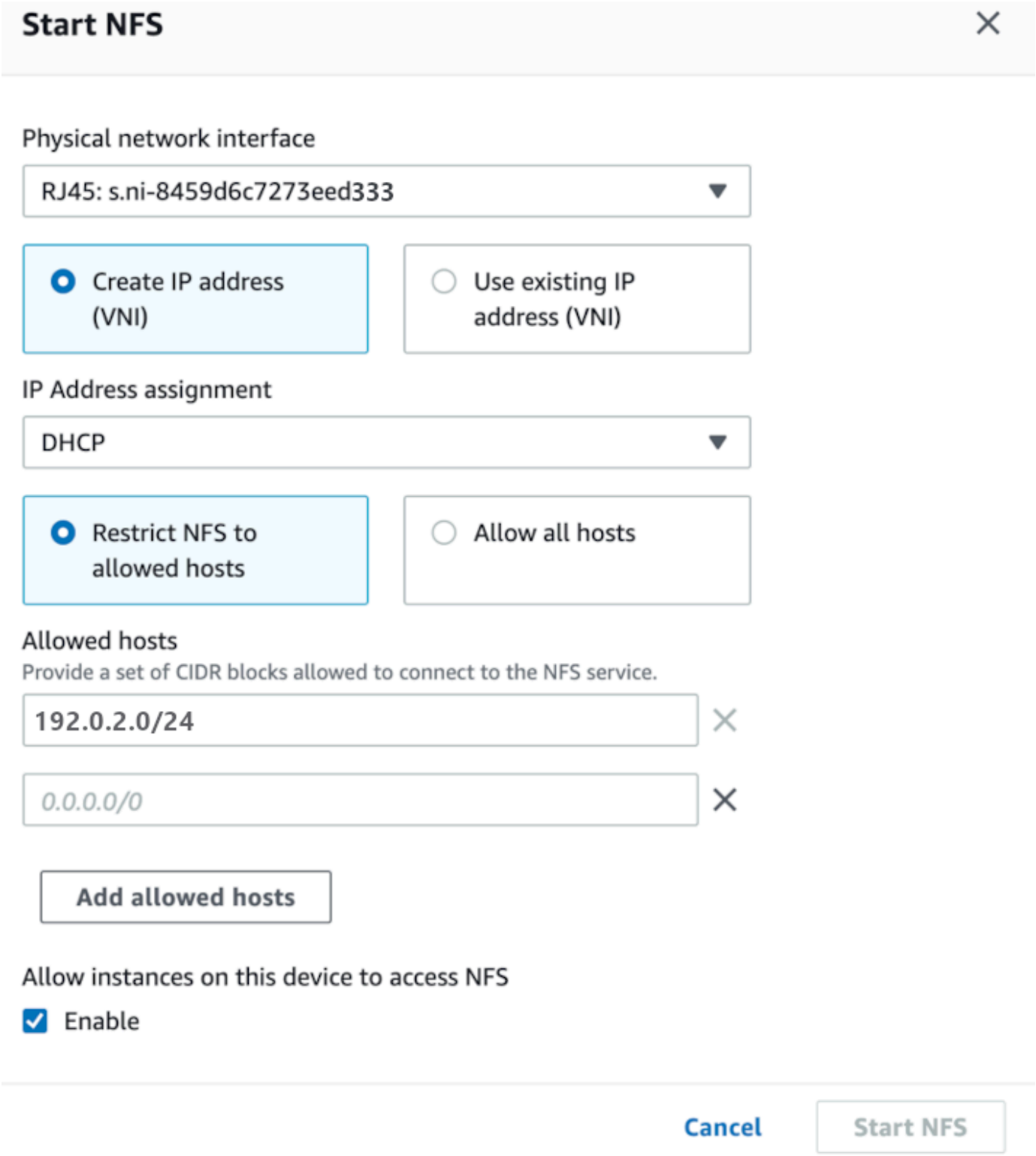
La interfaz NFS no se ejecuta en el dispositivo de la familia Snow de forma predeterminada, por lo que debe iniciarla para permitir la transferencia de datos en el dispositivo. Puede configurar

manualmente la interfaz NFS proporcionando la dirección IP de una interfaz de red virtual (VNI) que se ejecute en el dispositivo de la familia Snow y restringiendo el acceso a su recurso compartido de archivos, si es necesario. Antes de configurar la interfaz NFS manualmente, configure una interfaz de red virtual (VNI) en su dispositivo de la familia Snow. Para obtener más información, consulte Network Configuration for Compute Instances.

También puede hacer que el dispositivo de la familia Snow configure la interfaz NFS automáticamente. Para obtener más información, consulte Configuración automática de la interfaz NFS.

1. En la parte inferior de la sección Transferir datos en el panel, elija Configurar manualmente.

2. Elija Habilitar e iniciar para abrir el asistente Iniciar NFS. Se rellena el campo Interfaz de red física.



3. Elija Crear dirección IP (VNI) o elija Usar la dirección IP existente.

4. Si elige Crear dirección IP (VNI), elija DHCP o IP estática en el cuadro de lista Asignación de dirección IP.

   > **Important**
   >
   > Si utiliza una red DHCP, es posible que el servidor DCHP reasigne la dirección IP de la interfaz NFS. Esto puede suceder después de desconectar el dispositivo y reciclar las direcciones IP. Si establece un rango de hosts permitido y la dirección del cliente cambia, otro cliente puede elegir esa dirección. En este caso, el nuevo cliente tendrá acceso al recurso compartido. Para evitarlo, utilice reservas de DHCP o direcciones IP estáticas.

   Si elige Usar una dirección IP existente, elija una interfaz de red virtual en el cuadro de lista Interfaz de red virtual.

5. Elija restringir el acceso a la interfaz NFS y proporcionar un bloque de direcciones de red permitidas, o permitir que cualquier dispositivo de la red acceda a la interfaz NFS del dispositivo de la familia Snow.

   - Para restringir el acceso a la interfaz NFS en el dispositivo de la familia Snow, seleccione Restringir NFS a los hosts permitidos. En Hosts permitidos, introduzca un conjunto de bloques CIDR. Si desea permitir el acceso a más de un bloque CIDR, introduzca otro conjunto de bloques. Para eliminar un conjunto de bloques, seleccione la X situada junto al campo que contiene los bloques. Selecciona Añadir anfitriones permitidos.

     > **Note**
     >
     > Si selecciona Restringir el NFS a los hosts permitidos y no proporciona los bloques CIDR permitidos, el dispositivo de la familia Snow denegará todas las solicitudes de montaje de la interfaz NFS.

   - Para permitir que cualquier dispositivo de la red acceda a la interfaz NFS, seleccione Permitir todos los hosts.

6. Para permitir que las instancias compatibles con EC2 que se ejecutan en el dispositivo de la familia Snow accedan al adaptador NFS, seleccione Activar.

7. Elija Iniciar NFS. Podría tardar uno o dos minutos en iniciarse.

> **Important**
>
> No apague el dispositivo de la familia Snow mientras se esté iniciando la interfaz NFS.

En la sección Recursos del sistema de archivos de red (NFS), el estado de la interfaz NFS aparece como Activo. Necesitará la dirección IP indicada para montar la interfaz como almacenamiento local en los ordenadores cliente.

Administración de los puntos finales NFS en el dispositivo de la familia Snow

Cada depósito S3 del dispositivo de la familia Snow se representa como un punto final y aparece en las rutas de montaje. Una vez iniciada la interfaz NFS, monte un punto final para transferir archivos hacia o desde ese punto final. Solo se puede montar un punto final a la vez. Para montar un punto final diferente, desmonte primero el punto final actual.

Para montar un punto final

1. En la sección Rutas de montaje, realice una de las siguientes acciones para seleccionar un punto final:
   - En el campo Filtrar puntos de enlace, introduzca todo o parte del nombre de un depósito para filtrar la lista de puntos finales disponibles en su entrada y, a continuación, seleccione el punto final.
   - Elija el punto final que desee montar en la lista de rutas de montaje.
2. Elija el punto final Mount NFS. El dispositivo de la familia Snow monta el terminal para su uso.

Para desmontar un punto final

1. En la sección Rutas de montaje, elija el punto final que desee desmontar.
2. Seleccione Desmontar el punto final. El dispositivo de la familia Snow desmonta el terminal y ya no está disponible para su uso.

> **Note**
>
> Antes de desmontar un terminal, asegúrese de que no se estén copiando datos desde o hacia él.

Montaje de puntos finales NFS en ordenadores cliente

Una vez iniciada la interfaz NFS y montado un punto final, monte el punto final como almacenamiento local en los ordenadores cliente.

1. En Rutas de montaje, elija el icono de copia del punto final que desee montar. Péguelo en su sistema operativo al montar el punto final.
2. Los siguientes son los comandos de montaje predeterminados para los sistemas operativos Windows, Linux y 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
     ```

Detener la interfaz NFS

Detenga la interfaz NFS del dispositivo de la familia Snow cuando termine de transferir archivos hacia o desde él.

1. En el panel, elija Servicios y, a continuación, elija Almacenamiento de archivos.
2. En la página Almacenamiento de archivos seleccione Deshabilite la transferencia de datos. Por lo general, los puntos de conexión de NFS tardan hasta dos minutos en desaparecer del panel.

Administración de sus dispositivos

Se usa AWS OpsHub para administrar los dispositivos de la familia Snow. En la página de detalles del dispositivo, puede realizar las mismas tareas que cuando utiliza el AWS CLI, como cambiar el alias del dispositivo, reiniciarlo y comprobar si hay actualizaciones.

Temas

- Reinicio del dispositivo
- Apagado del dispositivo
- Edición del alias del dispositivo
- Administrar los certificados de clave pública mediante OpsHub
- Cómo obtener actualizaciones para su dispositivo y la AWS OpsHub aplicación
- Administración de perfiles

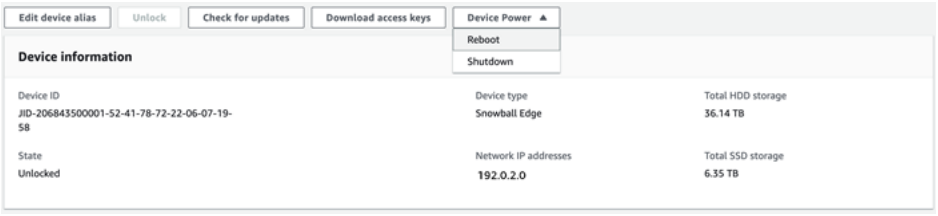
Reinicio del dispositivo

Sigue estos pasos AWS OpsHub para reiniciar tu dispositivo Snow.

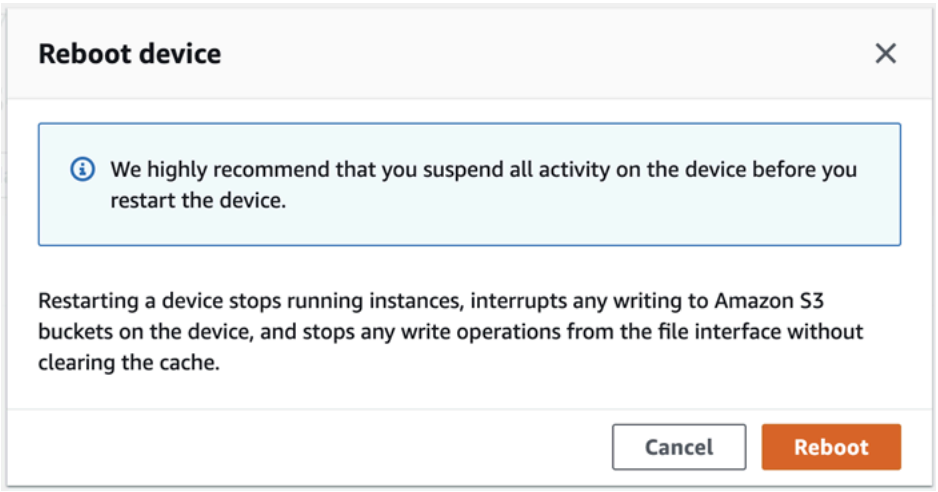
> **Important**
>
> Se recomienda encarecidamente suspender todas las actividades del dispositivo antes de reiniciarlo. Al reiniciar un dispositivo, se detienen las instancias en ejecución e interrumpe cualquier escritura en los buckets de Amazon S3 del dispositivo.

Para reiniciar un dispositivo

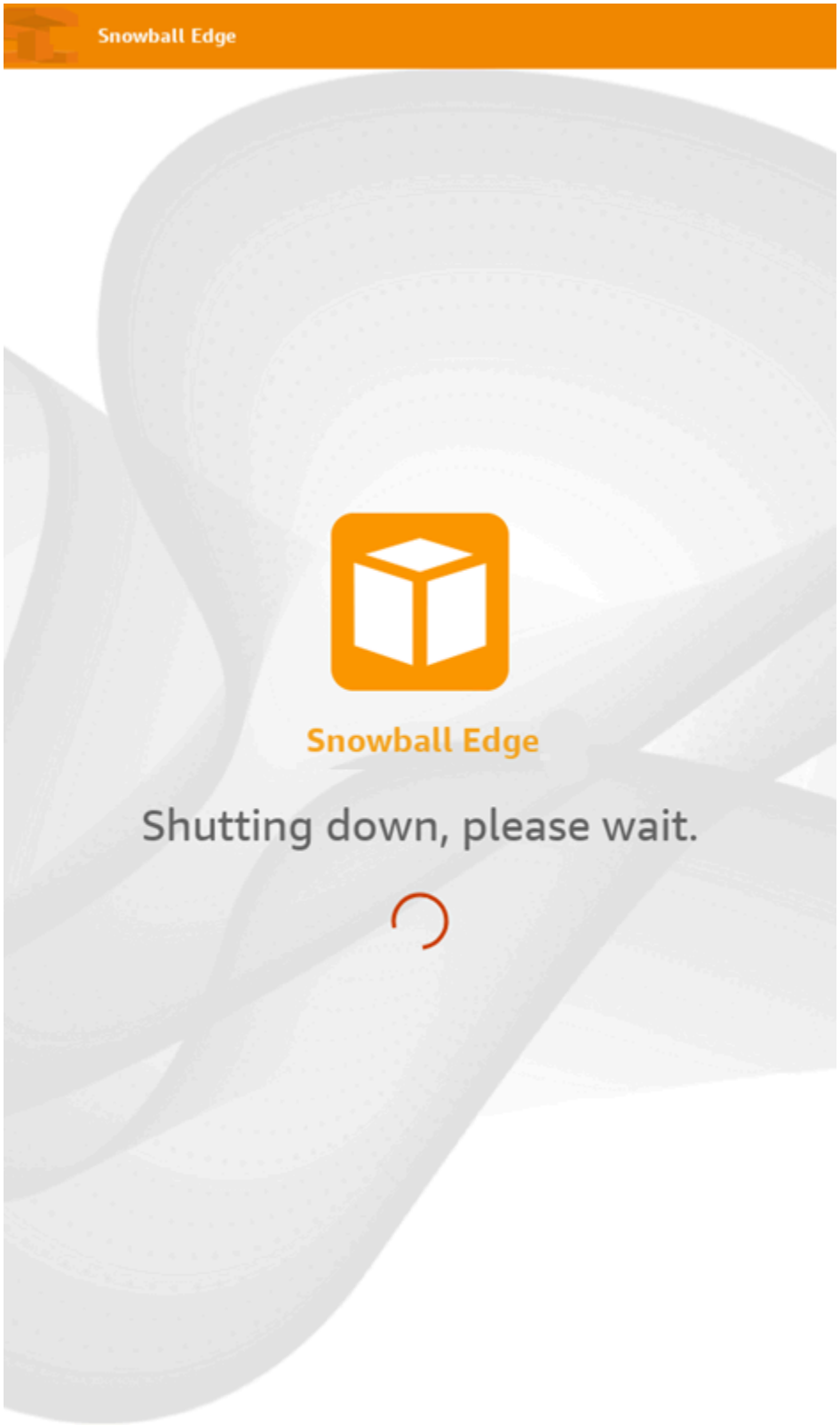
1. En el AWS OpsHub panel de control, busca tu dispositivo en Dispositivos. A continuación, seleccione el dispositivo para abrir la página de detalles del dispositivo.
2. Seleccione el menú Botón de alimentación del dispositivo y, a continuación, seleccione Reiniciar. Aparecerá un cuadro de diálogo.



3. En el cuadro de diálogo, elija Reiniciar. El dispositivo comienza a reiniciarse.



Mientras el dispositivo se apaga, la pantalla LCD muestra un mensaje que indica que el dispositivo se está apagando.


Snowball Edge
Snowball Edge
Shutting down, please wait.

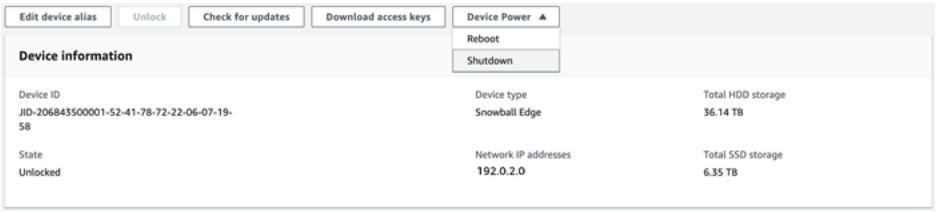
Apagado del dispositivo

Sigue estos pasos AWS OpsHub para apagar tu dispositivo Snow.

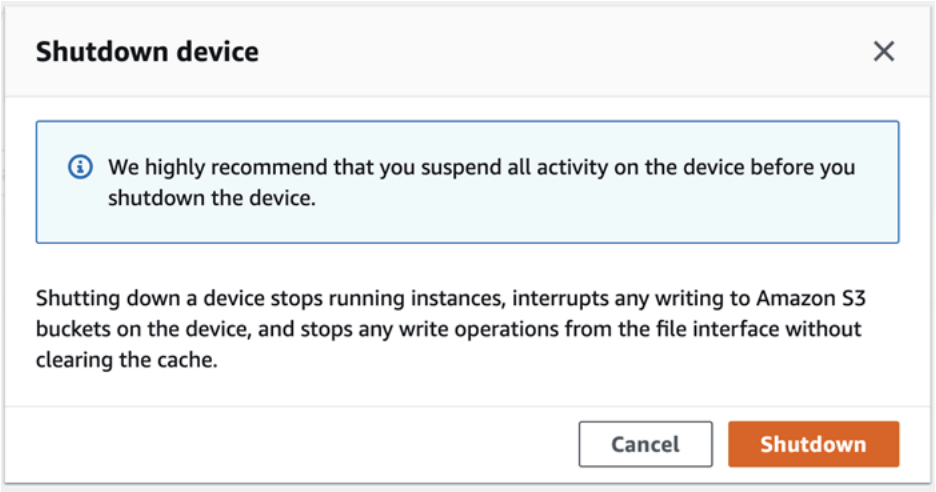
> **Important**
>
> Se recomienda encarecidamente suspender todas las actividades del dispositivo antes de apagarlo. Al apagar un dispositivo, se detienen las instancias en ejecución e interrumpe cualquier escritura en los buckets de Amazon S3 del dispositivo.

Para apagar un dispositivo

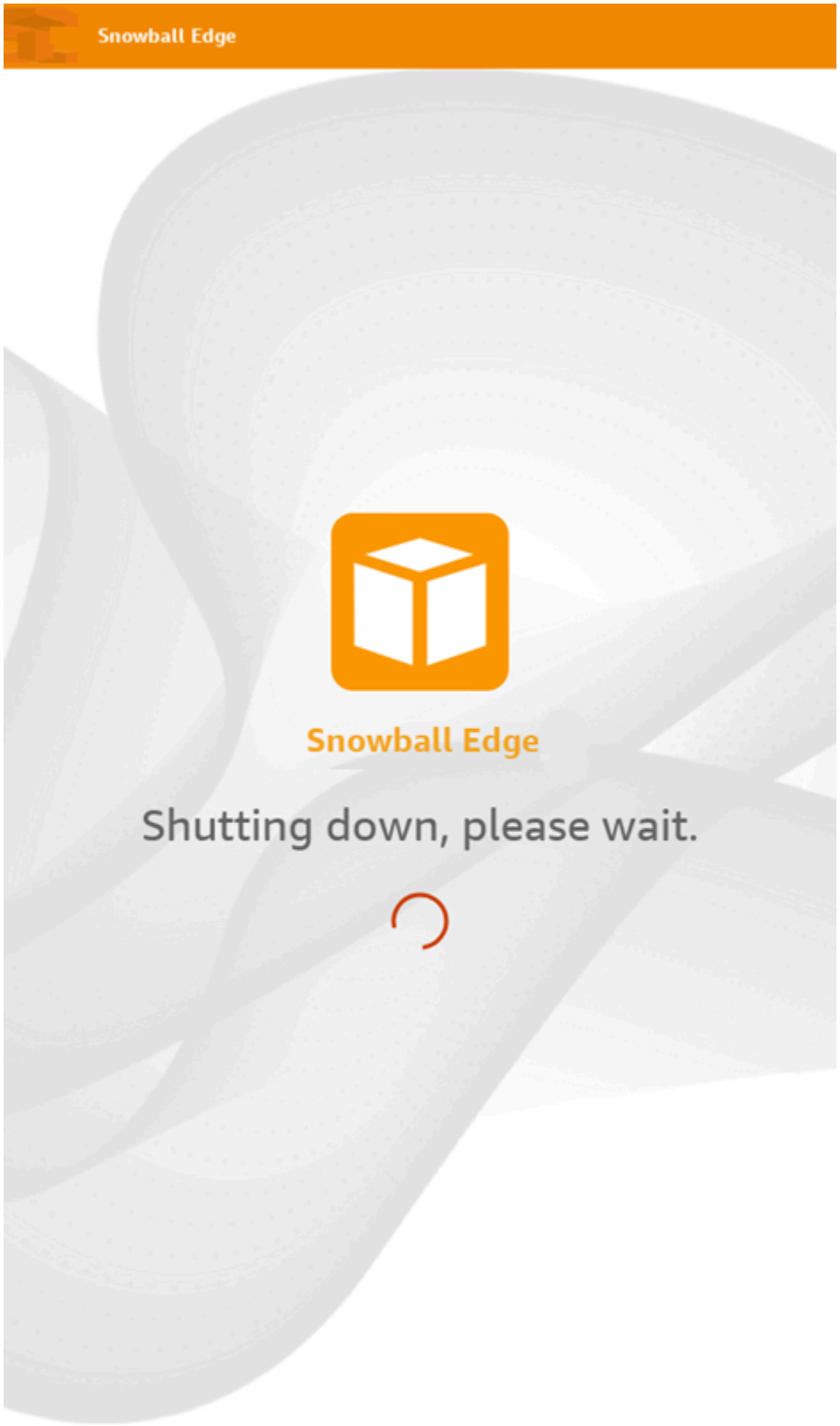
1. En el AWS OpsHub panel de control, busca tu dispositivo en Dispositivos. A continuación, seleccione el dispositivo para abrir la página de detalles del dispositivo.
2. Seleccione el menú Botón de alimentación del dispositivo y, a continuación, seleccione Apagar. Aparecerá un cuadro de diálogo.



3. En el cuadro de diálogo, elija Apagar. El dispositivo empieza a apagarse.



Mientras el dispositivo se apaga, la pantalla LCD muestra un mensaje que indica que el dispositivo se está apagando.

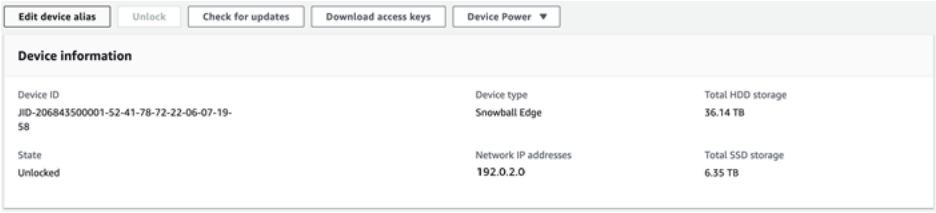

Snowball Edge
Snowball Edge
Shutting down, please wait.

Edición del alias del dispositivo

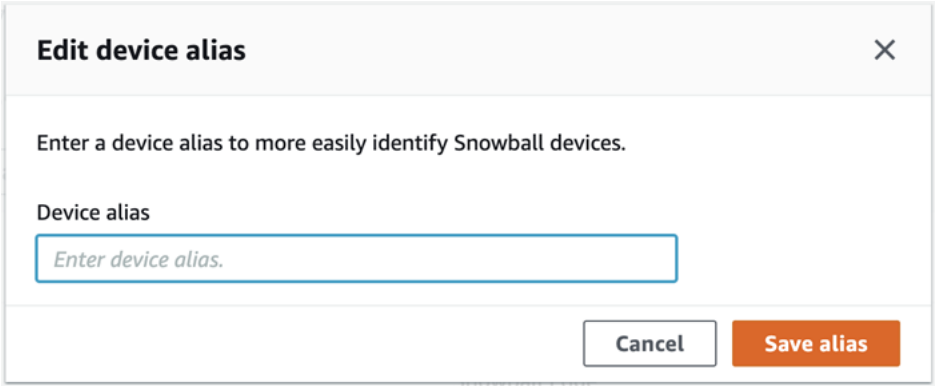
Sigue estos pasos para editar el alias de tu dispositivo utilizando AWS OpsHub.

Para editar el alias de un dispositivo

1. En el AWS OpsHub panel de control, busca tu dispositivo en Dispositivos. Seleccione el dispositivo para abrir la página de detalles del dispositivo.
2. Seleccione la pestaña Editar el alias del dispositivo.



3. En Alias del dispositivo, escriba un nuevo nombre y seleccione Guardar alias.



Administrar los certificados de clave pública mediante OpsHub

Puede interactuar de forma segura con AWS los servicios que se ejecutan en un dispositivo Snowball Edge o en un clúster de dispositivos Snowball Edge mediante el protocolo HTTPS proporcionando un certificado de clave pública. Puede utilizar el protocolo HTTPS para interactuar con AWS servicios como IAM, Amazon EC2, el adaptador S3, el almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow, Amazon EC2 Systems Manager AWS STS y los dispositivos Snowball Edge. En el caso de un clúster de dispositivos, se requiere un único certificado que cualquier dispositivo del clúster puede generar. Una vez que un dispositivo Snowball Edge genera el certificado y usted lo desbloquea, puede utilizar comandos del cliente de Snowball Edge para enumerar, obtener y eliminar el certificado.

Un dispositivo Snowball Edge genera un certificado cuando se producen los siguientes eventos:

- El dispositivo o el clúster de Snowball Edge se desbloquea por primera vez.
- El dispositivo o clúster Snowball Edge se desbloquea tras eliminar el certificado (mediante el `delete-certificate` comando o Renovar certificado en). AWS OpsHub
- El dispositivo o el clúster de Snowball Edge se reinicia y desbloquea cuando caduca el certificado.

Cada vez que se genera un certificado nuevo, el certificado anterior deja de ser válido. Un certificado es válido durante un año a partir del día en que se generó.

También puede utilizar el cliente de Snowball Edge para administrar certificados de clave pública. Para obtener más información, consulte Administración de certificados de clave pública.

Temas

- Descargue el certificado de clave pública mediante OpsHub
- Renovar el certificado de clave pública mediante OpsHub

Descargue el certificado de clave pública mediante OpsHub

Puede descargar el certificado de clave pública activo en su equipo.

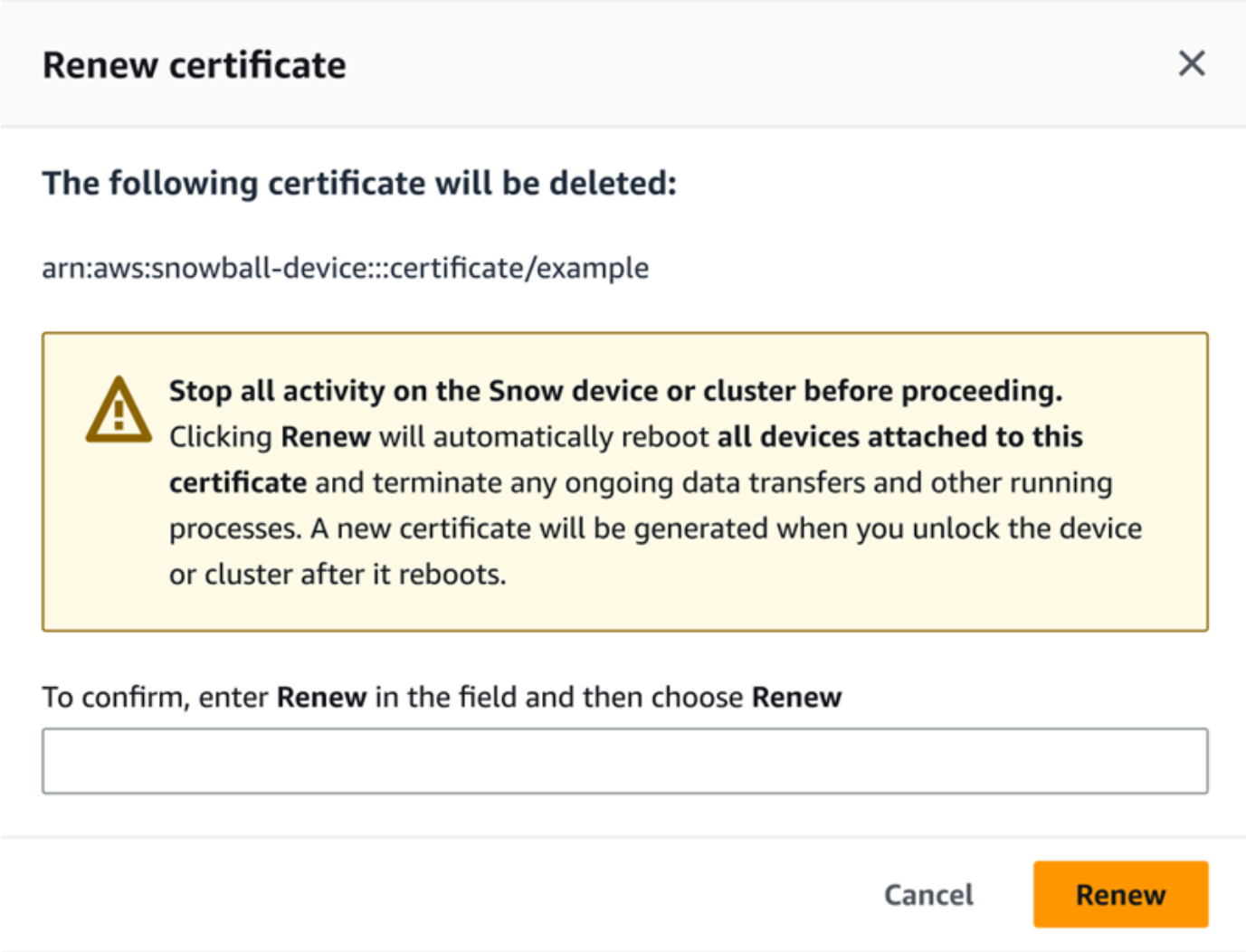
1. En el AWS OpsHub panel de control, busca tu dispositivo en Dispositivos. Seleccione el dispositivo para abrir la página de detalles del dispositivo.
2. En la página de detalles del dispositivo, seleccione el menú Administrar certificado. En el menú, seleccione Descargar certificado.
3. Aparece una ventana en la que puede asignar un nombre al archivo de certificado que desea descargar y elegir la ubicación del equipo en la que se descargará. Seleccione Guardar.

Renovar el certificado de clave pública mediante OpsHub

Antes de renovar el certificado de clave pública, detenga todas las transferencias de datos hacia o desde el dispositivo Snow Family y detenga todo el almacenamiento compatible con EC2 que esté en ejecución. Para obtener más información, consulte Detener una instancia compatible con Amazon EC2 en esta guía.

1. En el AWS OpsHub panel de control, busque su dispositivo en Dispositivos. Seleccione el dispositivo para abrir la página de detalles del dispositivo.

2. En la página de detalles del dispositivo, seleccione el menú Administrar certificado. En el menú, seleccione Renovar certificado.
3. En la ventana Renovar certificado, introduzca **Renew** en el campo y seleccione Renovar. El dispositivo Snow Family elimina el certificado de clave pública existente y reinicia el dispositivo o el clúster.



Cómo obtener actualizaciones para su dispositivo y la AWS OpsHub aplicación

Puede buscar actualizaciones para su dispositivo e instalarlas. También puede configurarla AWS OpsHub para que actualice automáticamente la aplicación a la última versión.

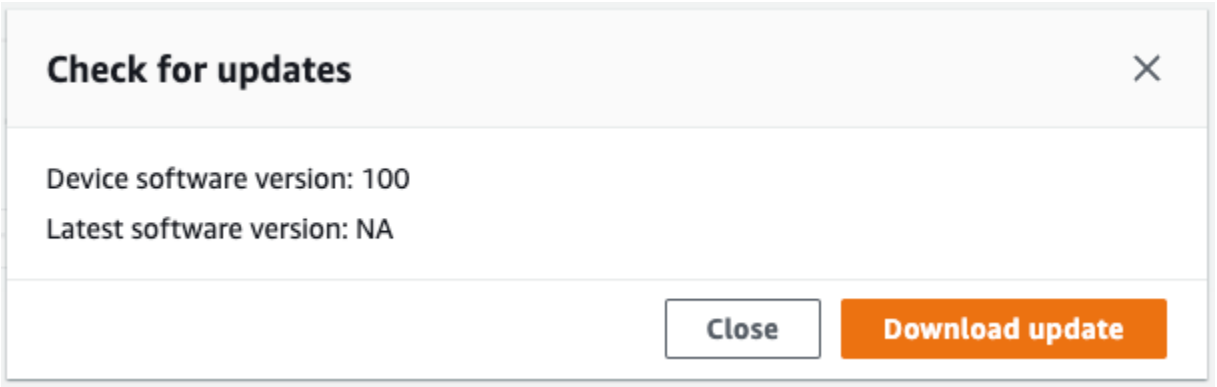
Actualización del dispositivo

Sigue estos pasos AWS OpsHub para actualizar tu dispositivo Snow.

Para actualizar el dispositivo

1. En el AWS OpsHub panel de control, busca tu dispositivo en Dispositivos. Seleccione el dispositivo para abrir la página de detalles del dispositivo.
2. Seleccione la pestaña Buscar actualizaciones.

   La página Buscar actualizaciones muestra la versión actual del software del dispositivo y la versión más reciente del software, si la hay.



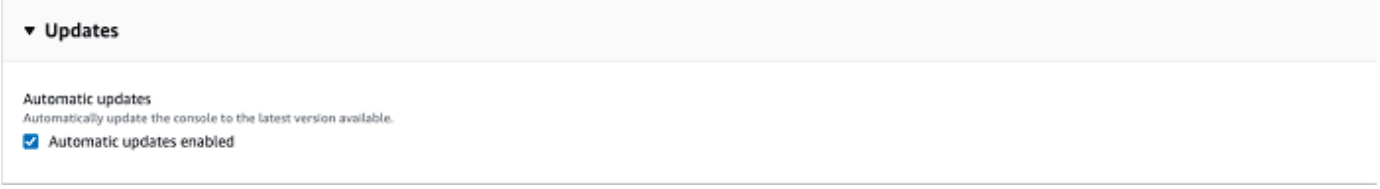
3. Si hay alguna actualización, seleccione Descargar actualización. De lo contrario, seleccione Cerrar.

Actualización de AWS OpsHub la aplicación

AWS OpsHub actualiza automáticamente la aplicación a la última versión. Siga estos pasos para comprobar que la actualización automática está habilitada.

Para comprobar que las actualizaciones automáticas están habilitadas para AWS OpsHub

1. En el AWS OpsHub panel, selecciona Preferencias.
2. Abra la pestaña Actualizaciones.
3. Compruebe que la opción Actualizaciones automáticas habilitadas está seleccionada. La actualización automática está habilitada de forma predeterminada.



Si no está seleccionada la opción Actualizaciones automáticas, no obtendrá la última versión de la AWS OpsHub aplicación.

Administración de perfiles

Puede crear un perfil para almacenar de forma persistente sus credenciales en el sistema de archivos local. Si lo usa AWS OpsHub, tiene la opción de crear un nuevo perfil cada vez que desbloquee el dispositivo utilizando la dirección IP del dispositivo, el código de desbloqueo y el archivo de manifiesto.

También puede utilizar el cliente de Snowball Edge para crear un perfil en cualquier momento. Consulte Configuración de un perfil para el cliente de Snowball Edge.

Para editar o eliminar perfiles, edite el archivo de perfil en un editor de texto.

Example Archivo **`snowball-edge.config`** de ejemplo

En este ejemplo se muestra un archivo de perfil que contiene tres perfiles: `SnowDevice1profile`, `SnowDevice2profile` y `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":[]
    }
}
```

Para crear un perfil

1. Desbloquee el dispositivo de forma local e inicie sesión según las instrucciones que se indican en Desbloqueo de un dispositivo.
2. Asigne un nombre al perfil y seleccione Guardar nombre de perfil.

Para editar un perfil

1. En un editor de texto, abra `snowball-edge.config` en `home directory\.aws\snowball\config`.
2. Edite el archivo según sea necesario. Por ejemplo, para cambiar la dirección IP de un dispositivo en el perfil, cambie la entrada `defaultEndpoint`.
3. Guarde y cierre el archivo.

Para eliminar un perfil

1. Con un editor de texto, abra `snowball-edge.config` en `home directory\.aws\snowball\config`.

2. Elimine la línea que contiene el nombre del perfil, las llaves { } que hay a continuación del nombre del perfil y el contenido de esas llaves.
3. Guarde y cierre el archivo.

Automatización de las tareas de administración

Puede utilizarlas AWS OpsHub para automatizar las tareas operativas que realiza con frecuencia en sus dispositivos de la familia Snow. Puede crear una tarea para las acciones recurrentes que desee realizar en los recursos, como reiniciar servidores virtuales, detener instancias compatibles con Amazon EC2, etc. Usted proporciona un documento de automatización que realiza las tareas operativas de forma segura y ejecuta la operación con AWS los recursos de forma masiva. También puede programar flujos de trabajo de TI comunes.

> **Note**
>
> No se pueden automatizar tareas en clústeres.
> Para utilizar tareas, primero se debe iniciar el servicio Systems Manager de Amazon EC2. Para iniciar un servicio en su dispositivo Snowball Edge, consulte Inicio de un servicio en su dispositivo Snowball Edge.

Temas

Creación e inicio de una tarea

Al crear una tarea, especifique los tipos de recursos en los que debe ejecutarse la tarea y, a continuación, proporcione un documento de tarea que contenga las instrucciones que ejecutan la tarea. El documento de tarea está en formato YAML o JSON. A continuación, proporcione los parámetros necesarios para la tarea e inicie la tarea.

Cómo crear una tarea

1. En la sección Lanzar tareas del panel, seleccione Comenzar para abrir la página Tareas. Si ha creado tareas, aparecerán en Tareas.
2. Seleccione Crear tarea y proporcione los detalles de la tarea.
3. En Nombre, escriba un nombre único para la tarea.

   > **Tip**
   >
   > El nombre debe tener entre 3 y 128 caracteres. Los caracteres válidos son `a-z`, `A-Z`, `0-9`, `.`, `_` y `-`.

4. Opcionalmente, puede elegir un tipo de destino en la lista Tipo de destino opcional. Este es el tipo de recurso en el que desea que se ejecute la tarea.

   Por ejemplo, puede especificar **`/AWS::EC2::Instance`** para que las tareas se ejecuten en una instancia compatible con Amazon EC2 o **`/`** para que se ejecuten en todos los tipos de recursos.
5. En la sección Contenido seleccione YAML o JSON y proporcione el script que realiza la tarea. Tiene dos opciones: formato YAML o JSON. Para ver ejemplos, consulte Ejemplos de tareas.
6. Seleccione Crear. La tarea que creó aparecerá en la página Tareas.

Para iniciar una tarea

1. En la sección Lanzar tareas del panel, seleccione Comenzar para abrir la página Tareas. Las tareas aparecen en Tareas.
2. Seleccione la tarea para abrir la página Iniciar tarea.
3. Seleccione Ejecución sencilla para que se ejecute en los destinos.

   Seleccione Control de velocidad para que se ejecute de forma segura en varios destinos y definir umbrales de concurrencia y error. En esta opción, proporcione información adicional sobre el destino y el umbral de error en la sección Control de velocidad.
4. Proporcione los parámetros de entrada necesarios y seleccione Iniciar tarea.

   El estado de la tarea es Pendiente y cambia a Correcto cuando la tarea se ha ejecutado correctamente.

Ejemplos de tareas

En el siguiente ejemplo, se reinicia una instancia compatible con Amazon EC2. Requiere dos parámetros de entrada: `endpoint` e `instance ID`.

Ejemplo 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}
```

Ejemplo 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}"
    }
  } ]
}
```

Consulta de los detalles de una tarea

Puede ver los detalles de una tarea de administración, como la descripción y los parámetros necesarios para ejecutar la tarea.

Para ver detalles de una tarea

1. En la sección Lanzar tareas del panel, seleccione Comenzar para abrir la página Tareas.
2. En la página Tareas, busque y seleccione la tarea cuyos detalles desea ver.
3. Seleccione Ver detalles y seleccione una de las pestañas para ver los detalles. Por ejemplo, la pestaña Parámetros muestra los parámetros de entrada del script.

Eliminación de una tarea

Siga estos pasos para eliminar una tarea de administración.

Para eliminar una tarea

1. En la sección Lanzar tareas del panel, seleccione Comenzar para abrir la página Tareas.
2. Busque la tarea que desea eliminar. Seleccione la tarea y a continuación, seleccione Eliminar.

Configuración de los servidores de tiempo NTP del dispositivo

Siga estos pasos para ver y actualizar con qué servidores de tiempo debe sincronizar la hora su dispositivo.

Para comprobar las fuentes de tiempo

1. En el AWS OpsHub panel de control, busca tu dispositivo en Dispositivos. Seleccione el dispositivo para abrir la página de detalles del dispositivo.
2. En la tabla Fuentes de tiempo verá una lista de fuentes de tiempo con las que el dispositivo está sincronizando la hora.

   La tabla Fuentes de tiempo tiene cuatro columnas:

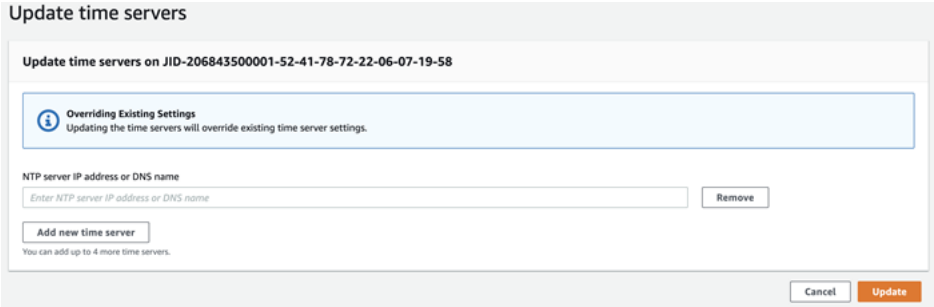
   - Address: el nombre DNS o la dirección IP de la fuente de tiempo
   - State: el estado actual de la conexión entre el dispositivo y esa fuente de tiempo. Hay 5 estados posibles:

  - CURRENT: la fuente de tiempo se está utilizando actualmente para sincronizar la hora
  - COMBINED: la fuente de tiempo se combina con la fuente actual
  - EXCLUDED: el algoritmo de combinación excluye la fuente de tiempo
  - LOST: se ha perdido la conexión con la fuente de tiempo
  - UNAVAILABILITY: una fuente de tiempo no válida en la que el algoritmo de combinación ha resultado ser inexacto o presenta demasiada variabilidad

- Type: las fuentes del Network Time Protocol (NTP) pueden ser un servidor o un par. El usuario puede configurar un servidor mediante el comando update-time-server, mientras que un par solo se puede configurar mediante otros dispositivos Snowball Edge del clúster y se configura automáticamente cuando se asocia el clúster.
- Stratum: el stratum de la fuente. Stratum 1 indica una fuente con un reloj de referencia conectado localmente. Una fuente que está sincronizada con una fuente Stratum 1 se establece en Stratum 2. Una fuente que está sincronizada con una fuente Stratum 2 se establece en Stratum 3 y así sucesivamente.

Para actualizar los servidores de tiempo

1. En el AWS OpsHub panel de control, busca tu dispositivo en Dispositivos. Seleccione el dispositivo para abrir la página de detalles del dispositivo.
2. En la tabla Fuentes de tiempo verá una lista de fuentes de tiempo con las que el dispositivo está sincronizando la hora.
3. Seleccione Actualizar servidores de tiempo en la tabla Fuentes de tiempo.
4. Introduzca el nombre DNS o la dirección IP de los servidores de tiempo con los que desea que su dispositivo sincronice la hora y seleccione Actualizar.



Tipos de dispositivos NTP y versiones de software compatibles

NTP no está disponible en ningún tipo de dispositivo de almacenamiento y computación de la versión 2. Sin embargo, los tipos de dispositivos de almacenamiento y computación de la versión 3 de Snowball Edge cuya versión del software es la 77 u otra posterior sí admiten NTP. Para comprobar si NTP está habilitado, utilice el comando `describe-time-sources` de la CLI de Snowball Edge.

Uso de un dispositivo AWS Snowball Edge

A continuación, encontrará una descripción general del AWS Snowball Edge dispositivo. Snowball Edge es un dispositivo físicamente robusto protegido por AWS Key Management Service (AWS KMS) que se utiliza para el almacenamiento y la computación locales, o para transferir datos entre sus servidores locales y Amazon Simple Storage Service (Amazon S3).

Para obtener información sobre cómo desbloquear un AWS Snowball Edge dispositivo, consulte. Desbloquear el dispositivo de la familia Snow

Al recibir el dispositivo, inspecciónelo para ver si ha sufrido daños o alteraciones evidentes.

> **Warning**
>
> Si observa cualquier indicio sospechoso en el dispositivo , no lo conecte a la red interna. En su lugar, contacte con AWS Support y se le enviará uno nuevo.

La siguiente imagen muestra el aspecto del AWS Snowball Edge dispositivo.

Tiene tres puertas: una delantera, otra posterior y una superior. Todas ellas se abren mediante pestañas. La puerta superior contiene el cable de alimentación del dispositivo. Las otras dos puertas se pueden abrir y deslizar en el interior del dispositivo, para que no estorben mientras se utiliza. Al abrir las puertas, puede obtener acceso a la pantalla LCD de tinta electrónica integrada en la parte delantera del dispositivo y a los puertos de alimentación y red de la parte posterior.

Una vez que el dispositivo llega y se enciende, está listo para utilizarse.

Temas

- Uso de los comandos del cliente Snowball Edge
- Transferencia de archivos mediante el adaptador de Amazon S3 para la migración de datos
- Administración de la interfaz NFS
- Uso de AWS IoT Greengrass para ejecutar software preinstalado en instancias compatibles con Amazon EC2

- Uso AWS Lambda con un AWS Snowball borde
- Uso de instancias de computación compatibles con Amazon EC2
- Uso del almacenamiento compatible con Amazon S3 en dispositivos Snow Family
- Uso de Amazon EKS Anywhere on AWS Snow
- Uso local de IAM
- Uso AWS Security Token Service
- Administración de certificados de clave pública
- Puertos necesarios para usar AWS los servicios en un dispositivo AWS Snowball perimetral

Uso de los comandos del cliente Snowball Edge

A continuación, encontrará información sobre los comandos del cliente Snowball Edge para su uso con los dispositivos de la familia Snow. Cada comando incluye ejemplos de uso y ejemplos de resultados. El cliente Snowball Edge es una aplicación de línea de comandos independiente que se ejecuta en el dispositivo para desbloquear el dispositivo de la familia Snow y configurarlo y controlarlo. También puede utilizar el cliente con clústeres de dispositivos de la familia Snow. Cuando utilice el cliente de Snowball Edge, puede obtener información de soporte adicional si ejecuta el comando `snowballEdge help`.

Para descargar el cliente de Snowball Edge, consulte. Descarga e instalación del cliente de Snowball Edge

Temas

- Configuración de un perfil para el cliente de Snowball Edge
- Obtención del código QR para validación por NFC
- Versión del cliente de Snowball Edge
- Desbloqueo de dispositivos Snowball Edge
- Actualización de un dispositivo Snowball Edge
- Obtención de credenciales
- Inicio de un servicio en su dispositivo Snowball Edge
- Detención de un servicio en su dispositivo Snowball Edge
- Inicio de NFS y restricción del acceso
- Restricción del acceso a recursos compartidos de NFS cuando NFS está en ejecución

- AWS Snowball Edge Registros
- Obtención del estado de los dispositivos
- Obtención del estado de los servicios
- Eliminación de un nodo de un clúster
- Adición de un nodo a un clúster
- Creación de etiquetas para su dispositivo
- Eliminación de etiquetas de su dispositivo
- Descripción de etiquetas en su dispositivo
- Crear una interfaz de red directa
- Obtener información sobre una interfaz de red directa
- Actualización de una interfaz de red directa
- Eliminar una interfaz de red directa
- Cree una interfaz de red virtual (VNI)
- Obtener información sobre una interfaz de red virtual
- Actualización de una interfaz de red virtual
- Eliminar una interfaz de red virtual
- Comprobación del estado de las características
- Configuración de servidores de tiempo
- Comprobación de las fuentes de tiempo
- Actualización del tamaño de la MTU

Configuración de un perfil para el cliente de Snowball Edge

Cada vez que ejecute un comando para el cliente de Snowball Edge, debe proporcionar el archivo de manifiesto, el código de desbloqueo y una dirección IP. Puede obtener los dos primeros desde la API de administración de trabajos Consola de administración de la familia de productos Snow de AWS o desde la misma. Para obtener más información sobre cómo obtener el manifiesto y el código de desbloqueo, consulte Obtener credenciales para acceder a un dispositivo de la familia Snow.

Si lo desea, puede utilizar el comando `snowballEdge configure` para almacenar la ruta al manifiesto, el código de desbloqueo de 29 caracteres y el punto de conexión como un perfil. Tras la configuración, puede utilizar otros comandos del cliente de Snowball Edge sin tener que escribir manualmente estos valores para un trabajo determinado. Después de configurar el cliente

de Snowball Edge, la información se guarda en un formato JSON de texto no cifrado en *home directory*/.aws/snowball/config/snowball-edge.config.

El punto de conexión es la dirección IP, a la que se añade https://. Puede localizar la dirección IP del AWS Snowball Edge dispositivo en la pantalla LCD del AWS Snowball Edge dispositivo. Cuando el AWS Snowball Edge dispositivo se conecta a la red por primera vez, obtiene automáticamente una dirección IP de DHCP, si hay un servidor DHCP disponible. Si desea utilizar otra dirección IP, puede cambiarla en la pantalla LCD. Para obtener más información, consulte Uso de un dispositivo AWS Snowball Edge.

> **Important**
>
> Cualquier persona que pueda obtener acceso al archivo de configuración puede obtener acceso a los datos de sus dispositivos o clústeres de Snowball Edge. La administración del control de acceso local para este archivo es una de sus responsabilidades administrativas.

Uso

Puede utilizar este comando de dos formas: insertado o cuando se le solicite. Este ejemplo de uso muestra el método cuando se le solicite.

```
snowballEdge configure
```

Example Salida

```
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
```

Puede tener varios perfiles si tiene varios trabajos a la vez, o si desea poder administrar un clúster desde diferentes puntos de conexión. Para obtener más información sobre varios AWS CLI perfiles, consulte Perfiles con nombre en la Guía del AWS Command Line Interface usuario.

Obtención del código QR para validación por NFC

Puede utilizar este comando para generar un código QR específico del dispositivo para su uso con la aplicación AWS Snowball Edge Verification. Para obtener más información sobre la validación por NFC, consulte Validación de etiquetas NFC.

Uso

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

Example Salida

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

Versión del cliente de Snowball Edge

Utilice el comando `version` para ver la versión del cliente de la interfaz de línea de comandos (CLI) de Snowball Edge.

Uso

```
snowballEdge version
```

Ejemplo de resultado

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

Desbloqueo de dispositivos Snowball Edge

Para desbloquear un AWS Snowball Edge dispositivo independiente, ejecute el `snowballEdge unlock-device` comando. Para desbloquear un clúster, use el comando `snowballEdge unlock-cluster`. Estos comandos sirven para autenticar su acceso al dispositivo AWS Snowball Edge .

> **Note**
>
> Para desbloquear los dispositivos asociados a su trabajo, deben estar in situ, conectados a la alimentación eléctrica y a la red y encendidos. Además, la pantalla LCD de la parte frontal del AWS Snowball Edge dispositivo debe indicar que el dispositivo está listo para su 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 desbloqueo de un solo dispositivo

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

Example Salida de desbloqueo de un solo dispositivo

```
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 en un clúster

Al desbloquear un clúster, debe proporcionar el punto de conexión de uno de los nodos y todas las direcciones IP de los demás dispositivos del clúster.

```
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 Salida de desbloqueo de un clúster

```
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.
```

Actualización de un dispositivo Snowball Edge

Utilice los siguientes comandos para descargar e instalar actualizaciones de un dispositivo Snowball Edge. Para obtener información sobre los procedimientos que utilizan estos comandos, consulte Actualización del software en dispositivos Snowball Edge.

`snowballEdge check-for-updates`: devuelve información sobre la versión del software de Snowball Edge disponible en la nube, así como la versión actual instalada en el dispositivo.

Uso (cliente de Snowball Edge configurado)

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

Example Salida

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

`snowballEdge describe-device-software`: devuelve la versión actual del software y la fecha de caducidad del certificado SSL del dispositivo. Además, si se está descargando o instalando una actualización, también se muestra su estado. A continuación, se muestra una lista de las posibles salidas:

- NA: actualmente no hay ninguna actualización de software en curso.
- `Downloading`: se está descargando software nuevo.
- `Installing`: se está instalando software nuevo.
- `Requires Reboot`: se ha instalado software nuevo y es necesario reiniciar el dispositivo.

> **Warning**
>
> Se recomienda encarecidamente suspender todas las actividades del dispositivo antes de reiniciarlo. Al reiniciar un dispositivo, se detienen las instancias en ejecución e interrumpe cualquier escritura en los buckets de Amazon S3 del dispositivo. Todos estos procesos pueden ocasionar pérdida de datos.

Uso (cliente de Snowball Edge configurado)

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

Example Salida

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

`snowballEdge download-updates`: inicia la descarga de las actualizaciones de software más recientes para el dispositivo Snowball Edge.

Uso (cliente de Snowball Edge configurado)

```
snowballEdge download-updates
```

Example Salida

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

`snowballEdge install-updates`: inicia la instalación de las actualizaciones de software más recientes para el dispositivo Snowball Edge que ya se han descargado.

Uso (cliente de Snowball Edge configurado)

```
snowballEdge install-updates
```

Example Salida

```
Installation started.
```

`snowballEdge reboot-device`: reinicia el dispositivo.

> **Warning**
>
> Se recomienda encarecidamente suspender todas las actividades del dispositivo antes de reiniciarlo. Al reiniciar un dispositivo, se detienen las instancias en ejecución e interrumpe cualquier escritura en los buckets de Amazon S3 del dispositivo. Todos estos procesos pueden ocasionar pérdida de datos.

Uso (cliente de Snowball Edge configurado)

```
snowballEdge reboot-device
```

Example Salida

```
Rebooting device now.
```

`snowballEdge configure-auto-update-strategies`: configura una estrategia de actualización automática.

Uso (cliente de Snowball Edge 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 Salida

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

`snowballEdge describe-auto-update-strategies`: devuelve cualquier estrategia de actualización automática configurada actualmente.

Uso (cliente de Snowball Edge configurado)

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

Example Salida

```
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;
]}
```

Obtención de credenciales

Con los `snowballEdge get-secret-access-key` comandos `snowballEdge list-access-keys` y, puede obtener las credenciales del usuario administrador de su cuenta Cuenta de AWS de Snowball Edge. Puede utilizar estas credenciales para crear AWS Identity and Access Management (usuarios de IAM) y funciones, y para autenticar sus solicitudes cuando utilice AWS CLI o utilice un SDK. AWS Estas credenciales están asociadas exclusivamente a un único trabajo de Snowball Edge y solo se pueden utilizar en el dispositivo o el clúster de dispositivos. El dispositivo o los dispositivos no tienen ningún permiso de IAM en la Nube de AWS.

> **Note**
>
> Si lo utiliza AWS CLI con Snowball Edge, debe utilizar estas credenciales al configurar la CLI. Para obtener información sobre cómo configurar las credenciales para la AWS CLI, consulte Configuración de la AWS CLI en la Guía del AWS Command Line Interface usuario.

Uso (cliente de Snowball Edge configurado)

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

Example Salida

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

Uso (cliente de Snowball Edge configurado)

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

Example Salida

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

Inicio de un servicio en su dispositivo Snowball Edge

Los dispositivos Snowball Edge admiten numerosos servicios, además de Amazon S3. Entre ellas se incluyen las instancias de procesamiento, la interfaz de archivos y AWS IoT Greengrass. Amazon S3 y Amazon EC2 siempre están activados de forma predeterminada y no se pueden detener ni reiniciar con el cliente de Snowball Edge. Sin embargo, la interfaz de archivos se AWS IoT Greengrass puede iniciar con el `snowballEdge start-service` comando. Para obtener el ID de servicio para cada servicio, puede usar el comando `snowballEdge list-services`.

Antes de ejecutar este comando, cree una interfaz de red virtual única para enlazar al servicio que va a iniciar. Para obtener más información, consulte Creación de una interfaz de red virtual.

Uso (cliente de Snowball Edge configurado)

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

Example Salida

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

Detención de un servicio en su dispositivo Snowball Edge

Para detener un servicio que se está ejecutando en su dispositivo Snowball Edge, puede usar el comando `snowballEdge stop-service`.

El adaptador Amazon S3, Amazon EC2 y los servicios de IAM no se pueden detener. AWS STS

> **Warning**
>
> Puede producirse pérdida de datos si la interfaz de archivos se detiene antes de que se escriban en el dispositivo los datos que aún están en el búfer. Para obtener más información acerca del uso de la interfaz de archivos, consulte Administración de la interfaz NFS.

> **Note**
>
> Al detener el almacenamiento compatible con Amazon S3 en dispositivos Snow Family, se deshabilita el acceso a los datos almacenados en los buckets de S3 del dispositivo o

el clúster. El acceso se restaura cuando se vuelve a iniciar el almacenamiento compatible con Amazon S3 en los dispositivos Snow Family. Para los dispositivos con almacenamiento compatible con Amazon S3 en dispositivos Snow Family, se recomienda iniciar el servicio después de encender el dispositivo Snowball Edge. Consulte Configuración de Snowball Edge en esta guía.

Uso (cliente de Snowball Edge configurado)

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

Example Salida

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

Inicio de NFS y restricción del acceso

Important

No inicie el servicio NFS si piensa utilizar Amazon Elastic Block Store (Amazon EBS). La primera vez que se inicia NFS, todo el almacenamiento se asigna a NFS. No es posible reasignar el almacenamiento de NFS a Amazon EBS, incluso aunque el servicio NFS esté detenido.

Note

Puede proporcionar bloques de CIDR para rangos de IP que puedan montar los recursos compartidos NFS expuestos por el dispositivo. Por ejemplo, `10.0.0.0/16`. Si no proporciona bloques de CIDR permitidos, se denegarán todas las solicitudes de montaje. Tenga en cuenta que los datos transferidos a través de NFS no se cifran en tránsito. Aparte de los hosts permitidos por los bloques de CIDR, Snowcone no proporciona ningún mecanismo de autenticación o autorización para los recursos compartidos de NFS.

Inicie NFS con el comando `snowballEdge start-service`. Para obtener el ID de servicio para el servicio NFS, puede usar el comando `snowballEdge list-services`.

Antes de ejecutar este comando, cree una interfaz de red virtual única para enlazar al servicio que va a iniciar. Para obtener más información, consulte Creación de una interfaz de red virtual. Puede restringir el acceso a los recursos compartidos de archivos y a los datos de sus buckets de Amazon S3 y ver qué restricciones existen actualmente. Para ello, debe asignar bloques de CIDR a los hosts permitidos que pueden obtener acceso a su recurso compartido de archivos y a los buckets de S3 al iniciar el servicio NFS.

Uso (cliente de Snowball Edge 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 Ejemplo de salida

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

Restricción del acceso a recursos compartidos de NFS cuando NFS está en ejecución

Puede restringir el acceso a los recursos compartidos de archivos y a los datos de sus buckets de Amazon S3 una vez que haya iniciado NFS. Puede ver las restricciones que están vigentes actualmente y asignar diferentes restricciones de acceso a cada bucket. Para ello, debe asignar bloques de CIDR a los hosts que pueden obtener acceso a su recurso compartido de archivos y a los buckets de S3 al iniciar el servicio NFS. El siguiente comando es un ejemplo.

Uso (cliente de Snowball Edge 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 las restricciones actuales, utilice el comando `describe-service`.

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

AWS Snowball Edge Registros

Al transferir datos entre el centro de datos en las instalaciones y un dispositivo Snowball Edge, se generan registros automáticamente. Si detecta errores inesperados durante la transferencia de datos al dispositivo, puede utilizar los siguientes comandos para guardar una copia de los registros en el servidor local.

Existen tres comandos relacionados con los registros:

- `list-logs`: devuelve una lista de registros en formato JSON. Esta lista informa sobre el tamaño de los registros en bytes, el ARN de los registros, el ID de servicio de los registros y el tipo de registros.

  Uso (cliente de Snowball Edge configurado)

  ```
  snowballEdge list-logs
  ```

  Example Salida

  ```
  {
    "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`— Descarga una copia de un registro específico de Snowball Edge a su servidor en una ruta específica. `CUSTOMER`los registros se guardan en este `.zip` formato y puede extraer este tipo de registro para ver su contenido. `SUPPORT`los registros están cifrados y solo los pueden leer los AWS Support ingenieros. Puede especificar un nombre y una ruta para el registro.

Uso (cliente de Snowball Edge configurado)

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

Example Salida

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

- `get-support-logs`: descarga una copia de todos los registros de tipo SUPPORT del dispositivo Snowball Edge en la ruta especificada de su servicio.

  Uso (cliente de Snowball Edge configurado)

  Cliente de Snowball Edge

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

  Example Salida

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

> **Important**
>
> El tipo `CUSTOMER` puede contener información confidencial sobre sus propios datos. Para proteger esta información potencialmente confidencial, recomendamos encarecidamente eliminar estos registros una vez que haya terminado con ellos.

Obtención del estado de los dispositivos

Puede determinar el estado y la situación general de sus dispositivos Snowball Edge con los siguientes comandos del cliente de Snowball Edge:

- `describe-device`

  Uso (cliente de Snowball Edge configurado)

```
snowballEdge describe-device
```

Example Salida

```
{
"DeviceId" : "JID-EXAMPLE12345-123-456-7-890",
"UnlockStatus" : {
  "State" : "UNLOCKED"
},
"ActiveNetworkInterface" : {
  "IpAddress" : "192.0.2.0"
},
"PhysicalNetworkInterfaces" : [ {
  "PhysicalNetworkInterfaceId" : "s.ni-EXAMPLEd9ecbf03e3",
  "PhysicalConnectorType" : "QSFP",
  "IpAddressAssignment" : "STATIC",
  "IpAddress" : "0.0.0.0",
  "Netmask" : "0.0.0.0",
  "DefaultGateway" : "192.0.2.1",
  "MacAddress" : "EX:AM:PL:E0:12:34",
  "MtuSize" : "1500"
}, {
  "PhysicalNetworkInterfaceId" : "s.ni-EXAMPLE4c3840068f",
  "PhysicalConnectorType" : "SFP_PLUS",
  "IpAddressAssignment" : "DHCP",
  "IpAddress" : "192.0.2.2",
  "Netmask" : "255.255.255.0",
  "DefaultGateway" : "192.0.2.1",
  "MacAddress" : "EX:AM:PL:E0:56:78",
  "MtuSize" : "5743"
}, {
  "PhysicalNetworkInterfaceId" : "s.ni-EXAMPLE0a3a6499fd",
  "PhysicalConnectorType" : "RJ45",
  "IpAddressAssignment" : "STATIC",
  "IpAddress" : "0.0.0.0",
  "Netmask" : "0.0.0.0",
  "DefaultGateway" : "192.0.2.1",
  "MacAddress" : "EX:AM:PL:E0:90:12",
  "MtuSize" : "1500"
} ],
"DeviceCapacities" : [ {
```

```
    "Name" : "HDD Storage",
    "Unit" : "Byte",
    "Total" : 39736350227824,
    "Available" : 39707789471744
  }, {
    "Name" : "SSD Storage",
    "Unit" : "Byte",
    "Total" : 6979321856000,
    "Available" : 6884832575488
  }, {
    "Name" : "vCPU",
    "Unit" : "Number",
    "Total" : 52,
    "Available" : 49
  }, {
    "Name" : "Memory",
    "Unit" : "Byte",
    "Total" : 223338299392,
    "Available" : 216895848448
  }, {
    "Name" : "GPU",
    "Unit" : "Number",
    "Total" : 0,
    "Available" : 0
  } ],
  "DeviceType" : "EDGE_C"
}
```

- `describe-cluster`

  Uso (cliente de Snowball Edge configurado)

```
snowballEdge describe-cluster
```

  Example Salida

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

Obtención del estado de los servicios

Puede determinar el estado y la situación general de los servicios que se ejecutan en dispositivos Snowball Edge con el comando `describe-service`. Puede ejecutar primero el comando `list-services` para ver qué servicios están ejecutándose.

- `list-services`

  Uso (cliente de Snowball Edge configurado)

```
snowballEdge list-services
```

Example Salida

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

- `describe-service`

  Este comando devuelve un valor de estado para un servicio. Incluye información de estado que podría ser útil para resolver problemas que se detecten en el servicio. Los estados son los siguientes.

  - `ACTIVE`: el servicio se está ejecutando y se puede usar.
  - `ACTIVATING`: el servicio se está iniciando pero aún no se puede usar.
  - `DEACTIVATING`: el servicio está cerrándose.
  - `DEGRADED`: para el almacenamiento compatible con Amazon S3 en dispositivos Snow Family, este estado indica que uno o más discos o dispositivos del clúster están inactivos. El almacenamiento compatible con Amazon S3 en dispositivos Snow Family funciona ininterrumpidamente, pero debe recuperar o reemplazar el dispositivo afectado antes de que se pierda el cuórum del clúster para minimizar el riesgo de pérdida de datos. Consulte Información general de la agrupación en clústeres en esta guía.
  - `INACTIVE`: el servicio no se está ejecutando y no se puede usar.

  Uso (cliente de Snowball Edge configurado)

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

  Example Salida

```
{
"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 Salida de servicio de almacenamiento compatible con Amazon S3 en dispositivos Snow Family

El `describe-service` comando proporciona el siguiente resultado para el valor *`s3-snow`* del `service-id` parámetro.

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

Eliminación de un nodo de un clúster

El comando `disassociate-device` elimina un nodo de un clúster de Snowball Edge. Si desea sustituir un nodo en mal estado, utilice este comando. Para obtener más información acerca de los clústeres, consulte Información general de la agrupación en clústeres en esta guía.

> **Important**
>
> Utilice el comando `disassociate-device` solo cuando vaya a eliminar un nodo en mal estado. Este comando falla y devuelve un error si intenta eliminar un nodo en buen estado.

No utilice este comando para eliminar un nodo que se ha apagado o desconectado de la red por accidente y, por lo tanto, no se encuentra disponible temporalmente para el resto del clúster. Los nodos eliminados con este comando no pueden agregarse a ningún clúster y se deben devolver a AWS.

Si un nodo se ha apagado o desconectado de la red por accidente, basta con volver a encender el nodo y conectarlo a la red y utilizar después el comando `associate-device`. No puede utilizar el comando `disassociate-device` para desasociar un nodo si está encendido y en buen estado.

Uso (cliente de Snowball Edge configurado)

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

Example Salida

```
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.
```

Adición de un nodo a un clúster

El comando `associate-device` agrega un nodo a un clúster de dispositivos Snowball Edge. Si apaga un nodo, pasa de estar desbloqueado a bloqueado. Para desbloquear ese nodo, puede utilizar este comando. Puede utilizar este comando para sustituir un nodo que no está disponible por otro que haya pedido como reemplazo. Para obtener más información sobre los clústeres, consulte Información general de la agrupación en clústeres en esta guía.

Uso (cliente de Snowball Edge configurado)

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

Example Salida

```
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.
```

Creación de etiquetas para su dispositivo

Agrega o sobrescribe las etiquetas especificadas en su dispositivo. Puede crear un máximo de 50 etiquetas. Cada etiqueta se compone de un par clave-valor. El valor es opcional.

> **Note**
>
> No incluya información confidencial en sus etiquetas.

Uso (cliente de Snowball Edge configurado)

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

Para obtener más información, ejecute el comando `describe-tags`.

Example Salida

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

Eliminación de etiquetas de su dispositivo

El comando `delete-tags` elimina las etiquetas especificadas de su dispositivo Snowball Edge.

Uso (cliente de Snowball Edge configurado)

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

Para obtener más información, ejecute el comando `describe-tags`.

> **Note**
>
> Si desea eliminar varias etiquetas a la vez, puede especificar varios pares clave-valor, como el siguiente comando:
> `delete-tags --tag Key=Name,Value=test --tag Key=Stage,Value=Beta`
> Si especifica una clave de etiqueta sin un valor de etiqueta, se eliminará cualquier etiqueta que tenga esta clave independientemente de su valor. Si especifica una clave de etiqueta con una cadena vacía como valor de etiqueta, solo se eliminarán las etiquetas que tengan una cadena vacía como valor.

Descripción de etiquetas en su dispositivo

El comando `describe-tags` describe las etiquetas de su dispositivo Snowball Edge.

Uso (cliente de Snowball Edge configurado)

```
snowballEdge describe-tags
```

Para obtener más información, ejecute el comando `describe-tags`.

Example Salida

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

Crear una interfaz de red directa

Utilice el `create-direct-network-interface` comando para crear interfaces de red directas en los dispositivos de la familia Snow. Se debe asociar una interfaz de red directa (DNI) a una instancia de AMI. Puede usar el `vlan` parámetro para asignar un ID de red de área local (VLAN) virtual a la interfaz para etiquetar todo el tráfico de la interfaz con ese ID de VLAN. Además, puede asignar una

dirección de control de acceso al medio (MAC) al DNI con el parámetro. `mac` Si no proporciona el `mac` parámetro y un valor, se asignará automáticamente una dirección MAC.

Puede usar el `describe-device` comando para recuperar el ID de la interfaz de red física. Para obtener más información, consulte Obtención del estado de los dispositivos.

```
snowballEdge create-direct-network-interface --instance-id AMI-instance-id --physical-
network-interface-id physical-network-interface-id --vlan vlan-id --mac MAC-address
```

Example del resultado del **`create-direct-network-interface`** comando

```
{
    "DirectNetworkInterface" : {
        "DirectNetworkInterfaceArn" : "arn:aws:snowball-device:::interface/s.ni-
x8a3b6k1e9n4r2s7o",
        "PhysicalNetworkInterfaceId : "s.ni-p5d2q8r3s9t4u7v1w",
        "InstanceId" : "s.i-g9h2j4k6l8m1n3p5q",
        "Driver" : "mlx5 core",
        "MacAddress" : "1A:2B:3C:4D:5E:6F",
        "MtuSize": "1500"
    }
}
```

Obtener información sobre una interfaz de red directa

Utilice el `describe-direct-network-interface` comando para ver información sobre las interfaces de red directas de un dispositivo de la familia Snow.

```
snowballEdge describe-direct-network-interfaces --endpoint https://snow-device-ip-
address --manifest-file path/to/manifest/file.bin --unlock-code unlock-code
```

Example de la salida del **`descibe-direct-network-interfaces`** comando

```
{
    "DirectNetworkInterface" : {
```

```
        "DirectNetworkInterfaceArn" : "arn:aws:snowball-device:::interface/s.ni-
x8a3b6k1e9n4r2s7o",
        "PhysicalNetworkInterfaceId : "s.ni-p5d2q8r3s9t4u7v1w",
        "InstanceId" : "s.i-g9h2j4k6l8m1n3p5q",
        "Driver" : "mlx5 core",
        "MacAddress" : "1A:2B:3C:4D:5E:6F",
        "MtuSize": "1500"
    }
}
```

Actualización de una interfaz de red directa

Utilice la `update-direct-network-interface` para cambiar las propiedades de una interfaz de red directa (DNI). Al cambiar un DNI adjunto a una instancia compatible con Amazon EC2, la interfaz se desconectará. Para cambiar la unidad de transmisión máxima (MTU) de la interfaz física que utiliza el DNI, utilice el comando. `update-mtu-size` Para obtener más información, consulte Actualización del tamaño de la MTU.

```
snowballEdge update-direct-network-interface --direct-network-interface-
arn directNetworkInterfaceArn //
  --endpoint https://snow-device-ip-address [--mac macAddress] //
  --manifest-file path/to/manifest/file.bin --unlock-code unlock-code //
  [--vlan vlanId] [--attach-instance-id instanceId | --detach]
```

Example de salida de comando **`update-direct-network-interface`**

```
{
    "DirectNetworkInterface" : {
        "DirectNetworkInterfaceArn" : "arn:aws:snowball-device:::interface/s.ni-
x8a3b6k1e9n4r2s7o",
        "PhysicalNetworkInterfaceId : "s.ni-p5d2q8r3s9t4u7v1w",
        "InstanceId" : "s.i-g9h2j4k6l8m1n3p5q",
        "Driver" : "mlx5 core",
        "MacAddress" : "2A:3B:5C:5D:6E:7F",
        "MtuSize": "1500"
    }
}
```

Eliminar una interfaz de red directa

Utilice el `delete-direct-network-interface` comando para eliminar una interfaz de red directa (DNI). Para eliminar un DNI asociado a una instancia de cómputo compatible con Amazon EC2, utilice primero el `detatch` parámetro del `update-direct-network-interface` comando para separar el DNI de la instancia. Para obtener más información, consulte Actualización de una interfaz de red directa.

```
snowballEdge delete-direct-network-interface --direct-network-interface-
arn directNetworkInterfaceArn //
  --endpoint https://snow-device-ip-address --manifest-file path/to/manifest/file.bin
 //
             [--profile profile] --unlock-code unlock-code
```

Example **`delete-direct-network-interface`**del resultado del comando

```
The direct network interface has been deleted from your Snowball Edge. You can
 determine the direct network interfaces available on your Snowball Edge using the
 describe-direct-network-interfaces command.
```

Cree una interfaz de red virtual (VNI)

Utilice el `create-virtual-network-interface` comando para crear interfaces de red virtuales en el dispositivo Snowball Edge. Puede utilizar el `describe-device` comando para recuperar el ID de la interfaz de red física. Para obtener más información, consulte Obtención del estado de los dispositivos.

> **Note**
>
> El `static-ip-address-configuration` parámetro solo es válido cuando se utiliza el `STATIC` valor del `ip-address-assignment` parámetro.

```
snowballEdge create-virtual-network-interface --endpoint https://ip-address-of-snow-
device --manifest-file /path/to/manifest/file.bin --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 de la salida del **`create-virtual-network-interface`** comando

```
{
    "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",
        "MtuSize" : "1500"
    }
}
```

Obtener información sobre una interfaz de red virtual

Utilice el `describe-virtual-network-interface` comando para ver información sobre las interfaces de red virtuales del dispositivo de la familia Snow.

```
snowballEdge describe-direct-network-interfaces --endpoint https://ip-address-of-snow-
device --manifest-file path/to/manifest/file.bin --unlock-code unlock-code
```

Example de la salida del **`descibe-virtual-network-interfaces`** comando

```
{
    "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",
        "MtuSize" : "1500"
    }
}
```

Actualización de una interfaz de red virtual

Utilice el `update-virtual-network-interface` comando para actualizar las interfaces de red virtuales del dispositivo de la familia Snow. Para cambiar la unidad de transmisión máxima (MTU) de la interfaz física que utiliza el DNI, utilice el comando. `update-mtu-size` Para obtener más información, consulte Actualización del tamaño de la MTU.

```
snowballEdge update-virtual-network-interface --direct-network-interface-
arn directNetworkInterfaceArn --endpoint https://ip-address-of-snow-device //
    --unlock-code unlock-code [--mac macAddress] --manifest-file path/to/manifest/
file.bin //
    [--vlan vlanId] [--attach-instance-id instanceId | --detach]
```

Example de salida de comando **`update-virtual-network-interface`**

```
{
    "VirtualNetworkInterface": {
        "VirtualNetworkInterfaceArn": "arn:aws:snowball-device:::interface/
s.ni-8EXAMPLE8EXAMPLEf",
        "PhysicalNetworkInterfaceId": "s.ni-8EXAMPLEaEXAMPLEd",
        "IpAddressAssignment": "DHCP",
        "IpAddress": "192.0.2.9",
        "Netmask": "255.255.255.0",
        "DefaultGateway": "192.0.2.1",
        "MacAddress": "EX:AM:PL:E1:23:45",
        "MtuSize" : "1500"
    }
}
```

Eliminar una interfaz de red virtual

Utilice el `delete-direct-network-interface` comando para eliminar una interfaz de red virtual (VNI).

```
snowballEdge delete-virtual-network-interface --virtual-network-interface-arn virtual-network-interface-ARN --endpoint https://endpoint  //
    --manifest-file path/to/manifest/file.bin] [--profile profile] --unlock-code unlock-code]
```

Example de la salida del **`delte-direct-network-interface`** comando

```
The virtual network interface has been deleted from your Snowball Edge. You can
 determine the virtual network interfaces available on your Snowball Edge using the
 describe-virtual-network-interfaces command.
```

Comprobación del estado de las características

Para ver el estado de las funciones disponibles en su dispositivo, utilice el `describe-features` comando.

`RemoteManagementState`: indica el estado de Snow Device Management y devuelve uno de los siguientes estados:

- `INSTALLED_ONLY`: la característica está instalada pero no habilitada.
- `INSTALLED_AUTOSTART`— La función está habilitada y el dispositivo intentará conectarse a ella Región de AWS cuando esté encendida.
- `NOT_INSTALLED`: el dispositivo no admite la característica o ya estaba sobre el terreno antes de su lanzamiento.

Uso (cliente de Snowball Edge configurado)

```
snowballEdge describe-features \
  --manifest-file manifest.bin path \
```

```
  --unlock-code unlock-code \
  --endpoint https://device-local-ip:9091
```

Ejemplo de salida

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

Configuración de servidores de tiempo

Puede configurar un servidor externo de Network Time Protocol (NTP). Puede usar los comandos de la CLI de NTP tanto cuando el dispositivo está bloqueado como cuando está desbloqueado. Se necesitan el manifiesto y el código de desbloqueo. Puede configurarlos con el comando `snowballEdge configure` o con las opciones `--manifest-file` y `--unlock-code`. Tenga en cuenta que puede usar la `snowballEdge` CLI tanto en AWS Snowcone Edge como en AWS Snowcone.

Es su responsabilidad proporcionar un servidor de tiempo NTP seguro. Para establecer a qué servidores de tiempo NTP se conecta el dispositivo, utilice el comando `update-time-servers` de la CLI.

> **Note**
>
> El comando `update-time-servers` anulará la configuración anterior de los servidores de tiempo NTP.

Tipos de dispositivos NTP y versiones de software compatibles

NTP no está disponible en ningún tipo de dispositivo de almacenamiento y computación de la versión 2. Sin embargo, los tipos de dispositivos de almacenamiento y computación de la versión 3 de Snowball Edge cuya versión del software es la 77 u otra posterior sí admiten NTP. Para comprobar si NTP está habilitado, utilice el comando `describe-time-sources` de la CLI de Snowball Edge.

Uso

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

Example Ejemplo de salida

```
Updating time servers now.
```

Comprobación de las fuentes de tiempo

Para ver a qué fuentes de tiempo NTP está conectado el dispositivo actualmente, utilice el comando `describe-time-sources` de la CLI de Snowball Edge.

Uso

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

Example Ejemplo de salida

```
{
  "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
  } ]
}
```

El comando `describe-time-sources` devuelve una lista de los estados de las fuentes de tiempo. Cada estado de la fuente de tiempo contiene los campos `Address`, `State`, `Type` y `Stratum`. A continuación se explican los significados de estos campos.

- `Address`: el nombre DNS o la dirección IP de la fuente de tiempo.
- `State`: el estado actual de la conexión entre el dispositivo y esa fuente de tiempo. Hay cinco estados posibles:
  - `CURRENT`: la fuente de tiempo se está utilizando actualmente para sincronizar la hora.
  - `COMBINED`: la fuente de tiempo se combina con la fuente actual.
  - `EXCLUDED`: el algoritmo de combinación excluye la fuente de tiempo.
  - `LOST`: se ha perdido la conexión con la fuente de tiempo.
  - `UNACCEPTABLE`: una fuente de tiempo no válida en la que el algoritmo de combinación ha resultado ser inexacto o presenta demasiada variabilidad.
- `Type`: una fuente de tiempo NTP puede ser un servidor o un par. Los servidores se pueden configurar mediante el comando `update-time-servers`. Los pares solo pueden ser otros dispositivos Snowball Edge del clúster y se configuran automáticamente cuando se asocia el clúster.
- `Stratum`: este campo muestra el stratum de la fuente. Stratum 1 indica una fuente con un reloj de referencia conectado localmente. Una fuente que está sincronizada con una fuente del stratum 1 está en el stratum 2. Una fuente que está sincronizada con una fuente del stratum 2 está en el stratum 3, y así sucesivamente.

Una fuente de tiempo NTP puede ser un servidor o un par. El usuario puede configurar un servidor con el comando `update-time-servers`, mientras que un par solo pueden ser otros dispositivos Snowball Edge del clúster. En el ejemplo de salida, se llama a `describe-time-sources` en un dispositivo Snowball Edge que está en un clúster de 5. La salida contiene 4 pares y 1 servidor. Los pares tienen un stratum de 10, mientras que el servidor tiene un stratum de 1; por tanto, se selecciona el servidor como la fuente de tiempo actual.

Actualización del tamaño de la MTU

Utilice el `update-mtu-size` comando para modificar el tamaño en bytes de la unidad de transmisión máxima (MTU) de una interfaz física de un dispositivo de la familia Snow. Todas las interfaces de red virtuales y las interfaces de red directas asociadas a esta interfaz de red física se configurarán con el mismo tamaño de MTU.

> **Note**
>
> El tamaño mínimo de la MTU es de 1500 bytes y el tamaño máximo es de 9216 bytes.

Puede usar el `describe-device` comando para recuperar los ID de las interfaces de red físicas y los tamaños de MTU actuales de esas interfaces. Para obtener más información, consulte Obtención del estado de los dispositivos.

Puede utilizar los `describe-virtual-network-interface` comandos `descibe-direct-network-interface` y para recuperar los tamaños de MTU actuales de esas interfaces. Para obtener más información, consulte Obtener información sobre una interfaz de red directa y Obtener información sobre una interfaz de red virtual.

Uso

```
snowballEdge update-mtu-size --physical-network-interface-id physical-network-interface-id --mtu-size size-in-bytes
```

Example de salida de **`update-mtu-size`**

```
{
    "PhysicalNetworkInterface": {
        "PhysicalNetworkInterfaceId": "s.ni-8c1f891d7f5b87cfe",
        "PhysicalConnectorType": "SFP_PLUS",
        "IpAddressAssignment": "DHCP",
        "IpAddress": "192.0.2.0",
        "Netmask": "255.255.255.0",
        "DefaultGateway": "192.0.2.255",
        "MacAddress": "8A:2r:5G:9p:6Q:4s",
        "MtuSize": "5743"
    }
}
```

Transferencia de archivos mediante el adaptador de Amazon S3 para la migración de datos

A continuación se presenta una descripción general del adaptador de Amazon S3, que puede utilizar para transferir datos mediante programación hacia y desde los buckets de S3 que ya están en el AWS Snowball Edge dispositivo mediante las acciones de la API REST de Amazon S3. Esta API de REST de Amazon S3 admite un subconjunto de acciones limitado. Puede usar este subconjunto de acciones con uno de los AWS SDK para transferir datos mediante programación. También puede utilizar el subconjunto de comandos admitidos de la AWS Command Line Interface (AWS CLI) para Amazon S3 a fin de transferir datos mediante programación.

Si la solución usa la AWS SDK for Java versión 1.11.0 o posterior, debe usar lo siguiente: `S3ClientOptions`

- `disableChunkedEncoding()`: indica que no se admite la codificación fragmentada con la interfaz.
- `setPathStyleAccess(true)`: configura la interfaz para usar el acceso de tipo ruta para todas las solicitudes.

Para obtener más información, consulte Class S3 ClientOptions .Builder en Amazon AppStream SDK for Java.

> **Important**
>
> Le recomendamos que utilice solo un método a la vez para leer y escribir datos en un depósito local de un AWS Snowball Edge dispositivo. El uso de la interfaz de archivos y el adaptador de Amazon S3 en el mismo bucket a la vez puede dar lugar a conflictos de lectura/escritura.
>
> En AWS Snowball Cuotas de Edge se detallan los límites.
>
> Para que AWS los servicios funcionen correctamente en un Snowball Edge, debe permitir los puertos para los servicios. Para obtener más detalles, consulte Puertos necesarios para usar AWS los servicios en un dispositivo AWS Snowball perimetral.

Temas

Descarga e instalación de la AWS CLI versión 1.16.14 para usarla con el adaptador Amazon S3

En la actualidad, los dispositivos Snowball Edge solo permiten usar la versión 1.16.14 y las versiones anteriores de la AWS CLI con el adaptador de Amazon S3. Las versiones más recientes no AWS CLI son compatibles con el adaptador Amazon S3 porque no admiten todas las funciones del adaptador S3.

> **Note**
>
> Si utiliza almacenamiento compatible con Amazon S3 en dispositivos Snow Family, puede utilizar la versión más reciente de la AWS CLI. Para descargar y utilizar la versión más reciente, consulte la Guía del usuario de AWS Command Line Interface.

Instálelo AWS CLI en sistemas operativos Linux

Ejecute este comando encadenado:

```
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;
```

Instálelo AWS CLI en los sistemas operativos Windows

Descargue y ejecute el archivo del instalador correspondiente a su sistema operativo:

- 32 bits
- 64 bits

Uso de las operaciones AWS CLI y de la API en los dispositivos Snowball Edge

Cuando utilice las AWS CLI operaciones de API para emitir comandos de IAM, Amazon S3 y Amazon EC2 en Snowball Edge, debe especificar la región como "». `snow` Puede hacerlo utilizando `AWS configure` o dentro del propio comando, como en los ejemplos siguientes.

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

Or (Disyunción)

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

Autorización con la interfaz API de Amazon S3 para AWS Snowball

Cuando utiliza el adaptador Amazon S3, todas las interacciones se firman con el algoritmo AWS Signature Version 4 de forma predeterminada. Esta autorización solo se usa para comprobar los datos en tránsito desde el origen hasta la interfaz. Todas las operaciones de cifrado y descifrado se realizan en el dispositivo. Nunca se almacenan datos sin cifrar en el dispositivo.

Al utilizar la interfaz, tenga en cuenta lo siguiente:

- Para obtener las credenciales locales de Amazon S3 a fin de identificar sus solicitudes en el dispositivo AWS Snowball Edge , ejecute los comandos `snowballEdge list-access-keys` y `snowballEdge get-secret-access-keys` del cliente de Snowball Edge. Para obtener más información, consulte Uso de los comandos del cliente Snowball Edge. Estas credenciales locales de Amazon S3 incluyen un par de claves: una clave de acceso y una clave secreta. Estas claves únicamente son válidas para los dispositivos asociados con el trabajo. No se pueden usar en el Nube de AWS porque no tienen una contraparte AWS Identity and Access Management (IAM).

- Las AWS credenciales que utilice no cambiarán la clave de cifrado. La firma con el algoritmo Signature Version 4 se utiliza únicamente para verificar los datos en tránsito desde su origen a la interfaz. Por lo tanto, esta firma no tiene en cuenta nunca las claves de cifrado utilizadas para cifrar los datos en el dispositivo Snowball.

Obtención y uso de las credenciales locales de Amazon S3

Cada interacción con un Snowball Edge se firma con el algoritmo AWS Signature Version 4. Para obtener más información acerca del algoritmo, consulte Proceso de firma de la versión 4 en Referencia general de AWS.

Puede obtener las credenciales locales de Amazon S3 para firmar sus solicitudes en el dispositivo Edge del cliente de Snowball Edge ejecutando `snowballEdge list-access-keys` y `snowballEdge get-secret-access-key`. Para obtener información sobre el cliente de Snowball Edge, consulte Obtención de credenciales. Estas credenciales locales de Amazon S3 incluyen un par de claves: un ID de clave de acceso y una clave secreta. Estas credenciales únicamente son válidas para los dispositivos asociados con su trabajo. No se pueden usar en el Nube de AWS porque no tienen una contraparte de IAM.

Puede añadir estas credenciales al archivo de AWS credenciales de su servidor. El archivo de perfiles de credenciales predeterminado suele estar en `~/.aws/credentials`, pero la ubicación puede variar en función de la plataforma. Muchos de los AWS SDK y el AWS CLI. Puede guardar las credenciales locales con un nombre de perfil, como en el ejemplo siguiente:

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

Especificación del adaptador de S3 como punto de conexión de AWS CLI

Cuando utilizas el AWS CLI para enviar un comando al AWS Snowball Edge dispositivo, especificas que el punto de conexión es el adaptador Amazon S3. Tiene la posibilidad de utilizar el punto de conexión HTTPS o un punto de conexión HTTP no protegido, tal y como se muestra a continuación.

Punto de conexión HTTPS protegido

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

Punto de conexión HTTP no protegido

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

Si utiliza el punto de conexión HTTPS de `8443`, los datos se transfieren de forma segura de su servidor al dispositivo Snowball Edge. Este cifrado está protegido con un certificado que el dispositivo Snowball Edge genera cuando obtiene una nueva dirección IP. Una vez que tenga el certificado, puede guardarlo en un archivo `ca-bundle.pem` local. A continuación, puede configurar su AWS CLI perfil para incluir la ruta al certificado, tal y como se describe a continuación.

Asociación del certificado con el punto de conexión de interfaz

1. Conecte el dispositivo Snowball Edge a la alimentación eléctrica y a la red y enciéndalo.
2. En cuanto el dispositivo termine de arrancar, anote su dirección IP en la red local.
3. En un terminal de la red, asegúrese de que puede hacer ping al dispositivo Snowball Edge.
4. Ejecute el comando `snowballEdge get-certificate` en el terminal. Para obtener más información acerca de este comando, consulte Administración de certificados de clave pública.
5. Guarde el resultado del comando `snowballEdge get-certificate` en un archivo, por ejemplo `ca-bundle.pem`.
6. Ejecute el siguiente comando desde el terminal.

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

Después de realizar este procedimiento, puede ejecutar comandos de la CLI con estas credenciales locales, su certificado y el punto de conexión especificado, como en el siguiente ejemplo.

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

Características de Amazon S3 para el adaptador de Amazon S3 no compatibles

El adaptador de Amazon S3 le permite transferir datos mediante programación desde y hacia un dispositivo Snowball Edge con acciones de la API de Amazon S3. Sin embargo, no todas las características de transferencia y acciones de la API de Amazon S3 pueden utilizarse con un dispositivo Snowball Edge cuando se usa el adaptador de Amazon S3. Por ejemplo, las siguientes características y acciones no se pueden usar con Snowball Edge:

- TransferManager— Esta utilidad transfiere archivos de un entorno local a Amazon S3 con el SDK for Java. Considere la posibilidad de utilizar las acciones de la API o los comandos de la AWS CLI admitidos con la interfaz.
- GET Bucket (List Objects) Version 2: esta implementación de la acción GET todos los objetos (hasta 1000), o parte de ellos, de un bucket. Considere la posibilidad de utilizar la acción GET Bucket (List Objects) Version 1 o el comando ls de la AWS CLI .
- ListBuckets— No se admite el punto final ListBuckets con el objeto. El siguiente comando no funciona con el almacenamiento compatible con Amazon S3 en dispositivos Snow Family:

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

Agrupación en lotes de archivos pequeños

Las operaciones de copia conllevan una sobrecarga debido al cifrado. Para acelerar el proceso de transferencia de archivos pequeños a su AWS Snowball Edge dispositivo, puede agruparlos en un solo archivo. Al agrupar los archivos por lotes, estos se pueden extraer automáticamente al importarlos a Amazon S3, siempre que para agruparlos se haya usado uno de los formatos de archivo compatibles.

Normalmente, los archivos de 1 MB o menores debe incluirse en lotes. No hay un límite establecido para el número de archivos que pueden incluirse en un lote, aunque se recomienda limitar los lotes a 10 000 archivos aproximadamente. Tener más de 100 000 archivos en un lote puede afectar a la rapidez con la que esos archivos se importan a Amazon S3 después de devolver el dispositivo. Recomendamos que el tamaño total de cada lote no supere los 100 GB.

La agrupación de archivos en lotes es un proceso manual administrado por el propio usuario. Después de agrupar los archivos, transfiéralos a un dispositivo Snowball Edge mediante el AWS CLI `cp` comando con la `--metadata snowball-auto-extract=true` opción. Cuando se especifica `snowball-auto-extract=true`, se extrae automáticamente el contenido de los archivos almacenados al importar los datos a Amazon S3, siempre y cuando el tamaño del archivo de lotes no supere los 100 GB.

> **Note**
>
> Los lotes con un tamaño superior a 100 GB no se extraen al importarlos a Amazon S3.

Para agrupar archivos pequeños por lotes

1. Decida qué formato quiere usar para agrupar los archivos pequeños por lotes. La característica de extracción automática admite los formatos `TAR`, `ZIP` y `tar.gz`.
2. Identifique los archivos que quiere agrupar por lotes, incluido su tamaño y el número total de archivos que desea incluir en cada lote.
3. Agrupe por lotes sus archivos en la línea de comandos, tal y como se muestra en los siguientes ejemplos.

   - Si utiliza Linux, puede agrupar por lotes los archivos en la misma línea de comandos que se usa para transferir los archivos al 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**
     >
     > También puede usar la utilidad de archivo que prefiera para agrupar los archivos por lotes en uno o varios archivos grandes. Sin embargo, este enfoque requiere espacio de almacenamiento local adicional, para guardar los archivos antes de transferirlos al dispositivo Snowball.

   - Para Windows, utilice el siguiente comando de ejemplo para agrupar los archivos cuando todos los archivos estén en el mismo directorio desde el que se ejecuta el comando:

     ```
     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 archivos desde un directorio diferente desde el que se ejecuta el comando, utilice el siguiente comando de ejemplo:

     ```
     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 Microsoft Windows 2016, tar no está disponible, pero puede descargarlo desde el sitio web de Tar para Windows.
> Puede descargar 7 ZIP desde el sitio web de 7ZIP.

4. Repita los pasos hasta que haya archivado todos los archivos pequeños que desea transferir a Amazon S3 mediante un dispositivo Snowball Edge.
5. Transfiera los archivos almacenados al dispositivo Snowball. Si desea que los datos se extraigan automáticamente y utilizó uno de los formatos de archivo compatibles mencionados anteriormente en el paso 1, utilice el AWS CLI `cp` comando con la `--metadata snowball-auto-extract=true` opción.

> **Note**
>
> Si hay archivos que no estén archivados, no utilice este comando.

Al crear los archivos de almacenamiento, la extracción mantendrá la estructura de datos actual. Esto significa que si crea un archivo de almacenamiento que contenga archivos y carpetas, Snowball Edge volverá a crearlo durante el proceso de ingesta en Amazon S3.

El archivo de almacenamiento se extraerá en el mismo directorio en el que está almacenado y las estructuras de carpetas se crearán en consecuencia. Tenga en cuenta que al copiar archivos de almacenamiento es importante establecer la marca `--metadata snowball-auto-extract=true`. De lo contrario, Snowball Edge no extraerá los datos al importarlos a Amazon S3.

Siguiendo el ejemplo del paso 3, si tiene la estructura de carpetas de /Logs/April/ que contiene los archivos `a.txt`, `b.txt` y `c.txt`, Si este archivo de almacenamiento se colocó en la raíz de / mybucket/, los datos tendrían el siguiente aspecto tras la extracción:

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

Si el archivo se colocó en /mybucket/test/, la extracción tendría el siguiente aspecto:

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

Comandos compatibles AWS CLI

A continuación, encontrará información sobre cómo especificar el adaptador Amazon S3 o el almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow como punto final para los comandos AWS Command Line Interface (AWS CLI) aplicables. También puede encontrar la lista de AWS CLI comandos de Amazon S3 compatibles para transferir datos al AWS Snowball Edge dispositivo con el adaptador o al almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow.

> **Note**
>
> Para obtener información sobre la instalación y configuración de AWS CLI, incluida la especificación de las regiones contra las que quieres realizar AWS CLI llamadas, consulta la Guía AWS Command Line Interface del usuario.

Actualmente, los dispositivos Snowball Edge solo son compatibles con la versión 1.16.14 y versiones anteriores de la AWS CLI cuando se utiliza el adaptador de Amazon S3. Consulte Versión del cliente de Snowball Edge. Si está usando almacenamiento compatible con Amazon S3 en dispositivos Snow Family, puede utilizar la versión más reciente de la AWS CLI. Para descargar y utilizar la versión más reciente, consulte la Guía del usuario de AWS Command Line Interface.

> **Note**
>
> No olvide instalar la versión 2.6.5+ o 3.4+ de Python antes de instalar la versión 1.16.14 de la AWS CLI.

AWS CLI Comandos compatibles con Amazon S3

A continuación se describe el subconjunto de AWS CLI comandos y opciones para Amazon S3 que admite el AWS Snowball Edge dispositivo. Si un comando o una opción no aparece en la lista siguiente, no está admitido. Puede declarar algunas opciones no admitidas (como `--sse` o `--`

`storage-class`) junto con un comando. Sin embargo, estas se pasan por alto y no afectan a la forma en que se importan los datos.

- cp — Copia un archivo u objeto hacia o desde el AWS Snowball Edge dispositivo. A continuación se enumeran las opciones de este comando:
  - `--dryrun` (booleano): se muestran las operaciones que se realizarían con el comando especificado, pero sin ejecutarse.
  - `--quiet` (booleano): las operaciones realizadas por el comando especificado no se muestran.
  - `--include` (cadena): no excluye los archivos u objetos del comando que coinciden con el patrón especificado. Para obtener más información, consulte Uso de filtros de exclusión e inclusión en la Referencia de comandos de AWS CLI .
  - `--exclude` (cadena): excluye todos los archivos u objetos del comando que coinciden con el patrón especificado.
  - `--follow-symlinks | --no-follow-symlinks` (booleano): los enlaces simbólicos (symlinks) solo se siguen al cargar recursos en Amazon S3 desde el sistema de archivos local. Amazon S3 no admite enlaces simbólicos, por lo que el contenido del destino del enlace se carga con el nombre del enlace. Si no se especifica ninguna de las opciones, la acción predeterminada es seguir los symlinks.
  - `--only-show-errors` (booleano): solo se muestran errores y advertencias. El resto de los resultados se suprime.
  - `--recursive` (booleano): el comando se ejecuta en todos los objetos o archivos del directorio especificado o con el prefijo indicado.
  - `--page-size` (entero): el número de resultados que se devuelven en cada respuesta a una operación de listado. El valor predeterminado es 1000 (el máximo permitido). El uso de un valor inferior podría ser de ayuda si se agota el tiempo de espera de una operación.
  - `--metadata` (mapa): un mapa de los metadatos que se van a almacenar con los objetos en Amazon S3. Este mapa se aplica a cada objeto que forma parte de esta solicitud. En una sincronización, esta funcionalidad significa que los archivos que no han cambiado no reciben los nuevos metadatos. Cuando la copia se realiza entre dos ubicaciones de Amazon S3, el argumento `metadata-directive` se establece en `REPLACE` de forma predeterminada, a menos que se especifique otro valor.
- ls — Muestra los objetos del AWS Snowball Edge dispositivo. A continuación se enumeran las opciones de este comando:
  - `--human-readable` (booleano): los tamaños de los archivos se muestran en un formato legible por el ser humano.

  - `--summarize` (booleano): se muestra un resumen de la información. Esta información es el número de objetos y su tamaño total.
  - `--recursive` (booleano): el comando se ejecuta en todos los objetos o archivos del directorio especificado o con el prefijo indicado.
  - `--page-size` (entero): el número de resultados que se devuelven en cada respuesta a una operación de listado. El valor predeterminado es 1000 (el máximo permitido). El uso de un valor inferior podría ser de ayuda si se agota el tiempo de espera de una operación.
- rm — Elimina un objeto del AWS Snowball Edge dispositivo. A continuación se enumeran las opciones de este comando:
  - `--dryrun` (booleano): se muestran las operaciones que se realizarían con el comando especificado, pero sin ejecutarse.
  - `--include` (cadena): no excluye los archivos u objetos del comando que coinciden con el patrón especificado. Para obtener más información, consulte Uso de filtros de exclusión e inclusión en la Referencia de comandos de AWS CLI .
  - `--exclude` (cadena): excluye todos los archivos u objetos del comando que coinciden con el patrón especificado.
  - `--recursive` (booleano): el comando se ejecuta en todos los objetos o archivos del directorio especificado o con el prefijo indicado.
  - `--page-size` (entero): el número de resultados que se devuelven en cada respuesta a una operación de listado. El valor predeterminado es 1000 (el máximo permitido). El uso de un valor inferior podría ser de ayuda si se agota el tiempo de espera de una operación.
  - `--only-show-errors` (booleano): solo se muestran errores y advertencias. El resto de los resultados se suprime.
  - `--quiet` (booleano): las operaciones realizadas por el comando especificado no se muestran.
- sync: sincroniza directorios y prefijos. Este comando copia los archivos nuevos y actualizados del directorio de origen al de destino. Este comando solo crea directorios en el destino si contienen uno o más archivos.

> **Important**
>
> No se admite la sincronización de un directorio en otro del mismo dispositivo Snowball Edge.
> No se admite la sincronización de un AWS Snowball AWS Snowball dispositivo a otro.

Solo puede utilizar esta opción para sincronizar el contenido entre el almacenamiento de datos en las instalaciones y un dispositivo Snowball Edge.

- `--dryrun` (booleano): se muestran las operaciones que se realizarían con el comando especificado, pero sin ejecutarse.
- `--quiet` (booleano): las operaciones realizadas por el comando especificado no se muestran.
- `--include` (cadena): no excluye los archivos u objetos del comando que coinciden con el patrón especificado. Para obtener más información, consulte Uso de filtros de exclusión e inclusión en la Referencia de comandos de AWS CLI .
- `--exclude` (cadena): excluye todos los archivos u objetos del comando que coinciden con el patrón especificado.
- `--follow-symlinks` o `--no-follow-symlinks` (booleano): los enlaces simbólicos (symlinks) solo se siguen al cargar recursos en Amazon S3 desde el sistema de archivos local. Amazon S3 no admite enlaces simbólicos, por lo que el contenido del destino del enlace se carga con el nombre del enlace. Si no se especifica ninguna de las opciones, la acción predeterminada es seguir los symlinks.
- `--only-show-errors` (booleano): solo se muestran errores y advertencias. El resto de los resultados se suprime.
- `--no-progress` (booleano): no se muestra el progreso de la transferencia de archivos. Esta opción solo se aplica cuando no se proporcionan las opciones `--quiet` y `--only-show-errors`.
- `--page-size` (entero): el número de resultados que se devuelven en cada respuesta a una operación de listado. El valor predeterminado es 1000 (el máximo permitido). El uso de un valor inferior podría ser de ayuda si se agota el tiempo de espera de una operación.
- `--metadata` (mapa): un mapa de los metadatos que se van a almacenar con los objetos en Amazon S3. Este mapa se aplica a cada objeto que forma parte de esta solicitud. En una sincronización, esta funcionalidad significa que los archivos que no han cambiado no reciben los nuevos metadatos. Cuando la copia se realiza entre dos ubicaciones de Amazon S3, el argumento `metadata-directive` se establece en `REPLACE` de forma predeterminada, a menos que se especifique otro valor.

> **Important**
>
> No se admite la sincronización de un directorio en otro del mismo dispositivo Snowball Edge.
> No se admite la sincronización de un AWS Snowball AWS Snowball dispositivo a otro. Solo puede utilizar esta opción para sincronizar el contenido entre el almacenamiento de datos en las instalaciones y un dispositivo Snowball Edge.

- `--size-only` (booleano): con esta opción, el tamaño de cada clave es el único criterio utilizado para decidir si se va a sincronizar desde el origen hasta el destino.
- `--exact-timestamps` (booleano): cuando se sincroniza desde Amazon S3 en almacenamiento local, los elementos que tienen el mismo tamaño solo se omiten si las marcas temporales coinciden exactamente. El comportamiento predeterminado es omitir los elementos que tienen el mismo tamaño a menos que la versión local sea más reciente que la versión de Amazon S3.
- `--delete` (booleano): los archivos existentes en el destino pero no en el origen se eliminan durante la sincronización.

Puede trabajar con archivos o carpetas que tengan espacios en sus nombres, como `my photo.jpg` o `My Documents`. Sin embargo, asegúrate de gestionar los espacios correctamente en los AWS CLI comandos. Para obtener más información, consulte Especificar valores de parámetros para la AWS CLI en la Guía del usuario de AWS Command Line Interface .

Acciones de la API de REST admitidas

A continuación, encontrará las acciones de la API REST que puede usar con un AWS Snowball Edge dispositivo y Amazon S3.

Temas

- Acciones de la API de REST admitidas para dispositivos Snowball Edge
- Acciones de la API de REST admitidas para el adaptador de Amazon S3

Acciones de la API de REST admitidas para dispositivos Snowball Edge

HEAD Snowball Edge

Descripción

En la actualidad, solo hay una operación de la API de REST de Snowball Edge, que puede utilizar para devolver información sobre el estado de un dispositivo concreto. Esta operación devuelve el estado de un dispositivo Snowball Edge. Este estado incluye información que puede utilizarse AWS Support para solucionar problemas.

No puedes usar esta operación con los AWS SDK o el AWS CLI. Le recomendamos que utilice `curl` o un cliente HTTP. No es necesario firmar la solicitud para esta operación.

Solicitud

En el siguiente ejemplo, la dirección IP del dispositivo Snowball Edge es *`192.0.2.0`*. Sustituya este valor por la dirección IP de su dispositivo.

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

Respuesta

```
<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>
```

Acciones de la API de REST admitidas para el adaptador de Amazon S3

A continuación, puede encontrar la lista de acciones de la API de REST de Amazon S3 compatibles con el uso del adaptador de Amazon S3. La lista incluye enlaces a información sobre cómo funcionan las acciones de la API con Amazon S3. La lista también incluye cualquier diferencia de

comportamiento entre la acción de la API de Amazon S3 y la contraparte del AWS Snowball Edge dispositivo. Todas las respuestas procedentes de un dispositivo AWS Snowball Edge declaran `Server` como `AWSSnowball`, como en el ejemplo siguiente.

```
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
```

Las llamadas a la API de REST de Amazon S3 requieren la firma de SigV4. Si utiliza el SDK AWS CLI o el AWS SDK para realizar estas llamadas a la API, la firma de SigV4 se gestiona automáticamente. De lo contrario, debe implementar su propia solución de firma de SigV4. Para obtener más información, consulte Autenticación de solicitudes (versión de AWS firma 4) en la Guía del usuario de Amazon Simple Storage Service.

- GET Bucket (List Objects) version 1: se admite. Sin embargo, en esta implementación de la operación GET, no se admite lo siguiente:
  - Paginación
  - Marcadores
  - Delimitadores
  - La lista que se devuelve no está ordenada

  Solo se admite la versión 1. No se admite GET Bucket (List Objects) version 2.
- Servicio de GET
- HEAD Bucket
- HEAD Object
- GET Object: es una DESCARGA de un objeto del bucket de S3 del dispositivo Snow.
- Objeto PUT: cuando se carga un objeto en un AWS Snowball Edge dispositivo mediante un dispositivo`PUT Object`, se genera una ETag.

  La ETag es un hash del objeto La ETag solo refleja los cambios en el contenido de un objeto, no en sus metadatos. La ETag puede ser o no un resumen MD5 de los datos del objeto. Para obtener más información sobre las ETags, consulte Encabezados de respuesta comunes en la Referencia de la API de Amazon Simple Storage Service.
- DELETE Object

- Iniciar la carga multiparte: en esta implementación, al iniciar una solicitud de carga multiparte para un objeto que ya se encuentra en el AWS Snowball Edge dispositivo, primero se elimina ese objeto. A continuación, lo copia en partes en el dispositivo. AWS Snowball Edge
- List Multipart Uploads
- Upload Part
- Complete Multipart Upload
- Abort Multipart Upload

> **Note**
>
> Las acciones de la API de REST de Amazon S3 que no se indican aquí no se admiten. Si se utiliza una acción de la API de REST no admitida por el dispositivo Snowball Edge, se muestra un mensaje de error que indica que la acción no se admite.

Administración de la interfaz NFS

Utilice la interfaz del sistema de archivos de red (NFS) para cargar archivos en el dispositivo de la familia Snow como si el dispositivo fuera el almacenamiento local de su sistema operativo. Esto permite un enfoque de transferencia de datos más fácil de usar, ya que puede utilizar funciones del sistema operativo, como copiar archivos, arrastrarlos y soltarlos, u otras funciones de la interfaz gráfica de usuario. Cada depósito S3 del dispositivo está disponible como terminal de interfaz NFS y se puede montar para copiar datos en él. La interfaz NFS está disponible para los trabajos de importación.

Puede utilizar la interfaz NFS si el dispositivo Snowball Edge se configuró para incluirla cuando se creó la tarea de pedido del dispositivo. Si el dispositivo no está configurado para incluir la interfaz NFS, utilice el adaptador S3 o el almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow para transferir datos. Para obtener más información sobre el adaptador S3, consulteAdministración del almacenamiento del adaptador de Amazon S3. Para obtener más información sobre el almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow, consulteConfiguración del almacenamiento compatible con Amazon S3 en dispositivos Snow Family.

Cuando se inicia, la interfaz NFS utiliza 1 GB de memoria y 1 CPU. Esto puede limitar la cantidad de otros servicios que se ejecutan en el dispositivo de la familia Snow o la cantidad de instancias compatibles con EC2 que se pueden ejecutar.

Los datos transferidos a través de la interfaz NFS no se cifran durante el tránsito. Al configurar la interfaz NFS, puede proporcionar bloques CIDR y el dispositivo de la familia Snow restringirá el acceso a la interfaz NFS desde los ordenadores cliente con direcciones en esos bloques.

Los archivos del dispositivo se transferirán a Amazon S3 cuando se devuelva a Amazon S3 AWS. Para obtener más información, consulte Importación de trabajos a Amazon S3 .

Para obtener más información sobre el uso de NFS con el sistema operativo de su ordenador, consulte la documentación del sistema operativo.

Tenga en cuenta los siguientes detalles cuando utilice la interfaz NFS.

- Los nombres de archivo son claves de objeto que se encuentran en el bucket de S3 local del dispositivo Snow Family. El nombre de clave es una secuencia de caracteres Unicode cuya codificación UTF-8 tiene una longitud máxima de 1024 bytes. Recomendamos utilizar NFSv4.1 siempre que sea posible y codificar los nombres de los archivos con Unicode UTF-8 para garantizar una importación de datos correcta. Es posible que los nombres de archivo que no estén codificados con UTF-8 no se carguen en S3 o que se carguen en S3 con un nombre de archivo diferente, según la codificación NFS que se utilice.
- Asegúrese de que la longitud máxima de la ruta del archivo sea inferior a 1024 caracteres. Los dispositivos Snow Family no admiten rutas de archivos de más de 1024 caracteres. Si se supera esta longitud de ruta de archivo, se producirán errores en la importación de archivos.
- Para obtener más información, consulte Claves de objeto en la Guía del usuario de Amazon Simple Storage Service.
- En el caso de las transferencias basadas en NFS, los metadatos de estilo POSIX estándar se añadirán a sus objetos a medida que se importen a Amazon S3 desde los dispositivos de la familia Snow. Además, verá los metadatos «x-amz-meta-user-agent aws-datasync» tal y como los utilizamos actualmente AWS DataSync como parte del mecanismo de importación interna a Amazon S3 para la importación de dispositivos de la familia Snow con la opción NFS.
- Puede transferir hasta 40 millones de archivos con un único dispositivo Snowball Edge. Si necesita transferir más de 40 millones de archivos en un solo trabajo, agrupe los archivos para reducir el número de archivos por cada transferencia. Los archivos individuales pueden ser de cualquier tamaño, siendo el tamaño máximo de 5 TB para los dispositivos Snowball Edge con la interfaz NFS mejorada o la interfaz de S3.

También puede configurar y administrar la interfaz NFS con una herramienta de interfaz gráfica AWS OpsHub de usuario. Para obtener más información, consulte Administración de la interfaz NFS mediante NFS .

Configuración de NFS para los dispositivos Snow Family

La interfaz NFS no se ejecuta en el dispositivo de la familia Snow de forma predeterminada, por lo que debe iniciarla para permitir la transferencia de datos al dispositivo. Puede configurar la interfaz NFS proporcionando la dirección IP de una interfaz de red virtual (VNI) que se ejecute en el dispositivo de la familia Snow y restringiendo el acceso a su recurso compartido de archivos, si es necesario. Antes de configurar la interfaz NFS, configure una interfaz de red virtual (VNI) en su dispositivo de la familia Snow. Para obtener más información, consulte Network Configuration for Compute Instances.

Configure los dispositivos de la familia Snow para la interfaz NFS

- Utilice el `describe-service` comando para determinar si la interfaz NFS está activa.

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

El comando devolverá el estado del servicio NFS, `ACTIVE` o `INACTIVE`

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

Si el valor del `State` nombre es`ACTIVE`, el servicio de interfaz NFS está activo y puede montar el volumen NFS del dispositivo de la familia Snow. Para obtener más información, consulte

Una vez iniciada la interfaz NFS, monte el punto final como almacenamiento local en los ordenadores cliente.

Los siguientes son los comandos de montaje predeterminados para los sistemas operativos Windows, Linux y 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
```

. Si el valor es`INACTIVE`, debe iniciar el servicio.

Iniciar el servicio NFS en el dispositivo de la familia Snow

Inicie una interfaz de red virtual (VNI), si es necesario, y, a continuación, inicie el servicio NFS en el dispositivo de la familia Snow. Si es necesario, al iniciar el servicio NFS, proporcione un bloque de direcciones de red permitidas. Si no proporciona ninguna dirección, el acceso a los puntos finales de NFS no estará restringido.

1. Utilice el `describe-virtual-network-interface` comando para ver las VNI disponibles en el dispositivo de la familia Snow.

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

   Si hay una o más VNI activas en el dispositivo de la familia Snow, el comando devuelve lo siguiente.

```
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"
  }
]
```

Anote el valor del `VirtualNetworkInterfaceArn` nombre del VNI que se va a utilizar con la interfaz NFS.

2. Si no hay ninguna VNI disponible, utilice el `create-virtual-network-interface` comando para crear una VNI para la interfaz NFS. Para obtener más información, consulte Configuración de una interfaz de red virtual (VNI).
3. Utilice el `start-service` comando para iniciar el servicio NFS y asociarlo al VNI. Para restringir el acceso a la interfaz NFS, incluya los `AllowedHosts` parámetros `service-configuration` y en el comando.

```
snowballEdge start-service --virtual-network-interface-arns arn-of-vni --service-id
 nfs --service-configuration AllowedHosts=CIDR-address-range
```

4. Utilice el `describe-service` comando para comprobar el estado del servicio. Se está ejecutando cuando el valor del `State` nombre es`ACTIVE`.

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

El comando devuelve el estado del servicio, así como la dirección IP y el número de puerto del punto final NFS y los rangos de CIDR permitidos para acceder al punto final.

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

Montaje de puntos finales NFS en ordenadores cliente

Una vez iniciada la interfaz NFS, monte el punto final como almacenamiento local en los ordenadores cliente.

Los siguientes son los comandos de montaje predeterminados para los sistemas operativos Windows, Linux y 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
```

Detener la interfaz NFS

Cuando termine de transferir los archivos a través de la interfaz NFS y antes de apagar el dispositivo de la familia Snow, utilice el `stop-service` comando para detener el servicio NFS.

```
snowballEdge stop-service --service-id nfs
```

Uso de AWS IoT Greengrass para ejecutar software preinstalado en instancias compatibles con Amazon EC2

AWS IoT Greengrass es un servicio en la nube y de tiempo de ejecución perimetral del Internet de las cosas (IoT) de código abierto que le ayuda a crear, implementar y administrar aplicaciones de IoT en sus dispositivos. Puede utilizarlo AWS IoT Greengrass para crear software que permita a sus dispositivos actuar de forma local a partir de los datos que generan, ejecutar predicciones basadas en modelos de aprendizaje automático y filtrar y agregar los datos de los dispositivos. Para obtener información detallada al respecto AWS IoT Greengrass, consulte ¿Qué es AWS IoT Greengrass? en la Guía para AWS IoT Greengrass Version 2 desarrolladores.

Al usarlo AWS IoT Greengrass en su dispositivo de la familia Snow, permite que el dispositivo recopile y analice los datos más cerca de donde se generan, reaccione de forma autónoma ante los eventos locales y se comunique de forma segura con otros dispositivos de la red local.

Configuración de la instancia compatible con Amazon EC2

> **Note**
>
> Para instalarlo AWS IoT Greengrass Version 2 en un dispositivo de la familia Snow, asegúrese de que el dispositivo esté conectado a Internet. Tras la instalación, no es necesaria la conexión a Internet para que funcione con un dispositivo de la familia Snow AWS IoT Greengrass.

Para configurar una instancia compatible con EC2 para AWS IoT Greengrass V2

1. Lance la AMI AWS IoT Greengrass validada con una dirección IP pública y una clave SSH:

   a. Uso de AWS CLI: run-instances.

   b. Uso AWS OpsHub: lanzamiento de una instancia compatible con Amazon EC2.

   > **Note**
   >
   > Anote la dirección IP pública y el nombre de la clave SSH asociados a la instancia.

2. Conéctese a la instancia compatible con EC2 mediante SSH. Para ello, ejecute el siguiente comando en el equipo que está conectado al dispositivo. Sustituya *ssh-key* por la clave que utilizó para lanzar la instancia compatible con EC2. *public-ip-address*Sustitúyala por la dirección IP pública de la instancia compatible con EC2.

   ```
   ssh -i ssh-key ec2-user@ public-ip-address
   ```

   > **Important**
   >
   > Si su equipo usa una versión anterior de Microsoft Windows, es posible que no tenga el comando SSH o que tenga SSH pero no pueda conectarse a la instancia compatible con EC2. Para conectarse a su instancia compatible con EC2, puede instalar y configurar PuTTY, que es un cliente de SSH de código abierto gratuito. Debe convertir la clave SSH del formato `.pem` al formato PuTTY y conectarse a su instancia de EC2. Para

obtener instrucciones sobre cómo convertir de `.pem` a formato PuTTY, consulte Convertir la clave privada con PuttyGen en la Guía del usuario de Amazon EC2.

¿Instalando AWS IoT Greengrass

A continuación, configura su instancia compatible con EC2 como un dispositivo AWS IoT Greengrass Core que puede utilizar para el desarrollo local.

Para instalar AWS IoT Greengrass

1. Utilice el siguiente comando para instalar el software necesario para AWS IoT Greengrass. Este comando instala AWS Command Line Interface (AWS CLI) v2, Python 3 y 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 al usuario root el permiso para ejecutar el AWS IoT Greengrass software y modifique el permiso root desde `root ALL=(ALL) ALL` a `root ALL=(ALL:ALL) ALL` en el archivo de configuración de sudoers.

```
sudo sed -in 's/root\tALL=(ALL)/root\tALL=(ALL:ALL)/' /etc/sudoers
```

3. Utilice el siguiente comando para descargar el software AWS IoT Greengrass principal.

```
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. Utilice los siguientes comandos para proporcionar las credenciales que le permitan instalar el software AWS IoT Greengrass Core. Sustituya los valores de ejemplo por sus credenciales:

```
export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE
export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
```

> **Note**
>
> Se trata de credenciales del usuario de IAM de la AWS región, no del dispositivo de la familia Snow.

5. Utilice el siguiente comando para instalar el software AWS IoT Greengrass principal. El comando crea AWS los recursos que el software principal necesita para funcionar y configura el software principal como un servicio del sistema que se ejecuta cuando se inicia la AMI.

   Sustituya los siguientes parámetros del comando:

   - `region`: La AWS región en la que se buscan o crean los recursos.
   - `MyGreengrassCore`: El nombre del AWS IoT dispositivo AWS IoT Greengrass principal.
   - `MyGreengrassCoreGroup`: El nombre del grupo de AWS IoT cosas del dispositivo AWS IoT Greengrass principal.

```
sudo -E java -Droot="/greengrass/v2" -Dlog.store=FILE \
    -jar ./GreengrassInstaller/lib/Greengrass.jar \
    --aws-region region \
    --thing-name MyGreengrassCore \
    --thing-group-name MyGreengrassCoreGroup \
    --thing-policy-name GreengrassV2IoTThingPolicy \
    --tes-role-name GreengrassV2TokenExchangeRole \
    --tes-role-alias-name GreengrassCoreTokenExchangeRoleAlias \
    --component-default-user ggc_user:ggc_group \
    --provision true \
    --setup-system-service true \
    --deploy-dev-tools true
```

> **Note**
>
> Este comando es aplicable a una instancia compatible con Amazon EC2 que ejecute una AMI de Amazon Linux 2. Para una AMI de Windows, consulte Instalación del software AWS IoT Greengrass principal.

Cuando haya terminado, tendrá un AWS IoT Greengrass núcleo funcionando en su dispositivo de la familia Snow para su uso local.

Uso AWS Lambda con un AWS Snowball borde

AWS Lambda powered by AWS IoT Greengrass es un servicio informático que permite ejecutar código sin servidor (funciones Lambda) de forma local en dispositivos Snowball Edge. Puede utilizar Lambda para invocar funciones de Lambda en un dispositivo Snowball Edge con mensajes de Message Queuing Telemetry Transport (MQTT), ejecutar código Python en funciones de Lambda y utilizarlas para llamar a puntos finales de servicio público en la nube. AWS Para utilizar las funciones de Lambda con los dispositivos Snowball Edge, debe crear los trabajos de Snowball Edge de una forma compatible con. Región de AWS AWS IoT Greengrass Para obtener una lista de las válidas Regiones de AWS, consulte AWS IoT Greengrassen. Referencia general de AWS Lambda en Snowball Edge está disponible en aquellas regiones en las que están disponibles Lambda y los dispositivos Snowball Edge.

> **Note**
>
> Si asigna la recomendación mínima de 128 MB de memoria para cada una de las funciones, puede tener hasta siete funciones de Lambda en un solo trabajo.

Temas

Antes de comenzar

Antes de crear una función de Lambda en el lenguaje Python para que se ejecute en su dispositivo Snowball Edge, es recomendable que se familiarice con los siguientes servicios, conceptos y temas relacionados.

Requisitos previos para AWS IoT Greengrass

AWS IoT Greengrass es un software que extiende Nube de AWS las capacidades a los dispositivos locales. AWS IoT Greengrass permite que los dispositivos locales recopilen y analicen datos más

cerca de la fuente de información y, al mismo tiempo, se comuniquen de forma segura entre sí en las redes locales. Más específicamente, los desarrolladores que lo utilicen AWS IoT Greengrass pueden crear código sin servidor (funciones Lambda) en. Nube de AWS A continuación, pueden implementar este código en los dispositivos para la ejecución local de las aplicaciones.

Es importante entender los siguientes AWS IoT Greengrass conceptos cuando se utiliza AWS IoT Greengrass con un Snowball Edge:

- AWS IoT Greengrass requisitos: para obtener una lista completa de AWS IoT Greengrass requisitos, consulte los requisitos en la guía para AWS IoT Greengrass Version 2 desarrolladores.
- AWS IoT Greengrass core: descargue el software AWS IoT Greengrass principal e instálelo en una instancia EC2 que se ejecute en el dispositivo. Consulte Uso AWS IoT Greengrass en instancias de Amazon EC2 en esta guía.

  Para utilizar las funciones de Lambda en un dispositivo Snowball Edge, primero debe instalar el software AWS IoT Greengrass Core en una instancia de Amazon EC2 del dispositivo. Las funciones Lambda que vaya a utilizar en el dispositivo Snowball Edge deben crearse con la misma cuenta que utilizará para instalarlas en AWS IoT Greengrass el dispositivo Snowball Edge. Para obtener información sobre AWS IoT Greengrass la instalación en el dispositivo Snowball Edge, consulte. Uso de AWS IoT Greengrass para ejecutar software preinstalado en instancias compatibles con Amazon EC2
- AWS IoT Greengrass grupo: un dispositivo Snowball Edge forma parte de un AWS IoT Greengrass grupo como dispositivo principal del grupo. Para obtener más información sobre los grupos, consulte Grupos de AWS Greengrass IoT en la Guía para desarrolladores de AWS IoT Greengrass .
- MQTT: AWS IoT Greengrass utiliza el protocolo MQTT ligero y estándar del sector para comunicarse dentro de un grupo. Cualquier dispositivo o software compatible con MQTT de su AWS IoT Greengrass grupo puede invocar mensajes MQTT. Estos mensajes pueden invocar funciones de Lambda si define el mensaje MQTT relacionado para hacerlo.

Requisitos previos para AWS Lambda

AWS Lambda es un servicio informático que permite ejecutar código sin aprovisionar ni administrar servidores. Es importante que entienda los siguientes conceptos de Lambda al utilizar Lambda con un dispositivo Snowball Edge:

- Funciones de Lambda: su código personalizado, cargado y publicado en Lambda y que se usa en un dispositivo Snowball Edge. Para obtener más información, consulte Funciones de Lambda en la Guía para desarrolladores de AWS Lambda .
- Consola de Lambda: la consola en la que cargará, actualizará y publicará sus funciones de Lambda en lenguaje Python para usarlas en un dispositivo Edge. Para obtener más información sobre la consola de Lambda, consulte Consola de Lambda en la Guía para desarrolladores de AWS Lambda .
- Python: el lenguaje de programación de alto nivel que se utiliza para las funciones de Lambda con tecnología AWS IoT Greengrass Snowball Edge. AWS IoT Greengrass es compatible con Python versión 3.8.x.

Implementación de una función de Lambda en un dispositivo Snowball Edge

Para ejecutar una función Lambda en un dispositivo Snowball Edge de un AWS IoT Greengrass grupo, importe la función como un componente. Para obtener información completa sobre la importación de una función como componente mediante la AWS IoT Greengrass consola, consulte Importación de una función Lambda como componente (consola) en la Guía para AWS IoT Greengrass Version 2 desarrolladores.

1. En la consola de AWS IoT, en la página de componentes de Greengrass, elija Crear componente.
2. En Origen del componente, elija Importar función Lambda. En Función de Lambda, elija el nombre de su función. En Versión de la función de Lambda, elija la versión de su función.
3. Para suscribir la función a los mensajes sobre los que puede actuar, elija Agregar origen de eventos y elija el evento. En Tiempo de espera (segundos), indique un período de tiempo de espera en segundos.
4. En Anclado, elija si desea anclar o no la función.
5. Elija Crear componente
6. Elija Desplegar.
7. En Implementación, elija Agregar a la implementación existente y, a continuación, elija su grupo de Greengrass. Elija Siguiente.
8. En Componentes públicos, elija estos componentes:

    - aws.greengrass.Cli

- aws.greengrass. LambdaLauncher
- aws.greengrass. LambdaManager
- aws.greengrass. LambdaRuntimes
- aws.greengrass.Nucleus

9. Elija Desplegar.

Uso de instancias de computación compatibles con Amazon EC2

En esta sección se proporciona información general sobre el uso de instancias informáticas compatibles con Amazon EC2 en un AWS Snowball Edge dispositivo, que incluye información conceptual, procedimientos y ejemplos.

Temas

- Uso del almacenamiento en bloques con sus instancias compatibles con Amazon EC2
- Grupos de seguridad en dispositivos Snowball Edge
- Datos de usuario y metadatos de instancia admitidos
- Detención de instancias compatibles con EC2
- Solución de problemas de las instancias de computación en dispositivos Snowball Edge

Información general

Puede ejecutar instancias de computación compatibles con Amazon EC2 en un dispositivo Snowball Edge con los tipos de instancia `sbe1`, `sbe-c` y `sbe-g`. El tipo de instancia `sbe1` funciona en dispositivos que tienen la opción Snowball Edge optimizado para almacenamiento. El tipo de instancia `sbe-c` funciona en dispositivos que tienen la opción Snowball Edge optimizado para computación. Los tipos de instancia `sbe-c` y `sbe-g` funcionan en dispositivos que tienen la opción Snowball Edge optimizado para computación con GPU. Para ver una lista de los tipos de instancia admitidos, consulte Cuotas de instancias de computación en un dispositivo Snowball Edge.

Los tres tipos de instancia de computación que se pueden utilizar con las diferentes opciones de dispositivos Snowball Edge son exclusivos de los dispositivos Snowball Edge. Al igual que ocurre con sus homólogas basadas en la nube, estas instancias requieren el lanzamiento de imágenes de máquina de Amazon (AMI). Antes de crear el trabajo de Snowball Edge puede elegir la AMI que será la imagen base de una instancia en la nube.

Para usar una instancia de cómputo en un Snowball Edge, cree un trabajo para solicitar un dispositivo de la familia Snow y especifique sus AMI. Puede hacerlo mediante el Consola de administración de la familia de productos Snow de AWS AWS CLI, el o uno de los AWS SDK. Normalmente, para poder utilizar las instancias, hay algunos requisitos organizativos previos que debe cumplir antes de crear el trabajo.

Cuando llegue el dispositivo, podrá comenzar a administrar las AMI y las instancias. Puede administrar las instancias de computación en un dispositivo Snowball Edge a través de un punto de conexión compatible con Amazon EC2. Este tipo de punto de conexión admite muchos de los comandos de la CLI compatibles con Amazon EC2 y de las acciones de los SDK de AWS . No puede usar Snowball Edge para administrar sus AMI e instancias de cómputo. AWS Management Console

Cuando haya terminado con el dispositivo, devuélvalo a AWS. Si el dispositivo se utilizó en un trabajo de importación, los datos transferidos mediante el adaptador de Amazon S3 o la interfaz de archivos NFS se importan a Amazon S3. De lo contrario, borraremos por completo el dispositivo cuando

lo devolvamos. AWS Esta operación de borrado se ajusta a los estándares 800-88 del Instituto Nacional de Normalización y Tecnología (NIST).

> **Important**
>
> - No se admite el uso de AMI cifradas en los dispositivos Snowball Edge.
> - Los datos de las instancias de procesamiento que se ejecutan en un Snowball Edge no se importan a. AWS

Diferencia entre las instancias de Amazon EC2 y las instancias compatibles con Amazon EC2 en dispositivos Snow Family

AWS Las instancias compatibles con EC2 de la familia Snow permiten a los clientes utilizar y gestionar instancias compatibles con Amazon EC2 mediante un subconjunto de API de EC2 y un subconjunto de AMI.

Precios de las instancias de computación en Snowball Edge

Hay costos adicionales asociados con el uso de instancias de computación. Para obtener más información, consulte AWS Snowball Edge Precios.

Uso de una AMI compatible con Amazon EC2 en dispositivos Snow Family

Para utilizar una imagen de máquina de Amazon (AMI) en su dispositivo de la familia AWS Snow, primero debe añadirla al dispositivo. Puede agregar una AMI de las siguientes maneras:

- Cargue la AMI cuando pida el dispositivo.
- Agregue la AMI cuando el dispositivo llegue a sus instalaciones.

Las instancias de computación de Amazon EC2 que vienen con los dispositivos Snow Family se lanzan en función de las AMI de Amazon EC2 que agregue al dispositivo. Las AMI compatibles con Amazon EC2 admiten los sistemas operativos Linux y Microsoft Windows.

Linux

Los sistemas operativos Linux admitidos son los siguientes:

- Amazon Linux 2 for Snow Family

> **Note**
>
> La última versión de esta AMI se proporcionará cuando su dispositivo de la familia Snow esté listo para su envío AWS. Para determinar la versión de esta AMI en el dispositivo cuando la reciba, consulteDeterminación de la versión de la AMI de Amazon Linux 2 para la familia Snow.

- CentOS 7 (x86_64) - with Updates HVM
- Ubuntu 16.04 LTS - Xenial (HVM)

> **Note**
>
> Ubuntu 16.04 LTS: las imágenes Xenial (HVM) ya no se admiten en los dispositivos Snowball Edge a través de Amazon EC2 VM Import/Export AWS Marketplace, pero se siguen utilizando en dispositivos Snowball Edge a través de Amazon EC2 VM Import/Export y se ejecutan localmente en las AMI.

- Ubuntu 20.04 LTS - Focal
- Ubuntu 22.04 LTS - Jammy

Como práctica recomendada de seguridad, mantenga las AMI de Amazon Linux 2 up-to-date en los dispositivos de la familia Snow a medida que se publiquen las nuevas AMI de Amazon Linux 2. Consulte Actualización de las AMI de Amazon Linux 2 en los dispositivos Snow Family.

Windows

Se admiten las siguientes versiones de los sistemas operativos Windows:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Puede agregar AMI de Windows a su dispositivo importando la imagen de su máquina virtual (VM) de Windows AWS mediante VM Import/Export. O bien, puede importar la imagen a su dispositivo

inmediatamente después de implementar el dispositivo en sus instalaciones. Para obtener más información, consulte Agregar una AMI de Microsoft Windows.

> **Note**
>
> Las AMI de Windows que se originaron en no se AWS pueden agregar al dispositivo. Las AMI importadas localmente deben estar en el modo de arranque del BIOS, ya que la UEFI no es compatible.

Snow Family admite el modelo Traiga su propia licencia (BYOL). Para obtener más información, consulte Agregar una AMI de Microsoft Windows.

> **Note**
>
> AWS Las instancias compatibles con EC2 de la familia Snow permiten a los clientes utilizar y gestionar instancias compatibles con Amazon EC2 mediante un subconjunto de API de EC2 y un subconjunto de AMI.

Temas

- Agregar una AMI al pedir el dispositivo
- Añadir una AMI desde AWS Marketplace
- Agregar una AMI localmente
- Agregar una AMI de Microsoft Windows
- Importación de una imagen de máquina virtual a su dispositivo
- Exportación de la AMI más reciente de Amazon Linux 2

Agregar una AMI al pedir el dispositivo

Cuando pida el dispositivo, podrá agregarle AMI seleccionándolas en la sección Compute using EC2 instances - optional de la Consola de administración de la familia de productos Snow de AWS. En la sección Compute using EC2 instances - optional se muestran todas las AMI que se pueden cargar en el dispositivo. Las AMI se dividen en las siguientes categorías:

- AMI de AWS Marketplace: son AMI creadas a partir de la lista de AMI compatibles. Para obtener información sobre la creación de una AMI a partir de las AMI compatibles de AWS Marketplace, consulteAñadir una AMI desde AWS Marketplace.
- AMI cargadas mediante VM Import/Export: cuando pide el dispositivo, las AMI que se cargaron mediante VM Import/Export aparecen en la consola. Para obtener más información, consulte Importación de una VM como una imagen utilizando VM Import/Export en la Guía del usuario de VM Import/Export. Para obtener información sobre los entornos de virtualización compatibles, consulte Requisitos de VM Import/Export.

Añadir una AMI desde AWS Marketplace

Para añadir muchas AMI AWS Marketplace a su dispositivo de la familia Snow, inicie la AWS Marketplace instancia, cree una AMI a partir de ella y configure la AMI en la misma región desde la que solicitará el dispositivo Snow. A continuación, puede optar por incluir la AMI en el dispositivo al crear un trabajo para encargar el dispositivo. Al elegir una AMI del Marketplace, asegúrese de que tenga un código de producto y una plataforma compatibles.

Temas

- Compruebe los códigos de producto y los detalles de la plataforma de las AWS Marketplace AMI
- Determinación de la versión de la AMI de Amazon Linux 2 para la familia Snow
- Configure la AMI para el dispositivo de la familia Snow

Compruebe los códigos de producto y los detalles de la plataforma de las AWS Marketplace AMI

Antes de comenzar el proceso de añadir una AMI AWS Marketplace a su dispositivo de la familia Snow, asegúrese de que el código de producto y los detalles de la plataforma de la AMI sean compatibles con su Región de AWS.

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación, seleccione la región en la que desea lanzar las instancias y desde la que creará la tarea necesaria para solicitar el dispositivo de la familia Snow. Puede seleccionar cualquier región que esté disponible para usted, independientemente de su ubicación.
3. En el panel de navegación, elija AMI.
4. Utilice las opciones de filtro y búsqueda para examinar la lista de AMI mostradas y ver solo las AMI que coincidan con sus criterios. Por ejemplo, las AMI proporcionadas por AWS Marketplace,

elija Imágenes públicas. A continuación, utilice las opciones de búsqueda para ampliar la lista de AMI mostradas:

- (Nueva consola) Seleccione la barra de búsqueda y, en el menú, elija el alias del propietario, el operador = y, por último, el valor amazon.
- (Consola antigua) Elija la barra Search (Búsqueda) y, en el menú, elija Owner (Propietario) y, a continuación, el valor Amazon images (Imágenes de Amazon).

> **Note**
>
> Las AMI de AWS Marketplace incluyen aws-marketplace en la columna Fuente.

5. En la columna ID de AMI, elija el ID de AMI de la AMI.
6. En el resumen de la imagen de la AMI, asegúrese de que su región admita los códigos de producto. Para obtener más información, consulte la tabla siguiente.

   Códigos de producto AWS Marketplace AMI compatibles

Sistema operativo AMI	Código de producto
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. A continuación, asegúrese también de que los detalles de la plataforma contengan una de las entradas de la siguiente lista.

   - Amazon Linux, Ubuntu o Debian
   - Red Hat Linux bring-your-own-license
   - Amazon RDS para Oracle bring-your-own-license
   - Windows bring-your-own-license

Determinación de la versión de la AMI de Amazon Linux 2 para la familia Snow

Utilice el siguiente procedimiento para determinar la versión de la AMI de Amazon Linux 2 para la familia Snow en el dispositivo de la familia Snow. Instale la última versión de AWS CLI antes de continuar. Para obtener más información, consulte Instalar o actualizar a la última versión de AWS CLI en la Guía del AWS Command Line Interface usuario.

- Utilice el `describe-images` AWS CLI comando para ver la descripción de la AMI. La versión está incluida en la descripción. Proporcione el certificado de clave pública del paso anterior. Para obtener más información, consulte describe-images en la AWS CLI Referencia de comandos.

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

Example de la salida del comando **`describe-images`**

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

En este ejemplo, la versión de la AMI de Amazon Linux 2 para la familia Snow es**`2.0.20240131.0`**. Se encuentra en el valor del `Description` nombre.

Configure la AMI para el dispositivo de la familia Snow

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Lance una nueva instancia de una AMI compatible en AWS Marketplace.

> **Note**
>
> Al lanzar la instancia, asegúrese de que el espacio de almacenamiento que asigne a la instancia sea adecuado para el uso que se le dará. En la consola de Amazon EC2, esta operación se lleva a cabo en el paso Agregar almacenamiento.

3. Instale y configure las aplicaciones que desea ejecutar en el dispositivo Snowball Edge y compruebe que funcionan según lo previsto.

> **Important**
>
> - Solo se admiten las AMI de un solo volumen.
> - El volumen de EBS de la AMI debe ser tener 10 TB como máximo. Le recomendamos que aprovisione el tamaño de volumen de EBS necesario para los datos de la AMI. Esto ayudará a reducir el tiempo que se tarda en exportar la AMI y cargarla en el dispositivo. Puede cambiar el tamaño de la instancia o agregarle más volúmenes después de implementar el dispositivo.

- La instantánea de EBS de la AMI no debe estar cifrada.

4. Realice una copia del archivo PEM o PPK que usó para el par de claves SSH al crear esta instancia. Guarde este archivo en el servidor que quiere utilizar para comunicarse con el dispositivo Snowball Edge. Anote la ruta de acceso a este archivo porque la necesitará cuando utilice SSH para conectarse a la instancia compatible con EC2 de su dispositivo.

> **Important**
>
> Si no sigue este procedimiento, no podrá conectarse a las instancias con SSH cuando reciba el dispositivo Snowball Edge.

5. Guarde la instancia como una AMI. Para obtener más información, consulte la Guía del usuario de Amazon EC2 para instancias de Linux en la Guía del usuario de Amazon EC2.
6. Repita los pasos 1 a 4 con cada una de las instancias que desee conectar mediante SSH. Asegúrese de hacer copias de cada uno de los pares de claves SSH y haga un seguimiento de las AMI a las que están asociados.
7. Ahora, cuando pida el dispositivo, estas AMI estarán disponibles y podrá agregarlas a su dispositivo.

Agregar una AMI localmente

Cuando el dispositivo llegue a sus instalaciones, podrá agregarle nuevas AMI. Para ver instrucciones, consulte Importación de una imagen de máquina virtual a un dispositivo de la familia Snow. Tenga en cuenta que, aunque se admiten todas las máquinas virtuales, solo se ha probado la funcionalidad completa de las AMI compatibles.

> **Note**
>
> Cuando utiliza VM Import/Export para agregar AMI a su dispositivo o cuando importa una máquina virtual después de implementar el dispositivo, puede agregar máquinas virtuales que usen cualquier sistema operativo. Sin embargo, solo los sistemas operativos compatibles se han probado y validado en los dispositivos Snow Family. Usted es responsable de cumplir los términos y condiciones de cualquier sistema operativo o software que se encuentre en la imagen virtual que importe a su dispositivo.

> **Important**
>
> Para que AWS los servicios funcionen correctamente en un Snowball Edge, debe permitir los puertos para los servicios. Para obtener más detalles, consulte Puertos necesarios para usar AWS los servicios en un dispositivo AWS Snowball perimetral.

Agregar una AMI de Microsoft Windows

En el caso de las máquinas virtuales (VM) que utilizan un sistema operativo Windows compatible, puede agregar la AMI importando la imagen de la máquina virtual de Windows AWS mediante VM Import/Export o importándola al dispositivo directamente después de implementarla en el sitio.

Traiga su propia licencia (BYOL)

Snowball Edge permite importar AMI de Microsoft Windows a su dispositivo con su propia licencia. Bring Your Own License (BYOL) es el proceso de traer una AMI de su propiedad con su licencia local. AWS AWS proporciona opciones de implementación compartidas y dedicadas para la opción BYOL.

Puede agregar su imagen de máquina virtual de Windows a su dispositivo importándola AWS mediante VM Import/Export o importándola a su dispositivo directamente después de implementarla en su sitio. No puede agregar las AMI de Windows que se originaron en. AWS Por lo tanto, debe crear e importar su propia imagen de máquina virtual de Windows y traer su propia licencia si quiere usar la AMI en su dispositivo Snow Family. Para obtener más información acerca de las licencias de Windows y BYOL, consulte Amazon Web Services y Microsoft: preguntas frecuentes.

Creación de una imagen de máquina virtual de Windows para importarla a su dispositivo

Para crear una imagen de máquina virtual de Windows, necesita un entorno de virtualización VirtualBox, por ejemplo, compatible con los sistemas operativos Windows y macOS. Al crear una máquina virtual para dispositivos Snow, le recomendamos que asigne al menos dos núcleos con 4 GB de RAM como mínimo. Cuando la máquina virtual esté en funcionamiento, debe instalar el sistema operativo (Windows Server 2012, 2016 o 2019). Para instalar los controladores necesarios para el dispositivo Snow Family, siga las instrucciones indicadas en esta sección.

Para que una AMI de Windows se ejecute en un dispositivo Snow, debe agregar VirtIO, FLR, NetVCM, Vioinput, Viorng, Vioscsi, Vioserial y los controladores. VioStor Puede descargar un

instalador de software de Microsoft (virtio-win-guest-tools-installer) para instalar estos controladores en imágenes de Windows desde el virtio-win-pkg-scripts GitHub repositorio.

> **Note**
>
> Si piensa importar la imagen de la máquina virtual directamente al dispositivo Snow implementado, el archivo de imagen de la máquina virtual debe tener el formato RAW.

Creación de una imagen de Windows

1. En su equipo con Microsoft Windows, seleccione Inicio y escriba **`devmgmt.msc`** para abrir el Administrador de dispositivos.
2. En el menú principal, elija Acción y, a continuación, seleccione Agregar hardware heredado.
3. En el asistente, elija Siguiente.
4. Seleccione Instalar el hardware seleccionado manualmente de una lista (avanzado) y elija Siguiente.
5. Seleccione Mostrar todos los dispositivos y, a continuación, elija Siguiente.
6. Seleccione Usar disco, abra la lista Copiar archivos del fabricante de y busque el archivo ISO.
7. En el archivo ISO, vaya al directorio `Driver\W2K8R2\amd64` y busque el archivo `.INF`.
8. Elija el archivo .INF, seleccione Abrir y, a continuación, elija Aceptar.
9. Cuando vea el nombre del controlador, elija Siguiente y, a continuación, elija Siguiente dos veces más. A continuación, elija Finalizar.

   De este modo, se instala un dispositivo con el nuevo controlador. El hardware real no existe, por lo que verá un signo de exclamación amarillo que indica que hay un problema en el dispositivo. Debe solucionar este problema.

Solución del problema de hardware

1. Abra el menú contextual (clic con el botón derecho) del dispositivo que tiene el signo de exclamación.
2. Seleccione Desinstalar, desactive Eliminar el software del controlador de este dispositivo y elija Aceptar.

   El controlador está instalado y ya puede lanzar la AMI en su dispositivo.

Importación de una imagen de máquina virtual a su dispositivo

Después de preparar la imagen de máquina virtual, puede utilizar una de las opciones disponibles para importar la imagen a su dispositivo.

- En la nube mediante VM Import/Export: al importar la imagen de la máquina virtual AWS y registrarla como una AMI, puede añadirla a su dispositivo al realizar un pedido en. Consola de administración de la familia de productos Snow de AWS Para obtener más información, consulte Importación de una VM como una imagen utilizando VM Import/Export en la Guía del usuario de VM Import/Export.
- Localmente en el dispositivo que esté desplegado en sus instalaciones: puede importar la imagen de la máquina virtual directamente a su dispositivo mediante AWS OpsHub for Snow Family o el AWS Command Line Interface ()AWS CLI.

  Para obtener información sobre el uso AWS OpsHub, consulte Uso local de instancias informáticas compatibles con Amazon EC2.

  Para obtener información sobre el uso de AWS CLI, consulte. Importación de una imagen de máquina virtual a un dispositivo de la familia Snow

Exportación de la AMI más reciente de Amazon Linux 2

Para actualizar las AMI de Amazon Linux 2 a la versión más reciente, exporte primero la imagen de máquina virtual más reciente de Amazon Linux 2 y AWS Marketplace, a continuación, importe esa imagen de máquina virtual al dispositivo Snow.

1. Utilice el `ssm get-parameters` AWS CLI comando para buscar el ID de imagen más reciente de la AMI de Amazon Linux 2 en 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
   ```

   El comando devuelve el ID de imagen más reciente de la AMI. Por ejemplo, `ami-0ccb473bada910e74`.
2. Exporte la imagen más reciente de Amazon Linux 2. Consulte Exportación de una máquina virtual directamente desde una imagen de máquina de Amazon (AMI) en la Guía del usuario de

Amazon EC2. Utilice el último identificador de imagen de la AMI de Amazon Linux 2 como valor del `image-id` parámetro del `ec2 export-image` comando.

3. Importe la imagen de la máquina virtual al dispositivo Snow mediante la AWS CLI tecla o AWS OpsHub.

   - Para obtener información sobre su uso AWS CLI, consulte[Importación de una imagen de máquina virtual a un dispositivo de la familia Snow](#).
   - Para obtener información sobre el uso AWS OpsHub, consulte[Importación de una imagen a su dispositivo como una AMI compatible con Amazon EC2](#) .

Importación de una imagen de máquina virtual a un dispositivo de la familia Snow

Puede utilizar el AWS CLI servicio VM Import/Export para importar una imagen de máquina virtual (VM) al dispositivo de la familia Snow como una imagen de máquina de Amazon (AMI). Tras importar una imagen de máquina virtual, registre la imagen como una AMI y ejecútela como una instancia compatible con Amazon EC2.

Puede añadir AMI de Amazon EC2 al dispositivo al crear una tarea para solicitar un dispositivo de la familia Snow. Siga este procedimiento después de recibir el dispositivo de la familia Snow. Para obtener más información, consulte [Paso 2: elija las opciones de computación y almacenamiento](#).

También puede utilizarlo AWS OpsHub para cargar el archivo de imagen de la máquina virtual. Para obtener más información, consulte [Importación de una imagen a su dispositivo como una AMI compatible con Amazon EC2](#) en esta guía.

Temas

- [Paso 1: Prepare la imagen de la máquina virtual y cárguela en el dispositivo de la familia Snow](#)
- [Paso 2: Configure los permisos necesarios](#)
- [Paso 3: Importe la imagen de la máquina virtual como una instantánea en el dispositivo](#)
- [Paso 4: Registrar la instantánea como AMI](#)
- [Paso 5: lance una instancia desde la AMI](#)
- [Acciones adicionales de AMI](#)

Paso 1: Prepare la imagen de la máquina virtual y cárguela en el dispositivo de la familia Snow

Prepare la imagen de máquina virtual exportando una imagen de máquina virtual desde una AMI o instancia de Amazon EC2 Nube de AWS mediante VM Import/Export o generando la imagen de máquina virtual de forma local con la plataforma de virtualización que elija.

Para exportar una instancia de Amazon EC2 como imagen de máquina virtual mediante VM Import/Export, consulte Exportación de una instancia como máquina virtual mediante VM Import/Export en la Guía del usuario de VM Import/Export. Para exportar una AMI de Amazon EC2 como una imagen de máquina virtual mediante VM Import/Export, consulte Exportación de una máquina virtual directamente desde una imagen de máquina de Amazon (AMI) en la Guía del usuario de VM Import/Export.

Si genera una imagen de máquina virtual desde su entorno local, asegúrese de que la imagen esté configurada para su uso como AMI en el dispositivo de la familia Snow. Es posible que necesite configurar los siguientes elementos, según su entorno.

- Configure y actualice el sistema operativo.
- Establezca un nombre de host.
- Asegúrese de que el protocolo de tiempo de red (NTP) esté configurado.
- Incluya las claves públicas de SSH, si es necesario. Haga copias locales de los pares de claves. Para obtener más información, consulte Uso de SSH para conectarse a sus instancias de cómputo en un Snowball Edge.
- Instale y configure cualquier software que vaya a utilizar en el dispositivo de la familia Snow.

> **Note**
>
> Tenga en cuenta las siguientes limitaciones al preparar una instantánea de disco para un dispositivo de la familia Snow.
>
> - Actualmente, los dispositivos Snow Family solo permiten importar instantáneas que tienen el formato de imagen RAW.
> - Actualmente, los dispositivos Snow Family solo permiten importar instantáneas cuyos tamaños oscilen entre 1 GB y 1 TB.

Carga de una imagen de máquina virtual a un bucket de Amazon S3 en el dispositivo de la familia Snow

Tras preparar una imagen de máquina virtual, cárguela en un bucket de S3 del dispositivo o clúster de la familia Snow. Puede utilizar el adaptador S3 o el almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow para cargar la instantánea.

Para cargar la imagen de la máquina virtual mediante el adaptador S3

- Utilice el `cp` comando para copiar el archivo de imagen de la máquina virtual en un depósito del dispositivo.

  ```
  aws s3 cp image-path s3://S3-bucket-name --endpoint http://S3-object-API-endpoint:443 --profile profile-name
  ```

  Para obtener más información, consulte AWS CLI los comandos compatibles en esta guía.

Para cargar la imagen de la máquina virtual mediante un almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow

- Utilice el `put-object` comando para copiar el archivo de instantáneas en un depósito del 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 obtener más información, consulte Trabajo con objetos S3 en un dispositivo Snowball Edge.

Paso 2: Configure los permisos necesarios

Para que la importación se realice correctamente, debe configurar los permisos para VM Import/Export en el dispositivo de la familia Snow, Amazon EC2 y el usuario.

> **Note**
>
> Los roles de servicio y las políticas que proporcionan estos permisos se encuentran en el dispositivo Snow Family.

Permisos necesarios para la importación y exportación de máquinas virtuales

Antes de iniciar el proceso de importación, debe crear un rol de IAM con una política de confianza que permita que VM Import/Export del dispositivo de la familia Snow asuma el rol. Se otorgan permisos adicionales a la función para permitir que VM Import/Export del dispositivo acceda a la imagen almacenada en el bucket S3 del dispositivo.

Creación de un archivo json de política de confianza

A continuación, se muestra un ejemplo de política de confianza que hay que adjuntar al rol para que VM Import/Export pueda obtener acceso a la instantánea que se debe importar del bucket de S3.

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

Creación de un rol con el archivo json de política de confianza

El nombre del rol puede ser vmimport. Puede cambiarlo mediante la opción --role-name del 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
```

A continuación se muestra un ejemplo de salida del 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"
   }
}
```

Creación de una política para el rol

La siguiente política de ejemplo tiene los permisos mínimos necesarios para obtener acceso a Amazon S3. Cambie el nombre del bucket de Amazon S3 por el del bucket que contiene sus imágenes. En el caso de un dispositivo Snowball Edge independiente, cambie *snow-id* por su ID de trabajo. Si se trata de un clúster de dispositivos, cambie *snow-id* por el ID del clúster. También puede usar prefijos para restringir aún más la ubicación desde la que VM Import/Export puede importar instantáneas. Cree un archivo 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/*"
            ]
      }
   ]
}
```

Creación de una política con el archivo 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
```

A continuación, se muestra un ejemplo de salida del 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"
   }
}
```

Asociación de la política al rol

Asocie una política al rol anterior y conceda permisos de acceso a los recursos necesarios. Esto permite que el servicio local VM Import/Export descargue la instantánea de Amazon S3 en el 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
```

Permisos requeridos por la persona que llama

Además del rol que debe asumir VM Import/Export de Snowball Edge, también debe asegurarse de que el usuario tenga los permisos que le permitan transferir el rol a VMIE. Si utiliza el usuario raíz predeterminado para realizar la importación, el usuario raíz ya tiene todos los permisos necesarios, por lo que puede omitir este paso e ir al paso 3.

Asocie los dos permisos de IAM siguientes al usuario que está realizando la importación.

- `pass-role`
- `get-role`

Creación de una política para el rol

A continuación se ofrece un ejemplo de una política que permite a un usuario realizar las acciones `get-role` y `pass-role` para el rol de 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"
                }
            }
        }
   ]
}
```

Creación de una política con el archivo 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
```

A continuación, se muestra un ejemplo de salida del 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"
   }
}
```

Una vez generada la política, asóciela a los usuarios de IAM que llamarán a la API o a la operación de la CLI de Amazon EC2 para importar la instantánea.

```
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
```

Permisos necesarios para llamar a las API de Amazon EC2 en su dispositivo

Para importar una instantánea, el usuario de IAM debe tener los permisos `ec2:ImportSnapshot`. Si no es necesario restringir el acceso al usuario, puede utilizar los permisos `ec2:*` para conceder acceso total a Amazon EC2. Los siguientes son los permisos que se pueden conceder o restringir para Amazon EC2 en su dispositivo. Se muestra el contenido de la creación de un archivo de política:

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

Creación de una política con el archivo 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
```

A continuación, se muestra un ejemplo de salida del 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"
        }
}
```

Una vez generada la política, asóciela a los usuarios de IAM que llamarán a la API o a la operación de la CLI de Amazon EC2 para importar la instantánea.

```
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
```

Paso 3: Importe la imagen de la máquina virtual como una instantánea en el dispositivo

El siguiente paso es importar la imagen de la máquina virtual como una instantánea en el dispositivo. El valor del `S3Bucket` parámetro es el nombre del depósito que contiene la imagen de la máquina virtual. El valor del `S3Key` parámetro es la ruta al archivo de imagen de máquina virtual de este depósito.

```
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 obtener más información, consulte import-snapshot en la Referencia de AWS CLI comandos.

Este comando no admite los siguientes modificadores.

- [--client-data `value`]
- [--client-token `value`]
- [--dry-run]
- [--no-dry-run]
- [--encrypted]
- [--no-encrypted]
- [--kms-key-id `value`]
- [--tag-specifications `value`]

Example salida del comando **`import-snapshot`**

```
{
   "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**
>
> Los dispositivos de la familia Snow actualmente solo permiten ejecutar un trabajo de importación activo a la vez, por dispositivo. Para iniciar una nueva tarea de importación, espere a que finalice la tarea actual o elija otro nodo disponible en un clúster. También puede optar por cancelar la importación actual si lo desea. Para evitar demoras, no reinicie el dispositivo Snow Family mientras la importación esté en curso. Si reinicia el dispositivo, se producirá un error en la importación y el progreso se eliminará cuando se pueda obtener acceso al dispositivo. Para comprobar el estado de la tarea de importación de instantáneas, use el comando siguiente:
>
> ```
> aws ec2 describe-import-snapshot-tasks --import-task-ids id --profile profile-name --endpoint http://snowball-ip:8008 --region snow
> ```

Paso 4: Registrar la instantánea como AMI

Cuando la importación de la instantánea al dispositivo se haya realizado correctamente, puede registrarla mediante el comando `register-image`.

> **Note**
>
> Solo puede registrar una AMI cuando todas sus instantáneas estén disponibles.

Para obtener más información, consulte register-image en la Referencia de comandos. AWS CLI

Example del comando **`register-image`**

```
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
```

El siguiente es un ejemplo de JSON de asignación de dispositivos de bloques. Para obtener más información, consulte el block-device-mapping parámetro register-image en la AWS CLI Referencia de comandos.

```
[
    {
        "DeviceName": "/dev/sda",
        "Ebs":
            {
                "Encrypted": false,
                "DeleteOnTermination": true,
                "SnapshotId": "snapshot-id",
                "VolumeSize": 30
            }
    }
]
```

Example del comando **`register-image`**

```
{
    "ImageId": "s.ami-8de47d2e397937318"
 }
```

Paso 5: lance una instancia desde la AMI

Para lanzar una instancia, consulta run-instances en la Referencia de AWS CLI comandos.

El valor del `image-id` parámetro es el valor del `ImageId` nombre como resultado del `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**
>
> También se puede utilizar AWS OpsHub para lanzar la instancia. Para obtener más información, consulte Lanzamiento de una instancia compatible con Amazon EC2 en esta guía.

Acciones adicionales de AMI

Puede utilizar AWS CLI comandos adicionales para supervisar el estado de importación de las instantáneas, obtener detalles sobre las instantáneas que se han importado, cancelar la importación de una instantánea y eliminar o anular el registro de las instantáneas una vez importadas.

Supervisar el estado de importación de instantáneas

Para ver el estado actual del progreso de la importación, puede ejecutar el comando `describe-import-snapshot-tasks` de Amazon EC2. Este comando admite la paginación y el `task-state` filtrado en.

Example del comando **`describe-import-snapshot-tasks`**

```
aws ec2 describe-import-snapshot-tasks --import-task-ids id --profile profile-name --
endpoint http://snowball-ip:8008 --region snow
```

Example de la salida del **`describe-import-snapshot-tasks`** 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**
>
> Este comando solo muestra el resultado de las tareas que se han completado correctamente o que se han marcado como eliminadas en los últimos 7 días. El filtrado solo admite `Name=task-state`, `Values=active | deleting | deleted | completed`

Este comando no admite los siguientes parámetros.

- [--dry-run]
- [--no-dry-run]

Cancelar una tarea de importación

Para cancelar una tarea de importación, ejecute el comando `cancel-import-task`.

Example del comando **`cancel-import-task`**

```
aws ec2 cancel-import-task --import-task-id import-task-id --profile profile-name --
endpoint http://snowball-ip:8008 --region snow
```

Example de la salida del **`cancel-import-task`** comando

```
{
        "ImportTaskId": "s.import-snap-8234ef2a01cc3b0c6",
        "PreviousState": "active",
        "State": "deleting"
}
```

> **Note**
>
> Solo se pueden cancelar las tareas que no tienen el estado completado.

Este comando no admite los siguientes parámetros.

- [--dry-run]
- [--no-dry-run]

Descripción de instantáneas

Después de importar una instantánea, puede usar este comando para describirla. Para filtrar las instantáneas, puede pasarlas en `snapshot-ids` con el ID de instantánea de la respuesta de la tarea de importación anterior. Este comando admite la paginación y el filtrado por `volume-idstatus`, `ystart-time`.

Example del **`describe-snapshots`** comando

```
aws ec2 describe-snapshots --snapshot-ids snapshot-id --profile profile-name --endpoint
 http://snowball-ip:8008 --region snow
```

Example de la salida del **`describe-snapshots`** 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
        }
    ]
 }
```

Este comando no admite los siguientes parámetros.

- [--restorable-by-user-ids `value`]
- [--dry-run]
- [--no-dry-run]

Eliminar una instantánea de un dispositivo de la familia Snow

Para eliminar instantáneas de su propiedad y que ya no necesita, puede usar el comando `delete-snapshot`.

Example del **`delete-snapshot`** comando

```
aws ec2 delete-snapshot --snapshot-id snapshot-id --profile profile-name --endpoint
 http://snowball-ip:8008 --region snow
```

> **Note**
>
> Snowball Edge no permite eliminar instantáneas que se encuentren en estado PENDIENTE o que estén designadas como dispositivo raíz para una AMI.

Este comando no admite los siguientes parámetros.

- [--dry-run]
- [--no-dry-run]

Anulación del registro de una AMI

Para anular el registro de las AMI que ya no necesita, puede ejecutar el comando `deregister-image`. Actualmente, no se puede anular el registro de una AMI que tiene el estado Pendiente.

Example del **`deregister-image`** comando

```
aws ec2 deregister-image --image-id image-id --profile profile-name --endpoint
 http://snowball-ip:8008 --region snow
```

Este comando no admite los siguientes parámetros.

- [--dry-run]
- [--no-dry-run]

Uso de las operaciones AWS CLI y de la API en Snowball Edge

Al utilizar las operaciones AWS Command Line Interface (AWS CLI) o API para emitir comandos de IAM, Amazon S3 y Amazon EC2 en Snowball Edge, debe especificar `region` «». `snow` Puede hacerlo utilizando `AWS configure` o dentro del propio comando, como en los ejemplos siguientes.

```
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
```

Or (Disyunción)

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

Cuotas de instancias de computación en un dispositivo Snowball Edge

A continuación se indican las cuotas de almacenamiento y las limitaciones de recursos compartidos para los recursos informáticos de un AWS Snowball Edge dispositivo.

Cuotas de almacenamiento

En los dispositivos Snowball Edge, el almacenamiento disponible para recursos de computación es un recurso independiente del almacenamiento de Amazon S3 dedicado. Las cuotas de almacenamiento son las siguientes:

- Cuotas de almacenamiento para la opción Snowball Edge optimizado para almacenamiento: el almacenamiento total disponible para Amazon S3 oscila entre 60 TB y 80 TB, en función de si utiliza o no instancias de computación en el dispositivo. Si se utilizan instancias de computación, el almacenamiento dedicado total que estará disponible para las instancias de computación de `sbe1` para la opción Snowball Edge optimizado para almacenamiento será de 1000 GB.
- Cuotas de almacenamiento para las opciones Snowball Edge optimizado para computación y Snowball Edge optimizado para almacenamiento con GPU: el almacenamiento dedicado total disponible para las instancias `sbe-c` y `sbe-g` es de 7,68 TB. El espacio de almacenamiento restante que está disponible es de 42 TB.

En las tablas siguientes, se describen los recursos de computación disponibles para los dispositivos Snowball Edge.

Característica	Limitación
Número de AMI en un único dispositivo con la opción Snowball Edge optimizado para almacenamiento	10
Número de AMI en un único dispositivo con la opción Snowball Edge optimizado para computación	20

Característica	Limitación
Número de AMI en un único dispositivo con la opción Snowball Edge optimizado para computación con GPU	20
Número de volúmenes por instancia	10
Instancias en ejecución (o detenidas) simultáneamente	Varía en función de los recursos disponibles

Tipo de instancia	Núcleos de CPU virtual	Memoria (GiB)	GPU	Opción de dispositivo compatible
`sbe1.small`	1	1	0	optimizado para almacenamiento
`sbe1.medium`	1	2	0	optimizado para almacenamiento
`sbe1.large`	2	4	0	optimizado para almacenamiento
`sbe1.xlarge`	4	8	0	optimizado para almacenamiento
`sbe1.2xlarge`	8	16	0	optimizado para almacenamiento
`sbe1.4xlarge`	16	32	0	optimizado para almacenamiento
`sbe1.6xlarge`	24	32	0	optimizado para almacenamiento

Tipo de instancia	Núcleos de CPU virtual	Memoria (GiB)	GPU	Opción de dispositivo compatible
sbe-c.small	1	2	0	optimizado para computación
sbe-c.medium	1	4	0	optimizado para computación
sbe-c.large	2	8	0	optimizado para computación
sbe-c.xlarge	4	16	0	optimizado para computación
sbe-c.2xlarge	8	32	0	optimizado para computación
sbe-c.4xlarge	16	64	0	optimizado para computación
sbe-c.8xlarge	32	128	0	optimizado para computación
sbe-c.12xlarge	48	192	0	optimizado para computación
sbe-c.16xlarge	64	256	0	optimizado para computación
sbe-c.24xlarge	96	384	0	optimizado para computación
sbe-g.small	1	2	1	con GPU
sbe-g.medium	1	4	1	con GPU
sbe-g.large	2	8	1	con GPU

Tipo de instancia	Núcleos de CPU virtual	Memoria (GiB)	GPU	Opción de dispositivo compatible
`sbe-g.xlarge`	4	16	1	con GPU
`sbe-g.2xlarge`	8	32	1	con GPU
`sbe-g.4xlarge`	16	64	1	con GPU
`sbe-g.8xlarge`	32	128	1	con GPU
`sbe-g.12xlarge`	48	192	1	con GPU

Limitaciones de los recursos de computación compartidos

Todos los servicios de los dispositivos Snowball Edge utilizan algunos de los recursos limitados del dispositivo. Los dispositivos Snowball Edge que tienen los máximos recursos de computación disponibles no pueden lanzar nuevos recursos de computación. Por ejemplo, si intenta iniciar la interfaz de NFS mientras está ejecutando una instancia de computación `sbe1.4xlarge` en un dispositivo optimizado para almacenamiento, el servicio de interfaz de NFS no se iniciará. A continuación, se describen los recursos disponibles en las diferentes opciones de dispositivo, así como los requisitos de recursos de cada servicio.

- Si no hay servicios de computación con el estado `ACTIVE`:
  - En el caso de una opción optimizada para almacenamiento, dispone de 24 vCPU y 32 GiB de memoria para las instancias de computación.
  - En el caso de una opción optimizada para computación, dispone de 52 vCPU y 208 GiB de memoria para las instancias de computación. Esto también es aplicable a la opción con GPU.
- Mientras AWS IoT Greengrass y AWS Lambda con tecnología de alimentación AWS IoT Greengrass están`ACTIVE`:
  - En el caso de una opción optimizada para almacenamiento, estos servicios utilizan 4 núcleos de vCPU y 8 GiB de memoria.
  - En el caso de una opción optimizada para computación, estos servicios utilizan 1 núcleo de vCPU y 1 GiB de memoria. Esto también es aplicable a la opción con GPU.

- Mientras la interfaz de NFS tiene el estado `ACTIVE`, utiliza 8 núcleos de vCPU y 16 GiB de memoria de un dispositivo Snowball Edge.
- Mientras el almacenamiento compatible con Amazon S3 en los dispositivos Snow Family tiene el estado ACTIVO:
  - En un dispositivo Snowball Edge optimizado para computación con AMD EPYC Gen2 y NVME, para un solo nodo con la configuración mínima de 3 TB de almacenamiento compatible con Amazon S3 en dispositivos Snow Family, utiliza 8 núcleos de vCPU y 16 GB de memoria. Para un solo nodo con más de 3 TB de almacenamiento compatible con Amazon S3 en dispositivos Snow Family, utiliza 20 núcleos de vCPU y 40 GB de memoria. Para un clúster, utiliza 20 núcleos de vCPU y 40 GB de memoria.
  - En un dispositivo Snowball Edge optimizado para computación con AMD EPYC Gen1, HDD y GPU opcional, para un solo nodo utiliza 8 núcleos de vCPU y 16 GB de memoria. Para un clúster, utiliza 20 núcleos de vCPU y 40 GB de memoria.

Para determinar si un servicio tiene el estado `ACTIVE` en un dispositivo Snowball Edge, utilice el comando `snowballEdge describe-service` del cliente de Snowball Edge. Para obtener más información, consulte Obtención del estado de los servicios.

Creación de un trabajo de computación

En esta sección, creará su primer trabajo de instancia de computación compatible con Amazon EC2 para un dispositivo AWS Snowball Edge.

> **Important**
>
> Tenga en cuenta lo siguiente antes de crear el trabajo:
>
> - Asegúrese de que los valores de vCPU, memoria y almacenamiento asociados a la AMI coinciden con el tipo de instancia que desea crear.
> - Si va a utilizar Secure Shell (SSH) para conectarse a la instancia después de lanzar dicha instancia en el dispositivo Snowball Edge, debe realizar primero el siguiente procedimiento. No es posible actualizar las AMI en su dispositivo Snowball Edge posteriormente. Debe completar este paso antes de crear el trabajo.

Configuración de una AMI de forma que utilice SSH para conectarse a instancias de computación lanzadas en el dispositivo

Si desea utilizar Secure Shell (SSH) para conectarse a las instancias de computación de los dispositivos Snowball Edge, debe realizar el procedimiento que se indica a continuación. Este procedimiento agrega la clave SSH a la AMI antes de crear el trabajo. También es conveniente que siga este procedimiento para configurar las aplicaciones de la instancia que piensa utilizar como AMI para el trabajo.

> **Important**
>
> Si no sigue este procedimiento, no podrá conectarse a las instancias con SSH cuando reciba el dispositivo Snowball Edge.

Cómo poner una clave SSH en una AMI

1. Lance una nueva instancia Nube de AWS basada en la imagen AMI de CentOS 7 (x86_64), con actualizaciones de HVM, Ubuntu 16.04 LTS, Xenial (HVM) y Amazon Linux 2 AMI, o Windows.

   Al lanzar la instancia, es conveniente que se asegure de que el espacio de almacenamiento que asigna a la instancia sea adecuado para el uso que se le dará en el dispositivo Snowball Edge. En la consola de Amazon EC2, esta operación se lleva a cabo en Step 4: Add Storage. Para obtener una lista de los tamaños admitidos para los volúmenes de almacenamiento de instancia de computación en un dispositivo Snowball Edge, consulte Cuotas de instancias de computación en un dispositivo Snowball Edge.
2. Instale y configure las aplicaciones que desea ejecutar en el dispositivo Snowball Edge y compruebe que funcionan según lo previsto.
3. Realice una copia del archivo PEM/PPK que usó para el par de claves SSH para crear esta instancia. Guarde este archivo en el servidor que quiere utilizar para comunicarse con el dispositivo Snowball Edge. Este archivo es necesario para utilizar SSH para conectarse a la instancia lanzada en el dispositivo; por lo tanto, anote la ruta de este archivo.
4. Guarde la instancia como una AMI. Para obtener más información, consulte Creación de una AMI de Linux respaldada por Amazon EBS en la Guía del usuario de Amazon EC2.
5. Repita este procedimiento con cada una de las instancias a las que desee conectarse mediante SSH. No olvide realizar copias de los distintos pares de claves SSH y tome nota de las AMI a las que están asociados.

Creación de un trabajo en la consola

El siguiente paso es crear un trabajo para solicitar un dispositivo de la familia Snow. El trabajo puede ser de cualquier tipo, incluido un clúster. Para ello Consola de administración de la familia de productos Snow de AWS, siga las instrucciones que se proporcionan en la sección Creación de un trabajo para solicitar un dispositivo de la familia Snow. Cuando llegue a la página Paso 3: proporcionar detalles del trabajo del asistente de creación de trabajos, lleve a cabo los siguientes pasos adicionales.

1. Elija Enable compute with EC2.
2. Elija Add an AMI.
3. En el cuadro de diálogo que aparece, elija una AMI y seleccione Save.
4. Añada hasta 20 AMI en total a su trabajo, según el tipo de dispositivo.
5. Continúe creando el trabajo como lo haría normalmente.

Creando tu trabajo en el AWS CLI

También puede crear el trabajo a través de la AWS CLI. Para ello, abra un terminal y ejecute el siguiente comando, reemplazando el texto rojo por sus valores reales.

```
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
```

Cuando llegue el dispositivo y lo desbloquee, tendrá que utilizar el cliente de Snowball Edge para obtener sus credenciales locales. Para obtener más información, consulte Obtención de credenciales.

Configuración de red para instancias de computación

Tras lanzar las instancias computación en un dispositivo Snow Family, debe crear una interfaz de red para proporcionarle una dirección IP. Los dispositivos Snow Family admiten dos tipos de interfaces de red: una interfaz de red virtual y una interfaz de red directa.

Interfaz de red virtual (VNI)

Una interfaz de red virtual es la interfaz de red estándar para conectarse a una instancia compatible con EC2 en su dispositivo Snow Family. Debe crear una VNI para cada una de sus instancias compatibles con EC2, independientemente de si también utiliza una interfaz de red directa o no. El tráfico que pasa a través de una VNI está protegido por los grupos de seguridad que configure. Solo puede asociar las VNI al puerto de red física que utilice para controlar su dispositivo Snow Family.

> **Note**
>
> La VNI usará la misma interfaz física (RJ45, SFP+ o QSFP) que se utiliza para administrar el dispositivo Snow Family. La creación de una VNI en otra interfaz física que la que se utiliza para la administración de dispositivos podría provocar resultados inesperados.

Interfaz de red directa (DNI)

Una interfaz de red directa (DNI) es una característica de red avanzada que permite casos de uso como las transmisiones multidifusión, el enrutamiento transitivo y el equilibrio de carga. Al proporcionar a las instancias acceso a la red de capa 2 sin ningún tipo de traducción o filtrado intermedio, puede aumentar la flexibilidad en la configuración de red de su dispositivo Snow Family y mejorar el rendimiento de la red. Las DNI admiten etiquetas de VLAN y permiten personalizar la dirección MAC. El tráfico en las DNI no está protegido por grupos de seguridad.

En los dispositivos Snowball Edge, las DNI se pueden asociar a los puertos RJ45, SFP o QSFP. Cada puerto físico admite un máximo de 63 DNI. Los DNI no tienen que estar asociados al mismo puerto de red físico que se utiliza para administrar el dispositivo de la familia Snow.

> **Note**
>
> Los dispositivos Snowball Edge optimizados para almacenamiento (con funcionalidad de computación de EC2) no admiten las DNI.

Temas

Requisitos previos

Antes de configurar una VNI o una DNI, asegúrese de que cumple los siguientes requisitos previos.

1. Asegúrese de que el dispositivo reciba alimentación eléctrica y que una de las interfaces de red física, como el puerto RJ45, esté conectada con una dirección IP.
2. Obtenga la dirección IP asociada a la interfaz de red física que está utilizando en el dispositivo Snow Family.
3. Configure el cliente de Snowball Edge. Para obtener más información, consulte Configuración de un perfil para el cliente de Snowball Edge.
4. Desbloquee el dispositivo. Te recomendamos que lo AWS OpsHub for Snow Family utilices para desbloquear el dispositivo. Para obtener instrucciones, consulte Desbloqueo de un dispositivo.

   Si desea utilizar el comando de la CLI, ejecute el siguiente comando y proporcione la información que aparece en el cuadro de diálogo.

   ```
   snowballEdge configure
   ```

   ```
   Snowball Edge Manifest Path: manifest.bin

   Unlock Code: unlock code

   Default Endpoint: https://device ip
   ```
5. Ejecute el siguiente comando de la .

   ```
   snowballEdge unlock-device
   ```

   La actualización de la pantalla del dispositivo indica que está desbloqueado.
6. Lance una instancia compatible con EC2 en el dispositivo. Asociará la VNI a esta instancia.
7. Ejecute el comando `snowballEdge describe-device` para obtener una lista de los ID de interfaz de red física.
8. Identifique el ID de la interfaz de red física que desea utilizar y anótelo.

Configuración de una interfaz de red virtual (VNI)

Una vez que haya identificado el ID de la interfaz de red física, puede configurar una interfaz de red virtual (VNI). Utilice el siguiente procedimiento para configurar una VNI. Asegúrese de realizar las tareas que son requisitos previos antes de crear una VNI.

Creación de una VNI y asociación de una dirección IP

1. Ejecute el comando `snowballEdge create-virtual-network-interface`. Los siguientes ejemplos muestran la ejecución de este comando con dos métodos de asignación de direcciones IP diferentes: `DHCP` o `STATIC`. El método `DHCP` utiliza el protocolo de configuración dinámica de host (DHCP).

   ```
   snowballEdge create-virtual-network-interface \
   --physical-network-interface-id s.ni-abcd1234 \
   --ip-address-assignment DHCP

           //OR//

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

   El comando devuelve una estructura JSON que incluye la dirección IP. Anote esa dirección IP para el `ec2 associate-address` AWS CLI comando que se ejecute más adelante en el proceso.

   Siempre que necesite esta dirección IP, puede utilizar el comando del cliente de `snowballEdge describe-virtual-network-interfaces` Snowball Edge o el `aws ec2 describe-addresses` AWS CLI comando para obtenerla.

2. Para asociar la dirección IP recién creada con la instancia, utilice el siguiente comando, reemplazando el texto rojo por sus valores:

   ```
   aws ec2 associate-address --public-ip 192.0.2.0 --instance-id s.i-0123456789012345 6
    --endpoint http://Snow Family device physical IP address:8008
   ```

Configuración de una interfaz de red directa (DNI)

> **Note**
>
> La función de interfaz de red directa estará disponible a partir del 12 de enero de 2021 y estará disponible Regiones de AWS en todos los dispositivos de la familia Snow.

Requisitos previos

Antes de configurar una interfaz de red directa (DNI), debe realizar las tareas que se describen en la sección de requisitos previos.

1. Realice las tareas que son requisitos previos antes de configurar la DNI. Para ver instrucciones, consulte Requisitos previos.
2. También debe lanzar una instancia en el dispositivo, crear una VNI y asociarla a la instancia. Para ver instrucciones, consulte Configuración de una interfaz de red virtual (VNI).

> **Note**
>
> Si ha añadido una red directa a su dispositivo existente mediante una actualización de in-the-field software, debe reiniciar el dispositivo dos veces para activar completamente la función.

Creación de una DNI y asociación de una dirección IP

1. Cree una interfaz de red directa y asóciela a la instancia compatible con Amazon EC2 ejecutando el siguiente comando. Necesitará la dirección MAC del dispositivo para el siguiente paso.

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

OPCIONES

`--endpoint <endpoint>` El punto de conexión al que se va a enviar esta solicitud. El punto de conexión de sus dispositivos será una URL que utilice el esquema `https` seguido de una dirección IP. Por ejemplo, si la dirección IP del dispositivo es 123.0.1.2, el punto de conexión del dispositivo sería https://123.0.1.2.

`--instance-id <instanceId>` El ID de instancia compatible con EC2 al que se va a asociar la interfaz (opcional).

`--mac <macAddress>` Establece la dirección MAC de la interfaz de red (opcional).

`--physical-network-interface-id <physicalNetworkInterfaceId>` El ID de la interfaz de red física en la que se va a crear una nueva interfaz de red virtual. Puede determinar las interfaces de red física disponibles en su dispositivo Snowball Edge mediante el comando `describe-device`.

`--vlan <vlanId>` Configure la VLAN asignada a la interfaz (opcional). Cuando se especifica, todo el tráfico enviado desde la interfaz se etiqueta con el ID de VLAN especificado. El tráfico entrante se filtra según el ID de VLAN especificado y se eliminan todas las etiquetas de VLAN antes de pasarlas a la instancia.

2. Si no asoció la DNI a una instancia en el paso 1, puede asociarla ahora ejecutando el comando Actualización de una interfaz de red directa.
3. Tras crear una DNI y asociarla a la instancia compatible con EC2, debe realizar dos cambios de configuración en la instancia compatible con Amazon EC2.

   - El primero consiste en garantizar que los paquetes destinados a la VNI asociada a la instancia compatible con EC2 se envíen a través de eth0.
   - El segundo cambio configura la interfaz de red directa para que utilice DCHP o una IP estática al arrancar.

   A continuación se muestran unos ejemplos de scripts de intérprete de comandos para Amazon Linux 2 y CentOS Linux que realizan estos cambios de configuración.

   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
```

Uso de SSH para conectarse a instancias de cómputo en un dispositivo de la familia Snow

Para usar Secure Shell (SSH) para conectarse a instancias de procesamiento en un dispositivo de la familia Snow, tiene las siguientes opciones para proporcionar o crear una clave SSH.

- Puedes proporcionar la clave SSH de la Amazon Machine Image (AMI) al crear un trabajo para pedir un dispositivo. Para obtener más información, consulte Configuración de una AMI de forma que utilice SSH para conectarse a instancias de computación lanzadas en el dispositivo.
- Puede proporcionar la clave SSH para la AMI al crear una imagen de máquina virtual para importarla a un dispositivo de la familia Snow. Para obtener más información, consulte Importación de una imagen de máquina virtual a un dispositivo de la familia Snow.

- Puede crear un par de claves en el dispositivo de la familia Snow y elegir lanzar una instancia con esa clave pública generada localmente. Para obtener más información, consulte Creación de un par de claves con Amazon EC2 en la Guía del usuario de Amazon EC2.

Para conectarse a una instancia mediante SSH

1. Asegúrese de que el dispositivo está encendido, conectado a la red y desbloqueado. Para obtener más información, consulte Conexión a la red local.
2. Asegúrese de que la red está configurada para las instancias de computación. Para obtener más información, consulte Configuración de red para instancias de computación.
3. Consulte en sus notas el par de claves PEM o PPK que usó con esta instancia específica. Copie los archivos en algún lugar del equipo. Anote la ruta del archivo PEM.
4. Conéctese a la instancia a través de SSH tal y como se muestra en el siguiente comando de ejemplo. La dirección IP es la dirección IP de la interfaz de red virtual (VNIC) que ha configurado en Configuración de red para instancias de computación.

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

   Para obtener más información, consulte Conexión a su instancia de Linux mediante SSH en la Guía del usuario de Amazon EC2.

Transferencia de datos de instancias de computación compatibles con EC2 a buckets de S3 en el mismo dispositivo Snowball Edge

Puede transferir datos entre instancias de computación y buckets de Amazon S3 en el mismo dispositivo Snowball Edge. Para ello, utilice los AWS CLI comandos compatibles y los puntos de enlace adecuados. Por ejemplo, supongamos que desea mover datos de un directorio de la instancia `sbe1.xlarge` al bucket `myBucket` de Amazon S3 en el mismo dispositivo. Suponga que está utilizando el almacenamiento compatible con Amazon S3 en el punto de conexión `https://S3-object-API-endpoint:443` de los dispositivos Snow Family. Use el procedimiento siguiente.

> **Note**
>
> Este procedimiento solamente funcionará si ha seguido las instrucciones de Configuración de una AMI de forma que utilice SSH para conectarse a instancias de computación lanzadas en el dispositivo.

Para transferir datos entre una instancia de computación y un bucket en el mismo dispositivo Snowball Edge

1. Use SSH para conectarse a la instancia de computación.
2. Descargue e instale el AWS CLI. Si la instancia todavía no tiene la AWS CLI, descárguela e instálela. Para obtener más información, consulte Instalación de la AWS Command Line Interface.
3. Configure AWS CLI en su instancia de cómputo para que funcione con el punto de conexión Amazon S3 en Snowball Edge. Para obtener más información, consulte Obtención y uso de las credenciales locales de Amazon S3.
4. Utilice los comandos de almacenamiento compatibles con Amazon S3 en los dispositivos de la familia Snow para transferir datos. Por ejemplo:

```
aws s3 cp ~/june2018/results s3://myBucket/june2018/results --recursive --endpoint
 https://S3-object-API-endpoint:443
```

Comandos del cliente de Snowball Edge para instancias de computación

El cliente de Snowball Edge es una aplicación de terminal independiente que puede ejecutar en el servidor local. Le permite realizar algunas tareas administrativas en el dispositivo o en el clúster de dispositivos Snowball Edge. Para obtener más información acerca de cómo utilizar el cliente de Snowball Edge (por ejemplo, cómo iniciar y detener servicios con él), consulte Uso de los comandos del cliente Snowball Edge.

A continuación, encontrará información acerca de los comandos del cliente de Snowball Edge que son específicos de las instancias de computación, incluidos ejemplos de uso.

Para obtener una lista de los comandos compatibles con Amazon EC2 que puede utilizar en su AWS Snowball Edge dispositivo, consulte. AWS CLI Comandos compatibles con Amazon EC2 compatibles con Snowball Edge

Creación de una configuración de lanzamiento para iniciar automáticamente instancias compatibles con Amazon EC2

Para iniciar automáticamente las instancias informáticas compatibles con Amazon EC2 en su AWS Snowball Edge dispositivo una vez desbloqueado, puede crear una configuración de lanzamiento. Para ello, utilice el comando `snowballEdge create-autostart-configuration`, tal y como se muestra a continuación.

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]
```

Actualización de una configuración de lanzamiento para iniciar automáticamente instancias compatibles con EC2

Para actualizar una configuración de lanzamiento existente en su dispositivo Snowball Edge, utilice el comando `snowballEdge update-autostart-configuration`. Puede ver su uso a continuación. Para habilitar o deshabilitar una configuración de lanzamiento, especifique el parámetro `--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]
```

Eliminación de una configuración de lanzamiento para iniciar automáticamente instancias compatibles con EC2

Para eliminar una configuración de lanzamiento que ya no se usa, utilice el comando `snowballEdge delete-autostart-configuration` como se muestra a continuación.

Uso

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

Enumeración de las configuraciones de lanzamiento para iniciar automáticamente instancias compatibles con EC2

Para mostrar las configuraciones de lanzamiento que ha creado en su dispositivo Snowball Edge, utilice el comando `describe-autostart-configurations` como se indica a continuación.

Uso

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

Creación de una interfaz de red virtual

Para ejecutar una instancia de computación o iniciar la interfaz de NFS en su dispositivo Snowball Edge, tiene que crear primero una interfaz de red virtual (VNIC). Cada dispositivo Snowball Edge tiene tres interfaces de red (NIC), que son los controladores de interfaz de red física del dispositivo. Son los puertos RJ45, SFP y QSFP de la parte posterior del dispositivo.

Cada VNIC se basa en una interfaz física; puede tener cualquier número de VNIC asociadas a cada NIC. Para crear un interfaz de red virtual, use el comando `snowballEdge create-virtual-network-interface`.

> **Note**
>
> El parámetro `--static-ip-address-configuration` solo es válido cuando se utiliza la opción `STATIC` para el parámetro `--ip-address-assignment`.

Uso

Puede utilizar este comando de dos formas: con el cliente de Snowball Edge configurado o sin configurar. En el siguiente ejemplo de uso se muestra el método con el cliente de 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]
```

En el siguiente ejemplo de uso se muestra el método con el cliente de Snowball Edge sin configurar.

```
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 Ejemplo: creación de VNIC (mediante 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",
    "MtuSize" : "1500"
  }
}
```

Descripción de las interfaces de red virtual

Para describir las VNIC que ha creado antes en su dispositivo, utilice el comando `snowballEdge describe-virtual-network-interfaces`. Puede ver su uso a continuación.

Uso

Puede utilizar este comando de dos formas: con el cliente de Snowball Edge configurado o sin configurar. En el siguiente ejemplo de uso se muestra el método con el cliente de Snowball Edge configurado.

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

En el siguiente ejemplo de uso se muestra el método con el cliente de Snowball Edge sin configurar.

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

Example Ejemplo: descripción de las VNIC

```
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",
    "MtuSize" : "1500"
  },{
    "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",
    "MtuSize" : "1500"
  }
]
```

Actualización de una interfaz de red virtual

Una vez creada una interfaz de red virtual (VNIC), puede actualizar su configuración mediante el comando `snowballEdge update-virtual-network-interface`. Después de proporcionar el nombre de recurso de Amazon (ARN) para una determinada VNIC, debe especificar valores únicamente para los elementos que vaya a actualizar.

Uso

Puede utilizar este comando de dos formas: con el cliente de Snowball Edge configurado o sin configurar. En el siguiente ejemplo de uso se muestra el método con el cliente de 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]
```

En el siguiente ejemplo de uso se muestra el método con el cliente de Snowball Edge sin configurar.

```
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 Ejemplo: actualización de una VNIC (mediante DHCP)

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

Eliminación de una interfaz de red virtual

Para eliminar una interfaz de red virtual, use el comando `snowballEdge delete-virtual-network-interface`.

Uso

Puede utilizar este comando de dos formas: con el cliente de Snowball Edge configurado o sin configurar. En el siguiente ejemplo de uso se muestra el método con el cliente de Snowball Edge configurado.

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

En el siguiente ejemplo de uso se muestra el método con el cliente de Snowball Edge sin configurar.

```
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 Ejemplo: eliminación de una VNIC

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

Uso del punto de conexión compatible con Amazon EC2

A continuación, se facilita información general sobre el punto de conexión compatible con Amazon EC2. Con este punto de conexión, puede administrar las imágenes de máquina de Amazon (AMI) y las instancias de computación mediante programación usando operaciones de API compatibles con Amazon EC2.

Especificar el punto de conexión compatible con Amazon EC2 como punto de conexión AWS CLI

Cuando utilice el AWS CLI para enviar un comando al AWS Snowball Edge dispositivo, puede especificar que el punto de conexión sea el punto de conexión compatible con Amazon EC2. Tiene la posibilidad de utilizar el punto de conexión HTTPS o un punto de conexión HTTP no protegido, tal y como se muestra a continuación.

Punto de conexión HTTPS protegido

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

Punto de conexión HTTP no protegido

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

Si utiliza el punto de conexión HTTPS de `8243`, se cifran los datos en tránsito. Este cifrado está protegido con un certificado generado por el dispositivo Snowball Edge siempre que se desbloquea. Una vez que tenga el certificado, puede guardarlo en un archivo `ca-bundle.pem` local. A continuación, puede configurar el perfil de la AWS CLI para incluir la ruta a su certificado, tal y como se describe a continuación.

Asociación del certificado al punto de conexión compatible con Amazon EC2

1. Conecte el dispositivo Snowball Edge a la alimentación eléctrica y a la red y enciéndalo.
2. En cuanto el dispositivo termine de desbloquearse, anote su dirección IP en la red local.
3. En un terminal de la red, asegúrese de que puede hacer ping al dispositivo Snowball Edge.
4. Ejecute el comando `snowballEdge get-certificate` en el terminal. Para obtener más información acerca de este comando, consulte Administración de certificados de clave pública.

5. Guarde el resultado del comando `snowballEdge get-certificate` en un archivo, por ejemplo `ca-bundle.pem`.
6. Ejecute el siguiente comando desde el terminal.

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

Después de realizar este procedimiento, puede ejecutar comandos de la CLI con estas credenciales locales, su certificado y el punto de conexión especificado.

AWS CLI Comandos compatibles con Amazon EC2 compatibles con Snowball Edge

Puede administrar las instancias de computación de un dispositivo Snow Family a través de un punto de conexión compatible con Amazon EC2. Este tipo de punto final admite muchos de los comandos y acciones de la CLI de Amazon EC2 de los AWS SDK. Para obtener información sobre la instalación y la configuración del AWS CLI, incluida la especificación de aquellos contra los que Regiones de AWS desea realizar AWS CLI llamadas, consulte la Guía del AWS Command Line Interface usuario.

Lista de comandos de la AWS CLI compatibles con Amazon EC2 admitidos en un dispositivo Snowball Edge

A continuación, encontrará una descripción del subconjunto de AWS CLI comandos y opciones de Amazon EC2 compatibles con los dispositivos Snowball Edge. Si un comando o una opción no aparece en la lista siguiente, no está admitido. Puede declarar algunas opciones no admitidas junto con un comando. Sin embargo, no se tendrán en cuenta.

- associate-address: asocia con una instancia la dirección IP virtual que se usará en una de las tres interfaces de red física en el dispositivo:
  - --instance-id: el ID de una sola instancia `sbe`.
  - --public-ip: la dirección IP virtual que desea usar para obtener acceso a la instancia.
- attach-volume: asocia un volumen de Amazon EBS a una instancia en ejecución o detenida en el dispositivo y lo expone a la instancia con el nombre de dispositivo especificado.
  - --device `value`: el nombre del dispositivo.
  - --instance-id: el ID de una instancia de destino compatible con Amazon EC2.
  - --volume-id `value`: el ID del volumen de EBS.
- authorize-security-group-egress— Añade una o más reglas de salida a un grupo de seguridad para usarlas con un dispositivo Snowball Edge. En concreto, esta acción permite que las instancias

puedan enviar tráfico a uno o varios rangos de direcciones CIDR IPv4 de destino. Para obtener más información, consulte Grupos de seguridad en dispositivos Snowball Edge.

- --group-id `value`: el ID del grupo de seguridad
- [--ip-permissions `value`]: uno o más conjuntos de permisos de IP.

- authorize-security-group-ingress— Añade una o más reglas de entrada a un grupo de seguridad. Al llamar a `authorize-security-group-ingress`, debe especificar un valor para `group-name` o para `group-id`.
  - [--group-name `value`]: el nombre del grupo de seguridad.
  - [--group-id `value`]: el ID del grupo de seguridad
  - [--ip-permissions `value`]: uno o más conjuntos de permisos de IP.
  - [--protocol `value`]: el protocolo IP. Los posibles valores son `tcp`, `udp` y `icmp`. El argumento `--port` es obligatorio a menos que se especifique el valor "all protocols" (-1).
  - [--port `value`]: para TCP o UDP, el rango de puertos que se permite. Este valor puede ser un número entero específico o un rango (mínimo-máximo).

    En el caso de ICMP, un valor entero específico o un rango (`type-code`) en el que `type` representa el número de tipo de ICMP y `code` representa el número de código de ICMP. El valor -1 indica todos los códigos de ICMP para todos los tipos de ICMP. Si solo `type` tiene el valor -1, indica todos los códigos de ICMP para el tipo de ICMP especificado.
  - [--cidr `value`]: el rango de IP del CIDR.
- create-launch-template— Crea una plantilla de lanzamiento. Una plantilla de lanzamiento contiene los parámetros necesarios para lanzar una instancia. Al lanzar una instancia mediante `RunInstances`, puede especificar una plantilla de lanzamiento en lugar de proporcionar los parámetros de lanzamiento en la solicitud. Puede crear hasta 100 plantillas por dispositivo .
  - -- launch-template-name `string` — Un nombre para la plantilla de lanzamiento.
  - -- launch-template-data `structure` — La información de la plantilla de lanzamiento. Se admiten los siguientes atributos:
    - `ImageId`
    - `InstanceType`
    - `SecurityGroupIds`
    - `TagSpecifications`
    - `UserData`

    Sintaxis de 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`]: una descripción de la primera versión de la plantilla de lanzamiento.
- --endpoint `snowballEndpoint`: un valor que le permite administrar sus instancias de computación mediante programación usando operaciones de API compatibles con Amazon EC2. Para obtener más información, consulte Especificar el punto de conexión compatible con Amazon EC2 como punto de conexión AWS CLI.

- create-launch-template-version— Crea una nueva versión de una plantilla de lanzamiento. Puede especificar una versión existente de una plantilla de lanzamiento en la que se basará la nueva versión. Las versiones de las plantillas de lanzamiento están numeradas en el orden en el que se han creado. No se puede especificar, cambiar ni sustituir la numeración de las versiones de las plantillas de lanzamiento. Puede crear hasta 100 versiones de cada plantilla de lanzamiento.

  Especifique el ID o el nombre de la plantilla de lanzamiento en la solicitud.

  - -- launch-template-id `string` — El ID de la plantilla de lanzamiento.
  - -- launch-template-name `string` — Un nombre para la plantilla de lanzamiento.
  - -- launch-template-data `structure` — La información de la plantilla de lanzamiento. Se admiten los siguientes atributos:
    - `ImageId`
    - `InstanceType`
    - `SecurityGroupIds`
    - `TagSpecifications`
    - `UserData`

  Sintaxis de 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`]: el número de versión de la plantilla de lanzamiento en la que se basará la nueva versión. La nueva versión hereda los mismos parámetros de lanzamiento que la versión de origen, a excepción de los que especifique en `launch-template-data`.
- [--version-description `string`]: una descripción de la primera versión de la plantilla de lanzamiento.
- --endpoint `snowballEndpoint`: un valor que le permite administrar sus instancias de computación mediante programación usando operaciones de API compatibles con Amazon EC2. Para obtener más información, consulte Especificar el punto de conexión compatible con Amazon EC2 como punto de conexión AWS CLI.

- create-tags: agrega o sobrescribe una o varias etiquetas para el recurso especificado. Cada recurso puede tener un máximo de 50 etiquetas. Cada etiqueta consta de una clave y un valor opcional. Las claves de etiqueta deben ser únicas para un recurso. Se admiten los siguientes recursos:
  - AMI
  - instancia
  - Plantilla de inicialización
  - Grupo de seguridad
  - Par de claves
- create-security-group— Crea un grupo de seguridad en tu Snowball Edge. Puede crear hasta 50 grupos de seguridad. Cuando cree un grupo de seguridad, especifique un nombre fácil de recordar:
  - --group-name `value`: el nombre del grupo de seguridad.
  - --description `value`: una descripción del grupo de seguridad. Su función es meramente informativa. Este valor puede tener 255 caracteres como máximo.
- create-volume: crea un volumen de Amazon EBS que se puede asociar a una instancia del dispositivo.

  - [--sizevalue]: el tamaño del volumen en pulgadas GiBs, que puede oscilar entre 1 GiB y 1 TB (GiBs1000).
  - [--snapshot-id `value`]: la instantánea a partir de la que se va a crear el volumen.
  - [--volume-type `value`]: el tipo de volumen. Si no se especifica ningún valor, el valor predeterminado es `sbg1`. Entre los valores posibles se incluyen:
    - `sbg1` para los volúmenes magnéticos
    - `sbp1` para los volúmenes SSD
  - [--tag-specification `value`]: una lista de etiquetas que se aplican al volumen durante su creación.
- delete-launch-template— Elimina una plantilla de lanzamiento. Al eliminar una plantilla de inicialización, también se eliminan todas sus versiones.

  Especifique el ID o el nombre de la plantilla de lanzamiento en la solicitud.
  - -- launch-template-id `string` — El ID de la plantilla de lanzamiento.
  - -- launch-template-name `string` — Un nombre para la plantilla de lanzamiento.
  - --endpoint `snowballEndpoint`: un valor que le permite administrar sus instancias de computación mediante programación usando operaciones de API compatibles con Amazon EC2. Para obtener más información, consulte Especificar el punto de conexión compatible con Amazon EC2 como punto de conexión AWS CLI.
- delete-launch-template-version— Elimina una o más versiones de una plantilla de lanzamiento. No puede eliminar la versión predeterminada de una plantilla de lanzamiento. Para poder hacerlo, primero debe asignar otra versión como predeterminada. Si la versión predeterminada es la única versión de la plantilla de lanzamiento, elimine toda la plantilla de lanzamiento con el comando `delete-launch-template`.

  Especifique el ID o el nombre de la plantilla de lanzamiento en la solicitud.
  - -- launch-template-id `string` — El ID de la plantilla de lanzamiento.
  - -- launch-template-name `string` — Un nombre para la plantilla de lanzamiento.
  - --versions (lista) `"string" "string"`: los números de versión de una o más versiones de la plantilla de lanzamiento que se van a eliminar.
  - --endpoint `snowballEndpoint`: un valor que le permite administrar sus instancias de computación mediante programación usando operaciones de API compatibles con Amazon EC2. Para obtener más información, consulte Especificar el punto de conexión compatible con Amazon EC2 como punto de conexión AWS CLI.
- delete-security-group— Elimina un grupo de seguridad.

Si intenta eliminar un grupo de seguridad asociado a una instancia, o si otro grupo de seguridad hace referencia a este, se produce un error `DependencyViolation` en la operación.

  - --group-name `value`: el nombre del grupo de seguridad.
  - --description `value`: una descripción del grupo de seguridad. Su función es meramente informativa. Este valor puede tener 255 caracteres como máximo.
- delete-tags: elimina el conjunto de etiquetas especificado del recurso indicado (AMI, instancia de computación, plantilla de lanzamiento o grupo de seguridad).
- delete-volume: elimina el volumen de Amazon EBS especificado. El volumen debe tener el estado `available` (no debe estar asociado a ninguna instancia).
  - --volume-id `value`: el ID del volumen.
- describe-addresses: describe una o más de las direcciones IP virtuales asociadas al mismo número de instancias `sbe` de su dispositivo.
  - --public-ips: una o más direcciones IP virtuales asociadas a sus instancias.
- describe-images: describe una o más de las imágenes (AMI) que tiene disponibles. Las imágenes que tiene disponibles se agregan al dispositivo Snowball Edge al crear el trabajo.
  - --image-id: el ID de AMI de Snowball de la AMI.
- describe-instance-attribute— Describe el atributo especificado de la instancia especificada. Solo puede especificar un atributo cada vez. Se admiten los siguientes atributos:
  - `instanceInitiatedShutdownBehavior`
  - `instanceType`
  - `userData`
- describe-instances: describe una o más de sus instancias. La respuesta devuelve los grupos de seguridad asignados a las instancias.
  - --instance-ids: los ID de una o más instancias `sbe` que se detuvieron en el dispositivo.
  - --page-size: el tamaño de cada página que se obtendrá en la llamada. Este valor no afecta a la cantidad de elementos que se devuelven en la salida del comando. Si se configura un tamaño de página menor se generan más llamadas al dispositivo y se recuperan menos elementos en cada llamada. Esta operación puede ayudar a evitar que las llamadas agoten el tiempo de espera.
  - --max-items: el número total de elementos que se devuelven en la salida del comando. Si el número total de elementos disponibles es mayor que el valor especificado, se proporciona

`NextToken` en la salida del comando. Para reanudar la paginación, proporcione el valor de `NextToken` en el argumento `starting-token` de un comando posterior.

- --starting-token: un token para especificar dónde iniciar la paginación. Este token es el valor `NextToken` de una respuesta anterior que estaba truncada.

- describe-instance-status— Describe el estado de las instancias especificadas o de todas las instancias. De forma predeterminada, solo se describen las instancias en ejecución, a menos que indique específicamente que se devuelva el estado de todas las instancias. El estado de la instancia incluye los siguientes componentes:
  - Comprobaciones de estado: el dispositivo Snow realiza comprobaciones de estado en las instancias compatibles con Amazon EC2 en ejecución para identificar problemas de hardware y software.
  - Estado de la instancia: puede administrar sus instancias desde el momento en que las lanza hasta su finalización.

  Con este comando, se admiten los siguientes filtros.

  - `[--filters]` (lista)

    Los filtros.

    - `instance-state-code`: el código del estado de la instancia, como un entero sin signo de 16 bits. El byte alto se utiliza para la elaboración de informes del servicio interno y se debe ignorar. El byte bajo se establece en función del estado representado. Los valores válidos son 0 (pendiente), 16 (en ejecución), 32 (apagando), 48 (finalizado), 64 (deteniendo) y 80 (detenido).
    - `instance-state-name`: el estado de la instancia (`pending` | `running` | `shutting-down` | `terminated` | `stopping` | `stopped`).
    - `instance-status.reachability`: filtra por el estado de la instancia, donde el nombre es `reachability` (`passed` | `failed` | `initializing` | `insufficient-data`).
    - `instance-status.status`: el estado de la instancia (ok| `impaired` | `initializing` | `insufficient-data` |`not-applicable`).
    - `system-status.reachability`: filtra por el estado del sistema, donde el nombre es accesibilidad (`passed` | `failed` | `initializing` | `insufficient-data`).
    - `system-status.status`: el estado del sistema de la instancia (ok | `impaired` | `initializing` | `insufficient-data` | `not-applicable`).
  - Sintaxis de JSON:

```
[
  {
    "Name": "string",
    "Values": ["string", ...]
  }
  ...
]
```

- `[--instance-ids]` (lista)

  Los ID de instancia.

  Valor predeterminado: describe todas las instancias.

- `[--dry-run|--no-dry-run]` (booleano)

  Comprueba si tiene los permisos necesarios para la acción, sin realizar realmente la solicitud, y proporciona una respuesta de error. Si tiene los permisos necesarios, la respuesta de error es `DryRunOperation`.

  De lo contrario, es `UnauthorizedOperation`.

- `[--include-all-instances | --no-include-all-instances]` (booleano)

  Cuando es `true`, incluye el estado de funcionamiento de todas las instancias. Cuando es `false`, incluye el estado de funcionamiento solo de las instancias en ejecución.

  Valor predeterminado: `false`

- `[--page-size]` (entero): el tamaño de cada página que se obtendrá en la llamada. Este valor no afecta a la cantidad de elementos que se devuelven en la salida del comando. Si se configura un tamaño de página menor se generan más llamadas al dispositivo y se recuperan menos elementos en cada llamada. Esta operación puede ayudar a evitar que las llamadas agoten el tiempo de espera.
- `[--max-items]` (entero): el número total de elementos que se devuelven en la salida del comando. Si el número total de elementos disponibles es mayor que el valor especificado, se proporciona `NextToken` en la salida del comando. Para reanudar la paginación, proporcione el valor de `NextToken` en el argumento `starting-token` de un comando posterior.
- `[--starting-token]` (cadena): un token para especificar dónde empezar a paginar. Este token es el valor `NextToken` de una respuesta anterior que estaba truncada.

- describe-launch-templates— Describe una o más plantillas de lanzamiento. El comando `describe-launch-templates` es una operación paginada. Puede hacer varias llamadas para recuperar todo el conjunto de datos de los resultados.

  Especifique los ID o los nombres de las plantillas de lanzamiento en la solicitud.

  - -- launch-template-ids (lista) `"string" "string"` — Una lista de los identificadores de las plantillas de lanzamiento.
  - -- launch-template-names (lista) `"string" "string"` — Una lista de nombres para las plantillas de lanzamiento.
  - --page-size: el tamaño de cada página que se obtendrá en la llamada. Este valor no afecta a la cantidad de elementos que se devuelven en la salida del comando. Si se configura un tamaño de página menor se generan más llamadas al dispositivo y se recuperan menos elementos en cada llamada. Esta operación puede ayudar a evitar que las llamadas agoten el tiempo de espera.
  - --max-items: el número total de elementos que se devuelven en la salida del comando. Si el número total de elementos disponibles es mayor que el valor especificado, se proporciona `NextToken` en la salida del comando. Para reanudar la paginación, proporcione el valor de `NextToken` en el argumento `starting-token` de un comando posterior.
  - --starting-token: un token para especificar dónde iniciar la paginación. Este token es el valor `NextToken` de una respuesta anterior que estaba truncada.
  - --endpoint `snowballEndpoint`: un valor que le permite administrar sus instancias de computación mediante programación usando operaciones de API compatibles con Amazon EC2. Para obtener más información, consulte Especificar el punto de conexión compatible con Amazon EC2 como punto de conexión AWS CLI.
- describe-launch-template-versions— Describe una o más versiones de una plantilla de lanzamiento específica. Puede describir todas las versiones, versiones individuales o un rango de versiones. El comando `describe-launch-template-versions` es una operación paginada. Puede hacer varias llamadas para recuperar todo el conjunto de datos de los resultados.

  Especifique los ID o los nombres de las plantillas de lanzamiento en la solicitud.

  - -- launch-template-id `string` — El ID de la plantilla de lanzamiento.
  - -- launch-template-name `string` — Un nombre para la plantilla de lanzamiento.
  - [--versions (lista) `"string" "string"`]: los números de versión de una o más versiones de la plantilla de lanzamiento que se van a eliminar.

- [--min-version `string`]: el número de versión después del cual se describen las versiones de la plantilla de lanzamiento.
- [--max-version `string`]: el número de versión hasta el que se describen las versiones de la plantilla de lanzamiento.
- --page-size: el tamaño de cada página que se obtendrá en la llamada. Este valor no afecta a la cantidad de elementos que se devuelven en la salida del comando. Si se configura un tamaño de página menor se generan más llamadas al dispositivo y se recuperan menos elementos en cada llamada. Esta operación puede ayudar a evitar que las llamadas agoten el tiempo de espera.
- --max-items: el número total de elementos que se devuelven en la salida del comando. Si el número total de elementos disponibles es mayor que el valor especificado, se proporciona `NextToken` en la salida del comando. Para reanudar la paginación, proporcione el valor de `NextToken` en el argumento `starting-token` de un comando posterior.
- --starting-token: un token para especificar dónde iniciar la paginación. Este token es el valor `NextToken` de una respuesta anterior que estaba truncada.
- --endpoint `snowballEndpoint`: un valor que le permite administrar sus instancias de computación mediante programación usando operaciones de API compatibles con Amazon EC2. Para obtener más información, consulte Especificar el punto de conexión compatible con Amazon EC2 como punto de conexión AWS CLI.

- describe-security-groups— Describe uno o más de sus grupos de seguridad.

  El comando `describe-security-groups` es una operación paginada. Puede emitir varias llamadas a la API para recuperar todo el conjunto de datos de los resultados.

  - [--group-name `value`]: el nombre del grupo de seguridad.
  - [--group-id `value`]: el ID del grupo de seguridad.
  - [--page-size`value`]: el tamaño de cada página para recibir la AWS llamada de servicio. Este tamaño no afecta a la cantidad de elementos que se devuelven en la salida del comando. Si se configura un tamaño de página menor, se generan más llamadas al servicio de AWS y se recuperan menos elementos en cada llamada. Este enfoque puede ayudar a evitar que se agote el tiempo de espera AWS de las llamadas de servicio. Para ver ejemplos de uso, consulte Paginación en la Guía del usuario de AWS Command Line Interface .
  - [--max-items `value`]: el número total de elementos que se devuelven en la salida del comando. Si el número total de elementos disponibles es mayor que el valor especificado, se proporciona `NextToken` en la salida del comando. Para reanudar la paginación, proporcione el valor

de `NextToken` en el argumento `starting-token` de un comando posterior. No utilice el elemento de respuesta `NextToken` directamente fuera de la AWS CLI. Para ver ejemplos de uso, consulte Paginación en la Guía del usuario de AWS Command Line Interface .

- [--starting-token `value`]: un token para especificar dónde iniciar la paginación. Este token es el valor `NextToken` de una respuesta anterior que estaba truncada. Para ver ejemplos de uso, consulte Paginación en la Guía del usuario de AWS Command Line Interface .

- describe-tags: describe una o varias etiquetas para el recurso especificado (`image`, `instance` o grupo de seguridad). Con este comando, se admiten los siguientes filtros:
  - launch-template
  - resource-id
  - resource-type: `image` o `instance`
  - key
  - valor
- describe-volumes: describe los volúmenes de Amazon EBS especificados.
  - [--max-items `value`]: el número total de elementos que se devuelven en la salida del comando. Si el número total de elementos disponibles es mayor que el valor especificado, se proporciona `NextToken` en la salida del comando. Para reanudar la paginación, proporcione el valor de `NextToken` en el argumento `starting-token` de un comando posterior.
  - [--starting-token `value`]: un token para especificar dónde iniciar la paginación. Este token es el valor `NextToken` de una respuesta anterior que estaba truncada.
  - [--volume-ids `value`]: uno o más ID de volumen.
- detach-volume: desasocia un volumen de Amazon EBS de una instancia detenida o en ejecución.
  - [--device `value`]: el nombre del dispositivo.
  - [--instance-id]: el ID de una instancia de Amazon EC2 de destino.
  - --volume-id `value`: el ID del volumen.
- disassociate-address: desasocia la dirección IP virtual de la instancia con la que está asociada.
  - --public-ip: la dirección IP virtual que desea desasociar de la instancia.
- get-launch-template-data— Recupera los datos de configuración de la instancia especificada. Puede utilizar estos datos para crear una plantilla de lanzamiento.
  - --instance-id: el ID de una sola instancia `sbe`.
  - --endpoint `snowballEndpoint`: un valor que le permite administrar sus instancias de computación mediante programación usando operaciones de API compatibles con Amazon

EC2. Para obtener más información, consulte Especificar el punto de conexión compatible con Amazon EC2 como punto de conexión AWS CLI.

- modify-launch-template— Modifica una plantilla de lanzamiento. Puede especificar qué versión de la plantilla de lanzamiento se establecerá como la versión predeterminada. Al lanzar una instancia sin especificar una versión de una plantilla de lanzamiento, se aplica la versión predeterminada de la plantilla de lanzamiento.

  Especifique el ID o el nombre de la plantilla de lanzamiento en la solicitud.

  - -- launch-template-id `string` — El ID de la plantilla de lanzamiento.
  - -- launch-template-name `string` — Un nombre para la plantilla de lanzamiento.
  - --default-version `string`: el número de versión de la plantilla de lanzamiento que se establecerá como la versión predeterminada.
  - --endpoint `snowballEndpoint`: un valor que le permite administrar sus instancias de computación mediante programación usando operaciones de API compatibles con Amazon EC2. Para obtener más información, consulte Especificar el punto de conexión compatible con Amazon EC2 como punto de conexión AWS CLI.
- modify-instance-attribute— Modifica un atributo de la instancia especificada. Se admiten los siguientes atributos:
  - `instanceInitiatedShutdownBehavior`
  - `userData`
- revoke-security-group-egress— Elimina una o más reglas de salida de un grupo de seguridad:
  - [--group-id `value`]: el ID del grupo de seguridad
  - [--ip-permissions `value`]: uno o más conjuntos de permisos de IP.
- revoke-security-group-ingress— Revoca una o más reglas de entrada a un grupo de seguridad. Al llamar a `revoke-security-group-ingress`, debe especificar un valor para `group-name` o `group-id`.
  - [--group-name `value`]: el nombre del grupo de seguridad.
  - [--group-id `value`]: el ID del grupo de seguridad.
  - [--ip-permissions `value`]: uno o más conjuntos de permisos de IP.
  - [--protocol `value`]: el protocolo IP. Los posibles valores son `tcp`, `udp` y `icmp`. El argumento `--port` es obligatorio a menos que se especifique el valor "all protocols" (-1).
  - [--port `value`]: para TCP o UDP, el rango de puertos que se permite. Un número entero específico o un rango (mínimo-máximo).

En el caso de ICMP, un valor entero específico o un rango (`type-code`) en el que `type` representa el número de tipo de ICMP y `code` representa el número de código de ICMP. El valor -1 indica todos los códigos de ICMP para todos los tipos de ICMP. Si solo `type` tiene el valor -1, indica todos los códigos de ICMP para el tipo de ICMP especificado.

- [--cidr `value`]: el rango de IP del CIDR.

- run-instances: lanza una serie de instancias de computación usando un ID de AMI de Snowball para una AMI.

> **Note**
>
> Puede tardar hasta una hora y media en lanzar una instancia de computación en un dispositivo Snowball Edge, según el tamaño y el tipo de instancia.

- [-- block-device-mappings `(list)`] — El dispositivo de bloques mapea las entradas. Se admiten los parámetros `DeleteOnTermination`, `VolumeSize` y `VolumeType`. Los volúmenes de arranque deben ser de tipo `sbg1`.

  La sintaxis JSON de este comando es la siguiente.

```
{
   "DeviceName": "/dev/sdh",
   "Ebs":
   {
      "DeleteOnTermination": true|false,
      "VolumeSize": 100,
      "VolumeType": "sbp1"|"sbg1"
   }
}
```

- --count: el número de instancias que va a lanzar. Si se proporciona un solo número, se entiende que es el mínimo (el valor predeterminado es 1). Si se proporciona un rango con el formato `min:max`, se entiende que el primer número indica la cantidad mínima de instancias que se van a lanzar y el segundo número indica la cantidad máxima.
- --image-id: el ID de AMI de Snowball de la AMI, que puede obtener con una llamada a `describe-images`. Se necesita una AMI para lanzar una instancia.

- -- InstanceInitiatedShutdownBehavior — De forma predeterminada, cuando inicias el cierre de la instancia (mediante un comando como shutdown o poweroff), la instancia se detiene. Puede cambiar este comportamiento para que se termine. Se admiten los parámetros `stop` y `terminate`. El valor predeterminado es `stop`. Para obtener más información, consulte Cambio del comportamiento de apagado iniciado por la instancia en la Guía del usuario de instancias de Linux de Amazon EC2.
- --instance-type: el tipo de instancia `sbe`.
- --launch-template `structure`: la plantilla de lanzamiento que se va a utilizar para lanzar las instancias. Cualquier parámetro que especifique en el comando `run-instances` anula esos mismos parámetros en la plantilla de lanzamiento. Puede especificar el nombre o el ID de una plantilla de lanzamiento, pero no ambos.

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

- -- security-group-ids — Uno o más identificadores de grupo de seguridad. Puede crear un grupo de seguridad mediante CreateSecurityGroup. Si no se proporciona ningún valor, el ID del grupo de seguridad predeterminado se asigna a las instancias creadas.
- --tag-specifications: las etiquetas que se aplicarán a los recursos durante el lanzamiento. Solo puede etiquetar instancias durante el lanzamiento. Las etiquetas especificadas se aplican a todas las instancias que se crean durante el lanzamiento. Para etiquetar un recurso una vez que se ha creado, utilice `create-tags`.
- --user-data: los datos de usuario que se van a poner a disposición de la instancia. Si está utilizando el AWS CLI, la codificación base64 se realizará automáticamente y podrá cargar el texto desde un archivo. De lo contrario, debe proporcionar texto codificado en base64.
- --key-name (cadena): el nombre del par de claves. Puede crear un par de claves mediante `CreateKeyPair` o`ImportKeyPair`.

> **Warning**
>
> Si no especifica un par de claves, no puede conectarse a la instancia a menos que elija una AMI que esté configurada para permitir a los usuarios otra forma de iniciar sesión.

- start-instances: inicia una instancia `sbe` que había detenido previamente. Todos los recursos asociados a la instancia se mantienen durante los procesos de inicio y detención, pero se borran si la instancia se termina.
  - --instance-ids: los ID de una o más instancias `sbe` que se detuvieron en el dispositivo.
- stop-instances: detiene una instancia `sbe` que está en ejecución. Todos los recursos asociados a la instancia se mantienen durante los procesos de inicio y detención, pero se borran si la instancia se termina.
  - --instance-ids: los ID de una o más instancias `sbe` que se van a detener en el dispositivo.
- terminate-instances: apaga una o más instancias. Esta operación es idempotente; si termina una instancia más de una vez, cada llamada se ejecuta correctamente. Todos los recursos asociados a la instancia se mantienen durante los procesos de inicio y detención, pero los datos se borran si la instancia se termina.

> **Note**
>
> De forma predeterminada, cuando se utiliza un comando como `shutdown` o `poweroff` para iniciar un cierre desde la instancia, la instancia se detiene. Sin embargo, puede utilizar el atributo `InstanceInitiatedShutdownBehavior` para cambiar este comportamiento de modo que estos comandos terminen la instancia. Para obtener más información, consulte Cambio del comportamiento de apagado iniciado por la instancia en la Guía del usuario de instancias de Linux de Amazon EC2.

  - --instance-ids: los ID de una o más instancias `sbe` que se van a terminar en el dispositivo. Se perderán todos los datos asociados almacenados para esas instancias.
- create-key-pair— Crea un par de claves RSA de 2048 bits con el nombre especificado. Amazon EC2 almacena la clave pública y muestra la clave privada para que la guarde en un archivo. La clave privada se devuelve como una clave privada PKCS#1 codificada en PEM descifrada. Si ya existe una clave con el nombre especificado, Amazon EC2 devuelve un error.
  - --key-name (cadena): un nombre único para el par de claves.

    Restricciones: hasta 255 caracteres ASCII.
  - [--tag-specifications] (lista): las etiquetas que se van a aplicar al nuevo par de claves.

```
{
    "ResourceType": "image"|"instance"|"key-pair"|"launch-template"|"security-group",
```

```
    "Tags": [
      {
        "Key": "string",
        "Value": "string"
      }
      ...
    ]
  }
  ...
```

- import-key-pair –
  - --key-name (cadena): un nombre único para el par de claves.

    Restricciones: hasta 255 caracteres ASCII.
  - -- public-key-material (blob) — La clave pública. Para las llamadas a la API, el texto debe estar codificado en base64. En las herramientas de la línea de comandos, la codificación base64 es automática.
  - [--tag-specifications] (lista): las etiquetas que se van a aplicar al nuevo par de claves.

```
{
    "ResourceType": "image"|"instance"|"key-pair"|"launch-template"|"security-group",
    "Tags": [
      {
        "Key": "string",
        "Value": "string"
      }
      ...
    ]
  }
```

- describe-key-pairs –

  [--filters] (lista): los filtros.
  - key-pair-id — El ID del key pair.
  - key-name: el nombre del par de claves.
  - tag-key: la clave de una etiqueta asignada al recurso. Utilice este filtro para buscar todos los recursos a los que se ha asignado una etiqueta con una clave específica, independientemente del valor de la etiqueta.
  - [--tag-specifications] (lista): las etiquetas que se van a aplicar al nuevo par de claves.

- tag :key: la combinación de clave/valor de una etiqueta asignada al recurso. Utilice la clave de etiqueta en el nombre del filtro y el valor de la etiqueta como valor del filtro. Por ejemplo, para buscar todos los recursos que tienen una etiqueta con la clave `Owner` y el valor `Team A`, especifique `tag:Owner` para el nombre del filtro y `Team A` para el valor del filtro.

```
{
    "Name": "string",
    "Values": ["string", ...]
  }
  ...
```

- [--key-names] (lista): los nombres de los pares de claves.

  Predeterminado: describe todos los pares de claves.
- [--key-pair-ids] (lista): los ID de los pares de claves.
- delete-key-pair –
  - [--key-name] (cadena): el nombre del par de claves.
  - [--key-pair-id] (string): el ID del par de claves.

Operaciones de API compatibles con Amazon EC2 admitidas

A continuación, encontrará las operaciones de API compatibles con Amazon EC2 que puede utilizar con un dispositivo Snowball Edge, con enlaces a sus descripciones en la Referencia de la API de Amazon EC2.Las llamadas a la API compatibles con Amazon EC2 requieren la firma de Signature Version 4 (SigV4). Si utilizas el SDK AWS CLI o un AWS SDK para realizar estas llamadas a la API, la firma de SigV4 se gestiona automáticamente. De lo contrario, debe implementar su propia solución de firma de SigV4. Para obtener más información, consulte Obtención y uso de las credenciales locales de Amazon S3.

- AssociateAddress— Asocia una dirección IP elástica a una instancia o una interfaz de red.
- AttachVolume— Se admiten los siguientes parámetros de solicitud:
  - `Device`
  - `InstanceId`
  - `VolumeId`

- AuthorizeSecurityGroupEgress— Añade una o más reglas de salida a un grupo de seguridad para usarlas con un dispositivo Snowball Edge. En concreto, esta acción permite que las instancias puedan enviar tráfico a uno o varios rangos de direcciones CIDR IPv4 de destino.
- AuthorizeSecurityGroupIngress— Añade una o más reglas de entrada a un grupo de seguridad. Al llamar AuthorizeSecurityGroupIngress, debe especificar un valor para `GroupName` o`GroupId`.
- CreateVolume— Se admiten los siguientes parámetros de solicitud:
  - `SnapshotId`
  - `Size`
  - `VolumeType`
  - `TagSpecification.N`
- CreateLaunchTemplate— Se admiten los siguientes parámetros de solicitud:
  - `ImageId`
  - `InstanceType`
  - `SecurityGroupIds`
  - `TagSpecifications`
  - `UserData`
- CreateLaunchTemplateVersion
- CreateTags— Se admiten los siguientes parámetros de solicitud:
  - `AMI`
  - `Instance`
  - `Launch template`
  - `Security group`
- CreateSecurityGroup— Crea un grupo de seguridad en tu Snowball Edge. Puede crear hasta 50 grupos de seguridad. Cuando cree un grupo de seguridad, especifique un nombre fácil de recordar.
- DeleteLaunchTemplate
- DeleteLaunchTemplateVersions
- DeleteSecurityGroup— Elimina un grupo de seguridad. Si intenta eliminar un grupo de seguridad asociado a una instancia, o si otro grupo de seguridad hace referencia a este, se produce un error `DependencyViolation` en la operación.
- DeleteTags— Elimina el conjunto de etiquetas especificado del conjunto de recursos especificado.
- DeleteVolume— Se admiten los siguientes parámetros de solicitud:

  - `VolumeId`
- DescribeAddresses
- DescribeImages
- DescribeInstanceAttribute— Se admiten los siguientes atributos:
  - `instanceType`
  - `userData`
- DescribeInstanceStatus
- DescribeLaunchTemplates
- DescribeLaunchTemplateVersions
- DescribeInstances
- DescribeSecurityGroups— Describe uno o más de sus grupos de seguridad. `DescribeSecurityGroups`es una operación paginada. Puede emitir varias llamadas a la API para recuperar todo el conjunto de datos de los resultados.
- DescribeTags— Con este comando, se admiten los siguientes filtros:
  - `resource-id`
  - `resource-type`: solo instancia de AMI o de computación
  - `key`
  - `value`
- DescribeVolume— Se admiten los siguientes parámetros de solicitud:
  - `MaxResults`
  - `NextToken`
  - `VolumeId.N`
- DetachVolume— Se admiten los siguientes parámetros de solicitud:
  - `Device`
  - `InstanceId`
  - `VolumeId`
- DisassociateAddress
- GetLaunchTemplateData
- ModifyLaunchTemplate
- ModifyInstanceAttribute— Solo se admite el `userData` atributo.
- RevokeSecurityGroupEgress— Elimina una o más reglas de salida de un grupo de seguridad.

- RevokeSecurityGroupIngress— Revoca una o más reglas de entrada a un grupo de seguridad. Al llamar RevokeSecurityGroupIngress, debe especificar un valor para `group-name` o. `group-id`
- RunInstances –

> **Note**
>
> Puede tardar hasta una hora y media en lanzar una instancia de computación en un dispositivo Snowball Edge, según el tamaño y el tipo de instancia.

- StartInstances
- StopInstances— Los recursos asociados a una instancia detenida persisten. Puede terminar la instancia para liberar estos recursos. Sin embargo, los datos asociados se eliminan.
- TerminateInstances

Inicio automático de instancias compatibles con Amazon EC2 con plantillas de lanzamiento

Puede iniciar automáticamente las instancias compatibles con Amazon EC2 en su AWS Snowball Edge dispositivo mediante plantillas de lanzamiento y comandos de configuración de lanzamiento del cliente Snowball Edge.

Una plantilla de lanzamiento contiene la información de configuración necesaria para crear una instancia compatible con Amazon EC2 en su dispositivo Snowball Edge. Puede utilizar una plantilla de lanzamiento para almacenar parámetros de lanzamiento, de forma que no tenga que especificarlos cada vez que inicie una instancia compatible con EC2 en su dispositivo Snowball Edge.

Cuando utiliza configuraciones de inicio automático en su dispositivo Snowball Edge, debe configurar los parámetros con los que desea que se inicie su instancia compatible con Amazon EC2. Una vez configurado su dispositivo Snowball Edge, al reiniciarlo y desbloquearlo, utiliza su configuración de inicio automático para lanzar una instancia con los parámetros que ha especificado. Si una instancia que ha lanzado mediante una configuración de inicio automático está detenida, la instancia comienza a ejecutarse en el momento en que se desbloquea el dispositivo.

> **Note**
>
> Después de configurar por primera vez una configuración de inicio automático, reinicie el dispositivo para lanzarla. Todos los lanzamientos de instancias posteriores (tras reinicios inesperados o programados) se realizan automáticamente después de desbloquear su dispositivo .

Una plantilla de lanzamiento puede especificar el ID de imagen de máquina de Amazon (AMI), el tipo de instancia, los datos de usuario, los grupos de seguridad y las etiquetas de una instancia compatible con Amazon EC2 cuando se lanza dicha instancia. Para ver una lista de los tipos de instancia admitidos, consulte Cuotas de instancias de computación en un dispositivo Snowball Edge.

Para lanzar automáticamente instancias compatibles con EC2 en su dispositivo Snowball Edge, siga estos pasos:

1. Cuando solicite su AWS Snowball Edge dispositivo, cree una tarea para solicitar un dispositivo de la familia Snow con instancias informáticas. Para obtener más información, consulte Creación de un trabajo de computación.
2. Tras recibir su dispositivo Snowball Edge, desbloquéelo.
3. Utilice el comando `aws ec2 create-launch-template` de la API compatible con EC2 para crear una plantilla de lanzamiento.
4. Utilice el comando `snowballEdge create-autostart-configuration` del cliente de Snowball Edge para enlazar su plantilla de lanzamiento de instancia compatible con EC2 con la configuración de red. Para obtener más información, consulte Creación de una configuración de lanzamiento para iniciar automáticamente instancias compatibles con Amazon EC2.
5. Reinicie y, a continuación, desbloquee el dispositivo. Las instancias compatibles con EC2 se inician automáticamente con los atributos especificados en la plantilla de lanzamiento y el comando `create-autostart-configuration` del cliente de Snowball Edge.

Para ver el estado de las instancias en ejecución, use el comando `describe-autostart-configurations` de la API compatible con EC2.

> **Note**
>
> No existe una consola ni una API de administración de trabajos que AWS Snowball soporte las plantillas de lanzamiento. Los comandos de la CLI del cliente de Snowball Edge y

compatibles con EC2 se utilizan para iniciar automáticamente instancias compatibles con EC2 en el dispositivo AWS Snowball Edge .

Uso del Servicio de metadatos de instancias para Snow con instancias compatibles con Amazon EC2

IMDS para Snow proporciona un servicio de metadatos de instancias (IMDS) para instancias compatibles con Amazon EC2 en Snow. Los metadatos de las instancias son categorías de información sobre las instancias. Incluyen categorías como nombre de host, eventos y grupos de seguridad. Con IMDS para Snow, también puede utilizar metadatos de instancias para obtener acceso a los datos de usuario que especificó al lanzar la instancia compatible con Amazon EC2. Por ejemplo, puede utilizar IMDS para Snow a fin de especificar parámetros para configurar la instancia o incluir estos parámetros en un script sencillo. Puede crear AMI genéricas y usar los datos de usuario para modificar los archivos de configuración proporcionados durante la inicialización.

Para obtener información sobre los metadatos de instancia, los datos de usuario y las instancias compatibles con Snow EC2, consulte Datos de usuario y metadatos de instancia admitidos en esta guía.

Important

Aunque solo se puede obtener acceso a los metadatos de instancia y a los datos de usuario desde la propia instancia, los datos no están protegidos con métodos criptográficos ni de autenticación. Cualquier persona con acceso directo a la instancia, y prácticamente cualquier software que se ejecute en la instancia, puede ver sus metadatos. Por ello, no debería almacenar información confidencial, como contraseñas y claves de cifrado de duración prolongada, como datos de usuario.

Note

En los ejemplos de esta sección, se utiliza la dirección IPv4 del servicio de metadatos de instancia: 169.254.169.254. No se admite la recuperación de los metadatos de instancias mediante la dirección IPv6 de enlace-local.

Temas

Versiones de IMDS

Para obtener acceso a metadatos de instancias desde una instancia en ejecución puede utilizar IMDS versión 2 o IMDS versión 1:

- Servicio de metadatos de instancias versión 2 (IMDSv2): un método orientado a la sesión
- Servicio de metadatos de instancias versión 1 (IMDSv1): un método de solicitud-respuesta

En función de la versión del software Snow, puede utilizar IMDSv1, IMDSv2 o ambos. También depende del tipo de AMI que se ejecute en la instancia compatible con EC2. Algunas AMI, como las que ejecutan Ubuntu 20.04, requieren IMDSv2. El servicio de metadatos de instancias distingue entre solicitudes IMDSv1 y IMDSv2 en función de la presencia de encabezados `PUT` o `GET`. IMDSv2 usa estos dos encabezados. IMDSv1 usa solo el encabezado `GET`.

AWS recomienda el uso de IMDSv2 en lugar de IMDSv1 porque IMDSv2 incluye una mayor seguridad. Para obtener más información, consulte Agregar defensa en profundidad contra firewalls abiertos, proxies inversos y vulnerabilidades SSRF con mejoras en el servicio de metadatos de instancias EC2.

IMDSv2

IMDSv2 usa solicitudes orientadas a la sesión. Las solicitudes orientadas a la sesión permiten crear un token de sesión que define la duración de la sesión. La duración de la sesión puede tener un valor mínimo de un segundo y un valor máximo de seis horas. Durante ese tiempo, puede utilizar el mismo token de sesión para solicitudes subsiguientes. Cuando la duración llegue a su fin, deberá crear un token de sesión nuevo para utilizarlo en las solicitudes futuras.

En el siguiente ejemplo se usa un script de intérprete de comandos de Linux e IMDSv2 para recuperar los elementos de metadatos de instancias de nivel superior. Este ejemplo:

1. Crea un token de sesión que dura seis horas (21 600 segundos) con la solicitud `PUT`.
2. Almacena el encabezado del token de sesión en una variable denominada `TOKEN`.
3. Solicita los elementos de metadatos de nivel superior con el token.

Puede ejecutar dos comandos por separado o combinarlos.

Comandos separados

Primero, genere un token con el siguiente comando.

> **Note**
>
> `X-aws-ec2-metadata-token-ttl-seconds` es un encabezado obligatorio. Si este encabezado no se incluye, recibirá un código de error 400 - Missing or Invalid Parameters que indica que faltan parámetros o que no son válidos.

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

A continuación, utilice el token para generar elementos de metadatos de nivel superior mediante el siguiente comando.

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

Comandos combinados

Puede almacenar el token y combinar los comandos. En el siguiente ejemplo se combinan los dos comandos anteriores y se almacena el encabezado del token de sesión en una variable denominada `TOKEN`.

> **Note**
>
> Si se produce un error al crear el token, en lugar de un token válido, se almacena un mensaje de error en la variable y el comando no 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/
```

Después de crear un token, puede volverlo a usar hasta que venza. El siguiente comando de ejemplo toma el ID de la AMI utilizada para lanzar la instancia y lo almacena en la `$TOKEN` creada en el ejemplo anterior.

Example de reutilizar un token

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

Al utilizar IMDSv2 para solicitar metadatos de instancias, la solicitud debe seguir estas reglas:

1. Use una solicitud `PUT` para iniciar una sesión en el servicio de metadatos de instancia. La solicitud `PUT` devuelve un token que debe incluirse en las solicitudes `GET` subsiguientes del servicio de metadatos de instancia. El token debe acceder a los metadatos con IMDSv2.
2. Incluya el token en todas las solicitudes `GET` del servicio de metadatos de instancias.
   a. El token es una clave específica de la instancia. El token no es válido en otras instancias compatibles con EC2 y se rechazará si intenta usarlo fuera de la instancia en la que se generó.
   b. La solicitud `PUT` debe incluir un encabezado que especifique el tiempo de vida (TTL) del token, en segundos, de un máximo de seis horas (21 600 segundos). El token representa una sesión lógica. El TTL especifica el período de tiempo que es válido el token y, en consecuencia, la duración de la sesión.
   c. Cuando un token caduca, para poder seguir accediendo a los metadatos de instancia hay que crear una sesión nueva con otra solicitud `PUT`.
   d. Puede elegir entre volver a utilizar un token o crear uno nuevo con cada solicitud. Si hay un número pequeño de solicitudes, puede ser más sencillo generar y usar inmediatamente un token cada vez que necesite acceder al servicio de metadatos de instancias. Pero para ser más eficientes, puede especificar una duración más larga para el token y volver a usarlo en vez de

escribir una solicitud PUT cada vez que tenga que solicitar metadatos de instancia. No existe ningún límite práctico en cuanto a la cantidad de tokens simultáneos, cada uno de los cuales representa su propia sesión.

Los métodos HTTP `GET` y `HEAD` están permitidos en las solicitudes de metadatos de instancias IMDSv2. Las solicitudes PUT se rechazan si contienen un encabezado `X-Forwarded-For`.

De forma predeterminada, la respuesta a las solicitudes PUT tiene un límite de saltos de respuesta (tiempo de vida) de 1 en el nivel del protocolo IP. IMDS para Snow no tiene la capacidad de modificar el límite de saltos en las respuestas PUT.

IMDSv1

IMDSv1 utiliza el modelo de solicitud-respuesta. Para solicitar metadatos de instancia, debe enviar una solicitud `GET` al servicio de metadatos de instancias.

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

Recuperación de metadatos de instancia

Los metadatos de la instancia están disponibles en la instancia en ejecución, por lo que no necesita utilizar la consola Amazon EC2 ni la AWS CLI para acceder a ella. Esto puede resultar de utilidad al escribir scripts para ejecutarlos desde la instancia. Por ejemplo, puede obtener acceso a la dirección IP local de la instancia desde los metadatos de la instancia para administrar una conexión a una aplicación externa. Los metadatos de instancia se dividen en categorías. Para obtener una descripción de cada categoría de metadatos de instancia, consulte Datos de usuario y metadatos de instancia admitidos en esta guía.

Para ver todas las categorías de metadatos de instancia dentro de una instancia en ejecución, utilice el siguiente URI IPv4:

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

Las direcciones IP son direcciones de enlace local y solo son válidas desde la instancia. Para obtener más información, consulte Dirección de enlace local en Wikipedia.

Respuestas y mensajes de error

Todos los metadatos de instancia se devuelven como texto (tipo de contenido HTTP `text/plain`).

La solicitud de un recurso de metadatos concreto devuelve el valor correspondiente, o bien un código de error HTTP 404 - Not Found si el recurso no está disponible.

La solicitud de un recurso de metadatos general (cuando el URI termina en un carácter `/`) devuelve una lista de recursos disponibles, o bien un código de error HTTP 404 - Not Found si no existe dicho recurso. Los elementos de la lista aparecen en líneas separadas que terminan con saltos de línea (código de carácter ASCII 10).

Para las solicitudes realizadas con IMDSv1, pueden aparecer los siguientes códigos de error HTTP:

- 400 - Missing or Invalid Parameters: la solicitud PUT no es válida.
- 401 - Unauthorized: la solicitud `GET` usa un token no válido. La acción recomendada es generar un token nuevo.
- 403 - Forbidden: la solicitud no está permitida o el servicio de metadatos de instancias está desactivado.

Ejemplos de recuperación de metadatos de instancia mediante IMDSv1 e IMDSv2

En los siguientes ejemplos se proporcionan comandos que puede utilizar en una instancia de Linux.

Example de obtención de las versiones disponibles de los metadatos de instancia

Este ejemplo obtiene las versiones disponibles de los metadatos de la instancia. Cada versión hace referencia a una compilación de metadatos de instancia correspondiente al momento en que se publicaron nuevas categorías de metadatos de instancia. Tiene disponibles las versiones anteriores en caso de que tenga scripts que se basen en la estructura y la información presente en la versión 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 de obtención de los elementos de metadatos de nivel superior

Este ejemplo obtiene los elementos de metadatos de nivel superior. Para obtener información sobre los elementos de metadatos de nivel superior, consulte Datos de usuario y metadatos de instancia admitidos en esta guía.

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 de obtención de los valores de los metadatos de nivel superior

En los siguientes ejemplos se obtienen los valores de algunos elementos de metadatos de nivel superior que se obtuvieron en el ejemplo anterior. Las solicitudes IMDSv2 usan el token almacenado creado en el comando de ejemplo anterior, siempre y cuando no haya vencido.

`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
```

Uso del almacenamiento en bloques con sus instancias compatibles con Amazon EC2

El almacenamiento en bloques de Snowball Edge le permite agregar o eliminar almacenamiento en bloques en función de las necesidades de las aplicaciones. Los volúmenes que están asociados a una instancia compatible con Amazon EC2 se exponen como volúmenes de almacenamiento que persisten independientemente de la duración de la instancia. Puede administrar el almacenamiento en bloques a través de la API conocida de Amazon EBS.

Algunos comandos de Amazon EBS se admiten a través del punto de conexión compatible con EC2. Estos son algunos de los comandos admitidos: `attach-volume`, `create-volume`, `delete-volume`, `detach-volume` y `describe-volumes`. Para obtener más información acerca del uso de estos comandos, consulte Lista de comandos de la AWS CLI compatibles con Amazon EC2 admitidos en un dispositivo Snowball Edge.

> **Important**
>
> Asegúrese de desmontar cualquier sistema de archivos del dispositivo dentro del sistema operativo antes de desasociar el volumen. Si no lo hace, podría perder datos.

A continuación, encontrará las cuotas de los volúmenes de Amazon EBS y las diferencias entre los volúmenes de Amazon EBS del dispositivo y los volúmenes de Amazon EBS en la nube:

- Los volúmenes de Amazon EBS solo están disponibles para las instancias compatibles con EC2 que están en ejecución en el dispositivo que aloja los volúmenes.
- Los volúmenes solo pueden ser de dos tipos: HDD optimizados para capacidad (`sbg1`) o SSD optimizados para rendimiento (`sbp1`). El tipo de volumen predeterminado es `sbg1`.
- Snowball Edge comparte memoria HDD entre los objetos de Amazon S3 y Amazon EBS. Si utiliza el almacenamiento en bloques basado en disco duro activado AWS Snowball Edge, se reduce la cantidad de memoria disponible para los objetos de Amazon S3. Del mismo modo, los objetos de Amazon S3 reducirán la cantidad de memoria disponible para el almacenamiento en bloques de Amazon EBS en volúmenes HDD.
- Los volúmenes raíz compatibles con Amazon EC2 siempre utilizan el controlador IDE. Otros volúmenes de Amazon EBS utilizarán preferentemente el controlador Virtio, si está disponible. Si el controlador Virtio no está disponible, SBE usará de manera predeterminada el controlador IDE. El controlador Virtio ofrece un mayor rendimiento y es la opción recomendada.

- No se puede usar el parámetro `encrypted` al crear volúmenes de Amazon EBS. Sin embargo, todos los datos del dispositivo se cifran de forma predeterminada.
- Los volúmenes pueden tener un tamaño de entre 1 GB y 10 TB.
- Se puede asociar un máximo de 10 volúmenes de Amazon EBS a cada instancia compatible con EC2.
- No hay ningún límite en cuanto al número de volúmenes de Amazon EBS que puede tener en su dispositivo AWS Snowball Edge . Sin embargo, la capacidad total del volumen de Amazon EBS estará limitada por el espacio disponible en su dispositivo.

Grupos de seguridad en dispositivos Snowball Edge

Un grupo de seguridad funciona como un firewall virtual que controla el tráfico de una o varias instancias. Cuando lanza una instancia, asocia uno o varios grupos de seguridad a la instancia. Puede añadir reglas a cada grupo de seguridad para permitir el tráfico desde sus instancias asociadas o hacia ellas. Para obtener más información, consulte Grupos de seguridad de Amazon EC2 para instancias de Linux en la Guía del usuario de Amazon EC2.

Los grupos de seguridad de los dispositivos Snowball Edge son similares a los grupos de seguridad de la nube de AWS . Las nubes privadas virtuales (VPC) no se admiten en los dispositivos Snowball Edge.

En la siguiente tabla, puede ver las demás diferencias que existen entre los grupos de seguridad de Snowball Edge y los grupos de seguridad de EC2-VPC:

- Cada dispositivo Snowball Edge tiene un límite de 50 grupos de seguridad.
- El grupo de seguridad predeterminado permite el tráfico de entrada y de salida.
- El tráfico entre las instancias locales puede utilizar la dirección IP de la instancia privada o una dirección IP pública. Por ejemplo, supongamos que desea conectarse a través de SSH desde la instancia A a la instancia B. En ese caso, la dirección IP de destino puede ser la dirección IP pública o la dirección IP privada de la instancia B, si la regla del grupo de seguridad permite el tráfico.
- Solo se admiten los parámetros enumerados para AWS CLI las acciones y las llamadas a la API. Normalmente conforman un subconjunto de los que se admiten en las instancias EC2-VPC.

Para obtener más información sobre AWS CLI las acciones compatibles, consulteLista de comandos de la AWS CLI compatibles con Amazon EC2 admitidos en un dispositivo Snowball Edge. Para

obtener más información acerca de las operaciones de API permitidas, consulte Operaciones de API compatibles con Amazon EC2 admitidas.

Datos de usuario y metadatos de instancia admitidos

Los metadatos de instancia son datos sobre una instancia que se pueden utilizar para configurar o administrar la instancia en ejecución. Snowball Edge admite un subconjunto de categorías de metadatos de instancia para sus instancias de computación. Para obtener más información, consulte Metadatos de instancia y datos de usuario en la Guía del usuario de Amazon EC2.

Se admiten las siguientes categorías. El uso de cualquier otra categoría devuelve un mensaje de error `404`.

Categorías de metadatos de instancia admitidos en Snowball Edge

Datos	Descripción
`ami-id`	El ID de la AMI utilizada para lanzar la instancia .
`hostname`	El nombre de host DNS IPv4 privado de la instancia.
`instance-id`	El ID de esta instancia.
`instance-type`	El tipo de instancia.
`local-hostname`	El nombre de host DNS IPv4 privado de la instancia.
`local-ipv4`	La dirección IPv4 privada de la instancia.
`mac`	La dirección de control de acceso de medios (MAC) de la instancia.
`network/interfaces/macs/` *`mac`*`/local-hostname`	El nombre de host local de la interfaz.
`network/interfaces/macs/` *`mac`*`/local-ipv4s`	Las direcciones IPv4 privadas asociadas a la interfaz.

Datos	Descripción
`network/interfaces/macs/ mac/mac`	La dirección MAC de la instancia.
`network/interfaces/macs/ mac/ public-ipv4s`	Las direcciones IP elásticas asociadas a la interfaz.
`public-ipv4`	La dirección IPv4 pública.
`public-keys/0/openssh-key`	Clave pública. Solo se encuentra disponible si se facilita en el momento de la inicialización de la instancia.
`reservation-id`	El ID de la reserva.
userData	Scripts de intérprete de comandos para enviar instrucciones a una instancia en el momento del lanzamiento.

Categorías de datos dinámicos de instancias admitidos en un dispositivo Snowball Edge

Datos	Descripción
instance-identity/document	JSON que contiene atributos de la instancia. Solo `instanceId` , `imageId`, `privateIp` y `instanceType` tienen valores; el resto de los atributos son nulos. Para obtener más información, consulte los documentos de identidad de las instancias en la Guía del usuario de Amazon EC2.

Datos de usuario en instancias de computación de Snowball

Se admiten datos de usuario para utilizarse con scripts de intérprete de comandos para instancias de computación en un dispositivo Snowball Edge. El uso de scripts de intérprete de comandos le permite enviar instrucciones a una instancia en el momento del lanzamiento. Puede cambiar los datos del usuario con el `modify-instance-attribute` AWS CLI comando o la acción de la `ModifyInstanceAttribute` API.

Para cambiar los datos de usuario

1. Detenga la instancia de cómputo con el `stop-instances` AWS CLI comando.
2. Con el `modify-instance-attribute` AWS CLI comando, modifica el `userData` atributo.
3. Reinicia la instancia de cómputo con el `start-instances` AWS CLI comando.

Solo se admiten scripts de intérprete de comandos con instancias de computación. No se admiten las directivas de paquetes `cloud-init` en instancias de computación que se ejecutan en un dispositivo Snowball Edge. Para obtener más información sobre cómo trabajar con AWS CLI comandos, consulta la Referencia de AWS CLI comandos.

Detención de instancias compatibles con EC2

Para evitar la eliminación accidental de las instancias compatibles con Amazon EC2 que crea en su dispositivo, no apague las instancias desde el sistema operativo. Por ejemplo, no utilice los comandos `shutdown` o `reboot`. El cierre de una instancia desde el sistema operativo tiene el mismo efecto que la llamada al comando terminate-instances.

En su lugar, utilice el comando stop-instances para suspender las instancias compatibles con Amazon EC2 que desea conservar.

Solución de problemas de las instancias de computación en dispositivos Snowball Edge

A continuación, encontrará consejos acerca de cómo solucionar problemas de los trabajos de Snowball Edge con instancias de computación.

Temas

- La interfaz de red virtual tiene una dirección IP de 0.0.0.0
- Snowball Edge se bloquea al lanzar una instancia de computación grande
- La instancia tiene un volumen raíz
- Error de archivo de clave privada no protegido

La interfaz de red virtual tiene una dirección IP de 0.0.0.0

Este problema puede ocurrir si la interfaz de red física (NIC) que ha asociado a la interfaz de red virtual (VNIC) tiene también la dirección IP 0.0.0.0. Este efecto puede producirse si la NIC no está

configurada con una dirección IP (por ejemplo, si se acaba de encender el dispositivo). También puede ocurrir si está utilizando la interfaz incorrecta. Por ejemplo, es posible que esté intentando obtener la dirección IP de la interfaz SFP+, pero es la interfaz RJ45 la que está conectada a la red.

Acción que ejecutar

Si esto ocurre, puede hacer lo siguiente:

- Crear una nueva VNIC, asociada a una NIC que tenga una dirección IP. Para obtener más información, consulte Configuración de red para instancias de computación.
- Actualizar una VNIC existente. Para obtener más información, consulte Actualización de una interfaz de red virtual.

Snowball Edge se bloquea al lanzar una instancia de computación grande

Puede parecer que Snowball Edge ha dejado de lanzar una instancia. Este no suele ser el caso. Sin embargo, puede tardar una hora o más en lanzar instancias de computación grandes.

Para comprobar el estado de las instancias, utilice el AWS CLI comando `aws ec2 describe-instances` run en el punto de conexión HTTP o HTTPS compatible con Amazon EC2 en Snowball Edge.

La instancia tiene un volumen raíz

Las instancias tienen una volumen raíz por diseño. Todas las instancias `sbe` tienen un único volumen raíz, pero con Snowball Edge, puede añadir o eliminar almacenamiento en bloques en función de las necesidades de sus aplicaciones. Para obtener más información, consulte Uso del almacenamiento en bloques con sus instancias compatibles con Amazon EC2.

Error de archivo de clave privada no protegido

Este error se produce si el archivo .pem de su instancia de computación no tiene suficientes permisos de lectura y escritura.

Acción que ejecutar

Para resolver este problema, cambie los permisos del archivo con el siguiente procedimiento:

1. Abra un terminal y diríjase a la ubicación donde ha guardado su archivo .pem.
2. Escriba el siguiente comando.

```
chmod 400 filename.pem
```

Uso del almacenamiento compatible con Amazon S3 en dispositivos Snow Family

El almacenamiento compatible con Amazon S3 en dispositivos Snow Family ofrece un almacenamiento seguro de objetos con mayor resiliencia, escalabilidad y un conjunto de características de la API de Amazon S3 ampliado para su uso en entornos robustos, móviles, periféricos y desconectados. Con el almacenamiento compatible con Amazon S3 en dispositivos Snow Family, puede almacenar datos y ejecutar aplicaciones de alta disponibilidad en dispositivos Snow Family para computación periférica.

Puede crear depósitos de Amazon S3 en los dispositivos Snowball Edge para almacenar y recuperar objetos de forma local para aplicaciones que requieren acceso a datos locales, procesamiento local de datos y residencia de datos. El almacenamiento compatible con S3 en dispositivos Snow Family proporciona una nueva clase de almacenamiento, `SNOW`, que utiliza las API de Amazon S3 y está diseñada para almacenar datos de manera duradera y redundante en múltiples dispositivos Snowball Edge. Puede usar las mismas API y características en los buckets de Snowball Edge que en Amazon S3, como políticas de ciclo de vida, cifrado y etiquetado. Cuando se devuelven el dispositivo o los dispositivos AWS, se borran todos los datos creados o almacenados en el almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow. Para obtener más información, consulte Trabajos exclusivos de computación y almacenamiento locales.

El almacenamiento compatible con Amazon S3 en dispositivos Snow Family se puede implementar en una configuración independiente o en una configuración de clúster. En la configuración independiente, se puede aprovisionar capacidad de S3 en el dispositivo y el resto queda disponible como almacenamiento en bloque. En la configuración de clúster, toda la capacidad del disco de datos se utiliza para el almacenamiento en S3. Un clúster puede constar de un mínimo de 3 dispositivos hasta un máximo de 16. Según el tamaño del clúster, el servicio S3 está diseñado para mantener la tolerancia a errores de 1 o 2 dispositivos.

Con AWS DataSync, puede transferir objetos entre el almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow de un dispositivo Snowball Edge y los servicios AWS de almacenamiento. Para obtener más información, consulte Configuración de transferencias con almacenamiento compatible con S3 en Snowball Edge en la Guía del AWS DataSync usuario.

A continuación se muestra la capacidad de almacenamiento compatible con Amazon S3 en dispositivos Snow Family y la capacidad de almacenamiento en bloque para un dispositivo independiente que utiliza almacenamiento compatible con Amazon S3 en dispositivos Snow Family. Para obtener información sobre la tolerancia a errores y la capacidad de almacenamiento de los clústeres, consultethis table.

Snowball Edge Compute Optimized and Compute Optimized with GPU

Capacidad de almacenamiento del almacenamiento compatible con Amazon S3 en dispositivos Snow Family y el almacenamiento en bloque de dispositivos Snowball Edge optimizados para computación (con AMD EPYC Gen1, HDD y GPU opcional)

Capacidad de almacenamiento compatible con Amazon S3 en dispositivos Snow Family (en TB)	Capacidad de almacenamiento en bloque (en TB)
2,5	41
5.5	37
8.5	33
11	29
14	25
17	21
19.5	17
22.5	13
25.5	9
28,5	5
31	1

Snowball Edge Compute Optimized with NVMe storage

Capacidad de almacenamiento del almacenamiento compatible con Amazon S3 en dispositivos Snow Family y el almacenamiento en bloque de dispositivos Snowball Edge optimizados para computación (con AMD EPYC Gen2 y NVMe)

Capacidad de almacenamiento compatible con Amazon S3 en dispositivos Snow Family (en TB)	Capacidad de almacenamiento en bloque (en TB)
3	17,5
5.5	14.5
10.5	8.5
12	6.5
13	5.5
16,5	1.5

Snowball Edge storage optimized 210 TB

Capacidad de almacenamiento del almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow y el almacenamiento en bloque de los dispositivos Snowball Edge de 210 TB optimizados para almacenamiento

Capacidad de almacenamiento compatible con Amazon S3 en dispositivos Snow Family (en TB)	Capacidad de almacenamiento en bloque (en TB)
20	206
40	182
60	158
80	134
100	110

Capacidad de almacenamiento compatible con Amazon S3 en dispositivos Snow Family (en TB)	Capacidad de almacenamiento en bloque (en TB)
120	86
140	62
160	38
180	14
190	2

Especificaciones del almacenamiento compatible con Amazon S3 en dispositivos Snow Family:

- La cantidad máxima de buckets de dispositivos Snow Family es de 100 por dispositivo o por clúster.
- La cuenta del propietario del bucket de S3 en dispositivos Snow Family es propietaria de todos los objetos del bucket.
- Solo la cuenta de propietario del bucket S3 en dispositivos Snow Family puede realizar operaciones en el bucket.
- Las limitaciones de tamaño de los objetos son las mismas que las de Amazon S3.
- Todos los objetos almacenados en S3 en dispositivos Snow Family tienen la clase de almacenamiento SNOW.
- De forma predeterminada, todos los objetos almacenados en la clase de almacenamiento SNOW se almacenan mediante cifrado del servidor con claves de cifrado administradas por Amazon S3 (SSE-S3). También puede elegir almacenar objetos mediante cifrado del servidor con claves de cifrado proporcionadas por el cliente (SSE-C).
- Si no hay suficiente espacio para almacenar un objeto en su dispositivo Snow Family, la API devuelve una excepción de capacidad insuficiente (ICE).

Temas

- Pedido de almacenamiento compatible con Amazon S3 en dispositivos Snow Family

- Configuración e inicio del almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow
- Trabajo con buckets de S3 en un dispositivo Snowball Edge
- Trabajo con objetos de S3 en un dispositivo Snowball Edge
- Acciones de la API de REST admitidas con el almacenamiento compatible de Amazon S3 en dispositivos Snow Family
- Uso del almacenamiento compatible con Amazon S3 en dispositivos de la familia Snow con un clúster de dispositivos Snow
- Configuración de las notificaciones de eventos del almacenamiento compatible con Amazon S3 en dispositivos Snow Family
- Configuración de notificaciones SMTP locales

Pedido de almacenamiento compatible con Amazon S3 en dispositivos Snow Family

El proceso de pedido de un dispositivo para el almacenamiento compatible con Amazon S3 en dispositivos Snow Family es muy similar al proceso de pedido de un dispositivo Snowball Edge. Para realizar un pedido, consulte Crear un trabajo para pedir un dispositivo de la familia Snow en esta guía y tenga en cuenta lo siguiente durante el proceso:

- En Elegir un tipo de trabajo, seleccione Solo computación y almacenamiento locales.
- En Dispositivos Snow, elija Snowball Edge Compute Optimized
- En Seleccionar el tipo de almacenamiento, seleccione Amazon S3 compatible storage on Snow Family devices.
- Si se trata de un dispositivo independiente, en Capacidad de almacenamiento, elija Único dispositivo y, a continuación, seleccione la cantidad de almacenamiento que desee.
- Si es un clúster, en Capacidad de almacenamiento, seleccione Clúster y, a continuación, seleccione la capacidad de almacenamiento y la tolerancia a errores que desee.

Configuración e inicio del almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow

Instale y configure herramientas de software en su entorno local AWS para interactuar con el dispositivo Snowball Edge o el clúster de dispositivos y el almacenamiento compatible con Amazon

S3 en los dispositivos de la familia Snow. A continuación, utilice estas herramientas para configurar el dispositivo o el clúster Snowball Edge e iniciar el almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow.

Requisitos previos

El almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow requiere que tenga el cliente Snowball Edge AWS CLI instalado en su entorno local. También puede utilizar AWS SDK for .NET AWS Herramientas para Windows PowerShell para trabajar con el almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow. AWS recomienda utilizar las siguientes versiones de estas herramientas:

- Snowball Edge Client: utilice la versión más reciente. Para obtener más información, consulte Descarga e instalación del cliente de Snowball Edge en esta guía.
- AWS CLI— Versión 2.11.15 o posterior. Para obtener más información, consulte Instalación, actualización y desinstalación de AWS CLI en la Guía del AWS Command Line Interface usuario.
- AWS SDK for .NET— AWSSDK .S3Control 3.7.304.8 o posterior. Para obtener más información, consulte AWS SDK for .NET.
- AWS Herramientas para Windows PowerShell: versión 4.1.476 o posterior. Si quiere obtener más información, consulte la Guía del usuario de AWS Tools for Windows PowerShell.

Configuración de su entorno local

En esta sección se describe cómo instalar y configurar el cliente Snowball Edge y su entorno local para su uso con el almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow.

Para configurar su entorno de

1. Descargue e instale la última versión del cliente de Snowball Edge. Para obtener más información, consulte Descarga e instalación del cliente de Snowball Edge en esta guía.
2. Ejecute los siguientes comandos para configurar las carpetas.

```
chmod u+x new_cli/bin/snowballEdge
chmod u+x new_cli/jre/bin/java
```

3. Agregue `new_cli/bin` a su `$PATH`.

4. Ejecute el comando `snowballEdge configure`. Verá una respuesta similar a la siguiente:

```
  Configuration will be stored at /home/user/.aws/snowball/config/snowball-
edge.config
```

5. Introduzca la información siguiente:

   - La ruta del manifiesto.
   - Un código de desbloqueo.
   - El punto de conexión predeterminado. Para los dispositivos Snowball Edge independientes, utilice la dirección IP del dispositivo. En el caso de un clúster de dispositivos, especifique la dirección IP de cualquier dispositivo del clúster. Para comprobar si los puntos finales predeterminados están disponibles en el cliente, utilice un comando similar al siguiente. Para el número de puerto, utilice 9091 (puerto de activación), 22 (SSH) y 8080 (punto final HTTP para s3).

     ```
     telnet snowball_ip port_number
     ```

6. Si lo está utilizando AWS SDK for .NET, defina el valor del `clientConfig.AuthenticationRegion` parámetro de la siguiente manera:

```
clientConfig.AuthenticationRegion = "snow"
```

Configuración del dispositivo Snowball Edge

Configuración de IAM en Snowball Edge

AWS Identity and Access Management (IAM) le ayuda a habilitar un acceso detallado a AWS los recursos que se ejecutan en sus dispositivos Snowball Edge. Utilice IAM para controlar quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos.

Snowball Edge admite IAM de forma local. Puede utilizar el servicio local de IAM para crear nuevos roles y asociarles políticas de IAM. Puede utilizar estas políticas para permitir el acceso necesario para realizar tareas asignadas.

El siguiente ejemplo permite obtener acceso completo a la API de Amazon S3:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "*"

        }
    ]
}
```

Para ver más ejemplos de políticas de IAM, consulte la Guía para desarrolladores de AWS Snowball Edge.

Inicio del servicio de almacenamiento compatible con Amazon S3 en dispositivos Snow Family

Siga las siguientes instrucciones para iniciar el servicio de almacenamiento compatible con Amazon S3 en dispositivos de la familia Snow en un dispositivo o clúster Snowball Edge.

> **Note**
>
> Si prefiere una experiencia más fácil de usar, puede iniciar el servicio de almacenamiento en dispositivos de la familia Snow compatible con Amazon S3 para un dispositivo independiente o un clúster de dispositivos que lo utilice AWS OpsHub. Consulte Configuración del almacenamiento compatible con Amazon S3 en dispositivos Snow Family.

1. Desbloquee el dispositivo o el clúster de dispositivos Snowball Edge ejecutando el siguiente comando:

   - Para un solo dispositivo:

     ```
     snowballEdge unlock-device --endpoint https://snow-device-ip
     ```

   - Para un clúster:

```
snowballEdge unlock-cluster
```

2. Ejecute el siguiente comando y asegúrese de que el dispositivo Snowball Edge o el clúster de dispositivos estén desbloqueados:

   - Para un solo dispositivo:

   ```
   snowballEdge describe-device --endpoint https://snow-device-ip
   ```

   - Para un clúster:

   ```
   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. En cada dispositivo (ya se trate de solo uno o de un clúster), para iniciar el almacenamiento compatible con Amazon S3 en dispositivos Snow Family, haga lo siguiente:

   a. Ejecute el siguiente comando `describe-device` para obtener el `PhysicalNetworkInterfaceId` del dispositivo:

   ```
   snowballEdge describe-device --endpoint https://snow-device-ip
   ```

   b. Ejecute dos veces el siguiente comando `create-virtual-network-interface` para crear las interfaces de red virtuales (VNI) para los puntos de conexión `s3control` (en caso de operaciones de bucket) y `s3api` (en caso de operaciones 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 obtener más información sobre estos comandos, consulte Creación de una interfaz de red virtual.

> **Note**
>
> El inicio del almacenamiento compatible con Amazon S3 en dispositivos Snow Family consume recursos de los dispositivos.

4. Inicie el servicio de almacenamiento compatible con Amazon S3 en dispositivos de la familia Snow ejecutando el siguiente `start-service` comando, que incluye las direcciones IP de sus dispositivos y los nombres de recursos de Amazon (ARN) de las VNI que creó para los `s3control` puntos de enlace y: `s3api`

   Inicio del servicio en un solo 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 el servicio en un clúster:

   ```
   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
   ```

   En `--virtual-network-interface-arns`, incluya los ARN para todas las VNI que creó en el paso anterior. Separe cada ARN con un espacio.

5. Ejecute el siguiente comando `describe-service` para un solo dispositivo:

   ```
   snowballEdge describe-service --service-id s3-snow
   ```

   Espere hasta que el estado del servicio sea `Active`.

   Ejecute el siguiente comando `describe-service` para un clúster:

   ```
   snowballEdge describe-service --service-id s3-snow \
     --device-ip-addresses snow-device-1-ip snow-device-2-ip snow-device-3-ip
   ```

Trabajo con buckets de S3 en un dispositivo Snowball Edge

Puede crear buckets de Amazon S3 en sus dispositivos Snowball Edge para almacenar y recuperar objetos en las instalaciones para las aplicaciones que requieren acceso local a los datos, procesamiento local de los datos y residencia de datos. El almacenamiento compatible con S3 en dispositivos Snow Family proporciona una nueva clase de almacenamiento, `SNOW`, que utiliza las API de Amazon S3 y está diseñada para almacenar datos de manera duradera y redundante en múltiples dispositivos Snowball Edge. Puede usar las mismas API y características en los buckets de Snowball Edge que en Amazon S3, como políticas de ciclo de vida, cifrado y etiquetado.

Uso del AWS CLI

Siga estas instrucciones para trabajar con buckets de Amazon S3 en su dispositivo mediante la AWS CLI.

Para configurar el AWS CLI

1. Cree un perfil para los puntos de conexión de objetos en `~/.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. Obtenga un certificado de su dispositivo. Para más información, consulte la Guía para desarrolladores de Snowball Edge.
3. Si instaló el SDK en un entorno virtual, actívelo con el siguiente comando:

   ```
   source your-virtual-environment-name/bin/activate
   ```

Después de configurar las operaciones, puede obtener acceso a ellas mediante llamadas a la API con la AWS CLI. En los ejemplos siguientes, *`cert`* es el certificado de dispositivo que acaba de obtener mediante IAM.

Acceso a operaciones de objetos

```
aws s3api --profile your-profile list-objects-v2 --endpoint-url
https://s3api-endpoint-ip
```

Acceso a operaciones de buckets

```
aws s3control --profile your-profile list-regional-buckets --account-id
bucket-owner --endpoint-url https://s3ctrlapi-endpoint-ip
```

Uso del SDK para Java

Utilice el siguiente ejemplo para trabajar con objetos de Amazon S3 mediante el SDK para Java.

```
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 de ARN de bucket

Puede utilizar el formato de nombre de recurso de Amazon (ARN) que se muestra aquí para identificar un bucket de Amazon S3 en un dispositivo Snowball Edge:

```
arn:partition:s3:snow:account-id:device/device-id/bucket/bucket-name
```

Donde *partition* es la partición de la región en la que pidió el dispositivo Snowball Edge. *device-id* es el job_id si se trata de un dispositivo Snowball Edge independiente o el *cluster_id* si tiene un clúster de Snowball Edge.

Creación de un bucket de S3 en un dispositivo Snowball Edge

Puede crear buckets de Amazon S3 en su dispositivo Snowball Edge para almacenar y recuperar objetos en la periferia para las aplicaciones que requieren acceso local a los datos, procesamiento local de los datos y residencia de datos. El almacenamiento compatible con S3 en dispositivos Snow Family proporciona una nueva clase de almacenamiento, `SNOW`, que utiliza Amazon S3 y está diseñada para almacenar datos de manera duradera y redundante en múltiples dispositivos. Puede usar las mismas API y características que en los buckets de Amazon S3, como políticas de ciclo de vida, cifrado y etiquetado.

En el siguiente ejemplo se crea un bucket de Amazon S3 para un dispositivo Snowball Edge mediante la AWS CLI. Para ejecutar este comando, sustituya los marcadores de posición de entrada del usuario con su propia información.

```
aws s3control --profile your-profile create-bucket --bucket your-snow-bucket --
endpoint-url https://s3ctrlapi-endpoint-ip
```

Crear y administrar una configuración del ciclo de vida de un objeto mediante AWS CLI

Puede utilizar Ciclo de vida de Amazon S3 para optimizar la capacidad del almacenamiento compatible con Amazon S3 en dispositivos Snow Family. Puede crear reglas de ciclo de vida para hacer que los objetos venzan a medida que lleguen al final de su ciclo de vida o para que se sustituyan por versiones más recientes. Puede crear, habilitar, deshabilitar o eliminar una regla de ciclo de vida. Para obtener más información sobre Ciclo de vida de Amazon S3, consulte Administración del ciclo de vida del almacenamiento.

> **Note**
>
> El Cuenta de AWS que crea el depósito es el propietario del mismo y es el único que puede crear, habilitar, deshabilitar o eliminar una regla del ciclo de vida.

Para crear y administrar una configuración de ciclo de vida para un bucket de almacenamiento compatible con Amazon S3 en dispositivos Snow Family mediante la AWS Command Line Interface (AWS CLI), consulte los siguientes ejemplos.

Uso de PUT para aplicar una configuración de ciclo de vida en un bucket de Snowball Edge

El siguiente AWS CLI ejemplo coloca una política de configuración del ciclo de vida en un bucket de Snowball Edge. Esta política especifica que todos los objetos que tienen el prefijo marcado (*myprefix*) y las etiquetas vencen después de 10 días. Para utilizar este ejemplo, reemplace cada marcador de posición de entrada del usuario con su propia información.

En primer lugar, guarde la política de configuración del ciclo de vida en un archivo JSON. En este ejemplo, el archivo se denomina **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
        }
    }]
}
```

Después de guardar el archivo, envíe el archivo JSON como parte del comando `put-bucket-lifecycle-configuration`. Para utilizar este comando, reemplace cada marcador de posición de entrada del usuario con su propia información.

```
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 obtener más información sobre este comando, consulte put-bucket-lifecycle-configurationla Referencia de AWS CLI comandos.

Trabajo con buckets de S3 en un dispositivo Snowball Edge

Con el almacenamiento compatible con Amazon S3 en dispositivos Snow Family, puede crear buckets de Amazon S3 en sus dispositivos Snowball Edge para almacenar y recuperar objetos en las instalaciones para las aplicaciones que requieren acceso local a los datos, procesamiento local de los datos y residencia de datos. El almacenamiento compatible con S3 en dispositivos Snow Family proporciona una nueva clase de almacenamiento, `SNOW`, que utiliza las API de Amazon S3 y está diseñada para almacenar datos de manera duradera y redundante en múltiples dispositivos Snowball Edge. Puede usar las mismas API y características en los buckets de Snowball Edge que en Amazon S3, como políticas de ciclo de vida, cifrado y etiquetado. Puede utilizar el almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow mediante AWS Command Line Interface (AWS CLI) o AWS los SDK.

Determinación de si puede obtener acceso a un bucket de almacenamiento compatible con Amazon S3 en dispositivos Snow Family

En el siguiente ejemplo, se utiliza el comando `head-bucket` para determinar si un bucket de Amazon S3 existe y si tiene permiso de acceso a él mediante la AWS CLI. Para utilizar este comando, reemplace cada marcador de posición de entrada del usuario con su propia información.

```
aws s3api head-bucket --bucket sample-bucket --profile your-profile --endpoint-url
 https://s3api-endpoint-ip
```

Obtenga una lista de depósitos o grupos regionales

Utilice `list-regional-buckets` o `list buckets` para enumerar el almacenamiento compatible con Amazon S3 en los cubos de dispositivos de la familia Snow utilizando el AWS CLI.

```
aws s3control list-regional-buckets --account-id 123456789012 --profile your-profile --
endpoint-url https://s3ctrlapi-endpoint-ip
```

Para obtener más información sobre el `list-regional-buckets` comando, consulte list-regional-bucketsla Referencia de AWS CLI comandos.

```
 aws s3 list-buckets --account-id 123456789012 --endpoint-url https://s3api-endpoint-ip
```

Para obtener más información sobre el *`list-buckets`* comando, consulte list-buckets en la Referencia de comandos AWS CLI

En el siguiente ejemplo de SDK para Java, se obtiene una lista de buckets en dispositivos Snowball Edge. Para obtener más información, consulte la referencia ListBucketsde la API de 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());
  }
```

En el siguiente PowerShell ejemplo, se obtiene una lista de los depósitos de los dispositivos Snowball Edge.

```
   Get-S3CRegionalBucketList -AccountId 012345678910 -Endpoint "https://snowball_ip" -
Region snow
```

En el siguiente ejemplo de.NET se obtiene una lista de los depósitos de los 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"
        });
    }
}
```

Obtención de un bucket

En el siguiente ejemplo, se obtiene un bucket de almacenamiento compatible con Amazon S3 en dispositivos Snow Family mediante la AWS CLI. Para utilizar este comando, reemplace cada marcador de posición de entrada del usuario con su propia información.

```
aws s3control get-bucket --account-id 123456789012 --bucket DOC-EXAMPLE-BUCKET --
profile your-profile --endpoint-url https://s3ctrlapi-endpoint-ip
```

Para obtener más información acerca de este comando, consulte get-bucket en la Referencia de comandos de AWS CLI .

En el siguiente ejemplo de almacenamiento compatible con Amazon S3 en dispositivos Snow Family, se obtiene un bucket mediante el SDK para Java. Para obtener más información, consulte la referencia GetBucketde la API de 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());
}
```

Eliminación de un bucket

> **Important**
>
> - El Cuenta de AWS que crea el depósito es el propietario del mismo y es el único que puede eliminarlo.
> - Los buckets de dispositivos Snow Family deben estar vacíos para poder eliminarlos.
> - No se puede recuperar un bucket después de que se haya eliminado.

En el siguiente ejemplo, se elimina un bucket de almacenamiento compatible con Amazon S3 en dispositivos Snow Family mediante la AWS CLI. Para utilizar este comando, reemplace cada marcador de posición de entrada del usuario con su propia información.

```
aws s3control delete-bucket --account-id 123456789012 --bucket DOC-EXAMPLE-BUCKET --
profile your-profile --endpoint-url https://s3ctrlapi-endpoint-ip
```

Para obtener más información acerca de este comando, consulte delete-bucket en la Referencia de comandos de AWS CLI .

Trabajo con objetos de S3 en un dispositivo Snowball Edge

En esta sección se describen varias operaciones que puede realizar con objetos en el almacenamiento compatible con Amazon S3 en dispositivos Snow Family.

Copia de un objeto a un bucket de almacenamiento compatible con Amazon S3 en dispositivos Snow Family

En el siguiente ejemplo, se carga un archivo denominado *sample-object.xml* en un bucket de almacenamiento compatible con Amazon S3 en dispositivos Snow Family para el que tiene permisos de escritura para usar la AWS CLI. Para utilizar este comando, reemplace cada marcador de posición de entrada del usuario con su propia información.

```
aws s3api put-object --bucket sample-bucket --key sample-object.xml --body sample-
object.xml --profile your-profile --endpoint-url s3api-endpoint-ip
```

En el siguiente ejemplo de almacenamiento compatible con Amazon S3 en dispositivos Snow Family, se copia un objeto a un objeto nuevo del mismo bucket mediante el SDK para Java. Para utilizar este comando, reemplace cada marcador de posición de entrada del usuario con su propia información.

```
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();
        }
```

```
    }
}
```

Obtención de un objeto de un bucket

En el siguiente ejemplo, se obtiene un objeto denominado *sample-object.xml* de un bucket de almacenamiento compatible con Amazon S3 en dispositivos Snow Family mediante la AWS CLI. El comando del SDK es `s3-snow:GetObject`. Para utilizar este comando, reemplace cada marcador de posición de entrada del usuario con su propia información.

```
aws s3api get-object --bucket sample-bucket --key sample-object.xml --profile your-profile --endpoint-url s3api-endpoint-ip
```

Para obtener más información acerca de este comando, consulte get-object en la Referencia de comandos de AWS CLI .

En el siguiente ejemplo de almacenamiento compatible con Amazon S3 en dispositivos Snow Family, se obtiene un objeto mediante el SDK para Java. Para utilizar este comando, reemplace cada marcador de posición de entrada del usuario con su propia información. Para obtener más información, consulte la referencia GetObjectde la API de 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();
```

```
    }
}
```

Obtención de una lista de los objetos de un bucket

En el siguiente ejemplo, se enumeran los objetos de un bucket de almacenamiento compatible con Amazon S3 en dispositivos Snow Family mediante la AWS CLI. El comando del SDK es `s3-snow:ListObjectsV2`. Para utilizar este comando, reemplace cada marcador de posición de entrada del usuario con su propia información.

```
aws s3api list-objects-v2 --bucket sample-bucket --profile your-profile --endpoint-
url s3api-endpoint-ip
```

Para obtener más información sobre este comando, consulte la list-objects-vsección 2 en la Referencia de AWS CLI comandos.

En el siguiente ejemplo de almacenamiento compatible con Amazon S3 en dispositivos Snow Family, se enumeran los objetos de un bucket mediante el SDK para Java. Para utilizar este comando, reemplace cada marcador de posición de entrada del usuario con su propia información.

En este ejemplo se utiliza ListObjectsla versión 2, que es la última revisión de la operación de la ListObjects API. Recomendamos usar esta operación de API revisada para el desarrollo de aplicaciones. Para garantizar la compatibilidad con versiones anteriores, Amazon S3 aún es compatible con la versión anterior de esta operación 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();
        }
    }
}
```

Eliminación de objetos de un bucket

Puede eliminar uno o más objetos de un bucket de almacenamiento compatible con Amazon S3 en dispositivos Snow Family. En el siguiente ejemplo se elimina un objeto denominado *sample-object.xml* mediante la AWS CLI. Para utilizar este comando, reemplace cada marcador de posición de entrada del usuario con su propia información.

```
aws s3api delete-object --bucket sample-bucket --key key --profile your-profile --
endpoint-url s3api-endpoint-ip
```

Para obtener más información sobre este comando, consulte delete-object en la Referencia de comandos de AWS CLI .

En el siguiente ejemplo de almacenamiento compatible con Amazon S3 en dispositivos Snow Family, se elimina un objeto de un bucket mediante el SDK para Java. Para utilizar este ejemplo, especifique el nombre de clave del objeto que desea eliminar. Para obtener más información, consulte la referencia DeleteObjectde la API de 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();
        }
    }
}
```

Acciones de la API de REST admitidas con el almacenamiento compatible de Amazon S3 en dispositivos Snow Family

Las siguientes listas muestran las operaciones de API que admite el almacenamiento compatible con Amazon S3 en dispositivos Snow Family e incluyen enlaces a las operaciones relacionadas con Amazon S3 en Regiones de AWS.

Operaciones de la API con buckets admitidas:

- CreateBucket
- DeleteBucket
- DeleteBucketLifecycle
- GetBucket
- GetBucketLifecycleConfiguration
- ListBuckets
- PutBucketLifecycleConfiguration

Operaciones de la API con objetos admitidas:

- AbortMultipartUpload
- CompleteMultipartUpload
- CopyObject
- CreateMultipartUpload
- DeleteObject

- DeleteObjects
- DeleteObjectTagging
- GetObject
- GetObjectTagging
- HeadBucket
- HeadObject
- ListMultipartUploads
- ListObjects
- ListObjectsV2
- ListParts
- PutObject
- PutObjectTagging
- UploadPart
- UploadPartCopy

Uso del almacenamiento compatible con Amazon S3 en dispositivos de la familia Snow con un clúster de dispositivos Snow

Un clúster es un conjunto de tres o más dispositivos de Snowball Edge que se utilizan como una sola unidad lógica con fines de almacenamiento local y procesamiento. Un clúster ofrece dos beneficios principales respecto a un dispositivo Snowball Edge independiente en lo que se refiere a los fines de computación y almacenamiento locales:

- Mayor durabilidad: los datos del S3 almacenados en un clúster de dispositivos Snowball Edge disfrutan de una mayor durabilidad de los datos en comparación con un solo dispositivo. Además, los datos del clúster permanecen seguros y viables, a pesar de las posibles interrupciones del hardware que afecten al clúster. Los clústeres pueden soportar la pérdida de un dispositivo en grupos de 3 y 4 dispositivos y de hasta dos dispositivos en grupos de 5 a 16 dispositivos antes de que los datos estén en peligro. Puede reemplazar los nodos en mal estado para mantener la durabilidad y la seguridad de los datos almacenados en el clúster.
- Mayor almacenamiento: con los dispositivos optimizados para el almacenamiento de Snowball Edge, puede crear un único clúster de 16 nodos con una capacidad de almacenamiento utilizable compatible con S3 de hasta 2,6 PB. Con los dispositivos optimizados para cómputo de Snowball

Edge, puede crear un único clúster de 16 nodos con una capacidad de almacenamiento utilizable compatible con S3 de hasta 501 TB.

Un clúster de dispositivos Snowball Edge no tiene ningún nodo principal. Cualquier nodo puede escribir y leer datos de todo el clúster, y todos los nodos son capaces de behind-the-scenes gestionar el clúster.

Cuando piense usar un clúster de dispositivos Snowball Edge, tenga en cuenta lo siguiente:

- Le recomendamos que proporcione una fuente de alimentación redundante para todos los dispositivos del clúster a fin de reducir los posibles problemas de rendimiento y estabilidad del clúster.
- Al igual que sucede con los trabajos de computación y almacenamiento locales independientes, los datos almacenados en un clúster no pueden importarse a Amazon S3 sin pedir dispositivos adicionales como parte de trabajos de importación independientes. Si pide dispositivos adicionales como trabajos de importación, puede transferir los datos del clúster a los dispositivos de los trabajos de importación.
- Para transferir datos a un clúster desde Amazon S3, utilice la API de Amazon S3 para crear buckets de Amazon S3 en el clúster para almacenar y recuperar objetos de S3. Además, puede utilizarlos AWS DataSync para transferir objetos entre los servicios de AWS almacenamiento y el almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow de un dispositivo Snowball Edge. Para obtener más información, consulte Configuración de transferencias con almacenamiento compatible con S3 en Snowball Edge.
- Puede crear una tarea para ordenar un clúster de dispositivos desde el Consola de administración de la familia de productos Snow de AWS AWS CLI, el o uno de los AWS SDK. Para obtener más información, consulte Introducción.
- Cada dispositivo del clúster tiene un ID de nodo. Un ID de nodo es un identificador único para cada dispositivo del clúster, como un ID de trabajo para un dispositivo independiente. Puede obtener los ID de nodo de los Consola de administración de la familia de productos Snow de AWS AWS CLI, los AWS SDK y el cliente de Snowball Edge. El cliente Snowball Edge ordena `describe-device` y `describe-cluster` devuelve los ID de los nodos con otra información sobre los dispositivos o el clúster.
- La duración de un clúster está limitada por el certificado de seguridad concedido a los dispositivos del clúster al aprovisionarlo. De forma predeterminada, los dispositivos Snowball Edge pueden utilizarse durante un máximo de 360 días antes de que haya que devolverlos. Al finalizar ese plazo, los dispositivos dejan de responder a las solicitudes de lectura/escritura. Si necesita

conservar uno o más dispositivos durante más de 360 días, póngase en contacto con nosotros AWS Support.

- Cuando AWS recibimos un dispositivo devuelto que formaba parte de un clúster, eliminamos por completo el dispositivo. Esta operación de borrado se ajusta a los estándares 800-88 del Instituto Nacional de Normalización y Tecnología (NIST).

Tolerancia a errores y capacidad de almacenamiento de un clúster de almacenamiento compatible con Amazon S3 en dispositivos Snow Family

Tamaño del clúster	Tolerancia a errores	Capacidad de almacenamiento de los dispositivos Snowball Edge Compute Optimized (con AMD EPYC Gen1, disco duro y GPU opcional) (en TB)	Capacidad de almacenamiento de los dispositivos Snowball Edge Compute Optimized (procesamiento optimizado con AMD EPYC Gen2 y NVMe) (en TB)	Capacidad de almacenamiento de los dispositivos Snowball Edge de 210 TB optimizados para almacenamiento (en TB)
3	Pérdida de hasta 1 nodo	83	38	438
4	Pérdida de hasta 1 nodo	125	57	657
5	Pérdida de hasta 2 nodos	125	57	657
6	Pérdida de hasta 2 nodos	167	76	904
7	Pérdida de hasta 2 nodos	209	95	1096

Tamaño del clúster	Tolerancia a errores	Capacidad de almacenamiento de los dispositivos Snowball Edge Compute Optimized (con AMD EPYC Gen1, disco duro y GPU opcional) (en TB)	Capacidad de almacenamiento de los dispositivos Snowball Edge Compute Optimized (procesamiento optimizado con AMD EPYC Gen2 y NVMe) (en TB)	Capacidad de almacenamiento de los dispositivos Snowball Edge de 210 TB optimizados para almacenamiento (en TB)
8	Pérdida de hasta 2 nodos	250	114	1315
9	Pérdida de hasta 2 nodos	292	133	1534
10	Pérdida de hasta 2 nodos	334	152	1754
11	Pérdida de hasta 2 nodos	370	165	1970
12	Pérdida de hasta 2 nodos	376	171	1973
13	Pérdida de hasta 2 nodos	418	190	2192
14	Pérdida de hasta 2 nodos	459	209	2411
15	Pérdida de hasta 2 nodos	495	225	2625
16	Pérdida de hasta 2 nodos	501	228	2631

Tras desbloquear un clúster, podrá almacenar datos en ese clúster y obtener acceso a ellos. Puede usar el punto de conexión compatible con Amazon S3 para leer datos de un clúster o escribir datos en él.

Para leer datos de un clúster o escribir datos en él, debe tener un cuórum de lectura/escritura que no sea mayor que el número permitido de nodos no disponibles en el clúster de dispositivos.

Cuórum de clúster en Snowball Edge

Un cuórum representa el número mínimo de dispositivos Snowball Edge de un clúster que deben comunicarse entre sí para que se mantenga un cuórum de lectura/escritura.

Cuando todos los dispositivos de un clúster están en buen estado, hay un quórum de lectura/escritura para el clúster. Si uno o dos de esos dispositivos se desconectan, se reduce la capacidad operativa del clúster. Sin embargo, sigue siendo posible leer y escribir en el clúster. Con todos los dispositivos en funcionamiento excepto uno o dos, el clúster sigue teniendo quórum de lectura/escritura. En this table se muestra el número de nodos que pueden desconectarse antes de que la capacidad operativa del clúster se vea afectada.

Es posible que se pierda Quorom si un clúster pierde más dispositivos de los indicados en. this table Cuando se pierde un quórum, el clúster está desconectado y los datos del clúster no están disponibles. Es posible que pueda solucionar este problema o que los datos se pierdan de forma permanente, según la gravedad del caso. Si se trata de una fuente de alimentación externa temporal y puede volver a encender los dispositivos Snowball Edge y desbloquear todos los nodos del clúster, los datos volverán a estar disponibles.

> **Important**
>
> Si no existe un quórum mínimo de nodos en buen estado, póngase en contacto con nosotros. AWS Support

Puede usar el `describe-cluster` comando para ver el estado de bloqueo y la accesibilidad de la red de cada nodo. Asegurarse de que los dispositivos de su clúster estén en buen estado y conectados es una responsabilidad administrativa que asume cuando utiliza el almacenamiento en clúster. Para obtener más información, consulte Obtener el estado de los dispositivos.

Si determina que uno o más nodos están en mal estado, puede reemplazar los nodos del clúster para mantener el quórum y el buen estado y la estabilidad de los datos. Para obtener más información, consulte Sustituir un nodo de un clúster.

Reconexión de un nodo de clúster no disponible

Un nodo, o dispositivo dentro de un clúster, puede no estar disponible temporalmente debido a un problema como una pérdida de red o de alimentación eléctrica sin que los datos del nodo sufran ningún daño. Cuando esto sucede, afecta al estado del clúster. El estado de bloqueo y de acceso a la red de un nodo se puede ver en el cliente de Snowball Edge mediante el comando `snowballEdge describe-cluster`.

Le recomendamos que sitúe el clúster físicamente de forma que tenga acceso a las partes delantera, posterior y superior de todos los nodos. De esta forma, puede obtener acceso a los cables de alimentación eléctrica y de red de la parte posterior, a las etiquetas de envío de la parte superior para ver los ID de nodo y a las pantallas LCD de la parte delantera de los dispositivos para obtener las direcciones IP y otros datos administrativos.

Cuando se detecta que un nodo no está disponible, recomendamos intentar uno de los siguientes procedimientos, según cuál sea la causa de la no disponibilidad del nodo.

Cómo volver a conectar un nodo no disponible

1. Asegúrese de que el nodo esté encendido.
2. Asegúrese de que el nodo esté conectado a la misma red interna que el resto del clúster.
3. Si necesita encender el nodo, tendrá que esperar hasta 20 minutos hasta que finalice.
4. Ejecute el comando `snowballEdge unlock-cluster` o el comando `snowballEdge associate-device`. Para ver un ejemplo, consulte Unlocking Snowball Edge devices.

Cómo volver a conectar un nodo que no está disponible y que ha perdido la conexión a la red pero no se ha apagado

1. Asegúrese de que el nodo esté conectado a la misma red interna que el resto del clúster.
2. Ejecute el comando `snowballEdge describe-device` para comprobar cuándo se vuelve a agregar al clúster el nodo que no estaba disponible. Para ver un ejemplo, consulte Obtención del estado de los dispositivos.

Cuando haya realizado los procedimientos anteriores, los nodos deberían funcionar correctamente. Además, debe tener cuórum de lectura/escritura. Si no es así, es posible que uno o varios de los nodos del clúster presente un problema más grave, en cuyo caso podría ser preciso eliminarlo del clúster.

Sustituir un nodo de un clúster

Para reemplazar un nodo, primero debe solicitar uno de reemplazo. Puede solicitar un nodo de reemplazo desde la consola AWS CLI, el o uno de los AWS SDK. Si solicita un nodo de repuesto desde la consola, puede solicitar repuestos para cualquier trabajo que no se haya cancelado o completado. A continuación, desasocie el nodo en mal estado del clúster, conecte el nodo de reemplazo a su red y desbloquee el clúster, incluido el nodo de reemplazo, asocie el nodo de reemplazo al clúster y reinicie el servicio de almacenamiento en dispositivos de la familia Snow compatible con Amazon S3.

Para solicitar un nodo de repuesto desde la consola

1. Inicie sesión en la Consola de administración de la familia de productos Snow de AWS.
2. Busque y elija un trabajo para un nodo que pertenezca al clúster que ha creado en el panel Trabajo.
3. En Acciones, elija Reemplazar nodo.

   Con ello se abre el último paso del asistente de creación de trabajo, exactamente con los mismos ajustes que al crear el clúster original.
4. Seleccione Crear trabajo.

El dispositivo Snowball Edge de repuesto ya está en camino. Utilice el siguiente procedimiento para eliminar el nodo en mal estado del clúster.

Para eliminar un nodo de un clúster

1. Apague el nodo que se va a quitar. Para obtener más información, consulte Apagar el Snowball Edge.
2. Utilice el `describe-cluster` comando para asegurarse de que no se pueda acceder al nodo en mal estado. Esto se indica con el valor de `UNREACHABLE` para el `State` nombre del `NetworkReachability` objeto.

```
snowballEdge describe-cluster --manifest-file path/to/manifest/file.bin --unlock-
code unlock-code --endpoint https://ip-address-of-device-in-cluster
```

Example de la salida de **`describe-cluster`**

```
{
    "ClusterId": "CID12345678-1234-1234-1234-123456789012",
    "Devices": [
        {
            "DeviceId": "JID12345678-1234-1234-1234-123456789012",
            "UnlockStatus": {
                "State": "UNLOCKED"
            },
            "ActiveNetworkInterface": {
                "IpAddress": "10.0.0.0"
            },
            "ClusterAssociation": {
                "ClusterId": "CID12345678-1234-1234-1234-123456789012",
                "State": "ASSOCIATED"
            },
            "NetworkReachability": {
                "State": "REACHABLE"
            },
            "Tags": []
        },
        {
            "DeviceId": "JID12345678-1234-1234-1234-123456789013",
            "UnlockStatus": {
                "State": "UNLOCKED"
            },
            "ActiveNetworkInterface": {
                "IpAddress": "10.0.0.1"
            },
            "ClusterAssociation": {
                "ClusterId": "CID12345678-1234-1234-1234-123456789012",
                "State": "ASSOCIATED"
            },
            "NetworkReachability": {
                "State": "REACHABLE"
            },
            "Tags": []
        },
        {
            "DeviceId": "JID12345678-1234-1234-1234-123456789014",
            "ClusterAssociation": {
```

```
                "ClusterId": "CID12345678-1234-1234-1234-123456789012",
                "State": "ASSOCIATED"
            },
            "NetworkReachability": {
                "State": "UNREACHABLE"
            }
        }
    ]
}
```

3. Utilice el `describe-service` comando para asegurarse de que el estado del `s3-snow` servicio es`DEGRADED`.

```
snowballEdge describe-service --service-id s3-snow --device-ip-addresses snow-device-1-address snow-device-2-address --manifest-file path/to/manifest/file.bin --unlock-code unlock-code --endpoint https://snow-device-ip-address
```

Example de la salida del **`describe-service`** comando

```
{
    "ServiceId": "s3-snow",
    "Autostart": true,
    "Status": {
        "State": "DEGRADED"
    },
    "ServiceCapacities": [
        {
            "Name": "S3 Storage",
            "Unit": "Byte",
            "Used": 38768180432,
            "Available": 82961231819568
        }
    ],
    "Endpoints": [
        {
            "Protocol": "https",
            "Port": 443,
            "Host": "10.0.0.10",
            "CertificateAssociation": {
```

```
                "CertificateArn": "arn:aws:snowball-
device:::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
            },
            "Description": "s3-snow bucket API endpoint",
            "DeviceId": "JID-beta-207012320001-24-02-05-17-17-26",
            "Status": {
                "State": "ACTIVE"
            }
        },
        {
            "Protocol": "https",
            "Port": 443,
            "Host": "10.0.0.11",
            "CertificateAssociation": {
                "CertificateArn": "arn:aws:snowball-
device:::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
            },
            "Description": "s3-snow object API endpoint",
            "DeviceId": "JID-beta-207012320001-24-02-05-17-17-26",
            "Status": {
                "State": "ACTIVE"
            }
        },
        {
            "Protocol": "https",
            "Port": 443,
            "Host": "10.0.0.12",
            "CertificateAssociation": {
                "CertificateArn": "arn:aws:snowball-
device:::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
            },
            "Description": "s3-snow bucket API endpoint",
            "DeviceId": "JID-beta-207012240003-24-02-05-17-17-27",
            "Status": {
                "State": "ACTIVE"
            }
        },
        {
            "Protocol": "https",
            "Port": 443,
            "Host": "10.0.0.13",
            "CertificateAssociation": {
                "CertificateArn": "arn:aws:snowball-
device:::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
```

```
            },
            "Description": "s3-snow object API endpoint",
            "DeviceId": "JID-beta-207012320001-24-02-05-17-17-27",
            "Status": {
                "State": "ACTIVE"
            }
        }
    ]
}
```

4. Utilice el `disassociate-device` comando para desasociar y eliminar el nodo en mal estado del clúster.

```
snowballEdge disassociate-device --device-id device-id --manifest-file path/to/
manifest/file.bin --unlock-code unlock-code --endpoint https://ip-address-of-
unhealthy-device
```

Example salida del comando **`disassociate-device`**

```
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.
```

5. Vuelva a utilizar el `describe-cluster` comando para asegurarse de que el nodo en mal estado esté disociado del clúster.

```
snowballEdge describe-cluster --manifest-file path/to/manifest/file.bin --unlock-
code unlock-code --endpoint https:ip-address-of-healthy-device
```

Example del **`describe-cluster`** comando que muestra que el nodo está disociado

```
{
```

```
    "ClusterId": "CID12345678-1234-1234-1234-123456789012",
    "Devices": [
        {
            "DeviceId": "JID12345678-1234-1234-1234-123456789012",
            "UnlockStatus": {
                "State": "UNLOCKED"
            },
            "ActiveNetworkInterface": {
                "IpAddress": "10.0.0.0"
            },
            "ClusterAssociation": {
                "ClusterId": "CID12345678-1234-1234-1234-123456789012",
                "State": "ASSOCIATED"
            },
            "NetworkReachability": {
                "State": "REACHABLE"
            },
            "Tags": []
        },
        {
            "DeviceId": "JID12345678-1234-1234-1234-123456789013",
            "UnlockStatus": {
                "State": "UNLOCKED"
            },
            "ActiveNetworkInterface": {
                "IpAddress": "10.0.0.1"
            },
            "ClusterAssociation": {
                "ClusterId": "CID12345678-1234-1234-1234-123456789012",
                "State": "ASSOCIATED"
            },
            "NetworkReachability": {
                "State": "REACHABLE"
            },
            "Tags": []
        },
        {
            "DeviceId": "JID12345678-1234-1234-1234-123456789014",
            "ClusterAssociation": {
                "ClusterId": "CID12345678-1234-1234-1234-123456789012",
                "State": "DISASSOCIATED"
            }
        }
    ]
```

```
}
```

6. Apague y vuelva a colocar el dispositivo en mal estado. AWS Para obtener más información, consulte Apagar el Snowball Edge y devolver el dispositivo Snowball Edge.

Cuando llegue el dispositivo de reemplazo, utilice el siguiente procedimiento para añadirlo al clúster.

Para añadir un dispositivo de reemplazo

1. Coloque el dispositivo de reemplazo para el clúster de forma que pueda acceder a la parte frontal, posterior y superior de todos los dispositivos.
2. Encienda el nodo y asegúrese de que esté conectado a la misma red interna que el resto del clúster. Para obtener más información, consulte Conexión a la red local.
3. Use el `unlock-cluster` comando e incluya la dirección IP del nuevo nodo.

```
snowballEdge unlock-cluster --manifest-file path/to/manifest/file.bin --unlock-
code unlock-code --endpoint https://ip-address-of-cluster-device --device-ip-
addresses node-1-ip-address node-2-ip-address new-node-ip-address
```

   El estado del nuevo nodo será `DEGRADED` hasta que lo asocie al clúster en el siguiente paso.

4. Utilice el `associate-device` comando para asociar el nodo de reemplazo al clúster.

```
snowballEdge associate-device --device-ip-address new-node-ip-address
```

   Example de la salida del **`associate-device`** comando

```
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-device command to determine the state of your devices.
```

5. Utilice el `describe-cluster` comando para asegurarse de que el nuevo nodo esté asociado al clúster.

```
snowballEdge describe-cluster --manifest-file path/to/manifest/file.bin --unlock-
code unlock-code --endpoint https://node-ip-address
```

Example de la salida del **`describe-cluster`** comando

```
{
    "ClusterId": "CID12345678-1234-1234-1234-123456789012",
    "Devices": [
        {
            "DeviceId": "JID12345678-1234-1234-1234-123456789012",
            "UnlockStatus": {
                "State": "UNLOCKED"
            },
            "ActiveNetworkInterface": {
                "IpAddress": "10.0.0.0"
            },
            "ClusterAssociation": {
                "ClusterId": "CID12345678-1234-1234-1234-123456789012",
                "State": "ASSOCIATED"
            },
            "NetworkReachability": {
                "State": "REACHABLE"
            },
            "Tags": []
        },
        {
            "DeviceId": "JID-CID12345678-1234-1234-1234-123456789013",
            "UnlockStatus": {
                "State": "UNLOCKED"
            },
            "ActiveNetworkInterface": {
                "IpAddress": "10.0.0.1"
            },
            "ClusterAssociation": {
                "ClusterId": "CID12345678-1234-1234-1234-123456789012",
                "State": "ASSOCIATED"
```

```
            },
            "NetworkReachability": {
                "State": "REACHABLE"
            },
            "Tags": []
        },
        {
            "DeviceId": "JID-CID12345678-1234-1234-1234-123456789015",
            "UnlockStatus": {
                "State": "UNLOCKED"
            },
            "ActiveNetworkInterface": {
                "IpAddress": "10.0.0.2"
            },
            "ClusterAssociation": {
                "ClusterId": "CID12345678-1234-1234-1234-123456789012",
                "State": "ASSOCIATED"
            },
            "NetworkReachability": {
                "State": "REACHABLE"
            },
            "Tags": []
        }
    }
]
}
```

6. En el nuevo nodo, cree dos interfaces de red virtuales (VNI). Para obtener más información, consulte Inicio del servicio de almacenamiento compatible con Amazon S3 en dispositivos Snow Family.

7. Utilice el `stop-service` comando para detener el servicio s3-snow.

```
snowballEdge stop-service --service-id s3-snow --device-ip-addresses cluster-
device-1-ip-address cluster-device-2-ip-address cluster-device-3-ip-address --
manifest-file path/to/manifest/file.bin --unlock-code unlock-code --endpoint
 https://snow-device-ip-address
```

Example de la salida del comando **`stop-service`**

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

8. Use el `start-service` comando para iniciar el servicio s3-snow después de agregar el nuevo nodo al clúster.

```
snowballEdge start-service --service-id s3-snow --device-ip-addresses cluster-
device-1-ip-address cluster-device-2-ip-address cluster-device-3-ip-address --
virtual-network-interface-arns "device-1-vni-ip-address-a" "device-1-vni-ip-
address-b" "device-2-vni-ip-address-a" "device-2-vni-ip-address-b" "device-3-vni-
ip-address-a" "device-3-vni-ip-address-b" --manifest-file path/to/manifest/file.bin
 --unlock-code unlock-code --endpoint https://snow-device-ip-address
```

Example del resultado del comando **`start-service`**

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

9. Utilice el `describe-service` comando para asegurarse de que se ha iniciado el servicio s3-snow.

```
snowballEdge describe-service --service-id s3-snow --device-ip-addresses snow-
device-1-address snow-device-2-address snow-device-3-address --manifest-file path/
to/manifest/file.bin --unlock-code unlock-code --endpoint https://snow-device-ip-
address
```

Example de la salida del comando **`descibe-service`**

```
{
    "ServiceId": "s3-snow",
    "Autostart": true,
    "Status": {
        "State": "ACTIVE"
    },
    "ServiceCapacities": [{
        "Name": "S3 Storage",
        "Unit": "Byte",
        "Used": 38768180432,
        "Available": 82961231819568
    }],
    "Endpoints": [{
            "Protocol": "https",
            "Port": 443,
            "Host": "10.0.0.10",
            "CertificateAssociation": {
                "CertificateArn": "arn:aws:snowball-
device:::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
            },
            "Description": "s3-snow bucket API endpoint",
            "DeviceId": "JID12345678-1234-1234-1234-123456789012",
            "Status": {
                "State": "ACTIVE"
            }
        }, {
            "Protocol": "https",
            "Port": 443,
            "Host": "10.0.0.11",
            "CertificateAssociation": {
                "CertificateArn": "arn:aws:snowball-
device:::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
            },
            "Description": "s3-snow object API endpoint",
            "DeviceId": "JID12345678-1234-1234-1234-123456789013",
            "Status": {
                "State": "ACTIVE"
            }
        }, {
            "Protocol": "https",
```

```
            "Port": 443,
            "Host": "10.0.0.12",
            "CertificateAssociation": {
                "CertificateArn": "arn:aws:snowball-
device:::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
            },
            "Description": "s3-snow bucket API endpoint",
            "DeviceId": "JID12345678-1234-1234-1234-123456789015",
            "Status": {
                "State": "ACTIVE"
            }
        }, {
            "Protocol": "https",
            "Port": 443,
            "Host": "10.0.0.13",
            "CertificateAssociation": {
                "CertificateArn": "arn:aws:snowball-
device:::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
            },
            "Description": "s3-snow object API endpoint",
            "DeviceId": "JID-beta-207012320001-24-02-05-17-17-27",
            "Status": {
                "State": "ACTIVE"
            }
        }, {
            "Protocol": "https",
            "Port": 443,
            "Host": "10.0.0.14",
            "CertificateAssociation": {
                "CertificateArn": "arn:aws:snowball-
device:::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
            },
            "Description": "s3-snow bucket API endpoint",
            "DeviceId": "JID-beta-207012240003-24-02-05-17-17-28",
            "Status": {
                "State": "ACTIVE"
            }
        }, {
            "Protocol": "https",
            "Port": 443,
            "Host": "10.0.0.15",
            "CertificateAssociation": {
                "CertificateArn": "arn:aws:snowball-
device:::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
```

```
            },
            "Description": "s3-snow object API endpoint",
            "DeviceId": "JID-beta-207012320001-24-02-05-17-17-28",
            "Status": {
                "State": "ACTIVE"
            }
        }
    }]
}
```

Configuración de las notificaciones de eventos del almacenamiento compatible con Amazon S3 en dispositivos Snow Family

El almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow admite las notificaciones de eventos de Amazon S3 para las llamadas a la API de objetos basadas en el protocolo Message Queuing Telemetry Transport (MQTT).

Puede utilizar almacenamiento compatible con Amazon S3 en dispositivos Snow Family para recibir notificaciones cuando se produzcan ciertos eventos en su bucket de S3. Para habilitar las notificaciones, agregue una configuración de notificación que identifique los eventos que desea que el servicio publique.

El almacenamiento compatible con Amazon S3 en dispositivos Snow Family admite los siguientes tipos de notificación:

- Eventos de creación de objetos nuevos
- Eventos de eliminación de objetos
- Eventos de etiquetado de objetos

Configuración de las notificaciones de eventos de Amazon S3

1. Antes de comenzar, debe tener una infraestructura de MQTT en su red.
2. En el cliente de Snowball Edge, ejecute el comando `snowballEdge configure` para configurar el dispositivo Snowball Edge.

   Cuando se le pida, proporcione la siguiente información:

- La ruta del archivo de manifiesto.
- El código de desbloqueo del dispositivo.
- *El punto final del dispositivo (por ejemplo, https://10.0.0.1).*

3. Ejecute el siguiente comando `put-notification-configuration` para enviar notificaciones a un agente 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. Ejecute el siguiente comando `get-notification-configuration` para comprobar que todo está configurado correctamente:

```
snowballEdge get-notification-configuration --service-id s3-snow
```

   Esto devuelve el punto de conexión del agente y el campo habilitado.

Tras configurar todo el clúster para enviar notificaciones al agente de MQTT de la red, cada llamada a la API de un objeto generará una notificación de evento.

> **Note**
>
> Debe suscribirse al tema s3SnowEvents/*Device ID* (o *Cluster ID* si es un clúster) / BucketName. *También puedes usar caracteres comodín, por ejemplo, el nombre del tema puede ser # o s3 /#. SnowEvents*

A continuación se muestra un ejemplo de registro de eventos de almacenamiento compatible con Amazon S3 en dispositivos Snow Family:


```
{
    "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 obtener más información acerca de las notificaciones de eventos de Amazon S3, consulte Notificaciones de eventos de Amazon S3.

Configuración de notificaciones SMTP locales

Puede configurar notificaciones locales para sus dispositivos Snowball Edge con el Protocolo simple de transferencia de correo (SMTP). Las notificaciones locales envían correos electrónicos a los servidores configurados cuando cambia el estado del servicio (Activo, Degradado o Inactivo) o si se superan los umbrales de utilización de la capacidad del 80 %, 90 % o 100 %.

Antes de comenzar, confirme lo siguiente:

- Tiene acceso a la última versión del cliente de Snowball Edge.
- El dispositivo está desbloqueado y listo para su uso.
- El dispositivo puede conectarse a Internet (si utiliza Amazon Simple Email Service o un servidor SMTP externo) o a un servidor SMTP local.

Configuración del dispositivo

Configure el dispositivo para que le envíe notificaciones por correo electrónico.

Configuración del dispositivo para las notificaciones SMTP

1. Ejecute el siguiente comando para agregar una configuración SMTP al 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"
```

   Si la agrega correctamente, recibirá un correo electrónico de prueba de example-sender@domain.com.

2. Pruebe la configuración mediante el siguiente comando `get-notification-configuration`:

```
snowballEdge get-notification-configuration \
  --service-id local-monitoring
```

   La respuesta no incluye una contraseña ni un certificado, aunque los proporcione.

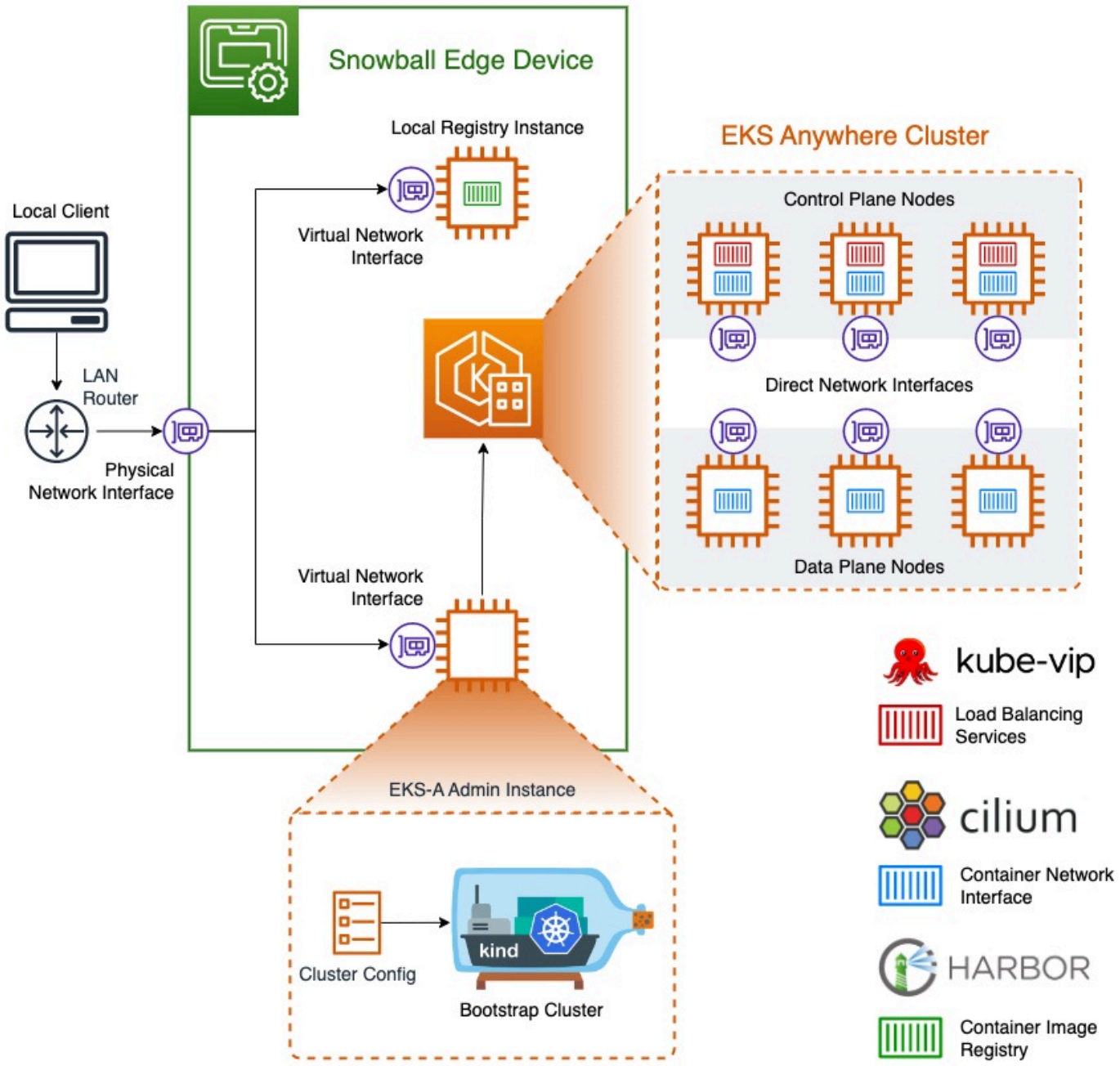
Uso de Amazon EKS Anywhere on AWS Snow

Amazon EKS Anywhere on AWS Snow le ayuda a crear y operar clústeres de Kubernetes en los dispositivos de la familia Snow. Kubernetes es un software de código abierto que se utiliza para automatizar la implementación, el escalado y la administración de aplicaciones en contenedores. Puede utilizar Amazon EKS Anywhere en un dispositivo Snowball Edge con una conexión de red externa o sin ella. Para utilizar Amazon EKS Anywhere en un dispositivo sin una conexión de red externa, proporcione un registro de contenedores para que se ejecute en el dispositivo Snowball Edge. Para obtener información general sobre Amazon EKS Anywhere, consulte la documentación de Amazon EKS Anywhere.

El uso de Amazon EKS Anywhere on AWS Snow le proporciona las siguientes capacidades:

- Aprovisionamiento de un clúster de Kubernetes (K8s) con la CLI de Amazon EKS Anywhere (eksctl anywhere) en dispositivos Snowball Edge optimizados para computación. Puede aprovisionar Amazon EKS Anywhere en un único dispositivo Snowball Edge o en tres o más dispositivos para obtener alta disponibilidad.
- Compatibilidad con el complemento Cilium Container Network Interface (CNI).
- Compatibilidad con Ubuntu 20.04 como sistema operativo de los nodos.

Este diagrama ilustra un clúster de Amazon EKS Anywhere implementado en un dispositivo Snowball Edge.



Le recomendamos que cree su clúster de Kubernetes con la última versión de Kubernetes disponible compatible con Amazon EKS Anywhere. Para obtener más información, consulte Amazon EKS-Anywhere Versioning. Si su aplicación requiere una versión específica de Kubernetes, utilice cualquier versión de Kubernetes que Amazon EKS ofrezca como soporte estándar o extendido. Tenga en cuenta las fechas de lanzamiento y soporte de las versiones de Kubernetes al planificar el ciclo de vida de su implementación. Esto le ayudará a evitar la posible pérdida de soporte para la

versión de Kubernetes que vaya a utilizar. Para obtener más información, consulte el calendario de versiones de Amazon EKS Kubernetes.

Para obtener más información sobre Amazon EKS Anywhere on AWS Snow, consulte la documentación de Amazon EKS Anywhere.

Temas

Acciones que se deben realizar antes de pedir un dispositivo Snowball Edge para Amazon EKS Anywhere on Snow AWS

En estos momentos, Amazon EKS Anywhere es compatible con dispositivos Snowball Edge optimizados para computación y optimizados para computación con unidad de procesamiento gráfico (GPU). Antes de pedir un dispositivo Snowball Edge, debe realizar algunas tareas preparatorias.

- Cree y proporcione una imagen del sistema operativo que se usará para crear máquinas virtuales en el dispositivo.
- Su red debe tener una dirección IP estática disponible para el punto final del plano de control del K8s y permitir el Protocolo de resolución de direcciones (ARP).
- El dispositivo Snowball Edge debe tener abiertos determinados puertos. Para obtener más información sobre los puertos, consulte Puertos y protocolos en la documentación de Amazon EKS Anywhere.

Temas

Creación de una AMI de Ubuntu EKS Distro

Para crear la AMI de Ubuntu EKS Distro, consulte Build Snow node images.

El nombre de la AMI generada seguirá el patrón `capa-ami-ubuntu-20.04-version-timestamp`. Por ejemplo, `capa-ami-ubuntu-20.04-v1.24-1672424524`.

Creación de una AMI de Harbor

Configure una AMI de registro privado de Harbor para incluirla en el dispositivo Snowball Edge de forma que pueda utilizar Amazon EKS Anywhere en el dispositivo sin necesidad de una conexión de red externa. Si no va a utilizar Amazon EKS Anywhere mientras el dispositivo Snowball Edge está desconectado de la red externa, o si tiene un registro privado de Kubernetes en una AMI para usarlo en el dispositivo, puede omitir esta sección.

Para crear la AMI del registro local de Harbor, consulte Build a Harbor AMI.

Pedir un dispositivo Snowball Edge para usarlo con Amazon EKS Anywhere on Snow AWS

Para pedir un dispositivo Snowball Edge optimizado para computación u optimizado para computación con GPU, consulte Crear un trabajo para pedir un dispositivo de la familia Snow en esta guía y tenga en cuenta lo siguiente durante el proceso de pedido:

- En el paso 1, elija el tipo de trabajo Solo computación y almacenamiento locales.
- En el paso 2, elija el tipo de dispositivo Snowball Edge Compute Optimized o Snowball Edge Compute Optimized con GPU.
- En el paso 3, elija Amazon EKS Anywhere on AWS Snow y, a continuación, elija la versión de Kubernetes que necesite.

> **Note**
>
> Para ofrecer el software más reciente, podemos configurar el dispositivo con una versión de ESK Anywhere más reciente que la que está disponible actualmente. Para obtener más información, consulte Control de versiones en la Guía del usuario de Amazon EKS.
> Le recomendamos que cree su clúster de Kubernetes con la última versión de Kubernetes disponible compatible con Amazon EKS Anywhere. Para obtener más información, consulte Amazon EKS-Anywhere Versioning. Si su aplicación requiere una versión

específica de Kubernetes, utilice cualquier versión de Kubernetes que Amazon EKS ofrezca como soporte estándar o extendido. Tenga en cuenta las fechas de lanzamiento y soporte de las versiones de Kubernetes al planificar el ciclo de vida de su implementación. Esto le ayudará a evitar la posible pérdida de soporte para la versión de Kubernetes que vaya a utilizar. Para obtener más información, consulte el calendario de versiones de Amazon EKS Kubernetes.

- Elija las AMI que desea incluir en el dispositivo, incluida la AMI de distribución de EKS (consulteCreación de una AMI de Ubuntu EKS Distro) y, opcionalmente, la AMI de Harbor que creó (consulte Creación de una AMI de Harbor).
- Si necesita varios dispositivos Snowball Edge para conseguir alta disponibilidad, elija el número de dispositivos que necesita en Alta disponibilidad.

Tras recibir su dispositivo o dispositivos Snowball Edge, configure Amazon EKS Anywhere según se indica en Configuración y ejecución de Amazon EKS Anywhere en dispositivos Snowball Edge.

Configuración y ejecución de Amazon EKS Anywhere en dispositivos Snowball Edge

Siga estos procedimientos para configurar e iniciar Amazon EKS Anywhere en sus dispositivos Snowball Edge. A continuación, para configurar Amazon EKS Anywhere de forma que funcione en dispositivos desconectados, debe realizar algunos procedimientos adicionales antes de desconectar esos dispositivos de la red externa. Para obtener más información, consulte Configuración de Amazon EKS Anywhere on AWS Snow para un funcionamiento desconectado.

Temas

- Configuración inicial de
- Configuración y ejecución automáticas de Amazon EKS Anywhere en dispositivos Snowball Edge
- Configuración y ejecución manuales de Amazon EKS Anywhere en dispositivos Snowball Edge

Configuración inicial de

Para realizar la configuración inicial en cada dispositivo Snowball Edge debe conectar el dispositivo a la red local, descargar el cliente de Snowball Edge, obtener las credenciales y desbloquear el dispositivo.

Realización de la configuración inicial

1. Descargue e instale el cliente de Snowball Edge. Para obtener más información, consulte Descarga e instalación del cliente de Snowball Edge.
2. Conecte el dispositivo a la red local. Para obtener más información, consulte Conexión a la red local.
3. Obtenga las credenciales para desbloquear el dispositivo. Para obtener más información, consulte Obtener credenciales para acceder a un dispositivo de la familia Snow.
4. Desbloquee el dispositivo. Para obtener más información, consulte Desbloquear el dispositivo de la familia Snow. También puede usar una herramienta de script en lugar de desbloquear los dispositivos manualmente. Consulte Desbloqueo de dispositivos.

Configuración y ejecución automáticas de Amazon EKS Anywhere en dispositivos Snowball Edge

Puede utilizar herramientas de script de ejemplo para configurar el entorno y ejecutar una instancia de administración de Amazon EKS Anywhere o bien puede hacerlo manualmente. Para usar las herramientas de script, consulte Desbloqueo de dispositivos y configuración del entorno para Amazon EKS Anywhere. Si una vez configurado el entorno y cuando la instancia de administración de Amazon EKS Anywhere está en ejecución necesita configurar Amazon EKS Anywhere para que funcione en el dispositivo Snowball Edge mientras está desconectado de la red, consulte Configuración de Amazon EKS Anywhere on AWS Snow para un funcionamiento desconectado. De lo contrario, consulte Creación y mantenimiento de clústeres en dispositivos Snowball Edge.

Para configurar manualmente el entorno y ejecutar una instancia de administración de Amazon EKS Anywhere, consulte Configuración y ejecución manuales de Amazon EKS Anywhere en dispositivos Snowball Edge.

Configuración y ejecución manuales de Amazon EKS Anywhere en dispositivos Snowball Edge

Temas

- Cree un perfil AWS CLI
- Creación de un usuario local de IAM para Amazon EKS Anywhere
- (Opcional) Creación e importación de una clave Secure Shell

- Ejecución de una instancia de administración de Amazon EKS Anywhere y transferencia de los archivos de credenciales y certificados a esa instancia

Cree un perfil AWS CLI

Cree un AWS CLI perfil para almacenar las credenciales y utilizarlas durante todo el proceso de configuración de los dispositivos Snowball Edge y la instancia de administración de Amazon EKS Anywhere. Para obtener más información sobre AWS CLI los perfiles, consulte los perfiles con nombre AWS CLI en la Guía del AWS Command Line Interface usuario.

Puede utilizar una herramienta de script de muestra para crear automáticamente el AWS CLI perfil y el usuario de IAM local de Amazon EKS Anywhere. Consulte Creación de credenciales y de un archivo de certificados. Después de usar el script, siga con (Opcional) Creación e importación de una clave Secure Shell. De lo contrario, siga este procedimiento y, a continuación, los procedimientos que se describen en Creación de un usuario local de IAM para Amazon EKS Anywhere.

> **Note**
>
> Debe hacer esto para cada dispositivo Snowball Edge que configure.

```
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" ]
}
```

Utilice el valor de `AccessKeyIds` como valor del parámetro `access-key-id` del 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
```

Utilice el valor de `aws_access_key_id` y `aws_secret_access_key` como valores de `AWS Access Key ID` y `AWS Secret Access Key` del 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
```

Creación de un usuario local de IAM para Amazon EKS Anywhere

Para seguir las prácticas recomendadas de seguridad, cree un usuario de IAM local para Amazon EKS Anywhere en el dispositivo Snowball Edge. Para hacerlo de forma manual, utilice los siguientes procedimientos.

> **Note**
>
> Debe hacerlo para cada dispositivo Snowball Edge que utilice.

Creación de un usuario local

Utilice el comando `create-user` para crear el usuario de IAM de 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"
        }
    }
```

Creación de una política para el usuario local

Cree un documento de política, utilícelo para crear una política de IAM y asocie esa política al usuario local de Amazon EKS Anywhere.

Cómo crear un documento de política y asociarlo al usuario local de Amazon EKS Anywhere

1. Cree un documento de política y guárdelo en su equipo. Copie al documento la política que se muestra a continuación.

```
{
  "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. Utilice el comando `create-policy` para crear una política de IAM basada en el documento de política. El valor del parámetro `--policy-document` debe usar la ruta absoluta al archivo de política. Por ejemplo, `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. Utilice el comando `attach-user-policy` para asociar la política de IAM al usuario local de Amazon EKS Anywhere.

```
aws iam attach-user-policy --policy-arn policy-arn --user-name user-name --endpoint
 http://snowball-ip:6078 --profile profile-name
```

Creación de una clave de acceso y un archivo de credenciales

Cree una clave de acceso para el usuario local de IAM de Amazon EKS Anywhere. A continuación, cree un archivo de credenciales e incluya en él los valores de `AccessKeyId` y `SecretAccessKey` generados para el usuario local. La instancia de administración de Amazon EKS Anywhere utilizará el archivo de credenciales más adelante.

1. Utilice el comando `create-access-key` para crear una clave de acceso para el usuario local de 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. Cree un archivo de credenciales. Guarde en él los valores de `AccessKeyId` y `SecretAccessKey` en el siguiente formato.

```
[snowball-ip]
aws_access_key_id = ABCDEFGHIJKLMNOPQR2T
aws_secret_access_key = AfSD7sYz/TBZtzkReBl6PuuISzJ2WtNkeePw+nNzJ
region = snow
```

> **Note**
>
> Si está trabajando con varios dispositivos Snowball Edge, el orden de las credenciales en el archivo no importa, pero las credenciales de todos los dispositivos deben estar en un solo archivo.

Creación de un archivo de certificados para la instancia de administración

La instancia de administración de Amazon EKS Anywhere necesita los certificados de los dispositivos Snowball Edge para poder ejecutarse en ellos. Cree un archivo de certificados que contenga el certificado para obtener acceso a los dispositivos Snowball Edge que la instancia de administración de Amazon EKS Anywhere usará más adelante.

Creación de un archivo de certificados

1. Utilice el comando `list-certificates` para obtener certificados para cada dispositivo Snowball Edge que vaya a utilizar.

```
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. Utilice el valor de `CertificateArn` como valor para el parámetro `--certificate-arn` del 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. Cree un archivo de certificados de los dispositivos. Coloque el resultado de `get-certificate` en el archivo de certificados. A continuación se muestra un ejemplo de cómo guardar la salida.

> **Note**
>
> Si está trabajando con varios dispositivos Snowball Edge, el orden de las credenciales en el archivo no importa, pero las credenciales de todos los dispositivos deben estar en un solo archivo.

```
-----BEGIN CERTIFICATE-----
ZWtzYSBzbm93IHRlc3QgY2VydGlmaWNhdGUgZWtzYSBzbm93IHRlc3QgY2VydGlm
aWNhdGVla3NhIHNub3cgdGVzdCBjZXJ0aWZpY2F0ZWVrc2Egc25vdyB0ZXN0IGNl
cnRpZmljYXRlZWtzYSBzbm93IHRlc3QgY2VydGlmaWNhdGVla3NhIHNub3cgdGVz
```

```
dCBjZXJ0aWZpY2F0ZQMIIDXDCCAkSgAwIBAgIJAISM0nTVmbj+MA0GCSqGSIb3DQ
...
-----END CERTIFICATE-----
```

4. Repita el procedimiento Creación de un usuario local de IAM para Amazon EKS Anywhere para crear un usuario local de IAM para Amazon EKS Anywhere en todos los dispositivos Snowball Edge.

(Opcional) Creación e importación de una clave Secure Shell

Utilice este procedimiento opcional para crear una clave Secure Shell (SSH) a fin de obtener acceso a todas las instancias de nodo de Amazon EKS Anywhere e importar la clave pública en todos los dispositivos Snowball Edge. Guarde y proteja este archivo de clave.

Si omite este procedimiento, Amazon EKS Anywhere creará e importará una clave SSH automáticamente cuando sea necesario. Esta clave se almacenará en la instancia de administración en `${PWD}/${CLUSTER_NAME}/eks-a-id_rsa`.

Creación de una clave SSH e importación a la instancia Amazon EKS Anywhere

1. Utilice el comando `ssh-keygen` para generar una clave SSH.

```
ssh-keygen -t rsa -C "key-name" -f path-to-key-file
```

2. Utilice el comando `import-key-pair` para importar la clave del equipo al dispositivo Snowball Edge.

> **Note**
>
> El valor del parámetro `key-name` debe ser el mismo al importar la clave a todos los 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"
}
```

Ejecución de una instancia de administración de Amazon EKS Anywhere y transferencia de los archivos de credenciales y certificados a esa instancia

Ejecución de una instancia de administración de Amazon EKS Anywhere

Siga este procedimiento para ejecutar manualmente una instancia de administración de Amazon EKS Anywhere, configurar una interfaz de red virtual (VNI) para la instancia de administración, comprobar el estado de la instancia, crear una clave SSH y conectarse a la instancia de administración con ella. Puede utilizar una herramienta de script de ejemplo para automatizar la creación de una instancia de administración de Amazon EKS Anywhere y la transferencia de archivos de credenciales y certificados a esta instancia. Consulte Creación de una instancia de administración de Amazon EKS Anywhere. Cuando la herramienta de script finaliza, puede obtener acceso a la instancia mediante ssh y crear clústeres; para ello, consulte Creación y mantenimiento de clústeres en dispositivos Snowball Edge. Si desea configurar la instancia de Amazon EKS Anywhere manualmente, siga estos pasos.

> **Note**
>
> Si está utilizando más de un dispositivo Snowball Edge para aprovisionar el clúster, puede lanzar una instancia de administración de Amazon EKS Anywhere en cualquiera de los dispositivos Snowball Edge.

Ejecución de una instancia de administración de Amazon EKS Anywhere

1. Utilice el comando `create-key-pair` para crear una clave SSH para la instancia de administración de Amazon EKS Anywhere. El comando guarda la clave en `$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. Utilice el comando `describe-images` para buscar en la salida el nombre de la imagen que comienza por `eks-anywhere-admin`.

```
aws ec2 describe-images --endpoint http://snowball-ip:8008 --profile profile-name
```

3. Utilice el comando `run-instance` para iniciar una instancia eks-a admin con la imagen de administración de 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. Utilice el comando `describe-instances` para comprobar el estado de la instancia de Amazon EKS Anywhere. Espere hasta que el comando indique que el estado de la instancia es `running` antes de continuar.

```
aws ec2 describe-instances --instance-id instance-id --endpoint http://snowball-
ip:8008 --profile profile-name
```

5. Examine la salida del comando `describe-device` y anote el valor de `PhysicalNetworkInterfaceId` de la interfaz de red física que está conectada a la red. Lo utilizará para crear una 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. Cree una VNI para la instancia de administración de Amazon EKS Anywhere. Utilice el valor de `PhysicalNetworkInterfaceId` como valor del parámetro `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. Utilice el valor de `IpAddress` como valor del parámetro `public-ip` del comando `associate-address` para asociar la dirección pública a la instancia de administración de Amazon EKS Anywhere.

```
aws ec2 associate-address --instance-id instance-id --public-ip VNI-IP --endpoint
 http://snowball-ip:8008 --profile profile-name
```

8. Conéctese a la instancia de administración de Amazon EKS Anywhere mediante SSH.

```
ssh -i path-to-key ec2-user@VNI-IP
```

Transferencia de los archivos de certificados y credenciales a la instancia de administración

Cuando la instancia de administración de Amazon EKS Anywhere esté en ejecución, transfiera las credenciales y los certificados de los dispositivos Snowball Edge a la instancia de administración. Ejecute el comando siguiente desde el mismo directorio en el que guardó los archivos de credenciales y certificados en los procedimientos Creación de una clave de acceso y un archivo de credenciales y Creación de un archivo de certificados para la instancia de administración.

```
scp -i path-to-key path-to-credentials-file path-to-certificates-file ec2-user@eks-
admin-instance-ip:~
```

Compruebe el contenido de los archivos en la instancia de administración de Amazon EKS Anywhere. A continuación se muestran ejemplos de los archivos de credenciales y 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-----
```

Configuración de Amazon EKS Anywhere on AWS Snow para un funcionamiento desconectado

Complete esta configuración adicional de Amazon EKS Anywhere en el dispositivo Snowball Edge mientras está conectado a una red para preparar Amazon EKS Anywhere de manera que se ejecute en un entorno sin conexión de red externa.

Para configurar Amazon EKS Anywhere para su uso sin conexión con su propio registro de Kubernetes local y privado, consulte Configuración del reflejo del registro en la documentación de EKS Anywhere.

Si creó una AMI de registro privado Harbor, siga los procedimientos de esta sección.

Temas

- Configuración de el registro Harbor en un dispositivo Snowball Edge
- Use el registro Harbor en la instancia de administración de Amazon EKS Anywhere

Configuración de el registro Harbor en un dispositivo Snowball Edge

Consulte Configuración de Harbor en un dispositivo Snowball Edge.

Use el registro Harbor en la instancia de administración de Amazon EKS Anywhere

Consulte Importación de imágenes de contenedores de Amazon EKS Anywhere al registro Harbor local en un dispositivo Snowball Edge.

Creación y mantenimiento de clústeres en dispositivos Snowball Edge

Prácticas recomendadas para crear clústeres

Para crear un clúster de Amazon EKS Anywhere, consulte Crear clústeres de Snow.

Tenga en cuenta las siguientes prácticas recomendadas al crear clústeres de Amazon EKS Anywhere en dispositivos Snowball Edge:

- Antes de crear un clúster en un rango de direcciones IP estáticas, asegúrese de que no haya otros clústeres en el dispositivo Snowball Edge que utilicen el mismo rango de direcciones IP.
- Antes de crear un clúster con direcciones DHCP en el dispositivo Snowball Edge, asegúrese de que todos los rangos de direcciones IP estáticas que se utilizan para los clústeres no estén en la subred del grupo de DHCP.
- Al crear más de un clúster, espere a que uno se aprovisione y ejecute correctamente antes de crear otro.

Actualización de clústeres

Para actualizar una AMI de administrador de Amazon EKS Anywhere o una AMI de distribución de EKS, póngase en contacto con AWS Support. AWS Support proporcionará una actualización de Snowball Edge con la AMI mejorada. A continuación, descargue e instale la actualización de Snowball Edge. Consulte Descarga de actualizaciones y Instalación de actualizaciones.

Tras actualizar la AMI de Amazon EKS Anywhere, debe iniciar una nueva instancia de administración de Amazon EKS Anywhere. Consulte Ejecución de una instancia de administración de Amazon EKS Anywhere. A continuación, copie los archivos de clave, la carpeta del clúster, las credenciales y los certificados de la instancia de administración anterior a la instancia actualizada. Se encuentran en una carpeta que tiene el mismo nombre que el clúster.

Limpiando los recursos del clúster

Si crea varios clústeres en los dispositivos Snowball Edge y no los elimina correctamente, o si hay un problema en el clúster y el clúster crea nodos de sustitución tras reanudarse, se producirá una pérdida de recursos. Hay disponible una herramienta de script de muestra para que la modifique y utilice para limpiar su instancia de administración de Amazon EKS Anywhere y sus dispositivos Snowball Edge. Consulte Amazon EKS Anywhere on AWS Snow sobre las herramientas de limpieza.

Uso local de IAM

AWS Identity and Access Management (IAM) le ayuda a controlar de forma segura el acceso a AWS los recursos que se ejecutan en su AWS Snowball Edge dispositivo. Utilice IAM para controlar quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos.

IAM puede utilizarse localmente en su dispositivo. Puede usar el servicio IAM local para crear nuevos usuarios y adjuntarles políticas de IAM. Puede utilizar estas políticas para permitir el acceso necesario para realizar tareas asignadas. Por ejemplo, puede otorgar a un usuario la capacidad de transferir datos, pero limitar su capacidad de crear nuevas instancias compatibles con Amazon EC2.

Además, puede crear credenciales locales basadas en sesiones utilizando AWS Security Token Service (AWS STS) en su dispositivo. Para obtener más información sobre el servicio IAM, consulte Introducción en la Guía del usuario de IAM.

Las credenciales raíz de tu dispositivo no se pueden deshabilitar y no puedes usar las políticas de tu cuenta para denegar explícitamente el acceso al usuario Cuenta de AWS raíz. Le recomendamos que proteja las claves de acceso de usuario raíz y que cree credenciales de usuario de IAM para la interacción diaria con su dispositivo.

> **Important**
>
> La documentación de esta sección se aplica al uso local de IAM en un dispositivo AWS Snowball Edge. Para obtener información sobre el uso de IAM en el Nube de AWS, consulteIdentity and Access Management en AWS Snowball.
> Para que AWS los servicios funcionen correctamente en un Snowball Edge, debe permitir los puertos para los servicios. Para obtener más detalles, consulte Puertos necesarios para usar AWS los servicios en un dispositivo AWS Snowball perimetral.

Temas

Uso de las operaciones AWS CLI y de la API en Snowball Edge

Cuando utilice las AWS CLI operaciones de API para emitir comandos de IAM AWS STS, Amazon S3 y Amazon EC2 en Snowball Edge, debe especificar `region` «». `snow` Puede hacerlo utilizando `aws configure` o dentro del propio comando, como en los ejemplos siguientes.

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

Or (Disyunción)

```
aws iam list-users --profile snowballEdge --endpoint http://192.0.2.0:6078 --region
 snow
```

> **Note**
>
> El identificador de la clave de acceso y la clave secreta de acceso que se utilizan localmente en AWS Snowball Edge no se pueden intercambiar con las claves del Nube de AWS.

Lista de AWS CLI comandos de IAM compatibles en un Snowball Edge

A continuación se describe el subconjunto de AWS CLI comandos y opciones de IAM compatibles con los dispositivos Snowball Edge. Si un comando o una opción no aparece en la lista siguiente, no está admitido. En la descripción se indican los parámetros no admitidos para los comandos.

- attach-role-policy— Adjunta la política gestionada especificada a la función de IAM especificada.
- attach-user-policy— Adjunta la política gestionada especificada al usuario especificado.
- create-access-key— Crea una nueva clave de acceso secreta de IAM local y el ID de clave de AWS acceso correspondiente para el usuario especificado.
- create-policy: crea una nueva política administrada de IAM para el dispositivo.
- create-role: crea un nuevo rol de IAM local para el dispositivo. Los siguientes parámetros no se admiten:
  - `Tags`
  - `PermissionsBoundary`
- create-user: crea un nuevo usuario de IAM local para el dispositivo. Los siguientes parámetros no se admiten:
  - `Tags`
  - `PermissionsBoundary`
- delete-access-key— Elimina una nueva clave de acceso secreta de IAM local y el ID de clave de AWS acceso correspondiente para el usuario especificado.
- delete-policy: elimina la política administrada especificada.
- delete-role: elimina el rol especificado.
- delete-user: elimina el usuario especificado.
- detach-role-policy— Elimina la política gestionada especificada del rol especificado.
- detach-user-policy— Elimina la política gestionada especificada del usuario especificado.
- get-policy: recupera información sobre la política administrada especificada, incluida la versión predeterminada de la política y el número total de usuarios, grupos y roles de IAM a los que se asocia dicha política.
- get-policy-version— Recupera información sobre la versión especificada de la política gestionada especificada, incluido el documento de política.
- get-role: recupera información sobre el rol especificado, incluidos la ruta del rol, el GUID, el ARN y la política de confianza del rol que concede permiso para asumir el rol.
- get-user: recupera información acerca del usuario de IAM especificado, incluidos la fecha de creación, la ruta, el ID exclusivo y el ARN del usuario.
- list-access-keys— Devuelve información sobre los ID de las claves de acceso asociados al usuario de IAM especificado.

- list-attached-role-policies— Muestra todas las políticas gestionadas asociadas a la función de IAM especificada.
- list-attached-user-policies— Muestra todas las políticas gestionadas que están asociadas al usuario de IAM especificado.
- list-entities-for-policy— Muestra todos los usuarios, grupos y funciones de IAM locales a los que está asociada la política gestionada especificada.
  - `--EntityFilter`: solo se admiten los valores `user` y `role`.
- list-policies: enumera todas las políticas administradas que están disponibles en su Cuenta de AWS local. El siguiente parámetro no se admite:
  - `--PolicyUsageFilter`
- list-roles: enumera los roles de IAM locales que tienen el prefijo de ruta especificado.
- list-users: enumera los usuarios de IAM que tienen el prefijo de ruta especificado.
- update-access-key— Cambia el estado de la clave de acceso especificada de Activa a Inactiva o viceversa.
- update-assume-role-policy— Actualiza la política que otorga permiso a una entidad de IAM para asumir un rol.
- update-role: actualiza la descripción o la configuración de duración máxima de la sesión de un rol.
- update-user: actualiza el nombre o la ruta del usuario de IAM especificado.

Operaciones de la API de IAM admitidas

A continuación, encontrará las operaciones de la API de IAM que puede utilizar con un dispositivo Snowball Edge, con enlaces a sus descripciones en la Referencia de la API de IAM.

- AttachRolePolicy— Adjunta la política gestionada especificada a la función de IAM especificada.
- AttachUserPolicy— Adjunta la política gestionada especificada al usuario especificado.
- CreateAccessKey— Crea una nueva clave de acceso secreta de IAM local y el ID de clave de AWS acceso correspondiente para el usuario especificado.
- CreatePolicy— Crea una nueva política gestionada de IAM para su dispositivo.
- CreateRole— Crea una nueva función de IAM local para su dispositivo.
- CreateUser— Crea un nuevo usuario de IAM local para su dispositivo.

  Los siguientes parámetros no se admiten:
  - `Tags`

  - `PermissionsBoundary`
- DeleteAccessKey— Elimina la clave de acceso especificada.
- DeletePolicy— Elimina la política gestionada especificada.
- DeleteRole— Elimina el rol especificado.
- DeleteUser— Elimina el usuario especificado.
- DetachRolePolicy— Elimina la política gestionada especificada del rol especificado.
- DetachUserPolicy— Elimina la política gestionada especificada del usuario especificado.
- GetPolicy— Recupera información sobre la política gestionada especificada, incluida la versión predeterminada de la política y el número total de usuarios, grupos y funciones de IAM locales a los que está asociada la política.
- GetPolicyVersion— Recupera información sobre la versión especificada de la política gestionada especificada, incluido el documento de política.
- GetRole— Recupera información sobre el rol especificado, incluida la ruta del rol, el GUID, el ARN y la política de confianza del rol que otorga permiso para asumir el rol.
- GetUser— Recupera información sobre el usuario de IAM especificado, incluida la fecha de creación del usuario, la ruta, el ID único y el ARN.
- ListAccessKeys— Devuelve información sobre los ID de las claves de acceso asociados al usuario de IAM especificado.
- ListAttachedRolePolicies— Muestra todas las políticas gestionadas asociadas a la función de IAM especificada.
- ListAttachedUserPolicies— Muestra todas las políticas gestionadas que están asociadas al usuario de IAM especificado.
- ListEntitiesForPolicy— Recupera información sobre el usuario de IAM especificado, incluida la fecha de creación del usuario, la ruta, el ID único y el ARN.
  - `--EntityFilter`: solo se admiten los valores `user` y `role`.
- ListPolicies— Enumera todas las políticas gestionadas que están disponibles en su local. Cuenta de AWS El siguiente parámetro no se admite:
  - `--PolicyUsageFilter`
- ListRoles— Muestra las funciones de IAM locales que tienen el prefijo de ruta especificado.
- ListUsers— Muestra los usuarios de IAM que tienen el prefijo de ruta especificado.
- UpdateAccessKey— Cambia el estado de la clave de acceso especificada de Activa a Inactiva o viceversa.

- UpdateAssumeRolePolicy— Actualiza la política que otorga permiso a una entidad de IAM para asumir un rol.
- UpdateRole— Actualiza la descripción o la configuración de duración máxima de la sesión de un rol.
- UpdateUser— Actualiza el nombre o la ruta del usuario de IAM especificado.

Compatibilidad de versión y gramática de la política de IAM

A continuación se presenta la versión local compatible de IAM 2012-10-17 de la política de IAM y un subconjunto de la gramática de políticas.

Tipo de política	Gramática compatible
Políticas basadas en la identidad (política de usuario/rol)	`"Effect"`, `"Action"` y `"Resource"` **Note** IAM local no admite `"Condition "`, `"NotAction "`, `"NotResource "` y `"Principal "`.
Políticas basadas en recursos (política de confianza de roles)	`"Effect"`, `"Action"` y `"Principal "` **Note** En el caso del principal, solo se permite el Cuenta de AWS ID o el ID principal.

Ejemplos de políticas de IAM

Note

AWS Identity and Access Management Los usuarios (IAM) necesitan `"snowballdevice:*"` permisos para usar la AWS OpsHub for Snow Family aplicación y administrar los dispositivos de la familia Snow.

A continuación se muestran ejemplos de políticas que conceden permisos para un dispositivo Snowball Edge.

Ejemplo 1: Permite GetUser llamar a un usuario de muestra a través de la API de IAM

Utilice la siguiente política para permitir la GetUser llamada de un usuario de muestra a través de la API de IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "iam:GetUser",
            "Resource": "arn:aws:iam:::user/example-user"
        }
    ]
}
```

Ejemplo 2: permite acceso total a la API de Amazon S3

Utilice la siguiente política para permitir el acceso total a la API de Amazon S3.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "*"

        }
    ]
}
```

Ejemplo 3: permite el acceso de lectura y escritura de un determinado bucket de Amazon S3

Utilice la siguiente política para permitir el acceso de lectura y escritura a un 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/*"
        }
    ]
}
```

Ejemplo 4: permite el acceso List, Get y Put para un bucket específico de Amazon S3

Utilice la siguiente política para permitir el acceso List, Get y Put para un bucket específico de S3.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::examplebucket/*"
        }
    ]
}
```

Ejemplo 5: permite acceso total a la API de Amazon EC2

Utilice la siguiente política para permitir acceso total a Amazon EC2.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*"
        }
    ]
}
```

Ejemplo 6: permite el acceso para iniciar y detener instancias compatibles con Amazon EC2.

Utilice la siguiente política para permitir el acceso para iniciar y detener instancias de Amazon EC2.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": "*"
        }
    ]
}
```

Ejemplo 7: Rechaza las llamadas DescribeLaunchTemplates pero permite que todas las llamadas DescribeImages

Utilice la siguiente política para denegar las llamadas a `DescribeLaunchTemplates` pero permitir todas las llamadas a `DescribeImages`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ec2:DescribeLaunchTemplates"
```

```
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImages"
            ],
            "Resource": "*"
        }
    ]
}
```

Ejemplo 8: política para llamadas a la API

Enumera todas las políticas administradas que están disponibles en su dispositivo Snow, incluidas sus propias políticas administradas definidas por el cliente. Hay más información disponible al respecto en 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"
        }
    ]
}
```

TrustPolicy Ejemplo

Una política de confianza devuelve un conjunto de credenciales de seguridad temporales que puede utilizar para acceder a AWS recursos a los que normalmente no tendría acceso. Las credenciales

temporales incluyen un ID de clave de acceso, una clave de acceso secreta y un token de seguridad. Normalmente, se utiliza `AssumeRole` en la cuenta para el acceso entre cuentas.

A continuación, se muestra un ejemplo de una política de confianza. Para obtener más información sobre la política de confianza, consulta AssumeRolela referencia de la AWS Security Token Service API.

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

Uso AWS Security Token Service

El AWS Security Token Service (AWS STS) le ayuda a solicitar credenciales temporales con privilegios limitados para los usuarios de IAM.

> **Important**
>
> Para que AWS los servicios funcionen correctamente en un Snowball Edge, debe permitir los puertos para los servicios. Para obtener más detalles, consulte Puertos necesarios para usar AWS los servicios en un dispositivo AWS Snowball perimetral.

Temas

- Uso de las operaciones AWS CLI y de la API en Snowball Edge
- AWS STSAWS CLI Comandos compatibles en un Snowball Edge

- Operaciones de AWS STS API compatibles

Uso de las operaciones AWS CLI y de la API en Snowball Edge

Cuando utilice las AWS CLI operaciones de API para emitir comandos de IAM AWS STS, Amazon S3 y Amazon EC2 en un dispositivo Snowball Edge, debe especificar `region` «». `snow` Puede hacerlo utilizando `AWS configure` o dentro del propio comando, como en los ejemplos siguientes.

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

Or (Disyunción)

```
aws iam list-users --profile snowballEdge --endpoint http://192.0.2.0:6078 --region
 snow
```

> **Note**
>
> El identificador de la clave de acceso y la clave secreta de acceso que se utilizan localmente en AWS Snowball Edge no se pueden intercambiar con las claves del Nube de AWS.

AWS STSAWS CLI Comandos compatibles en un Snowball Edge

El comando assume-role solo es compatible localmente.

Los siguientes parámetros son compatibles con `assume-role`:

- `role-arn`
- `role-session-name`
- `duration-seconds`

Comando de ejemplo

Para asumir un rol, utilice el siguiente 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 obtener más información sobre el uso del comando `assume-role`, consulte ¿Cómo asumo un rol de IAM mediante la AWS CLI?

Para obtener más información sobre el uso AWS STS, consulte Uso de credenciales de seguridad temporales en la Guía del usuario de IAM.

Operaciones de AWS STS API compatibles

Solo la AssumeRoleAPI se admite localmente.

Los siguientes parámetros son compatibles con `AssumeRole`:

- `RoleArn`
- `RoleSessionName`
- `DurationSeconds`

Ejemplo

Para asumir un rol, utilice lo siguiente.

```
https://sts.amazonaws.com/
?Version=2011-06-15
&Action=AssumeRole
&RoleSessionName=session-example
&RoleArn=arn:aws:iam::123456789012:role/demo
&DurationSeconds=3600
```

Administración de certificados de clave pública

Puede interactuar de forma segura con AWS los servicios que se ejecutan en un dispositivo Snowball Edge o en un clúster de dispositivos Snowball Edge mediante el protocolo HTTPS proporcionando un certificado de clave pública. Puede utilizar el protocolo HTTPS para interactuar con AWS servicios como IAM, Amazon EC2, el adaptador S3, el almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow, Amazon EC2 Systems Manager AWS STS y los dispositivos

Snowball Edge. En el caso de un clúster de dispositivos, se requiere un único certificado que cualquier dispositivo del clúster puede generar. Una vez que un dispositivo Snowball Edge genera el certificado y usted lo desbloquea, puede utilizar comandos del cliente de Snowball Edge para enumerar, obtener y eliminar el certificado.

Un dispositivo Snowball Edge genera un certificado cuando se producen los siguientes eventos:

- El dispositivo o el clúster de Snowball Edge se desbloquea por primera vez.
- El dispositivo o clúster Snowball Edge se desbloquea tras eliminar el certificado (mediante el `delete-certificate` comando o Renovar certificado en). AWS OpsHub
- El dispositivo o el clúster de Snowball Edge se reinicia y desbloquea cuando caduca el certificado.

Cada vez que se genera un certificado nuevo, el certificado anterior deja de ser válido. Un certificado es válido durante un año a partir del día en que se generó.

También se puede utilizar AWS OpsHub for Snow Family para gestionar los certificados de clave pública. Para obtener más información, consulte Administrar los certificados de clave pública mediante OpsHub esta guía.

Temas

Listado del certificado

Utilice el comando `list-certificates` para ver los Nombres de recurso de Amazon (ARN) del certificado actual.

```
snowballEdge list-certificates
```

Example de salida de **`list-certificates`**

```
{
```

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

Obtención de certificados

Use el comando `get-certificate` para ver el contenido del certificado según el ARN proporcionado. Utilice el comando `list-certificates` para obtener el ARN del certificado que se va a utilizar como parámetro `certificate-arn`.

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

Example de salida de **`get-certificate`**

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

Para obtener más información sobre cómo configurar su certificado, consulte Especificación del adaptador de S3 como punto de conexión de AWS CLI.

Eliminación de certificados

Use el comando `delete-certificate` para eliminar el certificado actual. Utilice el comando `list-certificates` para obtener el ARN del certificado que se va a utilizar como parámetro `certificate-arn`. Para generar un certificado nuevo, reinicie el dispositivo Snowball Edge o todos los dispositivos Snowball Edge de un clúster. Consulte Reinicio del dispositivo Snow Family o utilice el comando `snowballEdge reboot-device`.

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

Example de salida de **`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.
```

Puertos necesarios para usar AWS los servicios en un dispositivo AWS Snowball perimetral

Para que AWS los servicios funcionen correctamente en un dispositivo AWS Snowball Edge, debe permitir los puertos de red del servicio.

A continuación se muestra una lista de los puertos de red necesarios para cada servicio de AWS .

Puerto	Protocolo	Comentario
22 (HTTP)	TCP	Comprobación de estado del dispositivo y de SSH de EC2
443 (HTTPS)	TCP	Punto de conexión HTTPS de la API de S3 y de la API de control de S3
2049 (HTTP)	TCP	Punto de conexión NFS
6078 (HTTP)	TCP	Punto de conexión HTTP de IAM
6089 (HTTPS)	TCP	Punto de conexión HTTPS de IAM
7078 (HTTP)	TCP	Punto de conexión HTTP de STS
7089 (HTTPS)	TCP	Punto de conexión HTTPS de STS

Puerto	Protocolo	Comentario
8080 (HTTP)	TCP	Punto de conexión HTTP del adaptador de S3
8008 (HTTP)	TCP	Punto de conexión HTTP de EC2
8243 (HTTPS)	TCP	Punto de conexión HTTPS de EC2
8443 (HTTPS)	TCP	Punto final HTTPS del adaptador S3
9091 (HTTP)	TCP	Punto de conexión para la administración de dispositivos
9092	TCP	Entrada para el controlador de dispositivos de EKS Anywhere y CAPAS
8242	TCP	Entrada para el punto de conexión HTTPS de EC2 para EKS Anywhere
6443	TCP	Entrada para el punto de conexión de la API de Kubernetes de EKS Anywhere
2379	TCP	Entrada para el punto de conexión de la API de Etcd de EKS Anywhere
2380	TCP	Entrada para el punto de conexión de la API de Etcd de EKS Anywhere

Uso AWS Snow Device Management para administrar dispositivos

AWS Snow Device Management le permite administrar su dispositivo de la familia Snow y AWS los servicios locales de forma remota. Todos los dispositivos de la familia Snow son compatibles con la gestión de dispositivos Snow y viene instalada en los dispositivos nuevos en la mayoría Regiones de AWS de los dispositivos de la familia Snow disponibles.

Con Snow Device Management, puede realizar las siguientes tareas:

- Creación de una tarea
- Comprobación del estado de la tarea
- Comprobación de los metadatos de una tarea
- Cancelación de una tarea
- Comprobación de la información del dispositivo
- Comprobación del estado de la instancia compatible con Amazon EC2
- Obtención de una lista de comandos y sintaxis
- Obtención de una lista de los dispositivos que se pueden administrar de forma remota
- Obtención de una lista del estado de las tareas en distintos dispositivos
- Obtención de una lista de los recursos disponibles
- Obtención de una lista de tareas por estado
- Obtención de una lista de las etiquetas de un dispositivo o de una tarea
- Aplicación de etiquetas
- Eliminación de etiquetas

Temas

Elegir el estado de administración de dispositivos Snow al solicitar un dispositivo de la familia Snow

Al crear una tarea para solicitar un dispositivo de nieve, puede elegir en qué estado estará la gestión de dispositivos de nieve cuando reciba el dispositivo: instalado pero no activado o instalado y activado. Si está instalado pero no activado, necesitará usar AWS OpsHub el cliente Snowball Edge para activarlo antes de usarlo. Si está instalado y activado, podrá utilizar Snow Device Management después de recibir el dispositivo y conectarlo a la red local. Puede elegir el estado de administración de dispositivos de Snow al crear un trabajo para solicitar un dispositivo a través del Consola de administración de la familia de productos Snow de AWS cliente Snowball Edge o la AWS CLI API de administración de trabajos de Snow.

Para elegir el estado de administración de dispositivos de Snow en la Consola de administración de la familia de productos Snow de AWS

1. Para elegir que se instale y active la administración de dispositivos de nieve, elija Administrar su dispositivo de nieve de forma remota con AWS OpsHub o el cliente Snowball.
2. Para elegir que la administración de dispositivos Snow esté instalada pero no activada, no seleccione Administrar su dispositivo Snow de forma remota con AWS OpsHub un cliente Snowball.

Para obtener más información, consulte el paso 3: Elija las funciones y opciones en esta guía.

Para elegir el estado de administración de dispositivos de Snow desde el AWS CLI cliente Snowball Edge o la API de administración de trabajos de Snow:

- Utilice el `remote-management` parámetro para especificar el estado de administración de dispositivos de Snow. El `INSTALLED_ONLY` valor del parámetro significa que Snow Device Management está instalado pero no activado. El `INSTALLED_AUTOSTART` valor del parámetro significa que Snow Device Management está instalado y activado. Si no especifica ningún valor para este parámetro, `INSTALLED_ONLY` es el valor por defecto.

Example de la sintaxis del **`remote-management`** parámetro del **`create-job`** comando

```
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 obtener más información, consulta la referencia de la API de administración de trabajos en la referencia de la AWS Snowball API.

Activación de Snow Device Management

Siga este procedimiento para activar Snow Device Management mediante el cliente Snowball Edge.

Antes de utilizar este procedimiento, haga lo siguiente:

- Descargue e instale la última versión del cliente de Snowball Edge. Para obtener más información, consulte Descarga e instalación del cliente de Snowball.
- Descargue el archivo de manifiesto y obtenga el código de desbloqueo del dispositivo de la familia Snow. Para obtener más información, consulte Cómo obtener sus credenciales y herramientas.
- Conecte el dispositivo de la familia Snow a su red local. Para obtener más información, consulte las de conexión a la red local.
- Desbloquee el dispositivo de la familia Snow. Para obtener más información, consulte Desbloquear Snowball Edge Cómo desbloquear .

```
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
```

El cliente Snowball Edge devuelve lo siguiente cuando el comando se ejecuta correctamente.

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

Añadir permisos para Snow Device Management a una función de IAM

En el dispositivo Cuenta de AWS desde el que se realizó el pedido, cree un rol AWS Identity and Access Management (de IAM) y añada la siguiente política al rol. A continuación, asigne el rol al usuario de IAM que iniciará sesión para administrar su dispositivo de forma remota con Snow Device Management. Para obtener más información, consulte Creación de roles de IAM y Creación de un usuario de IAM en su Cuenta de 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 de la CLI de Snow Device Management

En esta sección se describen los AWS CLI comandos que puede utilizar para gestionar sus dispositivos de la familia Snow de forma remota con Snow Device Management. También puede realizar algunas tareas de administración remota utilizando AWS OpsHub for Snow Family. Para obtener más información, consulte Administrar AWS los servicios del dispositivo.

> **Note**
>
> Antes de administrar el dispositivo, asegúrate de que esté encendido, conectado a la red y de que pueda conectarse al Región de AWS lugar donde se aprovisionó.

Temas

Creación de una tarea

Para indicar a uno o más dispositivos de destino que realicen una tarea, como desbloquearse o reiniciarse, utilice `create-task`. Debe especificar los dispositivos de destino proporcionando una lista de los ID de dispositivo administrados con el parámetro `--targets` y las tareas que se van a realizar con el parámetro `--command`. Solo se puede ejecutar un comando en un dispositivo cada vez.

Comandos admitidos:

- `unlock` (sin argumentos)
- `reboot` (sin argumentos)

Para crear una tarea para que la ejecuten los dispositivos de destino, utilice el siguiente comando. Reemplace cada *`user input placeholder`* por su propia información.

Comando

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

Excepciones

```
ValidationException
ResourceNotFoundException
InternalServerException
ThrottlingException
AccessDeniedException
ServiceQuotaExceededException
```

Salida

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

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

Comprobación del estado de la tarea

Para comprobar el estado de una tarea remota que se ejecuta en uno o más dispositivos de destino, utilice el comando `describe-execution`.

Una tarea puede tener uno de los siguientes estados:

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

Para comprobar el estado de una tarea, utilice el siguiente comando. Reemplace cada *`user input placeholder`* por su propia información.

Comando

```
aws snow-device-management describe-execution \
--taskId st-ficthmqoc2phtlef \
--managed-device-id smd-fictqic6gcldf111
```

Salida

```
{
    "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"
}
```

Comprobación de la información del dispositivo

Para comprobar la información específica del dispositivo, como el tipo de dispositivo, la versión del software, las direcciones IP y el estado de bloqueo, utilice el comando `describe-device`. La salida incluye también lo siguiente:

- `lastReachedOutAt`: la última vez que el dispositivo contactó con la Nube de AWS. Indica que el dispositivo está en línea.
- `lastUpdatedAt`: cuándo se actualizaron los datos por última vez en el dispositivo. Indica cuándo se actualizó la memoria caché del dispositivo.

Para comprobar la información del dispositivo, utilice el siguiente comando. Reemplace cada *`user input placeholder`* por su propia información.

Comando

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

Excepciones

```
ValidationException
ResourceNotFoundException
InternalServerException
ThrottlingException
AccessDeniedException
```

Salida

```
{
    "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"
    }
}
```

Comprobación del estado de la instancia compatible con Amazon EC2

Para comprobar el estado actual de la instancia de Amazon EC2, utilice el comando `describe-ec2-instances`. El resultado es similar al del `describe-device` comando, pero los resultados se obtienen de la memoria caché del dispositivo Nube de AWS e incluyen un subconjunto de los campos disponibles.

Para comprobar el estado de la instancia compatible con Amazon EC2, utilice el siguiente comando. Reemplace cada *`user input placeholder`* por su propia información.

Comando

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

Excepciones

```
ValidationException
ResourceNotFoundException
InternalServerException
ThrottlingException
AccessDeniedException
```

Salida

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

Comprobación de los metadatos de una tarea

Para comprobar los metadatos de una tarea determinada en un dispositivo, utilice el comando `describe-task`. Los metadatos de una tarea incluyen los siguientes elementos:

- Los dispositivos de destino
- El estado de la tarea
- Cuándo se creó la tarea
- Cuándo se actualizaron los datos por última vez en el dispositivo
- Cuándo se completó la tarea
- La descripción (si la hay) que se proporcionó cuando se creó la tarea

Para comprobar los metadatos de una tarea, utilice el siguiente comando. Reemplace cada *`user input placeholder`* por su propia información.

Comando

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

Excepciones

```
ValidationException
ResourceNotFoundException
InternalServerException
ThrottlingException
AccessDeniedException
```

Salida

```
{
    "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"
}
```

Cancelación de una tarea

Para enviar una solicitud de cancelación para una tarea específica, utilice el comando `cancel-task`. Solo puede cancelar las tareas que se encuentren en el estado `QUEUED` y que aún no se hayan ejecutado. Las tareas que ya se están ejecutando no se pueden cancelar.

> **Note**
>
> Es posible que una tarea que está intentando cancelar siga ejecutándose si se procesa desde la cola antes de que el comando `cancel-task` cambie el estado de la tarea.

Para cancelar una tarea, utilice el siguiente comando. Reemplace cada *`user input placeholder`* por su propia información.

Comando

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

Excepciones

```
ValidationException
ResourceNotFoundException
InternalServerException
ThrottlingException
AccessDeniedException
```

Salida

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

Obtención de una lista de comandos y sintaxis

Para obtener una lista de todos los comandos compatibles con la API de Snow Device Management, utilice el comando `help`. También puede usar el comando `help` para devolver información detallada sobre un comando determinado y su sintaxis.

Para obtener una lista de todos los comandos admitidos, utilice el siguiente comando.

Comando

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

Para devolver información detallada y la sintaxis de un comando, utilice el siguiente comando. Sustituya *command* por el nombre del comando que le interesa.

Comando

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

Obtención de una lista de los dispositivos que se pueden administrar de forma remota

Para obtener una lista de todos los dispositivos de su cuenta que tienen habilitada Snow Device Management en la Región de AWS en la que se ejecuta el comando, utilice el comando `list-devices`. `--max-results` y `--next-token` son opcionales. Para obtener más información, consulte Uso de las opciones de AWS CLI paginación en la «Guía del usuario de la interfaz de línea de AWS comandos».

Para obtener una lista de los dispositivos que se pueden administrar de forma remota, utilice el siguiente comando. Reemplace cada *user input placeholder* por su propia información.

Comando

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

Excepciones

```
ValidationException
InternalServerException
ThrottlingException
```

```
AccessDeniedException
```

Salida

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

Obtención de una lista del estado de las tareas en distintos dispositivos

Para devolver el estado de las tareas de uno o más dispositivos de destino, utilice el comando `list-executions`. Para filtrar la lista devuelta y mostrar las tareas que se encuentran actualmente en un único estado específico, utilice el parámetro `--state`. `--max-results` y `--next-token` son opcionales. Para obtener más información, consulte Uso de las opciones de AWS CLI paginación en la «Guía del usuario de la interfaz de línea de AWS comandos».

Una tarea puede tener uno de los siguientes estados:

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

Para obtener una lista del estado de las tareas en distintos dispositivos, utilice el siguiente comando. Reemplace cada *`user input placeholder`* por su propia información.

Comando

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

Excepciones

```
ValidationException
InternalServerException
ThrottlingException
AccessDeniedException
```

Salida

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

Obtención de una lista de los recursos disponibles

Para obtener una lista de los AWS recursos disponibles para un dispositivo, utilice el `list-device-resources` comando. Para filtrar la lista por un tipo de recurso específico, utilice el parámetro `--type`. Actualmente, las instancias compatibles con Amazon EC2 son el único tipo de recurso admitido. `--max-results` y `--next-token` son opcionales. Para obtener más información, consulte Uso de las opciones de AWS CLI paginación en la «Guía del usuario de la interfaz de línea de AWS comandos».

Para obtener una lista de los recursos disponibles para un dispositivo, utilice el siguiente comando. Reemplace cada *user input placeholder* por su propia información.

Comando

```
aws snow-device-management list-device-resources \
--managed-device-id smd-fictbgr3rbcje111 \
--type AWS::EC2::Instance
--next-
token YAQGPwAT9l3wVKaGYjt4yS34MiQLWvzcShe9oIeDJr05AT4rXSprqcqQhhBEYRfcerAp0YYbJmRT=
--max-results 10
```

Excepciones

```
ValidationException
InternalServerException
ThrottlingException
AccessDeniedException
```

Salida

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

Obtención de una lista de las etiquetas de un dispositivo o de una tarea

Para devolver una lista de etiquetas de una tarea o un dispositivo administrado, utilice el comando `list-tags-for-resource`.

Para obtener una lista de las etiquetas de un dispositivo, utilice el siguiente comando. Sustituya el nombre de recurso de Amazon (ARN) de ejemplo por el ARN de su 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
```

Excepciones

```
AccessDeniedException
InternalServerException
ResourceNotFoundException
ThrottlingException
```

Salida

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

Obtención de una lista de tareas por estado

Utilice el `list-tasks` comando para obtener una lista de tareas de los dispositivos de la AWS región en la que se ejecuta el comando. Para filtrar los resultados por el estado `IN_PROGRESS`, `COMPLETED` o `CANCELED`, utilice el parámetro `--state`. `--max-results` y `--next-token` son opcionales. Para obtener más información, consulte Uso de las opciones de AWS CLI paginación en la «Guía del usuario de la interfaz de línea de AWS comandos».

Para obtener una lista de tareas por estado, utilice el siguiente comando. Reemplace cada *`user input placeholder`* por su propia información.

Comando

```
aws snow-device-management list-tasks \
--state IN_PROGRESS \
--next-token K8VAMqKiP2Cf4xGkmH8GMyZrgOF8FUb+d10KTP9+P4pUb+8PhW+6MiXh4= \
```

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

Excepciones

```
ValidationException
InternalServerException
ThrottlingException
AccessDeniedException
```

Salida

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

        }
    ]
}
```

Aplicación de etiquetas

Para agregar o reemplazar una etiqueta para un dispositivo o para una tarea de un dispositivo, utilice el comando `tag-resource`. El parámetro `--tags` acepta una lista separada por comas de pares `Key=Value`.

Para aplicar etiquetas a un dispositivo, utilice el siguiente comando. Reemplace cada *`user input placeholder`* por su propia información.

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
```

Excepciones

```
AccessDeniedException
InternalServerException
ResourceNotFoundException
ThrottlingException
```

Eliminación de etiquetas

Para eliminar una etiqueta de un dispositivo o de una tarea de un dispositivo, utilice el comando `untag-resources`.

Para eliminar etiquetas de un dispositivo, utilice el siguiente comando. Reemplace cada *user input placeholder* por su propia información.

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
```

Excepciones

```
AccessDeniedException
InternalServerException
ResourceNotFoundException
ThrottlingException
```

Descripción de AWS Snowball Edge Jobs

Un trabajo en AWS Snowball es una unidad de trabajo discreta, que se define al crearla en la consola o en la API de administración de trabajos. El AWS Snowball Edge dispositivo incluye tres tipos de trabajos diferentes, todos ellos con capacidad de almacenamiento local y funciones informáticas. Esta funcionalidad utiliza la interfaz de archivos o la interfaz de Amazon S3 para leer y escribir datos. Activa funciones Lambda en función de las acciones de la API de objetos PUT de Amazon S3 que se ejecutan localmente en el AWS Snowball Edge dispositivo.

- Importación de trabajos a Amazon S3: transferencia de 80 TB o menos de datos locales que se copian en un único dispositivo y, a continuación, se mueven a Amazon S3. En el caso de los trabajos de importación, los dispositivos Snowball y los trabajos tienen una one-to-one relación. A cada trabajo se le asocia un único dispositivo. Para importar más datos, puede crear nuevos trabajos de importación o clonar uno que ya exista. Al devolver un dispositivo de este tipo de trabajo, los datos que contiene se importan a Amazon S3.
- Exportación de trabajos desde Amazon S3— La transferencia de cualquier cantidad de datos (ubicada en Amazon S3), copiada en cualquier número de dispositivos Snowball Edge y, a continuación, trasladada un AWS Snowball Edge dispositivo a la vez a su destino de datos local. Al crear un trabajo de exportación, este se divide en partes. Cada parte del trabajo no tiene un tamaño superior a 80 TB y cada parte del trabajo tiene exactamente un AWS Snowball Edge dispositivo asociado. Al devolver un dispositivo de este tipo de trabajo, se borra.
- Trabajos de computación y almacenamiento local— Estos trabajos implican el uso de un AWS Snowball Edge dispositivo o de varios dispositivos en un clúster. Estos trabajos no se inician a partir de los datos contenidos en los buckets como ocurre con los trabajos de exportación ni conllevan la importación de datos a Amazon S3 al final como en los trabajos de importación. Al devolver un dispositivo de este tipo de trabajo, se borra. Con este tipo de trabajo, puede crear, si lo desea, un clúster de dispositivos. Un clúster mejora la durabilidad del almacenamiento local y se puede escalar verticalmente u horizontalmente en función de la capacidad de almacenamiento local requerida.

  En las regiones en las que Lambda no está disponible, este tipo de trabajo se denomina trabajo de almacenamiento local.

Detalles del trabajo

Antes de crear un trabajo, asegúrese de que se cumplen los requisitos previos. Cada trabajo se define mediante los detalles que se especifican al crearlo. En la siguiente tabla se describen todos los detalles de un trabajo.

Identificador de la consola	Identificador de la API	Descripción del detalle
Nombre del trabajo	`Description`	Nombre del trabajo, que contiene caracteres alfanumér icos, espacios y cualquier carácter especial Unicode.
Tipo de trabajo	`JobType`	Tipo de trabajo, que puede ser de importación, de exportaci ón o de computación y almacenamiento local.
ID del trabajo	`JobId`	Etiqueta exclusiva de 39 caracteres que identifica el trabajo. El ID del trabajo aparece en la parte inferior de la etiqueta de envío que se muestra en la pantalla de tinta electrónica y en el nombre del archivo de manifiesto del trabajo.
Dirección	`AddressId`	Dirección a la que se va a enviar el dispositivo. En el caso de la API, se trata del identificador del tipo de datos de dirección.
Fecha de creación	CreationDate	Fecha en la que se ha creado este trabajo.

Identificador de la consola	Identificador de la API	Descripción del detalle
Rapidez de envío	`ShippingOption`	Opciones de rapidez de envío, según la región. Para obtener más información, consulte Velocidades de envío.
ARN del rol de IAM	RoleARN	Este nombre de recurso de Amazon (ARN) es el rol AWS Identity and Access Management (IAM) que se crea durante la creación del trabajo con permisos de escritura para los buckets de Amazon S3. El proceso de creación es automático y la función de IAM que usted permite AWS Snowball asumir solo se usa para copiar los datos entre sus cubos de S3 y Snowball. Para obtener más información, consulte Permisos necesarios para usar la AWS Snowball consola.
AWS KMS clave	`KmsKeyARN`	En AWS Snowball, AWS Key Management Service (AWS KMS) cifra las claves de cada Snowball. Cuando crea su trabajo, también elige o crea un ARN para una clave de AWS KMS cifrado de su propiedad. Para obtener más información, consulte AWS Key Management Service en AWS Snowball Edge.

Identificador de la consola	Identificador de la API	Descripción del detalle
Capacidad de Snowball	`SnowballCapacityPreference`	La capacidad de almacenamiento del AWS Snowball dispositivo solicitado en este trabajo. El tamaño disponible depende de tu tamaño Región de AWS.
Servicio de almacenamiento	N/A	El servicio AWS de almacenamiento asociado a este trabajo, en este caso Amazon S3.
Recursos	`Resources`	Los recursos del servicio de AWS almacenamiento asociados a su trabajo. En este caso, se trata de los buckets de Amazon S3 que constituyen el origen o el destino de la transferencia de datos.
Tipo de trabajo	`JobType`	Tipo de trabajo, que puede ser de importación, de exportación o de computación y almacenamiento local.
Tipo de Snowball	`SnowballType`	El tipo de dispositivo de la familia Snow solicitado para este trabajo.
ID del clúster	`ClusterId`	Etiqueta exclusiva de 39 caracteres que identifica el clúster.

Estados de los trabajos

Cada tarea AWS Snowball Edge del dispositivo tiene un estado, que cambia para indicar el estado actual de la tarea. Esta información de estado del trabajo no refleja su estado de salud, la fase de procesamiento ni el espacio de almacenamiento que se utiliza para los dispositivos asociados.

Visualización del estado de un trabajo

1. Inicie sesión en la Consola de administración de la familia de productos Snow de AWS.
2. En el Panel de trabajos, elija el trabajo.
3. Haga clic en el nombre del trabajo en la consola.
4. El panel Estado del trabajo está cerca de la parte superior y refleja el estado del trabajo.

AWS Snowball Edge estados de las tareas del dispositivo

Identificador de la consola	Identificador de la API	Descripción del estado
Trabajo creado	`New`	El trabajo se acaba de crear. Este estado es el único durante el cual podrá cancelar un trabajo (o sus partes, si el trabajo es de exportación).
Preparing appliance	`PreparingAppliance`	AWS está preparando un dispositivo para su trabajo.
Exportando	`InProgress`	AWS está exportando sus datos de Amazon S3 a un dispositivo.
Preparando el envío	`PreparingShipment`	AWS se está preparando para enviarle un dispositi vo. La información de

Identificador de la consola	Identificador de la API	Descripción del estado
		seguimiento del envío prevista se proporcio na a los clientes en el estado.
En tránsito hacia usted	`InTransitToCustomer`	El dispositivo se ha enviado a la dirección proporcionada al crear el trabajo.
Entregado a usted	`WithCustomer`	El dispositivo ha llegado a la dirección proporcionada al crear el trabajo.
En tránsito a AWS	`InTransitToAWS`	Has devuelto el dispositivo a AWS.
En las instalaciones de clasificación	`WithAWSSortingFacility`	El dispositivo para este trabajo se encuentra en nuestras instalaciones de clasificación interna. Cualquier procesami ento adicional para los trabajos de importación en Amazon S3 empezará pronto, normalmente en un plazo de dos días.

Identificador de la consola	Identificador de la API	Descripción del estado
En AWS	`WithAWS`	El envío ha llegado ya a AWS. Si el trabajo es de importación, esta suele iniciarse en el plazo de un día desde la recepción.
Importando	`InProgress`	AWS está importando sus datos a Amazon Simple Storage Service (Amazon S3).
Completado	`Complete`	El trabajo o una parte de él se ha completado correctamente.
Cancelado	`Cancelled`	El trabajo se ha cancelado.

Estados de los clústeres

Cada clúster tiene un estado que cambia para indicar el progreso general del clúster. Cada nodo del clúster tiene su propio estado del trabajo.

Esta información de estado del clúster no refleja su estado de salud, la fase de procesamiento ni el espacio de almacenamiento que se utilizan para el clúster o sus nodos.

Identificador de la consola	Identificador de la API	Descripción del estado
Esperando cuórum	`AwaitingQuorum`	El clúster todavía no se ha creado porque no hay suficientes nodos para comenzar

Identificador de la consola	Identificador de la API	Descripción del estado
		a procesar la solicitud de clúster. Para crear un clúster, se requieren al menos cinco nodos.
Pendiente	`Pending`	El clúster se ha creado y estamos preparando los nodos para enviárselos. Puede realizar el seguimiento del estado de los nodos mediante el estado del trabajo de cada uno de ellos.
Entregado a usted	`InUse`	Al menos un nodo del clúster se encuentra en la dirección que proporcionó al crear el trabajo.
Completado	`Complete`	Se han devuelto todos los nodos del clúster AWS.
Cancelado	`Cancelled`	La solicitud de creación del clúster se ha cancelado. Las solicitudes de clúster solo se puede cancelar antes de que adquieran el estado Pendiente.

Importación de trabajos a Amazon S3

Con un trabajo de importación, los datos se copian en el AWS Snowball Edge dispositivo con el adaptador Amazon S3 integrado o el punto de montaje NFS. El origen de datos de un trabajo de importación debe encontrarse en las instalaciones. Es decir, los dispositivos de almacenamiento que contienen los datos que se van a transferir deben encontrarse físicamente en la dirección facilitada al crear el trabajo.

Al importar archivos, cada uno de ellos se convierte en un objeto de Amazon S3 y cada directorio se convierte en un prefijo. Si importa datos a un bucket existente, se sobrescribirán todos los objetos existentes que tengan el mismo nombre que los objetos importados. El tipo de trabajo de importación también admite la funcionalidad de computación y almacenamiento local. Esta funcionalidad utiliza la interfaz de archivos o el adaptador de Amazon S3 para leer y escribir datos, y activa funciones Lambda en función de las acciones de la API de objetos PUT de Amazon S3 que se ejecutan localmente en el AWS Snowball Edge dispositivo.

Cuando todos sus datos se hayan importado a los buckets de Amazon S3 especificados en Nube de AWS, AWS realizará un borrado completo del dispositivo. Esta operación de borrado es conforme con los estándares 800-88 del NIST.

Una vez completada la importación, puede descargar un informe del trabajo. En este informe se notifican todos los objetos cuyo proceso de importación no se ha realizado correctamente. Encontrará información adicional en los registros de operaciones correctas o con errores.

> **Important**
>
> No elimine las copias locales de los datos que se han transferido hasta que haya comprobado los resultados en el informe de finalización del trabajo y revisado los registros de importación.

Exportación de trabajos desde Amazon S3

> **Note**
>
> Actualmente, las etiquetas y los metadatos NO son compatibles; es decir, se eliminarán todas las etiquetas y los metadatos al exportar objetos de buckets de S3.

El origen de datos de un trabajo de exportación consta de uno o más buckets de Amazon S3. Una vez que los datos de una parte del trabajo se hayan trasladado de Amazon S3 a un AWS Snowball Edge dispositivo, puede descargar un informe del trabajo. En este informe se notifican los objetos cuya transferencia al dispositivo no se ha realizado correctamente. Encontrará información adicional en los registros de operaciones correctas o con errores del trabajo.

Puede exportar cualquier cantidad de objetos en cada trabajo de exportación y usar para ello tantos dispositivos como sean necesarios para completar la transferencia. Cada AWS Snowball Edge dispositivo de las piezas de un trabajo de exportación se entrega una tras otra, y los siguientes dispositivos se envían después de que la pieza de trabajo anterior pase al AWS estado En tránsito.

Al copiar objetos al destino de datos en las instalaciones desde un dispositivo mediante el adaptador de Amazon S3 o el punto de montaje de NFS, estos objetos se guardan como archivos. Si copia objetos a una ubicación que ya contiene archivos, los archivos existentes que tengan el mismo nombre se sobrescribirán. El tipo de trabajo de exportación también admite la funcionalidad de computación y almacenamiento local. Esta funcionalidad utiliza la interfaz de archivos o el adaptador de Amazon S3 para leer y escribir datos, y activa funciones Lambda en función de las acciones de la API de objetos PUT de Amazon S3 que se ejecutan localmente en el AWS Snowball Edge dispositivo.

Cuando AWS recibimos un dispositivo devuelto, lo borramos por completo siguiendo los estándares NIST 800-88.

> **Important**
>
> Los datos que desee exportar a un dispositivo Snow deben estar en Amazon S3. Todos los datos Amazon S3 Glacier que vaya a exportar al dispositivo Snow deberán descongelarse o trasladarse a la clase de almacenamiento S3 antes de poder exportarlos. Debe hacerlo antes de crear el trabajo de exportación de Snow.
>
> No modifique, actualice ni elimine los objetos de Amazon S3 exportados hasta que haya comprobado que todo el contenido del trabajo completo se ha copiado al destino de datos en las instalaciones.

Al crear un trabajo de exportación, puede exportar un bucket entero de Amazon S3 o solo un rango específico de claves de objetos.

Uso de los rangos de exportación

Al crear un trabajo de exportación en la Consola de administración de la familia de productos Snow de AWS o mediante la API de administración de trabajos, puede exportar un bucket entero de Amazon S3 o solo un rango específico de claves de objetos. Los nombres de las claves de objetos identifican de forma única los objetos de un bucket. Al exportar un rango, debe definir su longitud proporcionando el primer elemento incluido, el último elemento incluido o ambos.

Los rangos se ordenan según las normas de UTF-8 binario. Los datos UTF-8 binarios se ordenan de la siguiente forma:

- Los números 0-9 van antes que los caracteres del alfabeto inglés en mayúsculas y minúsculas.
- Los caracteres del alfabeto inglés en mayúsculas van antes que los caracteres en minúsculas.
- Los caracteres del alfabeto inglés en minúsculas van al final cuando el listado incluye números y caracteres en mayúsculas.
- Los caracteres especiales se ordenan entre los demás conjuntos de caracteres.

Para obtener más información sobre UTF-8, consulte UTF-8 en Wikipedia.

Ejemplos de rangos de exportación

Supongamos que dispone de un bucket que contiene los siguientes objetos y prefijos, en orden binario UTF-8:

- 01
- Aardvark
- Aardwolf
- Aasvogel/apple
- Aasvogel/arrow/object1
- Aasvogel/arrow/object2
- Aasvogel/banana
- Aasvogel/banker/object1
- Aasvogel/banker/object2
- Aasvogel/cherry
- Banana

- Car

Inicio de rango especificado	Final de rango especificado	Objetos del rango que se exportarán
(ninguno)	(ninguno)	Todos los objetos del bucket
(ninguno)	Aasvogel	01 Aardvark Aardwolf Aasvogel/apple Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana Aasvogel/banker/object1 Aasvogel/banker/object2 Aasvogel/cherry
(ninguno)	Aasvogel/banana	01 Aardvark Aardwolf

Inicio de rango especificado	Final de rango especificado	Objetos del rango que se exportarán
		Aasvogel/apple Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana
Aasvogel	(ninguno)	Aasvogel/apple Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana Aasvogel/banker/object1 Aasvogel/banker/object2 Aasvogel/cherry Banana Car

Inicio de rango especificado	Final de rango especificado	Objetos del rango que se exportarán
Aardwolf	(ninguno)	Aardwolf Aasvogel/apple Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana Aasvogel/banker/object1 Aasvogel/banker/object2 Aasvogel/cherry Banana Car

Inicio de rango especificado	Final de rango especificado	Objetos del rango que se exportarán
Aar	(ninguno)	Aardvark Aardwolf Aasvogel/apple Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana Aasvogel/banker/object1 Aasvogel/banker/object2 Aasvogel/cherry Banana Car

Inicio de rango especificado	Final de rango especificado	Objetos del rango que se exportarán
car	(ninguno)	No se exporta ningún objeto y se recibe un mensaje de error al intentar crear el trabajo. Tenga en cuenta que car se ordena debajo de Car de acuerdo con los valores de UTF-8 binario.
Aar	Aarrr	Aardvark Aardwolf
Aasvogel/arrow	Aasvogel/arrox	Aasvogel/arrow/object1 Aasvogel/arrow/object2
Aasvogel/apple	Aasvogel/banana	Aasvogel/apple Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana

Inicio de rango especificado	Final de rango especificado	Objetos del rango que se exportarán
Aasvogel/apple	Aasvogel/banana	Aasvogel/apple Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana Aasvogel/banker/object1 Aasvogel/banker/object2
Aasvogel/apple	Aasvogel/cherry	Aasvogel/apple Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana Aasvogel/banker/object1 Aasvogel/banker/object2 Aasvogel/cherry

Suponga que tiene estos tres buckets y desea copiar todos los objetos de folder2.

- s3://bucket/folder1/
- s3://bucket/folder2/
- s3://bucket/folder3/

Inicio de rango especificado	Final de rango especificado	Objetos del rango que se exportarán
folder2/	folder2/	Todos los objetos del bucket folder2.

Prácticas recomendadas para los trabajos de exportación

- Asegúrese de que los datos estén en Amazon S3 y agrupe los archivos pequeños por lotes
- Si el bucket contiene millones de objetos, asegúrese de que se han especificado los rangos de claves en la definición del trabajo de exportación
- Actualice las claves de objeto para eliminar la barra diagonal de sus nombres, ya que los objetos cuyos nombres contienen barras diagonales finales (/ o \) no se transfieren a Snowball Edge
- En el caso de los buckets de S3, el límite de longitud de los objetos es de 255 caracteres.
- En el caso de los buckets de S3 con control de versiones, solo se exporta la versión actual de los objetos.
- Los marcadores de eliminación no se exportan.

Trabajos de computación y almacenamiento local

Los trabajos de cómputo y almacenamiento locales le permiten utilizar el almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow de forma local, sin conexión a Internet.
No puede exportar datos de Amazon S3 al dispositivo ni importar datos a Amazon S3 cuando se devuelve el dispositivo.

Temas

Trabajos de almacenamiento local

Puede leer y escribir objetos en un AWS Snowball Edge dispositivo mediante el almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow o el adaptador S3. Cuando pides un dispositivo, si eliges usar el adaptador S3, también eliges qué cubos de Amazon S3 se incluirán en el dispositivo cuando lo recibas. Si opta por utilizar un almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow, no se incluirá ningún depósito de Amazon S3 en el dispositivo cuando lo reciba.

Puede crear depósitos de Amazon S3 en los dispositivos Snowball Edge para almacenar y recuperar objetos de forma local para aplicaciones que requieren acceso a datos locales, procesamiento local de datos y residencia de datos. El almacenamiento compatible con S3 en dispositivos Snow Family proporciona una nueva clase de almacenamiento, `SNOW`, que utiliza las API de Amazon S3 y está diseñada para almacenar datos de manera duradera y redundante en múltiples dispositivos Snowball Edge. Puede usar las mismas API y características en los buckets de Snowball Edge que en Amazon S3, como políticas de ciclo de vida, cifrado y etiquetado. Cuando se devuelven el dispositivo o los dispositivos AWS, se borran todos los datos creados o almacenados en el almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow. Para obtener más información, consulte Trabajos exclusivos de computación y almacenamiento locales.

Para obtener más información, consulte Almacenamiento compatible con Amazon S3 en dispositivos Snow Family en esta guía.

Cuando termines de usar el dispositivo, devuélvelo a AWS y el dispositivo se borrará. Esta operación de borrado se ajusta a los estándares 800-88 del Instituto Nacional de Normalización y Tecnología (NIST).

Opción de clúster local

Un clúster es una agrupación lógica de dispositivos Snowball Edge, en grupos de entre tres y 16 dispositivos. Un clúster se crea como una sola tarea, lo que ofrece una mayor durabilidad y tamaño de almacenamiento en comparación con otras ofertas de AWS Snowball trabajo. Para obtener más información sobre los trabajos de clúster, consulte Información general de la agrupación en clústeres en esta guía.

Clonación de un trabajo en la consola

Al crear por primera vez un trabajo de importación o un trabajo de cómputo y almacenamiento local, es posible que descubra que necesita más de un AWS Snowball Edge dispositivo. Puesto que los trabajos de importación y de computación y almacenamiento local están asociados con un único dispositivo, si necesita más de un dispositivo deberá crear más de un trabajo. Para crear los trabajos adicionales, puede volver a seguir el asistente de creación de trabajos en la consola, o bien clonar el trabajo que ya tiene.

> **Note**
>
> La clonación de trabajos es un método abreviado disponible en la consola para facilitar la creación de trabajos adicionales. Si está creando trabajos con la API de administración de trabajos, basta con ejecutar el comando de creación de trabajo de nuevo.

Clonar un trabajo supone volver a crearlo exactamente igual excepto por un nombre que se modifica automáticamente. La clonación es un proceso sencillo.

Para clonar un trabajo en la consola

1. En el Consola de administración de la familia de productos Snow de AWS, elige tu trabajo de la tabla.
2. En Acciones, elija Clonar trabajo.

   El asistente Crear trabajo se abre por la última página, Paso 6: Revisar.
3. Revise la información y haga los cambios que desee eligiendo el botón Editar correspondiente.
4. Para crear el trabajo clonado, elija Crear trabajo.

Los trabajos clonados reciben un nombre con el siguiente formato: ***Nombre del trabajo***-clone-***número***. El número se añade automáticamente al nombre del trabajo y representa el número de veces que se ha clonado este trabajo desde la primera vez que se clonó. Por ejemplo, AprilFinanceReports-clone representa el primer trabajo clonado del AprilFinanceReportstrabajo y DataCenterMigration-clone-42 representa el cuadragésimo segundo clon del trabajo. DataCenterMigration

Prácticas recomendadas para utilizar el dispositivo Snowball Edge

Para ayudarte a obtener el máximo beneficio y satisfacción con tu AWS Snowball Edge dispositivo, te recomendamos que sigas estas prácticas recomendadas.

Seguridad

Las siguientes son recomendaciones y prácticas recomendadas para mantener la seguridad al trabajar con un AWS Snowball Edge dispositivo.

Seguridad general

- Si observas algo sospechoso en el AWS Snowball Edge dispositivo, no lo conectes a la red interna. En su lugar, contacte con AWS Support y se le enviará un nuevo dispositivo AWS Snowball Edge .
- Recomendamos que no guarde una copia del código de desbloqueo en la misma ubicación de la estación de trabajo donde se encuentra el manifiesto de ese trabajo. Guardarlos en diferentes ubicaciones ayuda a evitar que personas no autorizadas accedan al AWS Snowball Edge dispositivo. Por ejemplo, puede guardar una copia del manifiesto en el servidor local y enviar el código por correo electrónico a un usuario, que será quien desbloquee el dispositivo. Este enfoque limita el acceso al AWS Snowball Edge dispositivo a las personas que tienen acceso a los archivos guardados en el servidor y a la dirección de correo electrónico del usuario.
- Las credenciales que se muestran al ejecutar los comandos list-access-keys del cliente de Snowball Edge son un par de claves de acceso que se utilizan para acceder al dispositivo. get-secret-access-key

  Estas claves solo están asociadas al trabajo y a los recursos locales del dispositivo. No se asignan a la suya Cuenta de AWS ni a ninguna otra Cuenta de AWS. Si intenta utilizar estas claves para acceder a los servicios y recursos del Nube de AWS, no funcionarán correctamente porque solo funcionan para los recursos locales asociados a su trabajo.
- Si cree que sus credenciales se han perdido o se han visto comprometidas, solicite un archivo de manifiesto y un código de desbloqueo nuevos siguiendo el proceso de actualización del certificado SSL del dispositivo. Consulte Actualización del certificado SSL.

Para obtener información sobre cómo utilizar las políticas AWS Identity and Access Management (de IAM) para controlar el acceso, consulteAWS-Políticas gestionadas (predefinidas) para Edge AWS Snowball.

Seguridad de la red

- Le recomendamos que solo utilice un método a la vez para leer y escribir datos en un depósito local de un AWS Snowball Edge dispositivo. El uso simultáneo de la interfaz de archivos y del adaptador de Amazon S3 en el mismo bucket de Amazon S3 puede dar lugar a conflictos de lectura/escritura.
- Para evitar que tus datos se dañen, no desconectes el AWS Snowball Edge dispositivo ni cambies su configuración de red mientras los transfieres.
- Los archivos que se están escribiendo en el dispositivo deben encontrarse en un estado estático. La modificación de archivos mientras se están escribiendo puede dar lugar a conflictos de lectura/escritura.
- Para obtener más información sobre cómo mejorar el rendimiento del AWS Snowball Edge dispositivo, consultaRendimiento.

Administración de recursos

Tenga en cuenta las siguientes prácticas recomendadas para administrar trabajos y recursos en su dispositivo AWS Snowball Edge .

- Los 10 días gratuitos para realizar la transferencia de datos local comienzan el día siguiente a la llegada del AWS Snowball Edge dispositivo a su centro de datos. Esto solo es aplicable a los tipos de dispositivo Snowball Edge.
- El estado Trabajo creado es el único en el que se puede cancelar un trabajo. Cuando un trabajo cambia a otro estado, no se puede cancelar. Esto es aplicable a los clústeres.
- Para los trabajos de importación, no elimine las copias locales de los datos transferidos hasta que estos se hayan importado correctamente a Amazon S3. Asegúrese de comprobar los resultados de la transferencia de datos como parte del proceso.

Rendimiento

> **Note**
>
> El desempeño de la transferencia de datos variará en función del entorno de red, los sistemas operativos, el método de copia, el protocolo, el desempeño de lectura de los datos de origen y las características del conjunto de datos, como el tamaño de archivo. Para determinar las velocidades y los tiempos de transferencia de datos precisos, le recomendamos que mida el rendimiento mediante proof-of-concept pruebas en su entorno.

A continuación, encontrará recomendaciones e información sobre el rendimiento AWS Snowball Edge del dispositivo. En esta sección se explica el desempeño en términos generales, puesto que en cada entorno en las instalaciones se trabaja de manera diferente; por ejemplo, se usan distintas tecnologías de red, hardware diferente, diversos sistemas operativos, distintos procedimientos, etc.

En la siguiente tabla se muestra cómo la velocidad de transferencia de la red afecta al tiempo que se tarda en llenar un dispositivo Snowball Edge con datos. La transferencia de archivos más pequeños reduce la velocidad de transferencia debido a una mayor sobrecarga. Si tiene muchos archivos pequeños, recomendamos comprimirlos en archivos zip mayores antes de transferirlos a un dispositivo Snowball Edge.

Velocidad (MB/s)	Tiempo de transferencia de 82 TB
800	1,22 días
450	2,11 días
400	2,37 días
300	3,16 días
277	3,42 días
200	4,75 días
100	9,49 días
60	15,53 días

Velocidad (MB/s)	Tiempo de transferencia de 82 TB
30	31,06 días
10	85,42 días

Para proporcionar una guía útil sobre el rendimiento, en las siguientes secciones se describe cómo determinar cuándo usar el AWS Snowball Edge dispositivo y cómo aprovechar al máximo el servicio.

Temas

Recomendaciones de desempeño

Es muy conveniente seguir las prácticas recomendadas que se indican a continuación, ya que permiten mejorar en gran medida el desempeño de la transferencia de datos:

- Recomendamos no tener más de 500 000 archivos o directorios en cada directorio.
- Se recomienda que todos los archivos transferidos a un dispositivo Snowball Edge tengan un tamaño mínimo de 1 MB.
- Si tiene muchos archivos cuyo tamaño es inferior a 1 MB, recomendamos comprimirlos en archivos zip mayores antes de transferirlos a un dispositivo Snowball Edge.

Agilización de la transferencia de datos

Una de las mejores maneras de mejorar el rendimiento de un AWS Snowball Edge dispositivo es acelerar la transferencia de datos que entran y salen de un dispositivo. En general, la velocidad de transferencia desde el origen de datos hasta el dispositivo puede mejorarse de las siguientes formas. La siguiente lista está ordenada de mayor a menor impacto positivo en el desempeño:

1. Realice varias operaciones de escritura a la vez: para ello, ejecute cada comando desde varias ventanas de terminal en un equipo que tenga una conexión de red a un solo dispositivo AWS Snowball Edge .
2. Transfiera los archivos pequeños por lotes: cada operación de copia conlleva una cierta sobrecarga debido al cifrado. Para acelerar el proceso, agrupe los archivos en uno solo. Al

agrupar los archivos, estos se pueden extraer automáticamente cuando se importan a Amazon S3. Para obtener más información, consulte Agrupación en lotes de archivos pequeños.

3. No realice otras operaciones con los archivos durante la transferencia: cambiar el nombre de los archivos durante la transferencia, modificar sus metadatos o escribir datos en los archivos durante una operación de copia tiene un impacto negativo importante en el desempeño de la transferencia. Recomendamos que los archivos permanezcan en un estado estático mientras se transfieren.
4. Reduzca el uso de la red local: el dispositivo AWS Snowball Edge se comunica a través de la red local. Por tanto, al reducir de otro modo el tráfico de red local entre el dispositivo AWS Snowball Edge , el conmutador al que se conecta y el equipo que aloja el origen de datos se puede acelerar significativamente la velocidad de transferencia de datos.
5. Elimine los saltos innecesarios: le recomendamos que configure el AWS Snowball Edge dispositivo, la fuente de datos y el ordenador desde el que se establece la conexión terminal entre ellos de forma que sean los únicos equipos que se comuniquen a través de un único conmutador. Esto puede mejorar la velocidad de transferencia de datos.

Actualización del software en dispositivos Snowball Edge

AWS le notificará cuando haya nuevo software disponible para los dispositivos de la familia Snow que tenga. La notificación se envía por correo electrónico y como un CloudWatch evento. AWS Health Dashboard La notificación por correo electrónico se envía desde Amazon Web Services, Inc. a la dirección de correo electrónico adjunta a la AWS cuenta utilizada para solicitar el dispositivo Snow Family. Cuando reciba la notificación, siga las instrucciones de este tema y descargue e instale la actualización lo antes posible para evitar la interrupción del uso del dispositivo. Para obtener más información al respecto AWS Health Dashboard, consulte la Guía AWS Health del usuario. Para obtener más información sobre CloudWatch los eventos, consulte la Guía del usuario de Amazon CloudWatch Events.

Puede descargar actualizaciones de software AWS e instalarlas en los dispositivos Snowball Edge de sus entornos locales. Estas actualizaciones se realizan en segundo plano. Puede seguir utilizando sus dispositivos con normalidad mientras se descarga el software más reciente de forma segura desde AWS su dispositivo. Sin embargo, para aplicar las actualizaciones descargadas, debe detener las cargas de trabajo del dispositivo y reiniciarlo.

Las actualizaciones de software proporcionadas AWS por los dispositivos Snowball Edge/Snowcone (dispositivos) son software de dispositivos según la sección 9 de las condiciones del servicio.

Las actualizaciones de software se proporcionan únicamente con el fin de instalar las actualizaciones de software en el Dispositivo correspondiente en nombre de AWS. Usted se abstendrá de (y no intentará), y no permitirá ni autorizará a terceros (ni intentará) (i) hacer copias de las actualizaciones de software que no sean las necesarias para instalar las actualizaciones de software en el Dispositivo correspondiente, ni (ii) eludir o deshabilitar cualquier característica o medida de las actualizaciones de software, incluido, entre otros, cualquier cifrado aplicado a la actualización de software. Una vez que las actualizaciones de software se hayan instalado en el Dispositivo correspondiente, usted acepta eliminar las actualizaciones de software de todos y cada uno de los medios utilizados para instalar las actualizaciones de software en el Dispositivo.

> **Warning**
>
> Es absolutamente recomendable que suspenda todas las actividades del dispositivo antes de instalar la actualización. Si se actualiza el dispositivo y se reinicia, se detendrán las instancias en ejecución e interrumpirán las escrituras en los buckets locales de Amazon S3.

Temas

Requisitos previos

Para poder actualizar un dispositivo, es necesario cumplir los siguientes requisitos previos:

- Debe haber creado un trabajo, tener el dispositivo en las instalaciones y que esté desbloqueado. Para obtener más información, consulte Introducción.
- La actualización de los dispositivos Snowball Edge se realiza mediante el cliente de Snowball Edge. La última versión del cliente Snowball Edge debe descargarse e instalarse en un ordenador de su entorno local que tenga una conexión de red con el dispositivo que desee actualizar. Para obtener más información, consulte Uso del cliente de Snowball Edge.
- (Opcional) Le recomendamos que configure un perfil para el cliente de Snowball Edge. Para obtener más información, consulte Configuración de un perfil para el cliente de Snowball Edge.
- Para el almacenamiento compatible con Amazon S3 en dispositivos Snow Family en dispositivos Snowball Edge agrupados, detenga el servicio S3-Snow y deshabilite su inicio automático. Consulte Configuración del servicio de almacenamiento compatible con Amazon S3 en dispositivos Snow Family para que se inicie automáticamente.

> **Note**
>
> En el caso de los dispositivos agrupados, todos los comandos deben ejecutarse para cada dispositivo.

Ahora que ha completado estas tareas, puede descargar e instalar las actualizaciones para los dispositivos Snowball Edge.

Descarga de actualizaciones

Existen dos formas principales de descargar una actualización para los dispositivos de la familia Snow:

- Puede activar las actualizaciones manualmente en cualquier momento utilizando comandos específicos del cliente de Snowball Edge.
- Puede establecer una hora mediante programación para que el dispositivo se actualice automáticamente.

En el siguiente procedimiento, se describe el proceso para descargar manualmente las actualizaciones. Para obtener información sobre la actualización automática del dispositivo Snowball Edge, consulte `configure-auto-update-strategy` Actualización de un Snowball Edge.

> **Note**
>
> Si su dispositivo no tiene acceso a Internet, puede descargar un archivo de actualización mediante la GetSoftwareUpdatesAPI. A continuación, señale la ubicación de un archivo local cuando llame `download-updates` mediante el `uri` parámetro, como en el siguiente ejemplo.
>
> ```
> snowballEdge download-updates --uri file:///tmp/local-update
> ```
>
> Para los sistemas operativos Windows, formatee el valor del `uri` parámetro de la siguiente manera:
>
> ```
> snowballEdge download-updates --uri file:/C:/path/to/local-update
> ```

Para buscar y descargar actualizaciones de software de Snowball Edge para dispositivos independientes

1. Abra una ventana de terminal y utilice el comando `describe-device` para asegurarse de que el dispositivo Snowball Edge está desbloqueado. Si el dispositivo está bloqueado, utilice el comando `unlock-device` para desbloquearlo. Para obtener más información, consulte Desbloquear los dispositivos de la familia Snow.

2. Cuando el dispositivo esté desbloqueado, ejecute el comando `snowballEdge check-for-updates`. Este comando devuelve la versión más reciente disponible del software de Snowball Edge, así como la versión actual instalada en el dispositivo.
3. Si el software del dispositivo no está actualizado, ejecute el comando `snowballEdge download-updates`.

   > **Note**
   >
   > Si el dispositivo no está conectado a Internet, primero descarga un archivo de actualización mediante la GetSoftwareUpdatesAPI. A continuación, ejecute el `snowballEdge download-updates` comando con el `uri` parámetro con una ruta local al archivo que descargó, como en el siguiente ejemplo.
   >
   > ```
   > snowballEdge download-updates --uri file:///tmp/local-update
   > ```
   >
   > Para los sistemas operativos Windows, formatee el valor del `uri` parámetro de la siguiente manera:
   >
   > ```
   > snowballEdge download-updates --uri file:/C:/path/to/local-update
   > ```

4. Puede comprobar el estado de la descarga con el comando `snowballEdge describe-device-software`. Mientras se descarga la actualización, puede usar este comando para ver el estado.

   Example salida del **`describe-device-software`** comando

   ```
   Install State: Downloading
   ```

Para buscar y descargar actualizaciones de software de Snowball Edge para clústeres de dispositivos

1. Abra una ventana de terminal y asegúrese de que todos los dispositivos Snowball Edge del clúster estén desbloqueados mediante el comando. `snowballEdge describe-device` Si los dispositivos están bloqueados, utilice el `snowballEdge unlock-cluster` comando para desbloquearlos. Para obtener más información, consulte Desbloquear Snowball Edge.

2. Cuando todos los dispositivos del clúster estén desbloqueados, ejecute el comando para cada dispositivo del clúster. `check-for-updates` Este comando devuelve la versión más reciente disponible del software de Snowball Edge, así como la versión actual instalada en el 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**
>
> El código de desbloqueo y el archivo de manifiesto son los mismos para todos los dispositivos del clúster.

Example del **`check-for-updates`** comando

```
{
"InstalledVersion" : "118",
"LatestVersion" : "119"
}
```

Si el valor del `LatestVersion` nombre es mayor que el valor del `InstalledVersion` nombre, hay una actualización disponible.

3. Para cada dispositivo del clúster, utilice el `download-updates` comando para descargar la actualización.

```
snowballEdge download-updates --uri file:///tmp/local-update
```

> **Note**
>
> Para los sistemas operativos Windows, formatee el valor del `uri` parámetro de la siguiente manera:

```
snowballEdge download-updates --uri file:/C:/path/to/local-update
```

4. Para comprobar el estado de esta descarga para cada dispositivo del clúster, utilice el `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 de la salida del **`describe-device-software`** comando

```
{
"InstalledVersion" : "118",
"InstallingVersion" : "119",
"InstallState" : "DOWNLOADED",
"CertificateExpiry" : "Sat Mar 30 16:47:51 UTC 2024"
}
```

Si el valor del `InstallState` nombre es`DOWNLOADED`, la actualización se ha terminado de descargar y está disponible para su instalación.

Instalación de actualizaciones

Una vez que se han descargado las actualizaciones, tiene que instalarlas y reiniciar el dispositivo para que se apliquen. En el siguiente procedimiento, se explica cómo instalar manualmente las actualizaciones.

En el caso de los clústeres de dispositivos Snowball Edge, la actualización debe descargarse e instalarse en cada uno de los dispositivos del clúster.

> **Note**
>
> Suspenda toda la actividad del dispositivo antes de instalar las actualizaciones de software. La instalación de actualizaciones detiene las instancias en ejecución e interrumpe cualquier

escritura en los buckets de Amazon S3 del dispositivo. Esto puede provocar la pérdida de datos

Para instalar las actualizaciones de software que ya se descargaron en los dispositivos independientes de la familia Snow

1. Abra una ventana de terminal y utilice el comando `describe-device` para asegurarse de que el dispositivo Snowball Edge está desbloqueado. Si el dispositivo está bloqueado, utilice el comando `unlock-device` para desbloquearlo. Para obtener más información, consulte Desbloquear Snowball Edge.
2. Ejecute el `list-services` comando para ver los servicios disponibles en el dispositivo. El comando devuelve los ID de servicio de cada servicio disponible en el dispositivo.

   ```
   snowballEdge list-services
   ```

   Example de la salida del **`list-services`** comando

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

3. Para cada ID de servicio identificado por el `list-services` comando, ejecute el `describe-service` comando para ver el estado. Utilice esta información para identificar los servicios que desee detener.

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

   Example de la salida del **`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"
  }
 } ]
}
```

Este resultado muestra que el `s3` servicio está activo y debe detenerse mediante el `stop-service` comando.

4. Utilice el `stop-service` comando para detener todos los servicios en los que el valor del `State` nombre `ACTIVE` aparezca en el resultado del `list-services` comando. Si hay más de un servicio en ejecución, detenga cada uno de ellos antes de continuar.

> **Note**
>
> El adaptador Amazon S3, Amazon EC2 y los servicios de IAM no se pueden detener. AWS STS Si se está ejecutando el almacenamiento compatible con Amazon S3 en dispositivos Snow Family, deténgalo antes de instalar las actualizaciones. El almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow tiene `s3-snow` como`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 de la salida del **`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. Ejecute el comando `snowballEdge install-updates`.
6. Puede comprobar el estado de esta instalación con el comando `snowballEdge describe-device-software`. Mientras se instala una actualización, este comando indica su estado.

   Ejemplo de resultado

   ```
   Install State: Installing //Possible values[NA, Installing, Requires
   Reboot]
   ```

   Ha instalado correctamente una actualización de software para un dispositivo Snowball Edge. Cuando se instala una actualización, esta no se aplica automáticamente al dispositivo. Para finalizar la instalación de una actualización, el dispositivo debe reiniciarse.

   > **Warning**
   >
   > Si el dispositivo Snow Family se reinicia sin detener todas las actividades, puede producirse una pérdida de datos.

7. Cuando todos los servicios del dispositivo se hayan detenido, reinicie el dispositivo, desbloquéelo y reinícielo de nuevo. Esto completa la instalación de las actualizaciones de software descargadas.
8. Cuando el dispositivo se encienda tras el segundo reinicio, desbloquéelo.
9. Ejecute el comando `check-for-updates`. Este comando devuelve la versión más reciente disponible del software de Snowball Edge, así como la versión actual instalada en el dispositivo.

Para instalar actualizaciones de software que ya se descargaron en un clúster de dispositivos Snowball Edge

1. Para cada dispositivo del clúster, ejecute el `describe-device` comando para determinar si los dispositivos están desbloqueados. Si los dispositivos están bloqueados, utilice el `unlock-cluster` comando para desbloquearlos. Para obtener más información, consulte Desbloquear Snowball Edge.
2. Para cada dispositivo del clúster, ejecute el `list-services` comando para ver los servicios disponibles en el dispositivo. El comando devuelve los ID de servicio de cada servicio disponible en el dispositivo.

   ```
   snowballEdge list-services
   ```

   Example de la salida del **`list-services`** comando

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

3. Para cada ID de servicio identificado por el `list-services` comando, ejecute el `describe-service` comando para ver el estado. Utilice esta información para identificar los servicios que desee detener.

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

   Example de la salida del **`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"
  }
 } ]
}
```

Este resultado muestra que el `s3` servicio está activo y debe detenerse mediante el `stop-service` comando.

4. Para cada dispositivo del clúster, utilice el `stop-service` comando para detener todos los servicios en los que el valor del `State` nombre `ACTIVE` aparezca en el resultado del `list-services` comando. Si hay más de un servicio en ejecución, detenga cada uno de ellos antes de continuar.

> **Note**
>
> El adaptador Amazon S3, Amazon EC2 y los servicios de IAM no se pueden detener. AWS STS Si se está ejecutando el almacenamiento compatible con Amazon S3 en dispositivos Snow Family, deténgalo antes de instalar las actualizaciones. El almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow tiene `s3-snow` como`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 de la salida del **`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. Ejecute el `install-updates` comando para cada dispositivo del clúster.

```
snowballEdge install-updates
```

6. Puede comprobar el estado de esta instalación con el comando `describe-device-software`.

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

Example de la salida del **`describe-device-service`** comando

```
Install State: Installing //Possible values[NA, Installing, Requires Reboot]
```

Una vez hecho `Install State` esto`Requires Reboot`, habrá instalado correctamente la actualización de software para su dispositivo Snowball Edge. Cuando se instala una actualización, esta no se aplica automáticamente al dispositivo. Para finalizar la instalación de una actualización, el dispositivo debe reiniciarse.

> **Warning**
>
> Si se reinicia el dispositivo Snowball Edge sin detener toda la actividad del dispositivo, se pueden perder datos.

7. Reinicie todos los dispositivos del clúster, desbloquee el clúster y vuelva a reiniciar todos los dispositivos del clúster. Esto completa la instalación de las actualizaciones de software

descargadas. Para obtener más información sobre el reinicio de los dispositivos, consulte Reiniciar el dispositivo de la familia Snow. Para obtener más información sobre cómo desbloquear el clúster de dispositivos, consulte Desbloquear Snowball Edge.

8. Después de que cada dispositivo del clúster se haya reiniciado dos veces, desbloquee el clúster y utilice el `check-for-updates` comando para comprobar que el dispositivo se ha actualizado. Este comando devuelve la versión más reciente disponible del software de Snowball Edge, así como la versión actual instalada en el dispositivo. Si la versión actual y la última versión disponible son las mismas, el dispositivo se actualizó correctamente.

Ya ha actualizado correctamente el dispositivo o el grupo de dispositivos de la familia Snow y ha confirmado la actualización a la versión más reciente del software de la familia Snow.

Actualización del certificado SSL

Si planea conservar su dispositivo Snow Family durante más de 360 días, tendrá que actualizar el certificado Secure Sockets Layer (SSL) del dispositivo para evitar la interrupción del uso del dispositivo. Si el certificado caduca, no podrá usar el dispositivo y tendrá que devolverlo a AWS.

AWS se lo notificará 30 días antes de que caduque el certificado SSL de los dispositivos de la familia Snow que tenga. La notificación se envía por correo electrónico y como un CloudWatch evento. AWS Health Dashboard La notificación por correo electrónico se envía desde Amazon Web Services, Inc. a la dirección de correo electrónico adjunta a la AWS cuenta utilizada para solicitar el dispositivo Snow Family. Cuando reciba la notificación, siga las instrucciones de este tema y solicite una actualización lo antes posible para evitar la interrupción del uso del dispositivo. Para obtener más información al respecto AWS Health Dashboard, consulte la Guía AWS Health del usuario. Para obtener más información sobre CloudWatch los eventos, consulte la Guía del usuario de Amazon CloudWatch Events.

La actualización del certificado SSL se realiza a través del cliente Snowball Edge. La última versión del cliente Snowball Edge debe descargarse e instalarse en un ordenador de su entorno local que tenga una conexión de red con el dispositivo que desee actualizar. Para obtener más información, consulte Uso del cliente Snowball Edge Uso del cliente AWS Edge.

En este tema se explica cómo determinar cuándo caducará el certificado y cómo actualizar el dispositivo.

1. Use el comando `snowballEdge describe-device-software` para determinar cuándo caducará el certificado. En la salida del comando, el valor de `CertificateExpiry` incluye la fecha y la hora en las que caducará el certificado.

   Example de la salida de **`describe-device-software`**

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

2. Póngase en contacto con AWS Support él y solicite una actualización del certificado SSL.
3. AWS Support proporcionará un archivo de actualización. Descargue e instale el archivo de actualización.
4. Usa el nuevo código de desbloqueo y el nuevo archivo de manifiesto al desbloquear un dispositivo de Snowball .

Actualización de las AMI de Amazon Linux 2 en los dispositivos Snow Family

Como práctica recomendada de seguridad, mantenga sus AMI de Amazon Linux 2 up-to-date en los dispositivos de la familia Snow. Compruebe periódicamente la AMI (HVM) de Amazon Linux 2 (HVM), tipo de volumen SSD (64 bits x86) en el AWS Marketplace para ver si hay actualizaciones. Cuando identifique la necesidad de actualizar la AMI, importe la imagen más reciente de Amazon Linux 2 al dispositivo Snow. Consulte Importación de una imagen a su dispositivo como una AMI compatible con Amazon EC2.

También puede obtener el ID de imagen más reciente de Amazon Linux 2 mediante el comando `ssm get-parameters` en la 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
```

El comando devuelve el ID de imagen más reciente de la AMI. Por ejemplo:

```
ami-0ccb473bada910e74
```

Seguridad para AWS Snowball Edge

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores independientes prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de conformidad aplicables AWS Snowball, consulte los AWS servicios incluidos en el ámbito de aplicación por programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AWS Snowball. Los siguientes temas muestran cómo configurarlo AWS Snowball para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus AWS Snowball recursos.

Temas

Protección de datos en AWS Snowball Edge

AWS Snowball se ajusta al modelo de responsabilidad AWS compartida, que incluye normas y directrices para la protección de datos. AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los AWS servicios. AWS mantiene el control de los datos alojados en esta infraestructura, incluidos los controles de configuración de seguridad para gestionar el contenido y los datos personales de los clientes. AWS los clientes y los socios de APN, que actúan como controladores o procesadores de datos, son responsables de cualquier dato personal que introduzcan en el Nube de AWS.

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS Identity and Access Management (IAM), de modo que cada usuario reciba únicamente los permisos necesarios para cumplir con sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Recomendamos TLS 1.2 o una versión posterior.

- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados de AWS los servicios.
- Utilice avanzados servicios de seguridad administrados, como Amazon Macie, que lo ayuden a detectar y proteger los datos personales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información acerca de los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Le recomendamos encarecidamente que nunca introduzca información de identificación confidencial, como, por ejemplo, números de cuenta de sus clientes, en los campos de formato libre, como el campo Nombre. Esto incluye cuando trabaja con AWS Snowball u otros AWS servicios mediante la consola, la API o los SDK. AWS CLI AWS Es posible que cualquier dato que ingrese en AWS Snowball o en otros servicios se incluya en los registros de diagnóstico. Cuando proporcione una URL a un servidor externo, no incluya información de credenciales en la URL para validar la solicitud para ese servidor.

Para obtener más información sobre la protección de datos, consulte la entrada de blog relativa al modelo de responsabilidad compartida de AWS y GDPR en el blog de seguridad de AWS .

Temas

Protección de los datos en la nube

AWS Snowball protege sus datos cuando importa o exporta datos a Amazon S3, cuando crea un trabajo para solicitar un dispositivo de la familia Snow y cuando su dispositivo se actualiza. En las siguientes secciones se describe cómo puede proteger sus datos cuando utiliza Snowball Edge y está conectado a Internet o interactúa con ellos AWS en la nube.

Temas

Cifrado para Edge AWS Snowball

Cuando se utiliza un dispositivo Snowball Edge para importar datos a S3, todos los datos transferidos a un dispositivo se protegen mediante cifrado SSL a través de la red. Para proteger los datos en reposo, AWS Snowball Edge utiliza el cifrado del servidor (SSE).

Cifrado del lado del servidor en Edge AWS Snowball

AWS Snowball Edge admite el cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 (SSE-S3). El cifrado del servidor se lleva a cabo para proteger los datos en reposo. SSE-S3 ofrece un cifrado sólido multifactor para proteger los datos en reposo en Amazon S3. Para obtener más información sobre SSE-S3, consulte Protecting Data Using Server-Side Encryption with Amazon S3-Managed Encryption Keys (SSE-S3) en la Guía del usuario de Amazon Simple Storage Service.

Actualmente, AWS Snowball Edge no ofrece cifrado del lado del servidor con claves proporcionadas por el cliente (SSE-C). El almacenamiento compatible con Amazon S3 en los dispositivos Snow Family ofrece SSS-C para trabajos de computación y almacenamiento local. Sin embargo, es posible que desee utilizar ese tipo de SSE para proteger los datos que se han importado o incluso que ya lo utilice en los datos que desea exportar. En estos casos, tenga en cuenta lo siguiente:

- Importación:

  Si desea utilizar SSE-C para cifrar los objetos que ha importado a Amazon S3, debería considerar la posibilidad de utilizar en su lugar el cifrado SSE-KMS o SSE-S3, establecido como parte de la política de bucket de ese bucket. Sin embargo, si tiene que usar SSE-C para cifrar los objetos que ha importado a Amazon S3, tendrá que copiar el objeto dentro de su bucket para cifrarlo con SSE-C. A continuación, se muestra un ejemplo de comando de la CLI para hacerlo:

  ```
  aws s3 cp s3://mybucket/object.txt s3://mybucket/object.txt --sse-c --sse-c-key
   1234567891SAMPLEKEY
  ```

  o

  ```
  aws s3 cp s3://mybucket s3://mybucket --sse-c --sse-c-key 1234567891SAMPLEKEY --
  recursive
  ```

- Exportación: si desea exportar objetos cifrados con SSE-C, cópielos primero a otro bucket que no tenga cifrado del servidor o que tenga una política en la cual se haya definido el cifrado SSE-KMS o SSE-S3.

Habilitación de SSE-S3 en los datos importados a Amazon S3 desde un dispositivo Snowball Edge

Utilice el siguiente procedimiento en la consola de administración de Amazon S3 a fin de habilitar SSE-S3 para los datos que se van a importar a Amazon S3. No es necesaria ninguna configuración en el Consola de administración de la familia de productos Snow de AWS propio dispositivo Snowball ni en él.

Para habilitar el cifrado SSE-S3 de los datos que va a importar a Amazon S3, solo tiene que configurar las políticas de todos los buckets a los que va a importar datos. Actualice las políticas para denegar el permiso de carga de objeto (`s3:PutObject`) si la solicitud de carga no incluye el encabezado `x-amz-server-side-encryption`.

Cómo habilitar SSE-S3 en los datos importados a Amazon S3

1. Inicie sesión en la consola de Amazon S3 AWS Management Console y ábrala en https://console.aws.amazon.com/s3/.
2. Elija el bucket al que desea importar datos en la lista de buckets.
3. Elija Permisos.

4. Elija Política de bucket.
5. En el Editor de políticas de bucket, escriba la política siguiente. Sustituya todas las instancias de *YourBucket* en esta política por el nombre real de su 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. Seleccione Guardar.

Ha finalizado la configuración de su bucket de Amazon S3. Cuando los datos se importan a este bucket, se protegen mediante SSE-S3. Repita este procedimiento para los demás buckets, según sea necesario.

AWS Key Management Service en AWS Snowball Edge

AWS Key Management Service (AWS KMS) es un servicio gestionado que le facilita la creación y el control de las claves de cifrado utilizadas para cifrar sus datos. AWS KMS utiliza módulos de seguridad de hardware (HSM) para proteger la seguridad de sus claves. En concreto, el nombre de recurso de Amazon (ARN) de la AWS KMS clave que elija para un trabajo en AWS Snowball Edge está asociado a una clave de KMS. Esta clave de KMS se utiliza para cifrar el código de desbloqueo del trabajo. El código de desbloqueo se utiliza para descifrar la capa superior de cifrado del archivo de manifiesto. Las claves de cifrado almacenadas en el archivo de manifiesto se utilizan para cifrar y descifrar los datos en el dispositivo.

En AWS Snowball Edge, AWS KMS protege las claves de cifrado utilizadas para proteger los datos de cada AWS Snowball Edge dispositivo. Al crear el trabajo, debe elegir también una clave de KMS. Al especificar el ARN de una AWS KMS clave, AWS Snowball se indica cuál se AWS KMS keys debe utilizar para cifrar las claves únicas del dispositivo. AWS Snowball Edge Para obtener más información sobre las server-side-encryption opciones de Amazon S3 compatibles con AWS Snowball Edge, consulteCifrado del lado del servidor en Edge AWS Snowball.

Uso del cliente gestionado AWS KMS keys para Snowball Edge

Si desea utilizar el cliente gestionado AWS KMS keys para Snowball Edge creado para su cuenta, siga estos pasos.

Selección de las AWS KMS keys de su trabajo

1. En Consola de administración de la familia de productos Snow de AWS, selecciona Crear trabajo.
2. Elija el tipo de trabajo y, a continuación, elija Siguiente.
3. Indique los datos de envío y elija Siguiente.
4. Rellene los datos del trabajo y elija Siguiente.
5. Establezca las opciones de seguridad. En Cifrado, para la clave de KMS, elija la clave Clave administrada de AWS o una clave personalizada que se haya creado anteriormente AWS KMS, o elija Introducir una clave ARN si necesita introducir una clave que sea propiedad de una cuenta independiente.

> **Note**
>
> El ARN de la AWS KMS key es un identificador único global para las claves administradas por el cliente.

6. Selecciona Siguiente para terminar de seleccionar tu. AWS KMS key
7. Conceda al usuario de IAM del dispositivo Snow acceso a la clave de KMS.
   a. En la consola de IAM (https://console.aws.amazon.com/iam/), vaya a Claves de cifrado y abra la clave de KMS que eligió usar para cifrar los datos del dispositivo.
   b. En Usuarios de claves, seleccione Agregar, busque el usuario de IAM del dispositivo Snow y seleccione Asociar.

Creación de una clave de cifrado de sobre KMS personalizada

Tiene la opción de usar su propia clave de cifrado de AWS KMS sobres personalizada con AWS Snowball Edge. Si decide crear su propia clave, debe crearla en la misma región en que se creó el trabajo.

Para crear tu propia AWS KMS clave para un trabajo, consulta Cómo crear claves en la Guía para AWS Key Management Service desarrolladores.

Protección de los datos de su dispositivo

Proteja su AWS Snowball ventaja

A continuación, se indican algunos puntos de seguridad que te recomendamos tener en cuenta al utilizar AWS Snowball Edge, así como información general sobre otras precauciones de seguridad que adoptamos cuando recibimos un dispositivo AWS para procesarlo.

Recomendamos los siguientes enfoques de seguridad:

- Al recibir el dispositivo, inspecciónelo para ver si ha sufrido daños o alteraciones evidentes. Si observa cualquier indicio sospechoso en el dispositivo , no lo conecte a la red interna. En su lugar, contacte con AWS Support y se le enviará un nuevo dispositivo.

- Es importante asegurarse de proteger las credenciales del trabajo para que no las conozca nadie más. Cualquier persona que tenga acceso al manifiesto y al código de desbloqueo de un trabajo podrá obtener acceso al contenido del dispositivo enviado para ese trabajo.
- Nunca deje el dispositivo en un muelle de carga. Si lo hiciera, podría quedar expuesto a las inclemencias meteorológicas. Si bien todos los dispositivos AWS Snowball Edge son resistentes, las inclemencias del tiempo pueden dañar el hardware más resistente. Si un dispositivo se extravía, es robado o se estropea, debe comunicarlo lo antes posible. Cuanto antes se notifique el problema, antes podremos enviarle otro para completar su trabajo.

> **Note**
>
> Los dispositivos AWS Snowball Edge son propiedad de. AWS La manipulación de un dispositivo constituye una infracción de la Política de uso AWS aceptable. Para obtener más información, consulte http://aws.amazon.com/aup/.

Adoptamos las siguientes medidas de seguridad:

- Al transferir datos con el adaptador de Amazon S3, los metadatos de los objetos no se almacenan de forma persistente. Los únicos metadatos que se conservan iguales son `filename` y `filesize`. Todos los demás metadatos se establecen como en el ejemplo siguiente: `-rw-rw-r-- 1 root root [filesize] Dec 31 1969 [path/filename]`
- Al transferir datos con la interfaz de archivos, los metadatos de los objetos se almacenan de forma persistente.
- Cuando recibimos un dispositivo AWS, lo inspeccionamos para detectar cualquier indicio de manipulación y verificamos que el módulo de plataforma segura (TPM) no haya detectado ningún cambio. AWS Snowball Edge utiliza varios niveles de seguridad diseñados para proteger sus datos, como carcasas a prueba de manipulaciones, cifrado de 256 bits y un TPM estándar del sector diseñado para proporcionar seguridad y una cadena de custodia completa para sus datos.
- Una vez que el trabajo de transferencia de datos se ha procesado y verificado, AWS realiza un borrado de software del dispositivo Snowball de conformidad con las directrices para el saneamiento de soportes del Instituto Nacional de Normalización y Tecnología (NIST, por sus siglas en inglés).

Validación de etiquetas NFC

Los dispositivos Snowball Edge optimizados para computación y Snowball Edge optimizados para almacenamiento (para transferencia de datos) tienen etiquetas NFC integradas. Puede escanear estas etiquetas con la aplicación AWS Snowball Edge Verification, disponible en Android. El escaneo y la validación de estas etiquetas NFC puede ayudarle a verificar que el dispositivo no se ha manipulado antes de utilizarlo.

La validación de etiquetas NFC incluye el uso del cliente de Snowball Edge para generar un código QR específico del dispositivo a fin de verificar que las etiquetas que está escaneando corresponden al dispositivo adecuado.

El siguiente procedimiento describe cómo validar las etiquetas NFC en un dispositivo Snowball Edge. Antes de empezar, asegúrese de haber realizado los siguientes cinco primeros pasos del ejercicio de introducción:

1. Cree su trabajo de Snowball Edge. Para obtener más información, consulte Crear una tarea para solicitar un dispositivo de la familia Snow
2. Recepción del dispositivo. Para obtener más información, consulte Recepción del dispositivo Snowball Edge.
3. Conexión a la red local. Para obtener más información, consulte Conexión a la red local.
4. Obtención de las credenciales y herramientas. Para obtener más información, consulte Obtener credenciales para acceder a un dispositivo de la familia Snow.
5. Descarga e instalación del cliente de Snowball Edge. Para obtener más información, consulte Descarga e instalación del cliente de Snowball Edge.

Validación de las etiquetas NFC

1. Ejecute el comando `snowballEdge get-app-qr-code` del cliente de Snowball Edge. Si ejecuta este comando para un nodo en un clúster, proporcione el número de serie (`--device-sn`) para obtener un código QR para un nodo único. Repita este paso para cada nodo del clúster. Para obtener más información acerca del uso de este comando, consulte Obtención del código QR para validación por NFC.

   El código QR se guarda en la ubicación que prefiera como archivo .png.
2. Vaya al archivo .png que ha guardado y ábralo para poder escanear el código QR con la aplicación.

3. Puede escanear estas etiquetas con la aplicación AWS Snowball Edge Verification en Android.

> **Note**
>
> La aplicación AWS Snowball Edge Verification no está disponible para su descarga, pero si tienes un dispositivo con la aplicación ya instalada, puedes usarla.

4. Inicie la aplicación y siga las instrucciones en pantalla.

Ahora ha escaneado y validado correctamente las etiquetas NFC para el dispositivo.

Si surge algún problema al escanear, pruebe lo siguiente:

- Confirme que su dispositivo tiene las opciones Snowball Edge optimizado para computación (con o sin GPU).
- Si tiene la aplicación en otro dispositivo, intente usar ese dispositivo.
- Mueva el dispositivo a una zona aislada de la habitación, alejada de interferencias de otras etiquetas NFC y vuelva a intentarlo.
- Si los problemas persisten, contacte con AWS Support.

Identity and Access Management en AWS Snowball

Todos los AWS Snowball trabajos deben estar autenticados. Para ello, debe crear y administrar los usuarios de IAM de su cuenta. IAM permite crear y administrar los usuarios y los permisos en AWS.

AWS Snowball los usuarios deben tener ciertos permisos relacionados con la IAM para acceder a ellos y crear AWS Snowball AWS Management Console trabajos. Un usuario de IAM que cree un trabajo de importación o exportación también debe tener acceso a los recursos correctos de Amazon Simple Storage Service (Amazon S3), como los buckets de Amazon S3 que se utilizarán para el trabajo AWS KMS , los recursos, el tema de Amazon SNS y la AMI compatible con Amazon EC2 para los trabajos de computación perimetral.

> **Important**
>
> Para obtener información sobre cómo usar IAM localmente en su dispositivo, consulte Uso local de IAM.

Temas

Control de acceso para la consola de Snow Family y creación de trabajos

Como ocurre con todos los AWS servicios, el acceso AWS Snowball requiere credenciales que AWS pueda utilizar para autenticar sus solicitudes. Esas credenciales deben tener permisos para acceder a AWS los recursos, como un bucket de Amazon S3 o una AWS Lambda función. AWS Snowball se diferencia de dos maneras:

1. Los trabajos en Amazon AWS Snowball no tienen nombres de recursos de Amazon (ARN).
2. El control de acceso a la red y físico de un dispositivo en las instalaciones es responsabilidad del usuario.

Consulte Identity and Access Management para AWS Snow Family para obtener más información sobre cómo puede utilizar AWS Identity and Access Management (IAM) y cómo ayudar AWS Snowball a proteger sus recursos controlando quién puede acceder a ellos en las Nube de AWS recomendaciones de control de acceso local.

Identity and Access Management para AWS Snow Family

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos. AWS Snow Family La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Temas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo en el que se realice. AWS Snow Family

Usuario del servicio: si utiliza el AWS Snow Family servicio para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más AWS Snow Family funciones para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en AWS Snow Family, consulte Solución de problemas de AWS Snow Family identidad y acceso.

Administrador de servicios: si estás a cargo de AWS Snow Family los recursos de tu empresa, probablemente tengas acceso total a ellos AWS Snow Family. Su trabajo consiste en determinar a qué AWS Snow Family funciones y recursos deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar la IAM AWS Snow Family, consulte¿Cómo AWS Snow Family funciona con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a AWS. Para ver ejemplos de políticas AWS Snow Family basadas en la identidad que puede utilizar en IAM, consulte. Ejemplos de políticas basadas en la identidad para AWS Snow Family

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, asumes un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Uso de la autenticación multifactor (MFA) en AWSen la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio

desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

- Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar un AWS rol a una instancia EC2 y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations .
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo AWS determinar si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

¿Cómo AWS Snow Family funciona con IAM

Antes de utilizar IAM para gestionar el acceso AWS Snow Family, infórmese sobre las funciones de IAM disponibles para su uso. AWS Snow Family

Funciones de IAM que puede utilizar con AWS Snow Family

Característica de IAM	AWS Snow Family soporte
Políticas basadas en identidades	Sí
Políticas basadas en recursos	Sí
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
ACL	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Sesiones de acceso directo (FAS)	Sí
Roles de servicio	Sí
Roles vinculados al servicio	No

Para obtener una visión general de cómo AWS Snow Family funcionan otros AWS servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en la identidad para AWS Snow Family

Compatibilidad con las políticas basadas en identidad	Sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en la identidad para AWS Snow Family

Para ver ejemplos de políticas AWS Snow Family basadas en la identidad, consulte. Ejemplos de políticas basadas en la identidad para AWS Snow Family

Políticas basadas en recursos incluidas AWS Snow Family

Compatibilidad con las políticas basadas en recursos	Sí

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico.

Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para más información, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Acciones políticas para AWS Snow Family

Admite acciones de política	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de AWS Snow Family acciones, consulta las acciones definidas AWS Snow Family en la Referencia de autorización del servicio.

Las acciones políticas AWS Snow Family utilizan el siguiente prefijo antes de la acción:

```
snowball
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "snowball:action1",
      "snowball:action2"
         ]
```

Para ver ejemplos de políticas AWS Snow Family basadas en la identidad, consulte. Ejemplos de políticas basadas en la identidad para AWS Snow Family

Recursos de políticas para AWS Snow Family

Admite recursos de políticas	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de los tipos de AWS Snow Family recursos y sus ARN, consulte los recursos definidos AWS Snow Family en la Referencia de autorización de servicios. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS Snow Family.

Para ver ejemplos de políticas AWS Snow Family basadas en la identidad, consulte. Ejemplos de políticas basadas en la identidad para AWS Snow Family

Claves de condición de la política para AWS Snow Family

Admite claves de condición de políticas específicas del servicio	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de claves de AWS Snow Family condición, consulte las claves de condición AWS Snow Family en la Referencia de autorización de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por AWS Snow Family.

Para ver ejemplos de políticas AWS Snow Family basadas en la identidad, consulte. Ejemplos de políticas basadas en la identidad para AWS Snow Family

ACL en AWS Snow Family

Admite las ACL	No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con AWS Snow Family

Admite ABAC (etiquetas en las políticas)	Parcial

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte ¿Qué es ABAC? en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Utilizar credenciales temporales con AWS Snow Family

Compatible con el uso de credenciales temporales	Sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida información sobre cuáles Servicios de AWS funcionan con

credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para más información sobre el cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Sesiones de acceso directo para AWS Snow Family

Admite Forward access sessions (FAS)	Sí

Cuando utiliza un usuario o un rol de IAM para realizar acciones en AWSél, se le considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información detallada sobre las políticas a la hora de realizar solicitudes de FAS, consulte Forward access sessions.

Roles de servicio para AWS Snow Family

Compatible con roles de servicio	Sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio puede interrumpir AWS Snow Family la funcionalidad. Edite las funciones de servicio solo cuando se AWS Snow Family proporcionen instrucciones para hacerlo.

Funciones vinculadas al servicio para AWS Snow Family

Compatible con roles vinculados al servicio	No

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en la identidad para AWS Snow Family

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de AWS Snow Family . Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS la API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos AWS Snow Family, incluido el formato de los ARN para cada uno de los tipos de recursos, consulte las claves de condición, recursos y acciones de la Referencia de autorización de servicios. AWS Snow Family

Temas

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear AWS Snow Family recursos de tu cuenta, acceder a ellos o eliminarlos. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para

más información, consulte Política de validación de Analizador de acceso de IAM en la Guía de usuario de IAM.

- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Mediante la consola de AWS Snow Family

Para acceder a la AWS Snow Family consola, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los AWS Snow Family recursos de su cuenta Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS API. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la AWS Snow Family consola, asocie también la AWS Snow Family *ConsoleAccess* política *ReadOnly* AWS gestionada a las entidades. Para más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o 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": "*"
        }
    ]
}
```

Solución de problemas de AWS Snow Family identidad y acceso

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas más comunes que pueden surgir al trabajar con una AWS Snow Family IAM.

Temas

- No estoy autorizado a realizar ninguna acción en AWS Snow Family
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis AWS Snow Family recursos

No estoy autorizado a realizar ninguna acción en AWS Snow Family

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `snowball:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 snowball:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `snowball:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, las políticas deben actualizarse a fin de permitirle pasar un rol a AWS Snow Family.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en AWS Snow Family. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis AWS Snow Family recursos

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para saber si AWS Snow Family es compatible con estas funciones, consulte¿Cómo AWS Snow Family funciona con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

El control de acceso en el Nube de AWS

Puede que tenga credenciales válidas para autenticar las solicitudes en AWS. Sin embargo, a menos que tenga permisos, no podrá crear AWS recursos ni acceder a ellos. Por ejemplo, debe tener permisos para crear un trabajo para solicitar un dispositivo de la familia Snow.

En las secciones siguientes se describe cómo administrar los permisos basados en la nube para AWS Snowball. Recomendamos que lea primero la información general.

- Descripción general de la gestión de los permisos de acceso a sus recursos en el Nube de AWS
- Uso de políticas basadas en la identidad (políticas de IAM) para AWS Snowball

Descripción general de la gestión de los permisos de acceso a sus recursos en el Nube de AWS

Cada AWS recurso es propiedad de un Cuenta de AWS, y los permisos para crear o acceder a un recurso se rigen por políticas de permisos. Un administrador de cuentas puede adjuntar políticas de permisos a las identidades de IAM (es decir, usuarios, grupos y roles), y algunos servicios (por ejemplo AWS Lambda) también permiten adjuntar políticas de permisos a los recursos.

> **Note**
>
> Un administrador de cuentas (o usuario administrador) es un usuario que tiene privilegios de administrador. Para obtener más información, consulte Prácticas recomendadas de IAM en la Guía del usuario de IAM.

Temas

- Recursos y operaciones
- Titularidad de los recursos
- Administrar el acceso a los recursos en el Nube de AWS
- Especificar elementos de política: acciones, efectos y entidades principales
- Especificación de las condiciones de una política

Recursos y operaciones

En AWS Snowball, el recurso principal es un trabajo. AWS Snowball también tiene dispositivos como el Snowball y el AWS Snowball Edge dispositivo, sin embargo, solo puedes usar esos dispositivos en el contexto de un trabajo existente. Los buckets de Amazon S3 y las funciones de Lambda son recursos de Amazon S3 y Lambda, respectivamente.

Como ya se ha mencionado anteriormente, los trabajos no tienen nombres de recurso de Amazon (ARN) asociados. Sin embargo, otros recursos de los servicios, como los buckets de Amazon S3, tienen asociados nombres de recurso de Amazon (ARN) únicos, como se muestra en la tabla siguiente.

AWS Snowball proporciona un conjunto de operaciones para crear y gestionar trabajos. Para ver una lista de las operaciones disponibles, consulte la Referencia de la API de AWS Snowball.

Titularidad de los recursos

Cuenta de AWS Es propietario de los recursos que se crean en la cuenta, independientemente de quién los haya creado. En concreto, el propietario del recurso es el Cuenta de AWS de la entidad principal (es decir, la cuenta raíz, un usuario de IAM o un rol de IAM) que autentica la solicitud de creación de recursos. Los siguientes ejemplos ilustran cómo funciona:

- Si utiliza las credenciales de su cuenta raíz Cuenta de AWS para crear un bucket de S3, Cuenta de AWS es el propietario del recurso (en este caso AWS Snowball, el recurso es la tarea).
- Si crea un usuario de IAM en su cuenta Cuenta de AWS y le concede permisos para crear un trabajo para solicitar un dispositivo de la familia Snow, el usuario puede crear un trabajo para solicitar un dispositivo de la familia Snow. Sin embargo, usted Cuenta de AWS, al que pertenece el usuario, es el propietario del recurso de trabajo.
- Si crea un rol de IAM Cuenta de AWS con permisos para crear un trabajo, cualquier persona que pueda asumir ese rol puede crear un trabajo para solicitar un dispositivo de la familia Snow. Usted Cuenta de AWS, al que pertenece el rol, es el propietario del recurso de trabajo.

Administrar el acceso a los recursos en el Nube de AWS

Una política de permisos describe quién tiene acceso a qué. En la siguiente sección se explican las opciones disponibles para crear políticas de permisos.

> **Note**
>
> En esta sección se analiza el uso de la IAM en el contexto de AWS Snowball. No se proporciona información detallada sobre el servicio de IAM. Para ver la documentación completa de IAM, consulte ¿Qué es IAM? en la Guía del usuario de IAM. Para obtener más información acerca de la sintaxis y las descripciones de las políticas de IAM, consulte Referencia de políticas de IAM de AWS en la Guía del usuario de IAM.

Las políticas asociadas a una identidad de IAM se denominan políticas basadas en la identidad (políticas de IAM) y las políticas asociadas a un recurso se denominan políticas basadas en recursos. AWS Snowball solo admite políticas basadas en la identidad (políticas de IAM).

Temas

- Políticas basadas en recursos

Políticas basadas en recursos

Otros servicios, como Amazon S3, también admiten políticas de permisos basadas en recursos. Por ejemplo, puede adjuntar una política a un bucket de S3 para administrar los permisos de acceso a ese bucket. AWS Snowball no admite políticas basadas en recursos.

Especificar elementos de política: acciones, efectos y entidades principales

En cada trabajo (consulte Recursos y operaciones), el servicio define un conjunto de operaciones de la API (consulte Referencia de la API de AWS Snowball) para la creación y administración de dicho trabajo. Para conceder permisos para estas operaciones de la API, AWS Snowball define un conjunto de acciones que puede especificar en una política. Por ejemplo, en el caso de un trabajo, se definen las acciones siguientes: `CreateJob`, `CancelJob` y `DescribeJob`. Tenga en cuenta que la realización de una operación de la API puede requerir permisos para más de una acción.

A continuación se indican los elementos más básicos de la política:

- Recurso: en una política, se usa un nombre de recurso de Amazon (ARN) para identificar el recurso al que se aplica la política. Para obtener más información, consulte Recursos y operaciones.

  > **Note**
  >
  > Esto es compatible con Amazon S3, Amazon EC2, AWS Lambda y muchos otros AWS KMS servicios.
  > Snowball no admite especificar un ARN de recurso en el elemento `Resource` de una declaración de política de IAM. Para permitir el acceso a Snowball, especifique `"Resource": "*"` en la política.

- Acción: utilice palabras clave de acción para identificar las operaciones del recurso que desea permitir o denegar. Por ejemplo, en función del elemento especificado para `Effect`, `snowball:*` permite o deniega los permisos de usuario para realizar todas las operaciones.

  > **Note**
  >
  > Esto es compatible con Amazon EC2, Amazon S3 e IAM.

- Efecto: especifique el efecto que se producirá cuando el usuario solicite la acción específica; puede ser permitir o denegar. Si no concede acceso de forma explícita (permitir) a un recurso, el

acceso se deniega implícitamente. También puede denegar explícitamente el acceso a un recurso para asegurarse de que un usuario no pueda obtener acceso a él, aunque otra política le conceda acceso.

> **Note**
>
> Esto es compatible con Amazon EC2, Amazon S3 e IAM.

- Entidad principal: en las políticas basadas en identidades (políticas de IAM), el usuario al que se asocia esta política es la entidad principal implícita. En el caso de las políticas basadas en recursos, debe especificar el usuario, la cuenta, el servicio u otra entidad para la que desea recibir los permisos (solo se aplica a las políticas basadas en recursos). AWS Snowball no admite políticas basadas en recursos.

Para obtener más información sobre la sintaxis y descripciones de las políticas de IAM, consulte Referencia de la política de IAM de AWS en la Guía del usuario de IAM.

Para ver una tabla que muestra todas las acciones de la AWS Snowball API, consulte. AWS Snowball Permisos de API: referencia de acciones, recursos y condiciones

Especificación de las condiciones de una política

Al conceder permisos, puede utilizar el lenguaje de la política de IAM para especificar las condiciones en la que se debe aplicar una política. Por ejemplo, es posible que desee que solo se aplique una política después de una fecha específica. Para obtener más información sobre cómo especificar condiciones en un lenguaje de política, consulte Condition en la Guía del usuario de IAM.

Para expresar condiciones, se usan claves de condición predefinidas. No hay claves de condición específicas para AWS Snowball. Sin embargo, hay claves AWS de condición generales que puede utilizar según convenga. Para obtener una lista completa de las claves AWS de ancho, consulte las claves disponibles para las condiciones en la Guía del usuario de IAM.

Uso de políticas basadas en la identidad (políticas de IAM) para AWS Snowball

Este tema ofrece ejemplos de políticas basadas en identidades que muestran cómo un administrador de cuentas puede asociar políticas de permisos a identidades de IAM (es decir, usuarios, grupos y roles). Por lo tanto, estas políticas otorgan permisos para realizar operaciones en AWS Snowball los recursos del. Nube de AWS

> **Important**
>
> Le recomendamos que consulte primero los temas de introducción en los que se explican los conceptos básicos y las opciones disponibles para administrar el acceso a sus recursos de AWS Snowball . Para obtener más información, consulte Descripción general de la gestión de los permisos de acceso a sus recursos en el Nube de AWS.

En las secciones de este tema se explica lo siguiente:

- Permisos necesarios para usar la AWS Snowball consola
- AWS-Políticas gestionadas (predefinidas) para Edge AWS Snowball
- Ejemplos de políticas administradas por el cliente

A continuación se muestra un ejemplo de una política de permisos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
       "Effect": "Allow",
       "Action": [
          "snowball:*",
          "importexport:*"
       ],
       "Resource": "*"
    }
  ]
}
```

La política tiene dos instrucciones:

- La primera instrucción concede permisos para tres acciones de Amazon S3 (`s3:GetBucketLocation`, `s3:GetObject` y `s3:ListBucket`) en todos los buckets de Amazon S3 que utilizan el nombre de recurso de Amazon (ARN) de `arn:aws:s3:::*`. El ARN especifica un carácter comodín (*), por lo que el usuario puede elegir cualquiera de los buckets de Amazon S3 o todos ellos desde los que exportar datos.
- La segunda declaración otorga permisos para todas AWS Snowball las acciones. Dado que estas acciones no admiten permisos de nivel de recursos, la política especifica el carácter comodín (*) y el valor `Resource` también especifica un comodín.

La política no especifica el elemento `Principal`, ya que en una política basada en identidades no se especifica la entidad principal que obtiene el permiso. Al asociar una política a un usuario, el usuario es la entidad principal implícita. Cuando se asocia una política de permisos a un rol de IAM, la entidad principal identificada en la política de confianza del rol obtiene los permisos.

Para ver una tabla que muestra todas las acciones de la API de administración de AWS Snowball trabajos y los recursos a los que se aplican, consulteAWS Snowball Permisos de API: referencia de acciones, recursos y condiciones.

Permisos necesarios para usar la AWS Snowball consola

La tabla de referencia de permisos enumera las operaciones de la API de administración de AWS Snowball trabajos y muestra los permisos necesarios para cada operación. Para obtener más información sobre las operaciones de API de administración de trabajos, consulte AWS Snowball Permisos de API: referencia de acciones, recursos y condiciones.

Para utilizarlos Consola de administración de la familia de productos Snow de AWS, debes conceder permisos para acciones adicionales, tal y como se muestra en la siguiente política de permisos:

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

La AWS Snowball consola necesita estos permisos adicionales por los siguientes motivos:

- `ec2:`: permite al usuario describir instancias compatibles con Amazon EC2 y modificar sus atributos con fines de computación local. Para obtener más información, consulte Uso de instancias de computación compatibles con Amazon EC2.
- `kms:`: el usuario puede crear o elegir la clave de KMS que cifrará sus datos. Para obtener más información, consulte AWS Key Management Service en AWS Snowball Edge.
- `iam:`— Permiten al usuario crear o elegir un ARN de rol de IAM AWS Snowball que asumirá para acceder a los recursos asociados a AWS la creación y el procesamiento de empleos.
- `sns:`: el usuario puede crear o elegir las notificaciones de Amazon SNS para los trabajos que crea. Para obtener más información, consulte Notificaciones para dispositivos Snow Family.

AWS-Políticas gestionadas (predefinidas) para Edge AWS Snowball

AWS aborda muchos casos de uso comunes al proporcionar políticas de IAM independientes que son creadas y administradas por. AWS Las políticas administradas conceden los permisos necesarios para casos de uso comunes, lo que le evita tener que investigar los permisos que se necesitan. Para más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

Puede utilizar las siguientes políticas AWS gestionadas con. AWS Snowball

Creación de una política de roles de IAM para Snowball Edge

La política de roles de IAM debe crearse con permisos de lectura y escritura para los buckets de Amazon S3. El rol de IAM también debe tener una relación de confianza con Snowball. Tener una relación de confianza significa que AWS puede escribir los datos en Snowball y en sus buckets de Amazon S3, en función de si está importando o exportando datos.

Al crear un trabajo para solicitar un dispositivo de la familia Snow Consola de administración de la familia de productos Snow de AWS, la creación de la función de IAM necesaria se realiza en el paso 4 de la sección de permisos. Este proceso es automático. El rol de IAM que permite que Snowball asuma se utiliza únicamente para escribir los datos en el bucket cuando el dispositivo Snowball con los datos que está transfiriendo llega a AWS. A continuación se describe ese proceso.

Para crear el rol de IAM para el trabajo de importación

1. Inicie sesión AWS Management Console y abra la AWS Snowball consola en https://console.aws.amazon.com/importexport/.
2. Seleccione Crear trabajo.
3. En el primer paso, rellene los detalles del trabajo de importación en Amazon S3 y, a continuación, elija Siguiente.
4. En el segundo paso, en Permiso, seleccione Crear o seleccionar rol de IAM.

   Se abrirá la Consola de administración de IAM, que mostrará el rol de IAM que AWS utiliza para copiar objetos en los buckets de Amazon S3 especificados.
5. Revise los detalles de esta página y elija Permitir.

   Vuelve a Consola de administración de la familia de productos Snow de AWS, donde el ARN del rol de IAM seleccionado contiene el nombre del recurso de Amazon (ARN) del rol de IAM que acaba de crear.

6. Elija Siguiente para terminar de crear el rol de IAM.

El procedimiento anterior crea un rol de IAM que tiene permisos de escritura para los buckets de Amazon S3 en los que tiene previsto importar los datos. El rol de IAM que se crea posee una de las siguientes estructuras, según sea para un trabajo de importación o de exportación.

Rol de IAM para un trabajo de importación

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

Si utiliza el cifrado del lado del servidor con claves AWS KMS administradas (SSE-KMS) para cifrar los buckets de Amazon S3 asociados a su trabajo de importación, también debe añadir la siguiente declaración a su función de IAM.

```
{
     "Effect": "Allow",
```

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

Si los tamaños de objeto son mayores, el cliente de Amazon S3 que se utiliza para el proceso de importación utiliza la carga multiparte. Si inicia una carga de varias partes mediante SSE-KMS, todas las partes cargadas se cifran con la clave especificada. AWS KMS Como las partes están cifradas, deben descifrarse para que puedan montarse para completar la carga multiparte. Por lo tanto, debe tener permiso para descifrar la AWS KMS clave (`kms:Decrypt`) cuando ejecute una carga multiparte en Amazon S3 con SSE-KMS.

A continuación se muestra un ejemplo de rol de IAM necesario para un trabajo de importación que necesita el permiso `kms:Decrypt`.

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

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

A continuación se muestra un ejemplo de un rol de IAM necesario para un trabajo de exportación.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": "arn:aws:s3:::*"
    }
```

```
  ]
}
```

Si utiliza el cifrado del lado del servidor con claves AWS KMS administradas para cifrar los buckets de Amazon S3 asociados a su trabajo de exportación, también debe añadir la siguiente declaración a su función de IAM.

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

Puede crear sus propias políticas de IAM personalizadas para permitir permisos para las operaciones de la API para la administración de trabajos. AWS Snowball Puede asociar estas políticas personalizadas a los grupos o usuarios de IAM que requieran esos permisos.

Ejemplos de políticas administradas por el cliente

En esta sección, encontrará ejemplos de políticas de usuario que otorgan permisos para diversas acciones de administración de AWS Snowball trabajos. Estas políticas funcionan cuando se utilizan los SDK de AWS o la AWS CLI. Cuando se utiliza la consola, debe conceder permisos adicionales específicos a la consola, tal y como se explica en Permisos necesarios para usar la AWS Snowball consola.

> **Note**
>
> Todos los ejemplos utilizan la región us-west-2 y contienen identificadores de cuenta ficticios.

Ejemplos

- Ejemplo 1: Política de roles que permite a un usuario crear un trabajo para solicitar un dispositivo de la familia Snow con la API
- Ejemplo 2: Política de roles para crear trabajos de importación
- Ejemplo 3: Política de roles para crear trabajos de exportación
- Ejemplo 4: Política de confianza y de permisos de rol esperados

- AWS Snowball Permisos de API: referencia de acciones, recursos y condiciones

Ejemplo 1: Política de roles que permite a un usuario crear un trabajo para solicitar un dispositivo de la familia Snow con la API

La política de permisos siguiente es un componente necesario de cualquier política que se utiliza para conceder permisos de creación de trabajos o clústeres con la API de administración de trabajos. La declaración es necesaria como declaración de política de relaciones de confianza para el rol de IAM de Snowball.

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

Ejemplo 2: Política de roles para crear trabajos de importación

Utilice la siguiente política de confianza de roles para crear trabajos de importación para Snowball Edge que utilicen AWS Lambda powered by AWS IoT Greengrass functions.

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

Ejemplo 3: Política de roles para crear trabajos de exportación

Utilice la siguiente política de confianza de roles para crear trabajos de exportación para Snowball Edge que utilicen AWS Lambda powered by AWS IoT Greengrass functions.

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

Ejemplo 4: Política de confianza y de permisos de rol esperados

La siguiente política de permisos de rol esperados es necesaria para que la utilice un rol de servicio existente. Se configura una sola 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"
                    }
            }
        }
    ]
}
```

La siguiente política de confianza de rol esperado es necesaria para que la utilice un rol de servicio existente. Se configura una sola vez.

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

AWS Snowball Permisos de API: referencia de acciones, recursos y condiciones

Cuando configure El control de acceso en el Nube de AWS y escriba una política de permisos que se pueda asociar a una identidad de IAM (políticas basadas en identidad), puede utilizar la siguiente lista como referencia. La incluye cada operación de la API de administración de AWS Snowball trabajos y las acciones correspondientes para las que puedes conceder permisos para realizar la acción. También incluye, para cada operación de API, el AWS recurso para el que puedes conceder

los permisos. Las acciones se especifican en el campo `Action` de la política y el valor del recurso se especifica en el campo `Resource` de la política.

Puedes usar claves AWS de condición generales en tus AWS Snowball políticas para expresar las condiciones. Para obtener una lista completa de las claves AWS anchas, consulta las claves disponibles en la Guía del usuario de IAM.

> **Note**
>
> Para especificar una acción, use el prefijo `snowball:` seguido del nombre de operación de la API (por ejemplo, `snowball:CreateJob`).

Registro y monitorización en AWS Snowball

El monitoreo es una parte importante del mantenimiento de la confiabilidad, la disponibilidad y el rendimiento de AWS Snowball sus AWS soluciones. Debe recopilar los datos de supervisión para poder depurar más fácilmente una falla multipunto en caso de que se produzca. AWS proporciona varias herramientas para supervisar sus AWS Snowball recursos y responder a posibles incidentes:

AWS CloudTrail Registros

CloudTrail proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en la API de administración de AWS Snowball trabajos o al usar la AWS consola. Con la información recopilada por CloudTrail, puede determinar la solicitud de API que se realizó al AWS Snowball servicio, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales. Para obtener más información, consulte Registrar llamadas a la API de AWS Snowball Edge con AWS CloudTrail.

Validación de conformidad para AWS Snowball

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

  > **Note**
  >
  > No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.

- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia

La infraestructura AWS global se basa en zonas Regiones de AWS de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS

Seguridad de la infraestructura en AWS Snowball

Como servicio gestionado, AWS Snow Family está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a AWS Snow Family través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM principal. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Validación de datos con trabajos de Snowball Edge

A continuación, encontrará información sobre cómo AWS Snowball Edge valida las transferencias de datos y los pasos manuales que puede seguir para garantizar la integridad de los datos durante y después de un trabajo.

Temas

Validación de la suma de comprobación de los datos transferidos

Cuando se copia un archivo de un origen de datos local con la interfaz de Amazon S3 al dispositivo Snowball Edge, se crea una serie de sumas de comprobación. Estas sumas de comprobación se utilizan para validar automáticamente los datos a medida que se transfieren.

A grandes rasgos, estas sumas de comprobación se crean para cada archivo (o para partes de archivos grandes). En el caso de Snowball Edge, estas sumas de comprobación están visibles al ejecutar el siguiente AWS CLI comando en un bucket del dispositivo. Las sumas de comprobación se utilizan para validar la integridad de los datos durante las transferencias y garantizan que los datos se copian correctamente.

```
aws s3api list-objects --bucket bucket-name --endpoint http://ip:8080 --profile edge-
profile
```

Cuando estas sumas de comprobación no coinciden, los datos asociados no se importan a Amazon S3.

Creación de un inventario local durante la transferencia de Snowball

Cree un inventario local de los archivos copiados al dispositivo Snowball cuando utilice el adaptador de Amazon S3 o la CLI. El contenido del inventario local se puede usar para compararlo con el contenido del almacenamiento o servidor local.

Por ejemplo,

```
aws s3 cp folder/ s3://bucket --recursive > inventory.txt
```

Errores de validación comunes

Siempre que se produce un error de validación, los datos correspondientes (un archivo o una parte de un archivo grande) no se escriben en el destino. Las siguientes son las causas más comunes de los errores de validación:

- Intento de copiar enlaces simbólicos.
- Intento de copiar archivos que se están modificando de forma activa. El intento no pasa la validación de la suma de comprobación y se marca como una transferencia fallida.
- Intento de copiar archivos con un tamaño superior a 5 TB.
- Intento de copiar partes de un archivo de un tamaño superior a 2 GiB.
- Intento de copiar archivos a un dispositivo Snowball Edge que ya se encuentra en su capacidad de almacenamiento de datos máxima.
- Intento de copiar archivos a un dispositivo Snowball Edge que no cumple las directrices de nomenclatura de claves de objeto para Amazon S3.

Cuando se produzca cualquiera de estos errores de validación, se registrará. Puede realizar los pasos para identificar manualmente qué archivos no han superado la validación y el motivo. Para obtener más información, consulte Validación de datos manual para Snowball Edge después de la importación a Amazon S3.

Validación de datos manual para Snowball Edge después de la importación a Amazon S3

Después de que se haya completado un trabajo de importación, dispone de varias opciones para validar manualmente los datos de Amazon S3, tal y como se describe a continuación.

Consulta del informe de finalización de trabajos y los registros asociados

Siempre que se importan o exportan datos en Amazon S3, se obtiene un informe del trabajo en PDF que se puede descargar. Para los trabajos de importación, este informe está disponible cuando

finaliza el proceso de importación. Para obtener más información, consulte Obtener el informe y los registros de finalización del trabajo.

Inventario de S3

Si ha transferido una gran cantidad de datos a Amazon S3 en varios trabajos, puede que ir a cada informe de finalización de trabajo no sea una forma eficiente de usar el tiempo. En su lugar, puede obtener un inventario de todos los objetos de uno o varios buckets de Amazon S3. El inventario de Amazon S3 proporciona un archivo de valores separados por comas (CSV) en el que se muestran sus objetos y sus metadatos correspondientes por días o por semanas. Este archivo abarca los objetos de un bucket de Amazon S3 o un prefijo compartido (es decir, objetos cuyos nombres empiezan por una cadena común).

Una vez que tenga el inventario de los buckets de Amazon S3 a los que ha importado datos, puede compararlo fácilmente con los archivos que ha transferido en su ubicación de datos de origen. De esta forma, puede identificar rápidamente qué archivos no se han transferido.

Uso del comando de sincronización de Amazon S3

Si su estación de trabajo puede conectarse a Internet, puede realizar una validación final de todos los archivos transferidos ejecutando el comando. AWS CLI `aws s3 sync` Este comando sincroniza los directorios y los prefijos de S3. Este comando copia de forma recursiva los archivos nuevos y actualizados del directorio de origen al destino. Para obtener más información, consulte sync en la Referencia de los comandos de la AWS CLI .

> **Important**
>
> Si especifica el almacenamiento local como el destino de este comando, asegúrese de que dispone de una copia de seguridad de los archivos en los que está efectuando la sincronización. Estos archivos se sobrescriben con el contenido del origen de Amazon S3 especificado.

Notificaciones para dispositivos Snow Family

Cómo Snow utiliza Amazon SNS

El servicio Snow está diseñado para utilizar las robustas notificaciones que proporciona Amazon Simple Notification Service (Amazon SNS). Al crear un trabajo para pedir un dispositivo Snow, puede proporcionar direcciones de correo electrónico donde recibir notificaciones sobre los cambios de estado de su trabajo. Cuando lo haga, elija un tema de SNS existente o cree uno nuevo. Si el tema de SNS está cifrado, debe habilitar el cifrado de KMS administrado por el cliente para el tema y configurar una política de claves de KMS administradas por el cliente. Consulte Selección de las preferencias de notificación.

Tras crear el trabajo, cada dirección de correo electrónico que especificó para recibir las notificaciones de Amazon SNS recibirá un mensaje de correo electrónico de las notificaciones en el que se solicita la confirmación de AWS la suscripción al tema. Un usuario de la cuenta de correo electrónico debe confirmar la suscripción eligiendo Confirmar suscripción. Los mensajes de correo electrónico de notificación de Amazon SNS están adaptados a cada estado del trabajo e incluyen un enlace a la Consola de administración de la familia de productos Snow de AWS.

También puede configurar Amazon SNS para que envíe mensajes de texto con estas notificaciones de cambio de estado desde la consola de Amazon SNS. Para obtener más información, consulte Mensajería de texto móvil (SMS) en la Guía para desarrolladores de Amazon Simple Notification Service.

Cifrado de los temas de SNS para los cambios de estado de los trabajos de Snow

Habilite el cifrado de KMS administrado por el cliente para que el tema de SNS reciba notificaciones sobre los cambios de estado de los trabajos de Snow. Los temas de SNS cifrados con un cifrado AWS administrado no pueden recibir cambios de estado en los trabajos de Snow porque el rol de IAM de importación de Snow no tiene acceso a la clave de KMS AWS administrada para realizar tareas y acciones. `Decrypt` `GenerateDataKey` Además, las políticas de las claves de KMS AWS administradas no se pueden editar.

Cómo habilitar el cifrado del servidor en un tema de SNS mediante la consola de administración de Amazon SNS

1. Inicie sesión en la consola de Amazon SNS AWS Management Console y ábrala en https://console.aws.amazon.com/sns/v3/home.
2. En el panel de navegación, elija Temas.
3. En la página Temas, elija el tema utilizado para las notificaciones de cambio de estado del trabajo y, a continuación, seleccione Editar.
4. Expanda la sección Cifrado y haga lo siguiente:
   a. Elija Habilitar el cifrado.
   b. Especifique la clave AWS KMS. Consulte
   c. Para cada tipo de KMS se muestran los valores de descripción, cuenta y ARN de KMS.
5. Para usar una clave personalizada de su AWS cuenta, elija el campo de clave de AWS KMS y, a continuación, elija los kilómetros de KMS personalizados de la lista. Para obtener instrucciones sobre cómo crear un KMS personalizado, consulte Creación de claves en la Guía para AWS Key Management Service desarrolladores.

   Para usar un ARN de KMS personalizado de su AWS cuenta o de otra AWS cuenta, introduzca el ARN de clave de KMS en el AWS campo de clave de KMS.
6. Elija Guardar cambios. El cifrado del servidor está habilitado para su tema y se muestra la página del tema.

Configuración de una política de claves de KMS administradas por el cliente

Tras habilitar el cifrado de los temas de SNS que recibirán notificaciones de cambios en el estado de los trabajos de Snow, actualice la política de KMS relativa al cifrado de los temas de SNS y permita que la entidad principal `"importexport.amazonaws.com"` del servicio Snow realice las acciones `"mks:Decrypt"` y `"mks:GenerateDataKey*"`.

Cómo permitir el rol de servicio de importación y exportación en la política de claves de KMS

1. Inicie sesión en la consola AWS Key Management Service (AWS KMS) AWS Management Console y ábrala en https://console.aws.amazon.com/kms.

2. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
3. En la esquina superior derecha de la consola, cambia la región Región de AWS de la consola a la misma región en la que se realizó el pedido del dispositivo Snow.
4. En el panel de navegación, elija Claves administradas por el cliente.
5. En la lista de claves de KMS, elija el alias o el ID de clave de la clave de KMS que desea actualizar.
6. Elija la pestaña Política de claves; en las declaraciones de la política de claves puede ver las entidades principales a las que la política de claves ha concedido acceso a la clave de KMS y las acciones que pueden realizar.
7. Para la entidad principal del servicio Snow `"importexport.amazonaws.com"`, agregue la siguiente declaración de política para las acciones `"kms:Decrypt"` y `"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. Seleccione Guardar cambios para aplicar los cambios y salir del editor de políticas.

Ejemplos de notificación de SNS

Las notificaciones de Amazon SNS generan los siguientes mensajes de correo electrónico cuando cambia el estado de su trabajo. Estos mensajes son ejemplos del protocolo de temas de SNS `Email-JSON`.

Estado del trabajo	JSON de notificación de SNS
Trabajo creado	{ "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

Estado del trabajo	JSON de notificación de SNS
	=arn:aws:sns:us-east-2:1111 22223333:ExampleTopic1:e103 9402-24e7-40a3-a0d4-797da162b297" }

Estado del trabajo	JSON de notificación de SNS

Preparing appliance	{
	"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"
	}

Estado del trabajo	JSON de notificación de SNS

Exportando	{
	"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"
	}

Estado del trabajo	JSON de notificación de SNS

En tránsito hacia usted	{
	"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"
	}

Estado del trabajo	JSON de notificación de SNS

Entregado a usted	{
	"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"
	}

Estado del trabajo	JSON de notificación de SNS

En tránsito 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"
	}

Estado del trabajo	JSON de notificación de SNS

En las instalaciones de clasificación	{
	"Type" : "Notification",
	"MessageId" : "dc1e94d9-56c5-5e96-808d-cc7f68faa162",
	"TopicArn" : "arn:aws:sns:us-east-2:111122223333:ExampleTopic1",
	"Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2-3f5a4dc9bd6d) is at AWS sorting facility. More info - https://console.aws.amazon.com/impor texport",
	"Timestamp" : "2023-02-23T00:27:58.831Z",
	"SignatureVersion" : "1",
	"Signature" : "FMG5tlZhJNHLHUXvZgtZzlk24FzVa7oX0T4P03neeXw8ZEXZx6z35j2FOTuNYShn2h0bKNC/zLTnMyIxEzmi2X1shOBWsJHkrW2xkR58ABZF+4uWHEE73yDVR4SyYAikP9jstZzDRm+bcVs8+T0yaLiEGLrIIIL4esi1llhIkgErCuy5btPcWXBdio2fpCRD5x9oR6gmE/rd5O7lX1c1uvnv4r1Lkk4pqP2/iUfxFZva1xLSRvgyfm6D9hNklVyPfy+7TalMD0lzmJuOrExtnSIbZew3foxgx8GT+lbZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/LsDr0Iak4ZDpg8dXg==",
	"SigningCertURL" : "https://sns.us-east-1.amazonaws.com/SimpleNotificationService-010a507c1833636cd94bdb98bd93083a.pem",
	"UnsubscribeURL" : "https://sns.us-east-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:111122223333:ExampleTopic1:e1039402-24e7-40a3-a0d4-797da162b297"
	}

Estado del trabajo	JSON de notificación de SNS

En 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"
	}

Estado del trabajo	JSON de notificación de SNS

Importando	{
	"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"
	}

Estado del trabajo	JSON de notificación de SNS

Completado	{
	"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"
	}

Estado del trabajo	JSON de notificación de SNS

Estado del trabajo	JSON de notificación de 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 llamadas a la API de AWS Snowball Edge con AWS CloudTrail

El servicio AWS Snowball o Snow Family se integra con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, función o servicio. CloudTrail captura todas las llamadas a la API del servicio AWS Snow Family. Las llamadas capturadas incluyen llamadas desde la consola de AWS Snowball Family y llamadas en código a la API de AWS Snowball Family Job Management. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos para las llamadas a la API de AWS Snowball Family. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puedes determinar la solicitud realizada con AWS Snowball Family API, la dirección IP de la solicitud realizada, quién hizo la solicitud, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulta la Guía AWS CloudTrail del usuario.

AWS Snowball Información sobre Edge en CloudTrail

CloudTrail está activado en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en AWS Snowball Edge, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos en la Guía del AWS CloudTrail usuario.

Para tener un registro continuo de tus eventos Cuenta de AWS, incluidos los de AWS Snowball Edge, crea una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De manera predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS . La ruta registra los eventos de toda Regiones de AWS la AWS partición y entrega los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para obtener más información, consulte los siguientes temas en la Guía del usuario de AWS CloudTrail :

- Introducción a la creación de registros de seguimiento
- CloudTrail Integraciones y servicios compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail

- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas las acciones de administración de trabajos se documentan en la referencia de la AWS Snowball API y se registran CloudTrail con las siguientes excepciones:

- La CreateAddressoperación no se registra para proteger la información confidencial de los clientes.
- Todas las llamadas a la API de solo lectura (para operaciones de API que comienzan con el prefijo `Get`, `Describe` o `List`) no registran elementos de respuesta.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales raíz o AWS Identity and Access Management (de usuario de IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el elemento CloudTrail UserIdentity en la Guía del usuario.AWS CloudTrail

Descripción de las entradas de archivos de registro de AWS Snowball Edge

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la DescribeJoboperación.

```
      {"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 Cuotas de Edge

A continuación, encontrará información sobre las limitaciones de uso del AWS Snowball Edge dispositivo.

> **Important**
>
> Al transferir datos a Amazon Simple Storage Service (Amazon S3) con un dispositivo Snowball Edge, tenga en cuenta que el tamaño de los objetos individuales de Amazon S3 puede variar desde un mínimo de 0 bytes hasta un máximo de 5 terabytes (TB).

Disponibilidad regional para AWS Snowball Edge

En la siguiente tabla se muestran las regiones en las AWS Snowball Edge que está disponible.

Región	Disponibilidad de Snowball Edge
US East (Ohio)	✓
Este de EE. UU. (Norte de Virginia)	✓
Oeste de EE. UU. (Norte de California)	✓
Oeste de EE. UU. (Oregón)	✓
AWS GovCloud (Este de EE. UU.)	✓
AWS GovCloud (Estados Unidos-Oeste)	✓
Canadá (centro)	✓
Asia-Pacífico (Yakarta)	✓
Asia-Pacífico (Bombay)	✓
Asia-Pacífico (Osaka)	✓
Asia-Pacífico (Seúl)	✓

Región	Disponibilidad de Snowball Edge
Asia-Pacífico (Singapur)	✓
Asia-Pacífico (Sídney)	✓
Asia-Pacífico (Tokio)	✓
Europa (Fráncfort)	✓
Europa (Irlanda)	✓
Europa (Londres)	✓
Europa (Milán)	✓
Europa (París)	✓
Europa (Estocolmo)	✓
Oriente Medio (EAU)	✓
América del Sur (São Paulo)	✓

Para obtener información sobre AWS las regiones y los puntos de enlace compatibles, consulte los puntos de enlace y las cuotas de la familia AWS Snow en la Referencia general de AWS

Limitaciones de los puestos de trabajo AWS Snowball Edge

Existen las siguientes limitaciones a la hora de crear tareas en los AWS Snowball Edge dispositivos:

- Por motivos de seguridad, los trabajos con un AWS Snowball Edge dispositivo deben completarse en un plazo de 360 días a partir de su preparación. Si necesita conservar uno o más dispositivos durante más de 360 días, consulteActualización del certificado SSL. De lo contrario, una vez transcurridos 360 días, el dispositivo se bloquea, ya no se puede acceder a él y debe devolverse. Si el AWS Snowball Edge dispositivo se bloquea durante un trabajo de importación, podemos seguir transfiriendo los datos existentes en el dispositivo a Amazon S3.
- AWS Snowball Edge admite el cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 (SSE-S3) y el cifrado del lado del servidor con claves administradas (SSE-KMS). AWS

Key Management Service El almacenamiento compatible con Amazon S3 en los dispositivos Snow Family admite SSS-C para trabajos de computación y almacenamiento local. Para obtener más información, consulte Protección de los datos con el cifrado del servidor en la Guía del usuario de Amazon Simple Storage Service.

- Si utiliza un AWS Snowball Edge dispositivo para importar datos y necesita transferir más datos de los que caben en un solo dispositivo Snowball Edge, cree trabajos adicionales. En cada trabajo de exportación se pueden utilizar varios dispositivos Snowball Edge.
- El límite de servicio predeterminado respecto al número de dispositivos Snowball Edge que puede tener a la vez es de 1 por cuenta y por Región de AWS. Si desea aumentar el límite de servicio o crear un trabajo de clúster, contacte con AWS Support.
- Los metadatos de los objetos transferidos a un dispositivo no se conservan. Los únicos metadatos que se conservan iguales son `filename` y `filesize`. Todos los demás metadatos se establecen como en el ejemplo siguiente:

```
-rw-rw-r-- 1 root root [filesize] Dec 31 1969 [path/filename]
```

Los límites de velocidad están activados AWS Snowball Edge

El limitador de velocidad se utiliza para controlar la velocidad de las solicitudes en un entorno de clúster de servidores.

Límite de conexiones del adaptador de S3 para Amazon Snow

El límite máximo de conexiones es de 1000 para Snowball Edge en Amazon S3. Cuando se llega al límite de 1000, cualquier conexión nueva se elimina.

Limitaciones relativas a la transferencia de datos en las instalaciones con un dispositivo Snowball Edge

Existen las siguientes limitaciones para la transferencia de datos hacia o desde un AWS Snowball Edge dispositivo local:

- Mientras se escriben los archivos, deben encontrarse en un estado estático. Los archivos que se modifican mientras se están transfiriendo no se importan a Amazon S3.
- No se admiten las tramas gigantes (jumbo frames); es decir, no se admiten las tramas de Ethernet con más de 1500 bytes de carga.

- Al seleccionar los datos que se van a exportar, tenga en cuenta que los objetos cuyo nombre contenga una barra diagonal al final (/ o \) no se transferirán. Antes de exportar cualquier objeto que lleve una barra diagonal al final, cambie su nombre para eliminarla.
- Cuando se utiliza la transferencia de datos multiparte, el tamaño máximo de cada parte es de 2 GiB.

Limitaciones relativas al envío de dispositivos Snowball Edge

Existen las siguientes limitaciones para el envío de un AWS Snowball Edge dispositivo:

- AWS no enviará un dispositivo Snowball Edge a un apartado de correos.
- AWS no enviará un dispositivo Snowball Edge entre regiones no estadounidenses, por ejemplo, de la UE (Irlanda) a la UE (Fráncfort) o a Asia Pacífico (Sídney).
- No está permitido mover un dispositivo Snowball Edge a una dirección fuera del país especificado cuando se creó el trabajo y constituye una infracción de las condiciones del AWS servicio.

Para obtener más información sobre el envío, consulte Consideraciones sobre el envío para los dispositivos Snow Family.

Limitaciones relativas al procesamiento de dispositivos Snowball Edge devueltos para su importación

Para importar los datos AWS, el dispositivo debe cumplir los siguientes requisitos:

- El AWS Snowball Edge dispositivo no debe estar comprometido. Salvo para abrir las tres puertas de la parte delantera, trasera y superior, o para añadir y sustituir el filtro de aire opcional, no abra el AWS Snowball Edge dispositivo por ningún motivo.
- El dispositivo no debe presentar daños físicos. Puede evitar daños cerrando las tres puertas del dispositivo Snowball Edge de forma que las pestañas queden bien cerradas (debe oír un sonido de clic).
- La pantalla de tinta electrónica del dispositivo Snowball Edge debe ser visible. También debe mostrar la etiqueta de devolución que se generó automáticamente cuando terminaste de transferir tus datos al AWS Snowball Edge dispositivo.

> **Note**
>
> Todos los dispositivos Snowball Edge devueltos que no cumplan estos requisitos se borrarán y no se llevará a cabo ningún trabajo con ellos.

Solución de problemas de AWS Snowball Edge

Tenga en cuenta las siguientes pautas generales a la hora de solucionar problemas.

- El tamaño de archivo máximo de los objetos en Amazon S3 es de 5 TB.
- Los objetos transferidos a un AWS Snowball Edge dispositivo tienen una longitud de clave máxima de 933 bytes. Los nombres de claves que incluyen caracteres que ocupan más de un byte también deben tener una longitud máxima de clave de 933 bytes. Al determinar la longitud de una clave, es preciso incluir tanto el archivo o nombre de objeto como su ruta o sus prefijos. Por lo tanto, un archivo cuyo nombre sea corto pero cuya ruta presente un nivel de anidación elevado puede tener una clave que supere los 933 bytes. El nombre del bucket no se contabiliza como parte de la ruta al determinar la longitud de la clave. A continuación se muestran algunos ejemplos.

Nombre del objeto	Nombre del bucket	Ruta y nombre del bucket	Longitud de clave
`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

Nombre del objeto	Nombre del bucket	Ruta y nombre del bucket	Longitud de clave
		`F$twRAjrD/fIMp/0NY`	

- Por motivos de seguridad, los trabajos con un AWS Snowball Edge dispositivo deben completarse en un plazo de 360 días a partir de su preparación. Si necesita conservar uno o más dispositivos durante más de 360 días, consulteActualización del certificado SSL. De lo contrario, una vez transcurridos 360 días, el dispositivo se bloquea, ya no se puede acceder a él y debe devolverse. Si el AWS Snowball Edge dispositivo se bloquea durante un trabajo de importación, podemos seguir transfiriendo los datos existentes en el dispositivo a Amazon S3.
- Si encuentra errores inesperados al utilizar un AWS Snowball Edge dispositivo, queremos informarnos al respecto. Copia los registros correspondientes e inclúyelos junto con una breve descripción de los problemas detectados en un mensaje AWS Support. Para obtener más información acerca de los registros, consulte Uso de los comandos del cliente Snowball Edge.

Temas

Cómo identificar su dispositivo

Utilice el comando `describe-device` para averiguar el tipo de dispositivo y, a continuación, busque el valor devuelto de `DeviceType` en la tabla siguiente a fin de determinar la configuración.

```
snowballEdge describe-device
```

Example de salida de **`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",
  "MtuSize" : "1500"
} ],
"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` y configuraciones de los dispositivos Snow Family

Valor de **`DeviceType`**	Configuración del dispositivo
`EDGE`	Snowball Edge optimizado para almacenamiento (con funcionalidad de computación de EC2)
`EDGE_C`	Snowball Edge optimizado para computación con AMD EPYC Gen1 y HDD
`EDGE_CG`	Snowball Edge optimizado para computación con AMD EPYC Gen1, HDD y GPU
`EDGE_S`	Snowball Edge optimizado para almacenamiento
`V3_5C`	Snowball Edge optimizado para computación con un procesador AMD EPYC Gen2 y NVME
`V3_5S`	Snowball Edge optimizado para almacenamiento con 210 TB

Para obtener más información sobre las configuraciones de los dispositivos Snowball Edge, consulte AWS Snowball Información sobre el hardware del dispositivo perimetral.

Solución de problemas de arranque

La siguiente información puede ayudarle a solucionar algunos problemas que pueden surgir al arrancar los dispositivos Snow Family.

- Espere 10 minutos para que el dispositivo arranque. Evite mover o usar el dispositivo durante este tiempo.
- Asegúrese de que ambos extremos del cable de alimentación estén bien conectados.
- Sustituya el cable de la fuente de alimentación por otro que sepa que funciona correctamente.
- Conecte el cable de la fuente de alimentación a otra fuente de alimentación que sepa que funciona correctamente.

Solución de problemas con la pantalla LCD durante el arranque

A veces, después de encender un dispositivo Snowball Edge, la pantalla LCD puede tener algún problema.

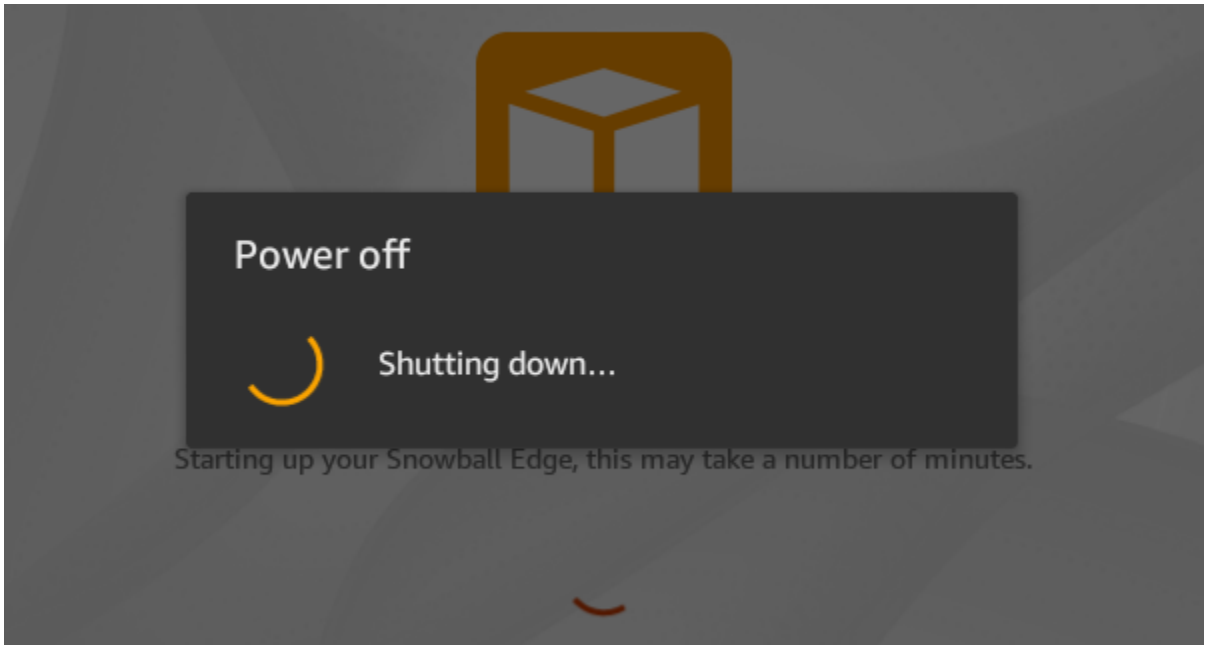
- La pantalla LCD está negra y no muestra ninguna imagen después de conectar el dispositivo Snowball Edge a la alimentación y pulsar el botón de encendido situado encima de la pantalla LCD.
- La pantalla LCD no avanza más allá de la configuración de su Snowball Edge, lo que puede tardar varios minutos. el mensaje y la pantalla de configuración de la red no aparecen.

Acción que se debe realizar cuando la pantalla LCD se ponga negra después de pulsar el botón de encendido

1. Asegúrese de que el dispositivo Snowball Edge esté conectado a una fuente de alimentación y que la fuente de alimentación esté suministrando energía.
2. Deje el dispositivo conectado a la fuente de alimentación durante 1 o 2 horas. Asegúrese de que las puertas de la parte delantera y trasera del dispositivo estén abiertas.
3. Regrese al dispositivo y la pantalla LCD estará lista para usarse.

Acción que se debe realizar cuando Snowball Edge no avanza a la pantalla de configuración de la red

1. Deje que la pantalla permanezca en el mensaje Setting you your Snowball Edge, this may take a number of minutes. durante 10 minutos.
2. En la pantalla, pulse el botón Restart display. Aparecerá el mensaje Shutting down… y, a continuación, aparecerá el mensaje Setting you your Snowball Edge, this may take a number of minutes. y el dispositivo se iniciará normalmente.



Si la pantalla LCD no avanza más allá del mensaje Setting you your Snowball Edge, this may take a number of minutes. después de utilizar el botón Restart display, siga este procedimiento.

Acción que debe ejecutarse

1. Sobre la pantalla LCD, pulse el botón de encendido para apagar el dispositivo.
2. Desconecte todos los cables del dispositivo.
3. Deje el dispositivo apagado y desconectado durante 20 minutos.
4. Conecte los cables de alimentación y de red.
5. Sobre la pantalla LCD, pulse el botón de encendido para encender el dispositivo.

Si el problema persiste, póngase en contacto con nosotros AWS Support para devolver el dispositivo y recibir un dispositivo Snowball Edge nuevo.

Solución de problemas con la pantalla de tinta electrónica durante el arranque

A veces, después de encender un dispositivo Snowball Edge, la pantalla de tinta electrónica situada en la parte superior del dispositivo puede mostrar el siguiente mensaje:

```
The appliance has timed out
```

Este mensaje no indica ningún problema con el dispositivo. Úselo normalmente y, cuando lo apague para devolverlo AWS, la información de envío de la devolución aparecerá tal y como era de esperar.

Solución de problemas de conexión

La siguiente información puede ayudarle a solucionar algunos problemas que pueden surgir con la conexión a un dispositivo Snowball Edge:

- Los routers y conmutadores que funcionan a una velocidad de 100 megabytes por segundo no funcionan con un dispositivo Snowball Edge. Le recomendamos que utilice un conmutador que funcione a una velocidad de 1 GB por segundo (o superior).
- Si se producen errores puntuales de conexión con el dispositivo, apague el dispositivo Snowball Edge, desenchufe todos los cables y espere 10 minutos. Al cabo de 10 minutos, reinicie el dispositivo y vuelva a intentar conectarlo.
- Asegúrese de que no haya software antivirus o un firewall bloqueando la conexión de red del dispositivo Snowball Edge.
- Tenga en cuenta que la interfaz de archivos y la interfaz de Amazon S3 tienen direcciones IP diferentes.

A continuación, se describen soluciones más avanzadas de problemas de conexión:

- Si no puede comunicarse con el dispositivo Snowball Edge, haga ping a la dirección IP del dispositivo. Si el ping devuelve `no connect`, confirme la dirección IP del dispositivo y la configuración de red local.
- Si la dirección IP es correcta y las luces en la parte posterior del dispositivo parpadean, utilice telnet para probar el dispositivo en los puertos 22, 9091 y 8080. La prueba del puerto 22 determina si el dispositivo Snowball Edge funciona correctamente. El puerto de prueba 9091 determina si se AWS CLI puede utilizar para enviar comandos al dispositivo. La prueba del puerto 8080 garantiza que el dispositivo pueda escribir en los buckets de Amazon S3 del dispositivo solo con el adaptador de S3. Si puede conectarse en el puerto 22, pero no en el puerto 8080, apague primero el dispositivo Snowball Edge y, a continuación, desenchufe todos los cables. Espere 10 minutos y, a continuación, vuelva a conectarlo y comience de nuevo.

Solución de problemas con los **`unlock-device`** comandos

Si el `unlock-device` comando vuelve a `connection refused` aparecer, es posible que haya escrito mal la sintaxis del comando o que la configuración del equipo o la red impida que el comando llegue al dispositivo Snow. Realice las siguientes acciones para resolver la situación:

1. Asegúrese de que el comando se haya introducido correctamente.
   a. Utilice la pantalla LCD del dispositivo para comprobar que la dirección IP utilizada en el comando es correcta.
   b. Asegúrese de que la ruta al archivo de manifiesto utilizado en el comando sea correcta, incluido el nombre del archivo.
   c. Utilice el Consola de administración de la familia de productos Snow de AWSpara comprobar que el código de desbloqueo utilizado en el comando es correcto.
2. Asegúrese de que el ordenador que está utilizando esté en la misma red y subred que el dispositivo Snow.
3. Asegúrese de que el ordenador que está utilizando y la red estén configurados para permitir el acceso al dispositivo Snow. Utilice el `ping` comando de su sistema operativo para determinar si el ordenador puede acceder al dispositivo Snow a través de la red. Compruebe las configuraciones del software antivirus, la configuración del firewall, la red privada virtual (VPN) u otras configuraciones del ordenador y la red.

Solución de problemas con los archivos de manifiesto

Cada trabajo tiene asociado un archivo de manifiesto específico. Si crea varios trabajos, debe saber a que trabajo corresponde cada manifiesto.

Si pierdes un archivo de manifiesto o si un archivo de manifiesto está dañado, puedes volver a descargar el archivo de manifiesto para un trabajo específico. Para ello AWS CLI, utilice la consola o una de las AWS API.

Solución de problemas con las credenciales

Utilice los siguientes temas como ayuda para resolver problemas de credenciales con el dispositivo Snowball Edge.

No se han podido localizar AWS CLI las credenciales

Si se está comunicando con el AWS Snowball Edge dispositivo a través de la interfaz de Amazon S3 mediante el AWS CLI, es posible que aparezca un mensaje de error que diga Unable to locate credentials. You can configure credentials by running "aws configure".

Acción que debe ejecutarse

Configure las AWS credenciales que AWS CLI utiliza para ejecutar los comandos por usted. Para obtener más información, consulte Configuración de la AWS CLI en la Guía del usuario de AWS Command Line Interface .

Mensaje de error: compruebe su clave de acceso secreta y su firma

Si utiliza la interfaz de Amazon S3 para transferir datos a un dispositivo Snowball Edge, puede que reciba el siguiente mensaje de error.

```
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
```

Acción que debe ejecutarse

Obtenga sus credenciales del cliente de Snowball Edge. Para obtener más información, consulte Obtención de credenciales.

Solución de problemas de la interfaz NFS

El dispositivo de la familia Snow puede indicar que el estado de la interfaz NFS es. `DEACTIVATED` Esto puede ocurrir si el dispositivo de la familia Snow se apagó sin detener primero la interfaz NFS.

Acción que debe ejecutarse

Para corregir el problema, detenga y reinicie el servicio NFS siguiendo estos pasos.

1. Utilice el `describe-service` comando para determinar el estado del servicio:

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

El comando devuelve lo siguiente.

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

2. Utilice el `stop-service` comando para detener el servicio NFS.

```
snowballEdge stop-service --service-id nfs
```

3. Utilice el `start-service` comando para iniciar el servicio NFS. Para obtener más información, consulte Iniciar el servicio NFS en el dispositivo de la familia Snow.

```
snowballEdge start-service  --virtual-network-interface-arns vni-arn --service-id
 nfs  --service-configuration  AllowedHosts=0.0.0.0/0
```

4. Utilice el `describe-service` comando para asegurarse de que el servicio se está ejecutando.

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

Si el valor del `State` nombre es`ACTIVE`, el servicio de interfaz NFS está activo.

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

Solución de problemas de transferencia de datos

Si surge cualquier problema de desempeño mientras transfiere datos a un dispositivo Snowball Edge o desde él, consulte Rendimiento para obtener recomendaciones y orientación sobre cómo mejorar el desempeño de transferencia. La siguiente información puede ayudarle a solucionar problemas que pudieran surgir con la transferencia de datos a un dispositivo Snowball Edge o desde él:

- No puede transferir datos al directorio raíz del dispositivo Snowball Edge. Si tiene problemas para transferir datos al dispositivo, asegúrese de no utilizar como destino un subdirectorio. Los subdirectorios de nivel superior tienen los nombres de los buckets de Amazon S3 que incluyó en el trabajo. Ponga sus datos en esos subdirectorios.
- Si utiliza Linux y no puede cargar archivos con caracteres UTF-8 a un dispositivo AWS Snowball Edge , podría deberse a que el servidor Linux no reconozca la codificación de caracteres UTF-8. Puede corregir este problema instalando el paquete `locales` en el servidor Linux y configurándolo para que utilice una de las configuraciones locales de UTF-8, como `en_US.UTF-8`. Puede configurar el paquete `locales` exportando la variable de entorno `LC_ALL`; por ejemplo, `export LC_ALL=en_US.UTF-8`.
- Si utiliza la interfaz de Amazon S3 con AWS CLI, puede trabajar con archivos o carpetas con espacios en sus nombres, como `my photo.jpg` o`My Documents`. Sin embargo, debe asegurarse de que especifica los espacios correctamente. Para obtener más información, consulte Especificación de valores de los parámetros para la AWS CLI en la Guía del usuario de AWS Command Line Interface .

Solución de AWS CLI problemas

Utilice los siguientes temas como ayuda para solucionar problemas cuando trabaja con un dispositivo AWS Snowball Edge y la AWS CLI.

AWS CLI mensaje de error: «El perfil no puede ser nulo»

Al trabajar con él AWS CLI, es posible que aparezca un mensaje de error que diga que el perfil no puede ser nulo. Puede aparecer este error si el perfil no se AWS CLI ha instalado o si no se ha configurado ningún AWS CLI perfil.

Acción que debe ejecutarse

Asegúrese de haberlo descargado y configurado AWS CLI en su estación de trabajo. Para obtener más información, consulte Instalación AWS CLI mediante el instalador incluido (Linux, macOS o Unix) en la Guía del AWS Command Line Interface usuario.

Error de puntero nulo al transferir datos con el AWS CLI

Al utilizar el AWS CLI para transferir datos, es posible que se produzca un error de puntero nulo. Este error puede producirse en las siguientes condiciones:

- Si el nombre del archivo especificado está mal escrito, por ejemplo, `flowwer.png` o `flower.npg` en lugar de `flower.png`
- Si la ruta especificada es incorrecta, por ejemplo, `C:\Doccuments\flower.png` en lugar de `C:\Documents\flower.png`
- Si el archivo está dañado

Acción que debe ejecutarse

Confirme que el nombre y la ruta del archivo son correctos e inténtelo de nuevo. Si sigue teniendo este problema, confirme que el archivo no se ha dañado, abandone la transferencia o intente reparar el archivo.

Solución de problemas con los trabajos de importación

En ocasiones, los archivos no se importan a Amazon S3. Si se presenta el siguiente problema, pruebe a realizar las acciones especificadas para resolverlo. Si se produce un error al importar un archivo, puede que deba intentar importarlo de nuevo. Para repetir la importación, es posible que se requiera un nuevo trabajo de Snowball Edge.

Se produce un error al importar archivos a Amazon S3 porque los nombres de los objetos contienen caracteres no válidos

Este problema se produce si el nombre de un archivo o de una carpeta contiene caracteres que Amazon S3 no admite. Amazon S3 tiene reglas respecto a qué caracteres pueden incluirse en los nombres de los objetos. Para obtener más información, consulte Creación de nombres de clave de objeto en la Guía del usuario de Amazon S3.

Acción que debe ejecutarse

Si detecta este problema, consulte la lista de archivos y carpetas que no se ha podido importar en el informe de finalización del trabajo.

En algunos casos, la lista es excesivamente larga o los archivos contenidos en ella son demasiado grandes para poder transferirlos a través de Internet. En estos casos, debe crear un nuevo trabajo de importación de Snowball, cambiar los nombres de los archivos y las carpetas de forma que cumplan las reglas de Amazon S3 y transferir los archivos de nuevo.

Si los archivos son pequeños y no hay una gran cantidad de ellos, puede copiarlos a Amazon S3 mediante el AWS CLI o el AWS Management Console. Para obtener más información, consulte ¿Cómo puedo cargar archivos y carpetas en un bucket de S3? en la Guía del usuario de Amazon Simple Storage Service.

Solución de problemas relacionados con los trabajos de exportación

A veces, los archivos no se exportan en la estación de trabajo. Si se presenta el siguiente problema, pruebe a realizar las acciones especificadas para resolverlo. Si se produce un error al exportar un archivo, puede que deba intentar exportarlo de nuevo. Para repetir la exportación, es posible que se requiera un nuevo trabajo de Snowball Edge.

Se ha producido un error al exportar archivos a Microsoft Windows Server

Puede producirse un error al exportar un archivo a Microsoft Windows Server si el nombre del propio archivo o de una de las carpetas relacionadas presenta un formato no compatible con Windows. Por ejemplo, si el nombre del archivo o de la carpeta contiene un signo de dos puntos (`:`), la exportación no se lleva a cabo porque Windows no permite este carácter en los nombres de los archivos y carpetas.

Acción que debe ejecutarse

1. Elabore una lista de los nombres que causan el error. Encontrará en los registros los nombres de los archivos y de las carpetas que no se han exportado. Para obtener más información, consulte AWS Snowball Edge Registros.
2. Cambie en Amazon S3 los nombres de los objetos causantes del problema para borrar o sustituir los caracteres no admitidos.
3. Si la lista de nombres es excesivamente larga o los archivos que contiene son demasiado grandes para transferirlos a través de Internet, cree un nuevo trabajo de exportación específicamente para esos objetos.

   Si los archivos son pequeños y no hay una gran cantidad de ellos, copie los objetos renombrados de Amazon S3 a través de AWS CLI o el AWS Management Console. Para obtener más información, consulte Para descargar un objeto desde un bucket de S3 en la Guía del usuario de Amazon Simple Storage Service.

Historial del documento

- Versión de la API: 1.0
- Última actualización de la documentación: 14 de marzo de 2024

En la siguiente tabla se describen los cambios importantes realizados en la Guía para desarrolladores de AWS Snowball Edge después de julio de 2018. Para obtener notificaciones sobre las actualizaciones de la documentación, puede suscribirse a la fuente RSS.

Cambio	Descripción	Fecha
Se ha dejado de usar Tape Gateway en los dispositivos Snowball Edge	La funcionalidad Tape Gateway ya no está disponible en los dispositivos Snowball Edge.	14 de marzo de 2024
Interfaz de archivos obsoleta	La interfaz de archivos ya no está disponible para la transferencia de datos.	1 de marzo de 2024
Almacenamiento compatible con Amazon S3 en dispositivos de la familia Snow disponible en dispositivos Snowball Edge de 210 TB optimizados para el almacenamiento	El almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow está disponible para el almacenamiento S3 en los dispositivos Snowball Edge de 210 TB optimizados para el almacenamiento. Para obtener más información, consulte Uso del almacenamiento compatible con Amazon S3 en los dispositivos de la familia Snow.	26 de febrero de 2024
Incluya AMI personalizadas al solicitar dispositivos	Las imágenes personalizadas de Amazon Machine ahora se	15 de noviembre de 2023

	pueden precargar al solicitar AWS Snow Family trabajos. Para obtener más informaci ón, consulte Añadir una AMI desde AWS Marketplace.	
Disponibilidad general del almacenamiento compatible con Amazon S3 en dispositi vos Snow Family	El almacenamiento compatibl e con Amazon S3 en dispositi vos Snow Family está disponible en los dispositi vos Snowball Edge optimizad os para computación. Para obtener más información, consulte Almacenamiento compatible con Amazon S3 en dispositivos Snow Family.	20 de abril de 2023
Nuevo Región de AWS compatible	AWS Snowball ahora es compatible en la región de Oriente Medio (EAU). Para obtener información acerca de los puntos de conexión de esta región, consulte Puntos de conexión y cuotas de Snowball Edge en la Referenci a general de AWS. Para obtener información acerca del envío, consulte Considera ciones sobre el envío de Snowball Edge.	6 de marzo de 2023

Nuevo Región de AWS compatible	AWS Snowball ahora es compatible en la región de Asia Pacífico (Yakarta). Para obtener información acerca de los puntos de conexión de esta región, consulte Puntos de conexión y cuotas de Snowball Edge en la Referenci a general de AWS. Para obtener información acerca del envío, consulte Considera ciones sobre el envío de Snowball Edge.	7 de septiembre de 2022
Migración de datos de gran tamaño para Snowball Edge	Snowball Edge admite ahora la automatización de un plan de migración de datos de gran tamaño. Para obtener más información, consulte Migración de datos de gran tamaño (pasos manuales) y Creación de un plan de migración de datos de gran tamaño para iniciar la automatización si lo desea.	27 de abril de 2022

Presentando AWS Snow Device Management	La gestión de dispositivos de nieve le permite gestionar su dispositivo Snowball Edge y los AWS servicios locales de forma remota. Todos los dispositivos Snowball Edge son compatibles con la administración de dispositivos de nieve y viene preinstalada en los nuevos dispositivos en la mayoría de los sitios donde está disponible Regiones de AWS Snowball Edge. Para obtener más información, consulte Uso para administrar dispositivos AWS Snow Device Management	27 de abril de 2022
Configuración de NFS para Snowball Edge	Se agregó Configuración de NFS para Snowball Edge para dispositivos optimizados para almacenamiento.	21 de abril de 2022
Límites de velocidad para Equilibrador de carga	Snowball Edge admite ahora límites de velocidad para distribuir las solicitudes en un entorno de clústeres de servidores.	19 de abril de 2022
Compatibilidad con Snowball Edge con Puerta de enlace de cinta	Ahora puede pedir un dispositivo Snowball Edge que esté configurado especialmente para alojar el servicio Puerta de enlace de cinta. Esta combinación de tecnologías facilita la migración segura de datos en cinta sin conexión.	30 de noviembre de 2021

Compatibilidad con la configuración de servidor de Network Time Protocol (NTP)	Ahora, los dispositivos Snowball Edge admiten la configuración de servidor externo de Network Time Protocol (NTP).	16 de noviembre de 2021
Compatibilidad con la transferencia de datos sin conexión de NFS	Ahora, los dispositivos Snowball Edge admiten la transferencia de datos sin conexión mediante NFS. Para obtener más información, consulte Uso de NFS para la transferencia de datos sin conexión.	4 de agosto de 2021
Nuevo Región de AWS compatible	Los dispositivos Snowball Edge ya están disponibles en África (Ciudad del Cabo). Región de AWS Para obtener más información, consulte Puntos de conexión y cuotas de Snowball Edge en la Referencia general de AWS. Para obtener información acerca del envío, consulte Consideraciones sobre el envío de Snowball Edge.	23 de noviembre de 2020

Posibilidad de importar su propia imagen a su dispositivo	Ahora puede importar una instantánea de la imagen al dispositivo Snowball Edge y registrarla como una Imagen de máquina de Amazon (AMI) compatible con Amazon EC2. Para obtener más información, consulte Importación de una imagen a su dispositivo como una AMI de Amazon EC2.	9 de noviembre de 2020
Nuevo compatible Región de AWS	Los dispositivos Snowball Edge ya están disponibles en Europa (Milán). Región de AWS Para obtener más información, consulte Puntos de conexión y cuotas de Snowball Edge en la Referenci a general de AWS. Para obtener información acerca del envío, consulte Considera ciones sobre el envío de Snowball Edge.	30 de septiembre de 2020
Reestructuración del contenido	Creé una sección de introducc ión que se ajusta al Consola de administración de la familia de productos Snow de AWS flujo de trabajo y actualizé otras secciones para mayor claridad. Para obtener más información, consulte Introducción a los dispositivos AWS Snowball Edge.	17 de septiembre de 2020

Presentamos AWS OpsHub for Snow Family	Los dispositivos de la familia Snow ahora ofrecen una herramienta fácil de usar que puede usar para administr ar sus dispositivos y AWS servicios locales. AWS OpsHub for Snow Family Para obtener más información, consulte Uso AWS OpsHub for Snow Family para gestionar dispositivos Snowball.	16 de abril de 2020
AWS Identity and Access Management (IAM) ahora está disponible localmente en el dispositivo AWS Snowball Edge	Ahora puede usar AWS Identity and Access Management (IAM) para controlar de forma segura el acceso a AWS los recursos que se ejecutan en su AWS Snowball Edge dispositivo. Para obtener más información, consulte Uso local de IAM.	16 de abril de 2020
Introducción de una nueva opción de dispositivo Snowball Edge optimizado para almacenamiento (para transferencia de datos)	Snowball cuenta ahora con un nuevo dispositivo optimizad o para almacenamiento que está basado en los actuales dispositivos optimizados para computación y con GPU. Para obtener más información, consulte Opciones de dispositi vo Snowball Edge.	23 de marzo de 2020

Compatibilidad con la validación de etiquetas por NFC	Los dispositivos Snowball Edge optimizados para computación (con o sin GPU) tienen etiquetas NFC integradas. Puedes escanear estas etiquetas con la aplicación AWS Snowball Edge Verification, disponible en Android. Para obtener más información, consulte Validación de etiquetas por NFC.	13 de diciembre de 2018
Los grupos de seguridad ya están disponibles para las instancias de computación	Los grupos de seguridad de los dispositivos Snowball Edge son similares a los grupos de seguridad de la Nube de AWS, salvo por algunas pequeñas diferencias. Para obtener más información consulte Grupos de seguridad en dispositivos Snowball Edge.	26 de noviembre de 2018
Introducción de la actualización en las instalaciones	Ahora, puede actualizar el software que hace que un dispositivo Snowball Edge se ejecute en el entorno local. Tenga en cuenta que las actualizaciones en las instalaciones requieren una conexión a Internet. Para obtener más información, consulte Actualización de un dispositivo Snowball Edge.	26 de noviembre de 2018

Introducción de nuevas opciones de dispositivo Snowball Edge	Existen tres opciones de dispositivo Snowball Edge: optimizados para almacenamiento, optimizados para computación y con GPU. Para obtener más información, consulte Opciones de dispositivo Snowball Edge.	15 de noviembre de 2018
Nuevo Región de AWS compatible	Los dispositivos Snowball Edge están disponibles ahora en la región de Asia-Pacífico (Bombay). Tenga en cuenta que las instancias de cómputo y las que AWS Lambda funcionan con tecnología no AWS IoT Greengrass son compatibles en esta región.	24 de septiembre de 2018
Introducción de la posibilidad de usar instancias de computación compatibles con Amazon EC2 en dispositivos Snowball Edge	AWS Snowball ahora admite trabajos locales mediante instancias informáticas de Amazon EC2 que se ejecutan en dispositivos Snowball Edge.	17 de julio de 2018
Mejoras del contenido de solución de problemas	El capítulo de solución de problemas se ha actualizado y reorganizado.	11 de julio de 2018

AWS Glosario

Para obtener la AWS terminología más reciente, consulte el AWS glosario de la Glosario de AWS Referencia.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.