AWS Snowcone

AWS Snowcone Guía del usuario

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

AWS Snowcone Guía del usuario: AWS Snowcone

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

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es AWS Snowcone? ... 1
Casos de uso ... 2
Precios ... 3
Cómo AWS Snowcone funciona ... 4
AWS Snowcone flujo de trabajo ... 5
Funcionamiento de los trabajos de importación ... 7
Transferencia de datos en línea entre Snowcone y AWS Storage Services con DataSync ... 7
Transferencia de datos sin conexión entre Snowcone y Amazon S3 ... 8
Almacenamiento de trabajos de importación ... 8
Almacenamiento de trabajos de computación ... 9
Especificaciones de los dispositivos ... 10
Resumen ... 10
Hardware y red ... 12
Vista superior ... 12
Panel posterior ... 12
Panel frontal ... 13
AWS Snowcone Especificaciones de Wi-Fi ... 14
Especificaciones de robustez ... 15
Fuente de alimentación y accesorios de los dispositivos Snowcone ... 15
Rendimiento del disco y la CPU ... 16
Configuración ... 17
Inscríbase en AWS ... 17
Antes de realizar el pedido ... 18
Acerca del entorno local ... 18
Trabajo con caracteres especiales ... 19
Amazon EC2 ... 20
Diferencia entre las instancias de Amazon EC2 y las instancias compatibles con Amazon EC2 en dispositivos Snow Family ... 21
Precios de las instancias de computación en Snowcone ... 21
Requisitos previos ... 21
Compruebe los códigos de producto y los detalles de la plataforma de las AMI AWS Marketplace ... 22
Creación de una AMI de Linux desde una instancia ... 24
Creación de una AMI de Linux a partir de una instantánea ... 24

Introducción 28
Crear un trabajo para pedir un dispositivo de la familia Snow 28
Paso 1: elija un tipo de trabajo 29
Paso 2: elija las opciones de computación y almacenamiento 30
Paso 3: elija las características y opciones que desee 33
Paso 4: elija las preferencias de seguridad, envío y notificación 33
Paso 5: revise el resumen del trabajo y cree el trabajo 36
Descarga AWS OpsHub 37
Cancelar un trabajo para solicitar un dispositivo de la familia Snow 38
Obtener credenciales para acceder a un dispositivo de la familia Snow 39
Desbloquear el dispositivo de la familia Snow 40
Solución de problemas al desbloquear un dispositivo de la familia Snow 42
Reinicio del dispositivo Snow Family 42
Uso AWS OpsHub para administrar dispositivos 47
Descarga AWS OpsHub para dispositivos de la familia Snow 48
Desbloqueo de un dispositivo 49
Desbloqueo de un dispositivo de forma local 49
Desbloqueo de un dispositivo de forma remota 52
Verificar la firma de AWS OpsHub 56
Administrar AWS los servicios 59
Uso local de instancias de computación 60
Administración de la interfaz NFS 68
Se utiliza AWS DataSync para transferir archivos a AWS 77
Transferir archivos 78
Administración de sus dispositivos 79
Reinicio del dispositivo 79
Apagado del dispositivo 80
Edición del alias del dispositivo 81
Obtención de actualizaciones 82
Administración de perfiles 83
Configuración de los servidores de tiempo NTP del dispositivo 85
Uso del AWS Snowball Edge cliente 88
Descarga e instalación del cliente de Snowball Edge 88
Comandos para el cliente de Snowball Edge 88
Configuración de un perfil para el cliente de Snowball Edge 90
Obtención del código QR para validación por NFC 91

Desbloquear un dispositivo AWS Snowcone 91
Actualización de un dispositivo Snowcone 92
Obtención de credenciales 95
Inicio de un servicio en su dispositivo Snowcone 96
Detención de un servicio en su dispositivo Snowcone 97
Obtención de su certificado para la transferencia de datos 97
AWS Snowcone Registros 98
Obtención del estado de los dispositivos 100
Obtención del estado de los servicios 102
Lanzamiento de la AWS DataSync AMI 103
Inicio de NFS y restricción del acceso 106
Restricción del acceso a recursos compartidos de NFS cuando NFS está en ejecución 107
Obtención de la ruta de exportación de un bucket de Amazon S3 108
Habilitar la depuración por AWS parte del operador local 108
Desactivación de la depuración por parte de operadores locales AWS 108
Creación de una interfaz de red directa 109
Obtención de información sobre una interfaz de red directa 109
Actualización de una interfaz de red directa 109
Eliminación de una interfaz de red directa 110
Comprobación del estado de las características 110
Cambio del estado de las características 111
Configuración de servidores de tiempo 112
Comprobación de las fuentes de tiempo 113
Uso de Snow Device Management para administrar dispositivos 115
Elegir el estado de administración de dispositivos Snow al solicitar un dispositivo de la familia Snow 116
Activación de Snow Device Management 117
Añadir permisos para Snow Device Management a una función de IAM 118
Comandos de la CLI de Snow Device Management 119
Creación de una tarea 120
Comprobación del estado de la tarea 121
Comprobación de la información del dispositivo 122
Comprobación del estado de la instancia compatible con Amazon EC2 124
Comprobación de los metadatos de una tarea 126
Cancelación de una tarea 127
Obtención de una lista de comandos y sintaxis 128

Obtención de una lista de los dispositivos que se pueden administrar de forma remota 129
Obtención de una lista del estado de las tareas en distintos dispositivos 130
Obtención de una lista de los recursos disponibles 131
Obtención de una lista de las etiquetas de un dispositivo o de una tarea 132
Obtención de una lista de tareas por estado 133
Aplicación de etiquetas 134
Eliminación de etiquetas 135
Uso de AWS los servicios 136
Uso de Amazon EC2 para computación 136
Información general 137
Requisitos previos 138
Creación de un trabajo con instancias de computación 139
Configuración de red para instancias de computación 144
Conexión a las instancias de computación de un dispositivo Snowcone mediante SSH 151
Comandos del cliente de Snowcone para instancias de computación 151
Uso del Servicio de metadatos de instancias para Snow con instancias compatibles con Amazon EC2 157
Uso del punto de conexión compatible con Amazon EC2 167
Inicio automático de instancias compatibles con Amazon EC2 con plantillas de lanzamiento 184
Uso del almacenamiento en bloques con sus instancias compatibles con EC2 186
Grupos de seguridad en dispositivos Snow 187
Datos de usuario y metadatos de instancia admitidos 188
Solución de problemas de Amazon EC2 191
DataSync Utilización para transferir archivos 192
Administración de la interfaz NFS 194
Configuración de NFS para los dispositivos Snow Family 195
Uso AWS IoT Greengrass en instancias compatibles con EC2 200
Configuración de la instancia compatible con Amazon EC2 200
Puertos necesarios para usar AWS los servicios 203
Devolución del dispositivo Snowcone 204
Desconexión del dispositivo Snowcone 204
Protección de los datos de su dispositivo 206
Protegiendo su AWS Snowcone 206
Validación de etiquetas NFC 207
Explicación de los estados de los trabajos 209

Notificaciones 211
Cómo Snow utiliza Amazon SNS 211
Cifrado de los temas de SNS para los cambios de estado de los trabajos de Snow 211
Configuración de una política de claves de KMS administradas por el cliente 212
Ejemplos de notificación de SNS 214
Descripción del proceso de pedido 227
Descripción del proceso de envío 227
Devolución de un dispositivo Snowcone 227
Usando el AWS Management Console 228
Pedido del dispositivo Snowcone desde la consola 228
Uso de las API de administración de trabajos 228
Usos comunes de JMAPI 228
Cadenas obligatorias de JMAPI 229
Puntos de conexión de MAPI 229
Comandos de la CLI de JMAPI 229
Ejemplos 230
Trabajos de EC2 232
Configuración de una AMI de forma que utilice SSH para conectarse a instancias de computación lanzadas en el dispositivo 232
Creación de un trabajo en la consola 233
Creación de un trabajo en la CLI de AWS 233
Consideraciones de envío 235
Preparar un AWS Snowcone dispositivo para su envío 235
Restricciones de envío en función de la región 236
Envío de un AWS Snowcone dispositivo 237
Transportistas 237
Actualización de dispositivos Snowcone 246
Requisitos previos 247
Descarga de actualizaciones 247
Instalación de actualizaciones 249
Actualización del certificado SSL 253
Actualización de las AMI de Amazon Linux 2 en los dispositivos Snow Family 254
Prácticas recomendadas 255
Seguridad 255
Network 256
Administración de recursos 256

Administración de instancias compatibles con EC2 256
Rendimiento 257
Cuotas de Snowcone 258
Cuotas de recursos de computación 258
Limitaciones para el envío de un dispositivo Snowcone 259
Limitaciones relativas al procesamiento de dispositivos Snowcone devueltos para importación 260
Disponible Regiones de AWS 260
Resolución de problemas 261
Solución de problemas de las instancias de computación 261
Problemas de red 261
La dirección IP es 0.0.0.0 261
No se puede desbloquear el dispositivo 262
Problemas con una instancia compatible con EC2 en Datasync 262
Error: no se pudo lanzar la instancia 262
Problemas de transferencia de datos 262
Acceso denegado por el servidor 262
La conexión agota el tiempo de espera durante la transferencia de datos 263
Spawn Showmount ENOENT 263
Solución de problemas con la devolución de dispositivos Snow Family 264
Referencia de la API 265
Historial de documentos 266
AWS Glosario 272
..... cclxxiii

¿Qué es AWS Snowcone?

AWS Snowcone es un dispositivo portátil, robusto y seguro para la computación periférica y la transferencia de datos. Puede utilizar un dispositivo Snowcone para recopilar, procesar y mover datos al Nube de AWS, ya sea sin conexión (enviando el dispositivo a AWS) o en línea (utilizando). AWS DataSync

Puede resultar difícil ejecutar aplicaciones en entornos periféricos austeros (que no sean centros de datos) o en los que no haya una conectividad de red uniforme. Estas ubicaciones suelen carecer del espacio, la alimentación y la refrigeración necesarios para los equipos de TI de los centros de datos.

Hay dos tipos de dispositivos Snowcone:

- Snowcone: Snowcone tiene dos vCPU, 4 GB de memoria y 8 TB de almacenamiento en disco duro (HDD).
- Snowcone SSD: Snowcone SSD tiene dos vCPU, 4 GB de memoria y 14 TB de almacenamiento en unidades de estado sólido (SSD).

Con dos CPU y varios terabytes de almacenamiento, un dispositivo Snowcone puede ejecutar cargas de trabajo de computación periférica que utilizan instancias de Amazon Elastic Compute Cloud (Amazon EC2) y almacenar datos de forma segura.

Los dispositivos Snowcone son pequeños (8,94» x 5,85» x 3,25» /227 mm x 148,6 mm x 82,65 mm), por lo que se pueden colocar junto a la maquinaria de una fábrica para recopilar, formatear y transportar datos para su almacenamiento y análisis. AWS Un dispositivo Snowcone pesa alrededor de 2 kg (4,5 libras), por lo que se puede llevar en una mochila, usar con batería y utilizar la interfaz wifi para recopilar datos de sensores.

> **Note**
>
> El Wi-Fi solo está disponible en Norteamérica. Regiones de AWS

Los dispositivos Snowcone ofrecen una interfaz compatible con el sistema de archivos de red (NFS). Los dispositivos Snowcone permiten transferir datos de servidores Windows, Linux y macOS en las instalaciones y aplicaciones basadas en archivos a través de la interfaz NFS.

Por ejemplo AWS Snowball, AWS Snowcone tiene múltiples capas de capacidades de cifrado de seguridad. Puede utilizar cualquiera de estos servicios para recopilar, procesar y transferir datos y ejecutar cargas de trabajo de edge computing que utilizan instancias compatibles con Amazon EC2. AWS Snowcone está diseñado para satisfacer necesidades de migración de datos de hasta varias docenas de terabytes. Se puede utilizar en entornos con limitaciones de espacio en los que no caben los dispositivos Snowball Edge.

Casos de uso

Puede usar los AWS Snowcone dispositivos para los siguientes casos de uso:

- En el caso de las aplicaciones de computación periférica, para recopilar datos, procesarlos para obtener información inmediata y, a continuación, transferirlos en línea a AWS.
- Para transferir los datos que generan continuamente los sensores o las máquinas en línea a AWS una fábrica o a otros lugares periféricos.
- Para distribuir contenido multimedia, científico o de otro tipo procedente de los servicios de AWS almacenamiento a sus socios y clientes.
- Para agregar contenido mediante la transferencia de contenido multimedia, científico o de otro tipo desde sus ubicaciones periféricas a AWS.
- Para los escenarios de migración de datos únicos en los que los datos están listos para ser transferidos, Snowcone ofrece una forma rápida y económica de transferir hasta 8 TB o 14 TB de datos al dispositivo devolviendo el dispositivo a. Nube de AWS AWS

Para despliegues móviles, un dispositivo Snowcone puede funcionar con una batería determinada. Para una carga de trabajo ligera con un 25 % de uso de la CPU, el dispositivo puede funcionar con batería durante aproximadamente 6 horas. Puede utilizar la interfaz wifi del dispositivo Snowcone para recopilar datos de sensores inalámbricos. Un AWS Snowcone dispositivo es de bajo consumo, portátil, liviano y resistente a las vibraciones, por lo que puede usarlo en una amplia variedad de ubicaciones remotas y austeras.

> **Note**
>
> El Wi-Fi solo está disponible Regiones de AWS en Norteamérica.

Precios

Puede pedir un dispositivo Snowcone pagando por su uso y conservarlo durante un máximo de cuatro años. Para obtener información sobre AWS Snowcone los precios y las tarifas, consulta AWS Snowcone los precios.

Cómo AWS Snowcone funciona

AWS Snowcone es un dispositivo portátil que se utiliza para la computación periférica y la transferencia de datos. Para empezar, debe solicitar uno o más dispositivos Snowcone en AWS Management Console función de la cantidad de datos que necesite transferir y del rendimiento informático requerido. Los buckets de Amazon Simple Storage Service (Amazon S3), los datos y las imágenes de máquina de Amazon (AMI) de Amazon Elastic Compute Cloud (Amazon EC2) que elija se configuran, cifran y preinstalan automáticamente en sus dispositivos. El AWS DataSync agente también viene preinstalado antes de que se le envíen los dispositivos.

Cuando llegue el dispositivo, debe conectarlo a la red en las instalaciones y configurar la dirección IP de forma manual o automática con el Protocolo de configuración dinámica de host (DHCP). Debe descargar e instalar AWS OpsHub for Snow Family una aplicación de interfaz gráfica de usuario (GUI) para administrar su dispositivo Snowcone. Puede instalarla en cualquier equipo cliente Windows o macOS, como un portátil.

Al abrir AWS OpsHub y desbloquear el dispositivo, verá un panel de control en el que se muestran las métricas del dispositivo y del sistema. A continuación, puede lanzar instancias para implementar sus aplicaciones periféricas o migrar sus datos al dispositivo con tan solo unos clics en AWS OpsHub.

Cuando haya completado su trabajo de procesamiento o transferencia de datos y el dispositivo esté listo para su devolución, la etiqueta de envío de tinta electrónica actualiza automáticamente la dirección de devolución, lo que garantiza que el dispositivo Snowcone se entregue en la instalación correcta AWS . Cuando el dispositivo se envía, puede recibir el estado de seguimiento a través de mensajes enviados por Amazon Simple Notification Service (Amazon SNS), mensajes de texto y correos electrónicos generados o directamente desde la consola.

Temas

- AWS Snowcone flujo de trabajo
- Funcionamiento de los trabajos de importación
- Almacenamiento de trabajos de importación
- Almacenamiento de trabajos de computación

AWS Snowcone flujo de trabajo

Puede crear tres tipos de trabajo diferentes. Si bien los tipos de trabajo difieren en sus casos de uso, todos tienen el siguiente flujo de trabajo para pedir, recibir y devolver el dispositivo.

El flujo de trabajo

1. Creación del trabajo: debe crear cada trabajo en la Consola de administración de la familia de productos Snow de AWS o mediante programación a través de API de administración de trabajos y elegir un tipo de dispositivo, Snowcone o Snowcone SSD según su caso de uso. Puede realizar un seguimiento del estado del trabajo en la API de Snowcone AWS Management Console o a través de ella.
2. Un dispositivo está preparado para su trabajo: AWS prepara un AWS Snowcone dispositivo para su trabajo y el estado de su trabajo cambia a Preparando Snowcone.
3. Envío de un dispositivo a través del transportista de la región: el transportista se hace cargo a partir de este punto y el estado del trabajo cambia ahora a En tránsito hacia usted. Puedes encontrar tu número de seguimiento y un enlace al sitio web de seguimiento en la Consola de administración de la familia de productos Snow de AWS consola o en la API de gestión de trabajos. Para obtener información acerca del transportista de su región, consulte Consideraciones de envío para AWS Snowcone.
4. Obtención de una fuente de alimentación Snowcone: para mantener el tamaño más reducido posible, los dispositivos Snowcone no vienen con fuente de alimentación. Snowcone utiliza una fuente de alimentación conectada por USB-C de 45 vatios. También se puede alimentar con una batería portátil. Para obtener más información, consulte AWS Snowcone Fuente de alimentación y accesorios.
5. Recibe el dispositivo: unos días después, la empresa de transporte de tu región entrega el AWS Snowcone dispositivo a la dirección que indicaste al crear el trabajo. El estado de su trabajo cambia a Entregado a usted. El dispositivo no viene en una caja porque es su propio contenedor de transporte.
6. Obtenga sus credenciales y descargue el AWS OpsHub cliente Snowball Edge para la aplicación Snow Family. Prepárese para empezar a transferir datos obteniendo sus credenciales, su lista de trabajo y el código de desbloqueo del manifiesto y, a continuación, descargando el cliente Snowball Edge.
   - Puede obtener el manifiesto del dispositivo en la consola o mediante la API de administración de trabajos una vez que el dispositivo se encuentre en las instalaciones. El manifiesto se utiliza

para autenticar su acceso al dispositivo. El manifiesto está cifrado para que solamente lo pueda descifrar el código de desbloqueo.

- 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. Para evitar el acceso no autorizado al dispositivo mientras esté en las instalaciones, te recomendamos que guarde el código de desbloqueo en un lugar seguro que no sea el que aparece en el manifiesto.
- AWS OpsHub for Snow Family es una aplicación para gestionar los dispositivos de la familia Snow, incluido Snowcone. La GUI de AWS OpsHub for Snow Family le ayuda a configurar y administrar dispositivos Snowcone para que pueda ejecutar rápidamente sus cargas de trabajo de computación periférica y migrar datos a la Nube de AWS. Con solo unos pocos clics, puede utilizar AWS OpsHub para desbloquear y configurar su dispositivo Snowcone, arrastrar y soltar datos, iniciar aplicaciones o supervisar las métricas del dispositivo. Puede descargarlo e instalarlo en máquinas cliente Windows o macOS, como un portátil. El uso de AWS OpsHub no supone costo alguno.

  Descarga AWS OpsHub desde los AWS Snowball recursos. Para obtener más información al respecto AWS OpsHub, consulteUso AWS OpsHub for Snow Family para administrar dispositivos.
- 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.

7. Colocación del hardware: lleve el dispositivo al centro de datos y ábralo siguiendo las instrucciones de la carcasa. Conecte el dispositivo a una fuente de alimentación y a la red local.
8. Encendido el dispositivo: encienda el dispositivo pulsando el botón de encendido situado encima de la pantalla LCD. Espere unos minutos y aparecerá la pantalla Ready.
9. Obtención de la dirección IP del dispositivo: la pantalla LCD contiene la pestaña CONNECTION. Pulse esta pestaña y obtenga la dirección IP del AWS Snowcone dispositivo.
10. Se utiliza AWS OpsHub para desbloquear el dispositivo: para desbloquear el AWS Snowcone dispositivo, se introduce la dirección IP del dispositivo, se carga el manifiesto y el código de desbloqueo. AWS OpsHub descifra el manifiesto y lo usa para autenticar tu acceso al dispositivo. Para obtener más información al respecto AWS OpsHub, consulte. Uso AWS OpsHub for Snow Family para administrar dispositivos
11. Use el dispositivo: AWS OpsHub utilícelo para configurar y administrar AWS Snowcone dispositivos, de modo que pueda ejecutar rápidamente sus cargas de trabajo de computación perimetral y transferir datos al Nube de AWS. Con solo unos pocos clics, puede utilizar AWS

OpsHub para desbloquear y configurar su dispositivo Snowcone, arrastrar y soltar datos, iniciar aplicaciones o supervisar las métricas del dispositivo. Para obtener más detalles, consulte Uso AWS OpsHub for Snow Family para administrar dispositivos.

12 No desenchufe los cables Ethernet o de alimentación: no desenchufe el cable Ethernet, la fuente de alimentación USB-C o la batería durante la transferencia de datos o las operaciones de computación. Para apagar el dispositivo Snowcone una vez finalizada la transferencia de datos o el trabajo de computación, pulse el botón de encendido.

13 Prepare el dispositivo para el viaje de vuelta: cuando haya terminado de colocar el dispositivo en sus instalaciones, pulse el botón de encendido situado sobre la pantalla LCD para apagar el dispositivo. Desenchufe el dispositivo y guarde sus cables de alimentación en el soporte situado en la parte superior. A continuación, cierre las tres puertas del dispositivo. El dispositivo está listo para su devolución.

14 El operador de tu región devuelve el dispositivo AWS: cuando el transportista tiene el AWS Snowcone dispositivo, el estado del trabajo cambia a En tránsito a AWS.

Funcionamiento de los trabajos de importación

Puede utilizar Snowcone para transferir datos en línea entre su dispositivo y los servicios AWS de almacenamiento mediante. AWS DataSync También puede transferir datos sin conexión desde los dispositivos de almacenamiento en las instalaciones a su dispositivo Snowcone.

Transferencia de datos en línea entre Snowcone y AWS Storage Services con DataSync

AWS DataSynces un servicio de transferencia de datos en línea que simplifica, automatiza y acelera la copia de grandes cantidades de datos hacia y desde los servicios de AWS almacenamiento a través de Internet o. AWS Direct Connect El dispositivo Snowcone tiene preinstalado un AWS DataSync agente que se utiliza para transferir datos entre el dispositivo y los buckets de Amazon S3, los sistemas de archivos Amazon Elastic File System (Amazon EFS) y Amazon FSx for Windows File Server. DataSync gestiona automáticamente los archivos y objetos en movimiento, programa las transferencias de datos, supervisa el progreso de las transferencias, cifra los datos, verifica las transferencias de datos y notifica a los clientes cualquier problema.

El DataSync agente viene preinstalado en el dispositivo Snowcone como Amazon Machine Image (AMI) durante la preparación del trabajo en Snowcone. Para transferir datos en línea AWS, conecte el dispositivo Snowcone a la red externa y utilice AWS OpsHub for Snow Family o AWS Command

Line Interface (AWS CLI) para iniciar la DataSync AMI del agente. Active el DataSync agente mediante el AWS Management Console o el AWS CLI. A continuación, configure la tarea de transferencia de datos en línea entre el almacén del AWS Snowcone Network File System (NFS) y Amazon S3, Amazon EFS o Amazon FSx.

Puedes usar la opción de DataSync correr en Snowcone para lo siguiente:

- En el caso de las aplicaciones de computación periférica, para recopilar datos, procesarlos para obtener información inmediata y, a continuación, transferirlos en línea a AWS.
- Para transferir a AWS los datos que generan continuamente los sensores o las máquinas en línea de una fábrica o de otras ubicaciones periféricas.
- Para distribuir contenido multimedia, científico o de otro tipo en línea desde los servicios de AWS almacenamiento a sus socios y clientes.
- Para agregar contenido mediante la transferencia de contenido multimedia, científico o de otro tipo en línea desde sus ubicaciones periféricas a AWS.

Para flujos de trabajo únicos de procesamiento perimetral o transferencia de datos o para flujos de trabajo de Snowcone en ubicaciones perimetrales sin un enlace de red de área amplia (WAN) o un ancho de banda WAN inadecuado, recomendamos devolver el dispositivo Snowcone AWS a donde se complete la transferencia de datos.

Transferencia de datos sin conexión entre Snowcone y Amazon S3

Para los trabajos de importación de datos sin conexión, debe conectar el dispositivo Snowcone a la red local y, a continuación, utilizarlo AWS OpsHub para desbloquear el dispositivo. AWS OpsHub Descárguelo desde la página de AWS Snowball recursos. Puede copiar datos de los dispositivos de almacenamiento locales a su dispositivo Snowcone a través de la interfaz NFS. Tras copiar los datos en el dispositivo Snowcone, la etiqueta de envío de tinta electrónica del dispositivo garantiza que el dispositivo se envía automáticamente a la instalación correcta AWS . Puede hacer un seguimiento del dispositivo Snowcone mediante mensajes de texto o correos electrónicos generados por Amazon SNS y la consola.

Almacenamiento de trabajos de importación

Internamente, un dispositivo Snowcone contiene 8 TB o 14 TB de almacenamiento en disco que se puede utilizar con el servicio interno de Sistema de archivos de red (NFS) o con instancias locales compatibles con Amazon EC2 mediante una presentación del volumen local de Amazon Elastic

Block Store (Amazon EBS). Puede utilizar 8 TB o 14 TB para el volumen de almacenamiento de NFS y 150 GB para el volumen de almacenamiento de Amazon EBS en disco duro con capacidad optimizada (`sbg1`).

Almacenamiento de trabajos de computación

Si el tipo de trabajo es computación local, puede crear un total de 8 TB o 14 TB de volúmenes de Amazon EBS de disco duro local con capacidad optimizada (`sbg1`) y adjuntarlos a instancias compatibles con Amazon EC2. El uso de volúmenes de Amazon EBS permite que las instancias locales compatibles con Amazon EC2 obtengan acceso a más capacidad local que el volumen raíz por sí solo. Como se trata únicamente de almacenamiento local, los datos escritos en los volúmenes de Amazon EBS se pierden cuando se devuelve el dispositivo, AWS ya que no se pueden importar a Amazon S3.

> **Note**
>
> El servidor de NFS no está disponible para trabajos de computación. Si necesita importar o exportar datos hacia o desde un agente Nube de AWS o para ejecutar un AWS DataSync agente, no elija el tipo de trabajo informático local al realizar el pedido.

AWS Snowcone Especificaciones del dispositivo

En esta sección se proporciona información sobre las especificaciones y los requisitos del AWS Snowcone dispositivo en cuanto al hardware, la red, la red Wi-Fi y la fuente de alimentación.

Temas

- Resumen de características y especificaciones
- Hardware y red
- AWS Snowcone Especificaciones de Wi-Fi
- Especificaciones de robustez
- AWS Snowcone Fuente de alimentación y accesorios
- Rendimiento del disco y la CPU

Resumen de características y especificaciones

En la tabla siguiente se resumen las características y especificaciones del dispositivo Snowcone.

Elemento	Especificación
Situación de uso	Internet industrial de las cosas (IoT), transporte, IoT para el sector de sanidad, distribución de contenido, computación periférica táctica, logística, vehículo autónomo, migración de datos
Tamaño del dispositivo	9 pulgadas de largo, 6 pulgadas de ancho y 3 pulgadas de alto (227 mm x 148,6 mm x 82,65 mm)
Peso del dispositivo	2,04 kg (4,5 libras) para Snowcone y SSD Snowcone de 4,6 libras (2,09 kg)
Capacidad de almacenamiento	8 TB utilizables para Snowcone y 14 TB utilizables para Snowcone SSD
Opciones de computación incorporada	Imágenes de máquina de Amazon (AMI) de Amazon EC2

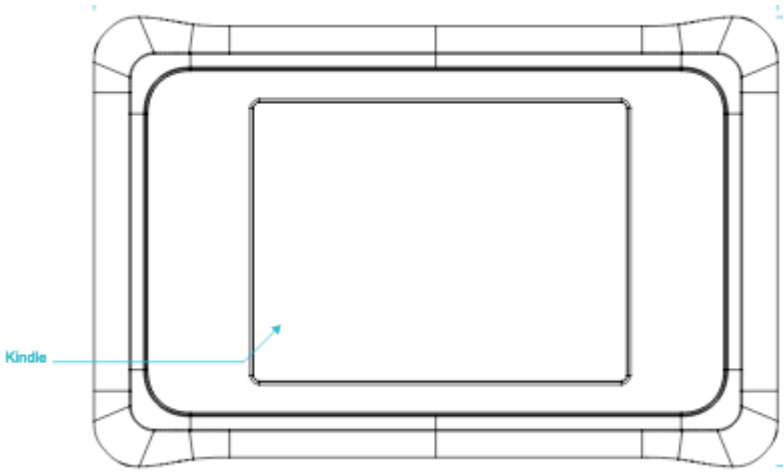
Elemento	Especificación
Cifrado	Sí, 256 bits
Transferencias a través del Sistema de archivos de red (NFS)	Sí
Transferencias mediante la API de Amazon S3	No
Portabilidad	Funcionamiento a batería
Red inalámbrica	Wifi **Note** La conexión inalámbrica solo está disponible en Regiones de AWS Norteamérica.
Cantidad de vCPU utilizables	2 vCPU
Memoria disponible	4 GB
Interfaces de red	2 x 1/10 gigabit (Gb): RJ45
AWS DataSync agente preinstalado	Sí
Duración típica de un trabajo	Transferencia de datos en línea o sin conexión: de días a semanas Computación periférica: de semanas a meses
Duración máxima del trabajo	Computación periférica o transferencia de datos continua: hasta 360 días

Hardware y red

Un dispositivo Snowcone proporciona 8 TB o 14 TB de almacenamiento disponible. Ejecuta instancias específicas de Amazon Elastic Compute Cloud (Amazon EC2) con dos CPU disponibles y 4 GB de memoria disponible para respaldar sus aplicaciones y funciones. AWS IoT Greengrass En esta sección, puede encontrar información sobre el dispositivo físico, como las interfaces, el botón de encendido y los requisitos de alimentación, tal como aparecen en las distintas vistas del dispositivo.

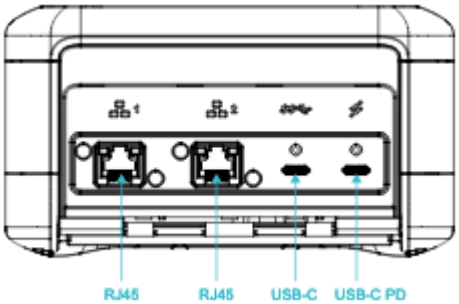
Vista superior

La superficie superior del dispositivo Snowcone incluye una pantalla táctil integrada de tinta electrónica que se utiliza como interfaz de operador para configurar redes por cable e inalámbricas. También muestra una etiqueta de envío electrónica. La etiqueta de envío electrónica está preprogramada con etiquetas de envío entrantes y salientes que cambian automáticamente después de encender el dispositivo por primera vez.



Panel posterior

Todas las conexiones de cables se realizan en el panel posterior. En esta sección se describe cada uno de los conectores.



Alimentación

La alimentación se suministra al dispositivo a través de la conexión USB-C situada más a la derecha mediante un adaptador de alimentación adecuado que pueda suministrar al menos 45 W.

> **Note**
>
> AWS Snowcone no incluye fuente de alimentación porque se entrega con el factor de forma más pequeño posible. Para obtener más detalles, consulte AWS Snowcone Fuente de alimentación y accesorios.

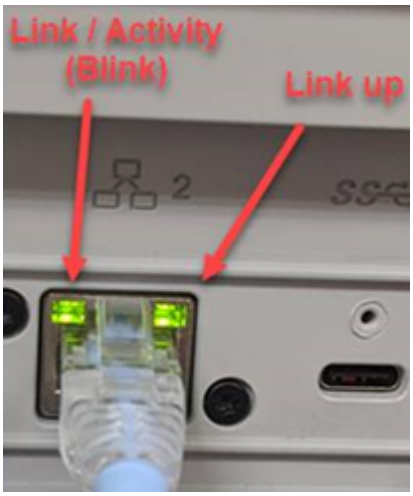
USB

La primera conexión USB-C no está activa.

Conectores Ethernet 1 y 2

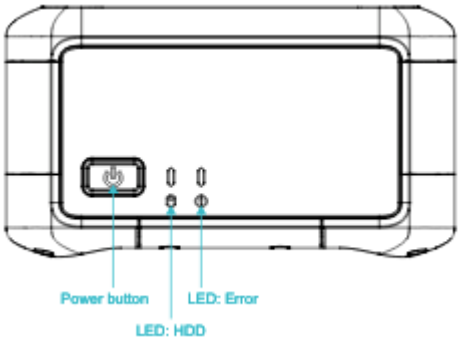
En las redes por cable, el dispositivo Snowcone proporciona dos puertos que negocian automáticamente para las redes Ethernet de 1 gigabit (Gb) o 10 Gb.

Puertos Ethernet RJ45 10/1G Base-T: estos puertos negocian automáticamente entre 10 Gb y 1 Gb según la capacidad de conexión del extremo lejano. No negocian velocidades inferiores a 1 Gb (por ejemplo, 100 Mb o 10 Mb). El LED de enlace está situado a la derecha de cada conector y el LED de actividad está a la izquierda.



Panel frontal

El panel frontal contiene el botón de encendido y los indicadores LED de estado.



Interruptor de alimentación

Para encender el dispositivo, presione momentáneamente el botón de encendido. El botón se ilumina, la pantalla de tinta electrónica cambia a una barra de progreso y aparece el mensaje Please wait.

Para apagar el dispositivo, mantenga pulsado el interruptor de alimentación durante dos segundos o hasta que en la pantalla de tinta electrónica aparezca Please wait.

> **Note**
>
> Si mantiene pulsado el botón de encendido durante más de cinco segundos, el dispositivo se apaga. No se recomienda hacerlo porque podría provocar la pérdida de datos de los búferes. Tras una pérdida de alimentación de CA, el dispositivo restablece automáticamente la alimentación al último estado de funcionamiento.

LED de estado

Junto al botón de encendido hay dos LED de estado. El LED izquierdo parpadea para indicar que hay actividad en el disco y el LED derecho se ilumina en caso de avería.

AWS Snowcone Especificaciones de Wi-Fi

AWS Snowcone admite redes Wi-Fi gigabit con el estándar IEEE 802.11ac y también redes 802.11abgn. Para maximizar el rendimiento inalámbrico de Snowcone, utilice 2x2 canales 802.11ac de 160 MHz, que pueden ser hasta 10 veces más rápidos que las redes 1x1 802.11bgn básicas. Las especificaciones de wifi de Snowcone son IEEE 802.11abgn+ac, 2x2, MIMO, doble banda de 2 GHz y 5G (160 MHz). Las frecuencias de funcionamiento son 2 GHz y 5 GHz.

Puede conectar el dispositivo Snowcone a la red en las instalaciones mediante un cable físico Ethernet o puede conectarlo de forma inalámbrica mediante wifi. Con la conexión Wi-Fi, puede gestionar el dispositivo Snowcone utilizando AWS OpsHub y transferir datos entre Snowcone y los dispositivos de almacenamiento locales.

> **Note**
>
> El Wi-Fi solo está disponible Regiones de AWS en Norteamérica.

Especificaciones de robustez

AWS Snowcone Los dispositivos están diseñados para cumplir con los estrictos estándares de robustez, incluidos el ISTA-3A, la ASTM D4169 y la MIL-STD-810G en materia de golpes de caída libre, vibraciones operativas y más. Se han diseñado para tolerar caídas de hasta 1,15 metros (3,8 pies). También cumplen con el estándar IEC de marca de protección internacional IP65, lo que significa que son herméticos al polvo (no permiten la entrada de polvo en la carcasa cuando están sellados) y resistentes al agua (incluida la protección contra chorros de agua por todos los lados).

Los dispositivos tienen un amplio rango de temperaturas de funcionamiento, desde temperaturas bajo cero (0 grados C o 32 grados F) hasta condiciones desérticas (Snowcone: 38 grados C o 100 grados F; Snowcone SSD: 45 grados C o 113 grados F). Cuando los dispositivos Snowcone se almacenan o se envían, soportan temperaturas aún más duras (-32 grados C o -25,6 grados F a 63 grados C o 145,4 grados F).

AWS Snowcone Fuente de alimentación y accesorios

AWS Snowcone los dispositivos no incluyen una fuente de alimentación ni un cable Ethernet (RJ45) porque se envían con el formato más pequeño posible. Tiene la opción de hacer funcionar su dispositivo Snowcone mediante una fuente de alimentación enchufable o una batería. Estos son los detalles que le servirán de guía a la hora de pedir una fuente de alimentación y un cable Ethernet:

Adaptador de alimentación USB-C: utilice un adaptador de alimentación USB-C con el dispositivo Snowcone si desea usarlo con un transformador de alimentación o para entornos operativos estacionarios (no móviles). Para alimentar su dispositivo Snowcone, puede adquirir uno de los siguientes adaptadores de alimentación AWS USB-C probados:

- Apple 61W USB-C Power Adapter

- Lenovo USB-C 65W Standard AC Adapter

O bien, puede usar cualquier adaptador de alimentación USB-C con una potencia nominal de más de 45 W y la temperatura ambiente.

Batería USB-C: utilice una batería USB-C para alimentar el dispositivo Snowcone en entornos operativos móviles o portátiles. Para alimentar su dispositivo Snowcone, puede utilizar una batería externa Plus para portátiles Dell (USB C, 65 Wh, PW7018LC) o cualquier batería USB-C con una potencia mínima de 45 W.

Cable Ethernet (RJ45): para conectar el dispositivo Snowcone a la red local, utilice un cable Ethernet (RJ45). Si no tiene, debe comprar uno.

Rendimiento del disco y la CPU

AWS Snowcone es un dispositivo de transferencia de informáticos/datos de última generación diseñado específicamente. El rendimiento del disco y de la CPU variará en función de diversos factores. En Rendimiento de Snowcone puede ver algunas cifras de rendimiento de ejemplo para las transferencias

Configuración AWS para AWS Snowcone

Antes de crear su primer AWS Snowcone trabajo, siga estas instrucciones para asegurarse de preparar adecuadamente su entorno.

Temas

- Inscríbase en AWS

Inscríbase en AWS

Cuando te registras en Amazon Web Services (AWS), tu cuenta se registra automáticamente para todos los AWS servicios. AWS solo te cobra por los servicios que utilizas. Después de configurar su cuenta, puede solicitar, configurar y administrar su AWS Snowcone dispositivo a través del Consola de administración de la familia de productos Snow de AWS. Para obtener más información sobre los precios y las tarifas de Snowcone, consulte Precios de AWS Snowcone.

Si ya tienes una Cuenta de AWS, anota tu Cuenta de AWS número. Si no tienes uno Cuenta de AWS, sigue estos pasos:

Para crear un 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.

Anota tu Cuenta de AWS número, que necesitarás para el siguiente paso.

Antes de pedir un dispositivo Snowcone

AWS Snowcone es un servicio específico de una región, así que asegúrese de que el servicio esté disponible en su región antes de planificar el trabajo. Asegúrese de que su ubicación y el depósito de Amazon S3 estén dentro del mismo lugar, Región de AWS ya que esto afectará a su capacidad de pedir el dispositivo. Existen algunas limitaciones en el envío del dispositivo Snowcone fuera de las fronteras nacionales de una región. Para obtener más información, consulte Restricciones de envío en función de la región.

Los envíos internacionales a ubicaciones fuera de la tuya solo Región de AWS están disponibles Consola de administración de la familia de productos Snow de AWS para los clientes que figuran en la lista permitida para un conjunto selecto de ubicaciones de regiones específicas (por ejemplo, de EE. UU. a México). Debe hablar con su equipo de cuentas sobre el destino, los costos y los plazos para atender estas solicitudes.

Como parte del proceso de pedido, se crea un rol AWS Identity and Access Management (de IAM) y una clave AWS Key Management Service (AWS KMS). KMS protege las claves de cifrado que se utilizan para proteger los datos de cada dispositivo. Para obtener más información, consulte Crear una tarea para solicitar un dispositivo de la familia Snow.

Temas

- Preguntas sobre el entorno local
- Trabajo con archivos que contienen caracteres especiales
- Uso de Amazon EC2 en Snowcone

Preguntas 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 su pedido.

¿Se obtendrá acceso a los datos durante la transferencia?

> Para evitar que los datos resulten dañados, no desconecte el dispositivo Snowcone ni modifique la configuración de red mientras se están transfiriendo datos. Los archivos deben encontrarse en un estado estático mientras se escriben en el dispositivo. Modificar archivos mientras se están escribiendo en el dispositivo puede dar lugar a conflictos de lectura/escritura.

Trabajo con archivos que contienen caracteres especiales

Es importante tener en cuenta que si los archivos 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 los archivos tienen uno o más de estos caracteres, cámbieles el nombre antes de copiarlos en el AWS Snowcone dispositivo. Los usuarios de Windows cuyos nombres de archivo contengan espacios en blanco deben tener cuidado al copiar objetos individuales o ejecutar un comando recursivo. Ponga entre comillas los objetos individuales cuyos nombres contengan 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”
Mac	/Users/<username>/test\ file.txt

Sistema operativo	Nombre de archivo: **`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. Sin embargo, AWS DataSync conserva las listas de control de acceso (ACL). Para obtener más información, consulte Cómo se DataSync gestionan los metadatos y los archivos especiales en la Guía del AWS DataSync usuario.

Uso de Amazon EC2 en Snowcone

En esta sección se proporciona información general sobre el uso de instancias de computación compatibles con Amazon EC2 en un dispositivo AWS Snowcone .

Debe usar las instancias compatibles con Amazon EC2 cuando tenga una aplicación en ejecución en la periferia que se administre e implemente como una máquina virtual (una imagen de máquina de Amazon o AMI). Snowcone admite el tipo de instancia SNC1 con tres instancias, incluidas snc1.micro (1 CPU y 1 GB de RAM), snc1.small (1 CPU y 2 GB de RAM) y snc1.medium (2 CPU y 4 GB de RAM). La posibilidad de usar instancias compatibles con EC2 en Snowcone le permite crear y probar su aplicación en Amazon EC2. Puede habilitar y aprovisionar las AMI compatibles con EC2 durante la creación del AWS Snowcone trabajo mediante el AWS Management Console AWS Snowball SDK o. AWS CLI

Tipos de instancias de Amazon EC2 admitidas

Utilice los siguientes tipos de instancias de Amazon EC2 para sus trabajos de computación.

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

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

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

AWS OpsHub Úselo para gestionar sus instancias en Snowcone. AWS OpsHub Descárguelo desde el sitio web de AWS Snowball recursos. Tras desbloquear el dispositivo mediante AWS OpsHub, vaya a la página de Amazon EC2. Elija Crear instancia para crear una instancia compatible con

EC2 basada en la AMI que había precargado en el dispositivo al crear el trabajo. A continuación, podrá conectarse a las instancias y ejecutar su aplicación perimetral. AWS OpsHub también incluye botones con un solo clic para iniciar, detener, finalizar y reiniciar las instancias compatibles con EC2. Para obtener más información, consulte Uso AWS OpsHub for Snow Family para administrar dispositivos.

Cuando haya terminado con el dispositivo, devuélvalo a. AWS Si el dispositivo se utilizó en un trabajo de importación, los datos transferidos mediante la interfaz de archivos se importan a Amazon S3 con la interfaz NFS de Snowcone. 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**
>
> Los datos de las instancias de computación que se ejecutan en un dispositivo Snowcone 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 Snowcone

Hay costos adicionales asociados con el uso de instancias de computación. Para más información, consulte Precios de AWS Snowcone.

Requisitos previos

Antes de crear un trabajo, tenga en cuenta la siguiente información:

- Para poder agregar cualquier AMI al trabajo, tiene que haber creado en su Cuenta de AWS una AMI de un tipo de imagen compatible. En estos momentos, las AMI compatibles se basan en las imágenes Amazon Linux 2, CentOS 7 (x86_64) - with Updates HVM o Ubuntu 16.04 LTS - Xenial (HVM). Puede obtener estas imágenes de AWS Marketplace.

Antes de agregar cualquier AMI a su solicitud de creación de trabajo, asegúrese de que tiene una o más AMI compatibles en su Cuenta de AWS. Al elegir una AMI del Marketplace, asegúrese de que tenga un código de producto y una plataforma compatibles. Para obtener más información, consulte Compruebe los códigos de producto y los detalles de la plataforma de las AMI AWS Marketplace.

- Todas las AMI deben residir en Amazon Elastic Block Store (Amazon EBS) y tener un solo volumen.
- Si tiene previsto conectarse a instancias de computación que se ejecutan en un dispositivo Snowcone, debe usar Secure Shell (SSH). Para ello, primero debe agregar el par de claves.

Compruebe los códigos de producto y los detalles de la plataforma de las AMI AWS Marketplace

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**
>
> AWS Marketplace Entre las AMI de aws-marketplace se incluye 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

Creación de una AMI de Linux desde una instancia

Puede crear una AMI mediante la consola o la línea de comandos. Comience con una AMI existente; lance una instancia; personalícela; cree una nueva AMI a partir de ella y, finalmente, lance una instancia de la nueva AMI.

Para crear una AMI a partir de una instancia mediante la consola

1. Seleccione la AMI con respaldo EBS adecuada que servirá como punto de partida de la nueva AMI y configúrela como sea necesario antes de lanzarla. Para obtener más información, consulte Lanzamiento de una instancia con el asistente de inicialización de instancias.
2. Elija Lanzar para lanzar una instancia de la AMI con respaldo EBS que ha seleccionado. Acepte los valores predeterminados a medida que avanza por el asistente. Para obtener más información, consulte Lanzamiento de una instancia con el asistente de inicialización de instancias.
3. Mientras la instancia está en ejecución, conéctese a ella. Puede realizar cualquiera de las siguientes acciones en la instancia con el fin de personalizarla para que se ajuste a sus necesidades:

   - Instalar software y aplicaciones.
   - Copiar datos.
   - Reducir el tiempo de inicio eliminando los archivos temporales, desfragmentando el disco duro y dejando el espacio libre en cero
   - Adjuntar volúmenes adicionales de Amazon EBS
4. (Opcional) Cree instantáneas de todos los volúmenes asociados a la instancia. Para más información sobre la creación de instantáneas, consulte Creación de instantáneas de Amazon EBS.
5. En el panel de navegación, elija Instancias y seleccione la instancia. Elija Acciones, seleccione Imagen y Crear imagen

   > **Tip**
   >
   > Si se deshabilita esta opción, la instancia no es una instancia con respaldo Amazon EBS.
6. En el cuadro de diálogo Crear imagen, especifique la información siguiente y, a continuación, elija Crear imagen.

- Nombre de la imagen: indique un nombre único para la imagen.
- Descripción de la imagen: si lo desea, incluya una descripción de la imagen con un máximo de 255 caracteres.
- Sin reiniciar: esta opción no está seleccionada de forma predeterminada. Amazon EC2 apaga la instancia; toma instantáneas de todos los volúmenes asociados, crea y registra la AMI y después reinicia la instancia. Seleccione Sin reiniciar para evitar que se apague la instancia.

  > **Warning**
  >
  > Si elige Sin reiniciar, no podemos garantizar la integridad del sistema de archivos de la imagen creada.

- Volúmenes de instancia: los campos de esta sección le permiten modificar el volumen raíz, así como agregar más volúmenes de Amazon EBS y de almacén de instancias. Si desea obtener información acerca de cada campo, deténgase sobre el icono i que aparece junto a él para que se muestre la información correspondiente. A continuación se apuntan algunos aspectos importantes.
  - Para cambiar el tamaño del volumen raíz, localice Raíz en la columna Tipo de volumen. En Tamaño (GiB), introduzca el valor necesario.
  - Si selecciona Eliminar al terminar, cuando termine la instancia creada a partir de esta AMI se eliminará el volumen de Amazon EBS. Si desactiva Eliminar al terminar, cuando termine la instancia no se eliminará el volumen de Amazon EBS. Para obtener más información, consulte Conservación de los volúmenes de Amazon EBS al término de la instancia en la Guía del usuario de Amazon EC2.
  - Para agregar un volumen de EBS, elija Agregar nuevo volumen (lo que agrega una fila nueva). En Tipo de volumen, elija EBS y complete los campos de la fila. Cuando lanza una instancia desde la nueva AMI, los volúmenes adicionales se asocian de forma automática a la instancia. Los volúmenes vacíos se tienen que formatear y montar. Los volúmenes basados en una instantánea se deben montar.
  - Para agregar un volumen de almacén de instancias, consulte Agregar volúmenes de almacén de instancias a una AMI. Cuando inicia una instancia desde la nueva AMI, los volúmenes adicionales se inicializan y se montan de forma automática. Estos volúmenes no contienen datos de los volúmenes de almacén de instancias de la instancia en ejecución en la que ha basado la AMI.

7. Para ver el estado de la AMI mientras se crea, elija AMI en el panel de navegación. Al principio, el estado es pendiente, pero debe cambiar a disponible después de unos minutos.

   (Opcional) Para ver la instantánea creada para la nueva AMI elija Instantáneas. Cuando se lanza una instancia desde esta AMI, se usa esta instantánea para crear su volumen de dispositivo raíz.
8. Lance una instancia desde la nueva AMI. Para obtener más información, consulte Lanzamiento de una instancia con el asistente de inicialización de instancias.
9. La nueva instancia en ejecución contiene todas las personalizaciones que ha aplicado en pasos anteriores.

Creación de una AMI a partir de una instancia mediante la línea de comandos

Puede utilizar uno de los siguientes comandos. Para obtener más información acerca de estas interfaces de línea de comandos, consulte Acceso a Amazon EC2.

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

Creación de una AMI de Linux a partir de una instantánea

Si tienes una instantánea del volumen del dispositivo raíz de una instancia, puedes crear una AMI a partir de esta instantánea mediante la línea de comandos AWS Management Console o la línea de comandos.

Creación de una AMI a partir de una instantánea mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, bajo Elastic Block Store, elija Snapshots.
3. Seleccione la instantánea y elija Acciones, Crear imagen.
4. En el cuadro de diálogo Crear imagen a partir de una instantánea de EBS, rellene los campos para crear la AMI y, a continuación, elija Crear. Si está creando de nuevo una instancia principal, elija las mismas opciones que las de la instancia principal original.

   - Arquitectura: elija i386 para 32 bits o x86_64 para 64 bits.
   - Nombre del dispositivo raíz: escriba el nombre adecuado para el volumen raíz. Para obtener más información, consulte Nombres de dispositivos en instancias de Linux.

- Tipo de virtualización: elija si las instancias lanzadas desde esta AMI usan virtualización paravirtual (PV) o de máquina virtual de hardware (HVM). Para obtener más información, consulte Tipos de virtualización de una AMI de Linux.
- (Solo para el tipo de virtualización de PV) ID de kernel e ID de disco de RAM: elija la AKI y la ARI en las listas. Si elige la AKI predeterminada o no elige ninguna, debe especificar una AKI cada vez que lance una instancia usando esta AMI. Además, la instancia podría no superar las comprobaciones de estado si la AKI predeterminada es incompatible con la instancia.
- (Opcional) Asignación de dispositivos de bloques: agregue volúmenes o amplíe el tamaño predeterminado del volumen raíz de la AMI. Para obtener más información sobre cómo ampliar el sistema de archivos de la instancia, consulte Ampliar un sistema de archivos Linux después de cambiar el tamaño de un volumen.

Creación de una AMI a partir de una instantánea mediante la línea de comandos

Puede utilizar uno de los siguientes comandos. Para obtener más información acerca de estas interfaces de línea de comandos, consulte Acceso a Amazon EC2.

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

Introducción

En esta sección se proporcionan instrucciones generales para crear y completar su primer AWS Snowcone trabajo en el Consola de administración de la familia de productos Snow de AWS. Para obtener una descripción general del AWS Snowcone dispositivo, consulteCómo AWS Snowcone funciona.

En esta documentación de introducción se supone que utiliza el Consola de administración de la familia de productos Snow de AWSpara crear su trabajo y que utiliza el cliente o la AWS OpsHub for Snow Family aplicación de Snowball Edge para desbloquear el AWS Snowcone dispositivo. 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 Snowcone.

Antes de empezar, debe crear un usuario administrador en AWS Identity and Access Management (IAM) Cuenta de AWS y un usuario administrador. Para obtener más información, consulte Configuración AWS para AWS Snowcone.

Para empezar AWS Snowcone, consulte Crear una tarea para solicitar un dispositivo de la familia Snow.

Temas

- Crear un trabajo para pedir un dispositivo de la familia Snow
- Cancelar un trabajo a través del Consola de administración de la familia de productos Snow de AWS
- Obtener credenciales para acceder a un dispositivo de la familia Snow
- Desbloquear el dispositivo de la familia Snow
- Reinicio del dispositivo Snow Family

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.

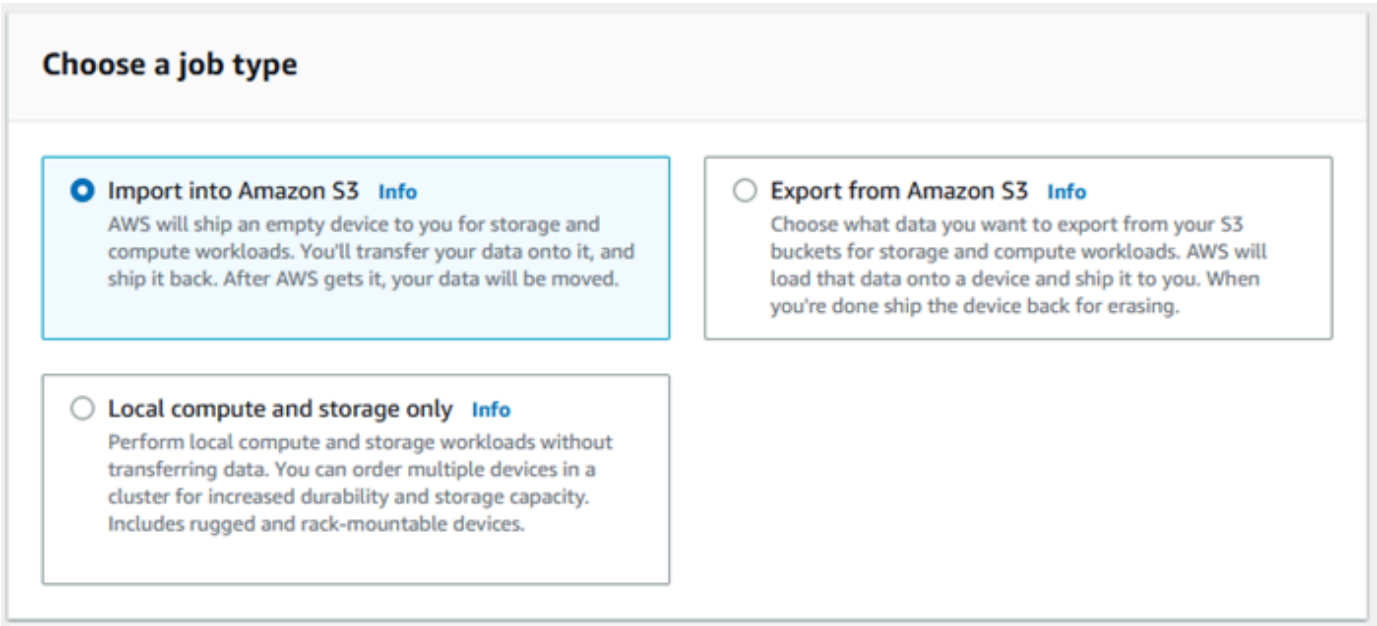
Para elegir el tipo de trabajo

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:

   - Import into Amazon S3: solicite que AWS le envíe un dispositivo Snowcone vacío. Conecta el dispositivo a su red local y configura el dispositivo mediante OpsHub. Los datos se copian en el dispositivo mediante NFS Share, se devuelven al AWS dispositivo y se cargan en Amazon S3.
   - Solo informático y almacenamiento locales: ejecute cargas de trabajo de computación y almacenamiento en el dispositivo sin transferir datos.



5. Elija Siguiente para continuar.

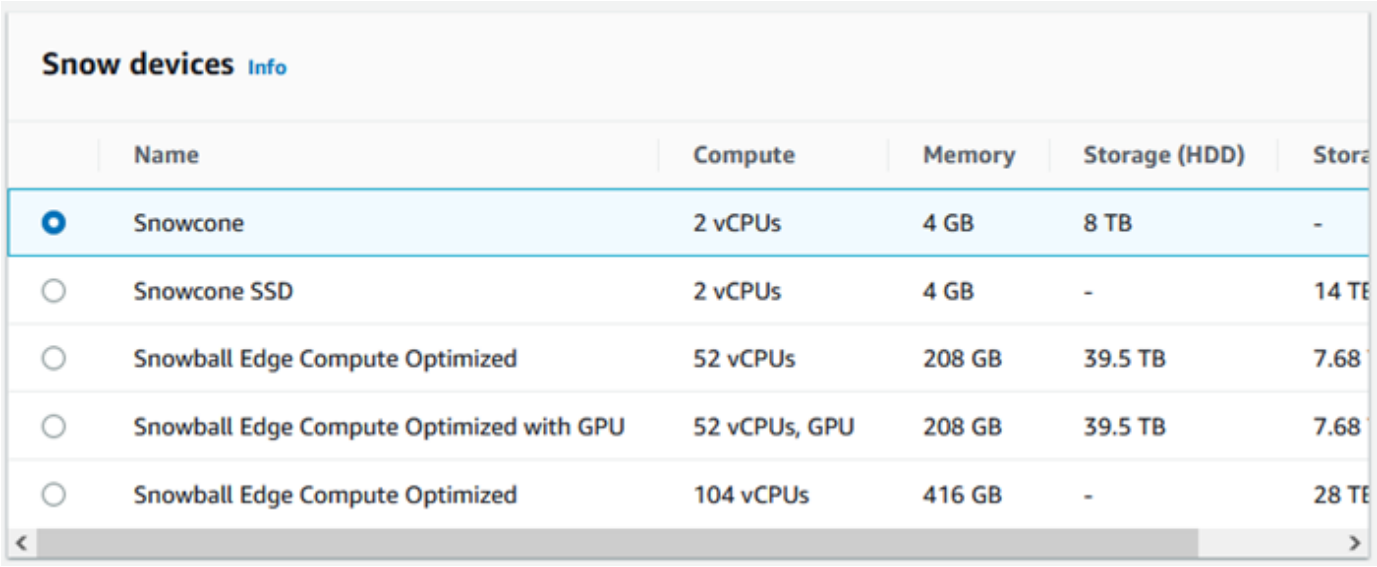
Paso 2: elija las opciones de computación y almacenamiento

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 Fuente de alimentación de Snowcone, seleccione I will provide my own power supply and Ethernet cable. Para obtener información sobre las fuentes de alimentación, consulte Fuentes de alimentación y accesorios de AWS Snowcone.
3. 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. Para ver los precios de los dispositivos, consulte Precios de AWS Snowcone.
4. En la sección Seleccionar el tipo de almacenamiento, elija la opción que mejor se adapte a sus necesidades:

   - 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 del AWS Snowcone usuario para obtener más información.

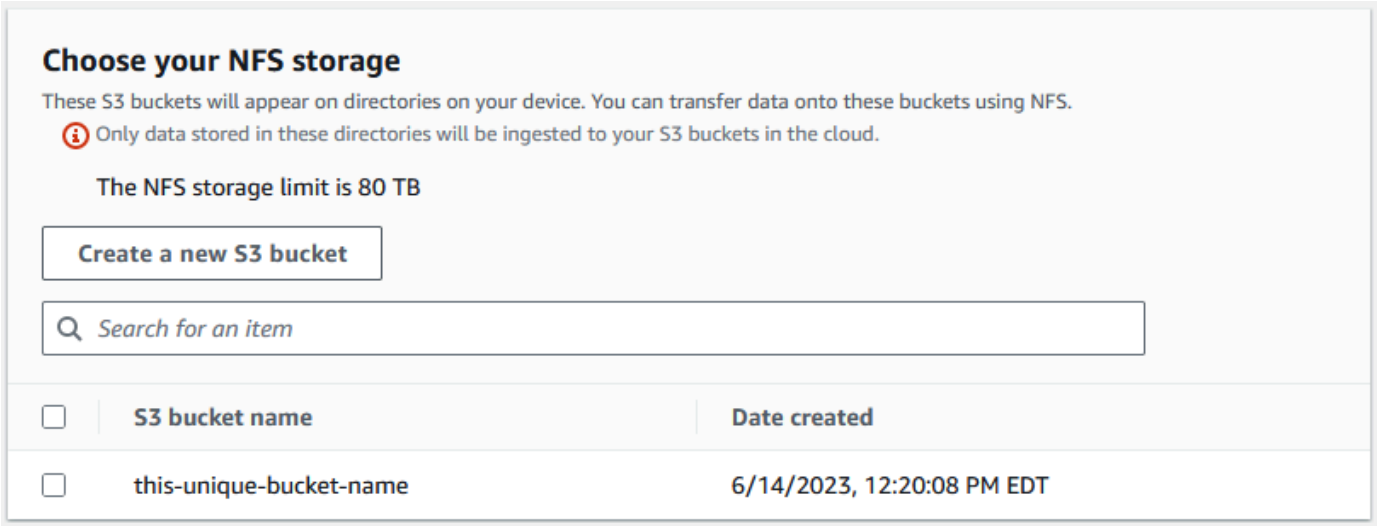
5. Si seleccionó Transferencia de datos basada en NFS como tipo de almacenamiento, en la sección Select your S3 buckets, realice una o varias de las siguientes acciones para seleccionar uno o más buckets de S3:

   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.

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



6. 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 Creación de un trabajo con instancias de computación en esta guía.

Esta característica conlleva cargos adicionales. Para más información, consulte Precios de AWS Snowball Edge.

7. 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. Para habilitar la red inalámbrica en su dispositivo Snowcone, seleccione Habilitar la conexión inalámbrica en Snowcone.
2. 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.
3. 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 laboral y los temas de SNS cifrados, consulte Notificaciones para 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

> **Note**
>
> Los dispositivos Snowcone no vienen con cables de alimentación y debe conseguir uno por su cuenta. Para obtener más información, consulte Fuente de AWS Snowcone alimentación y accesorios.

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.

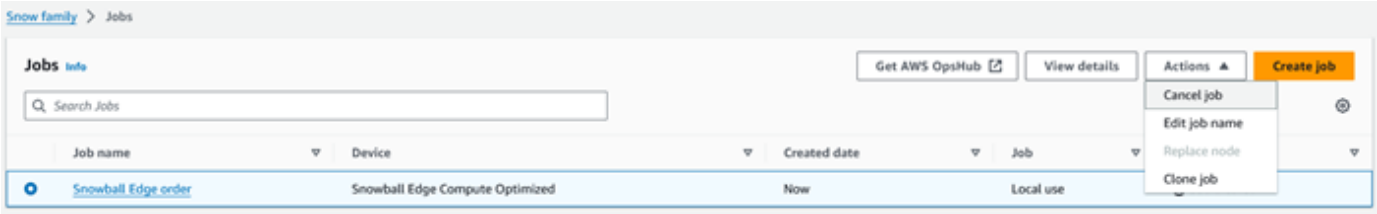
Para descargar e instalar AWS OpsHub for Snow Family

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.

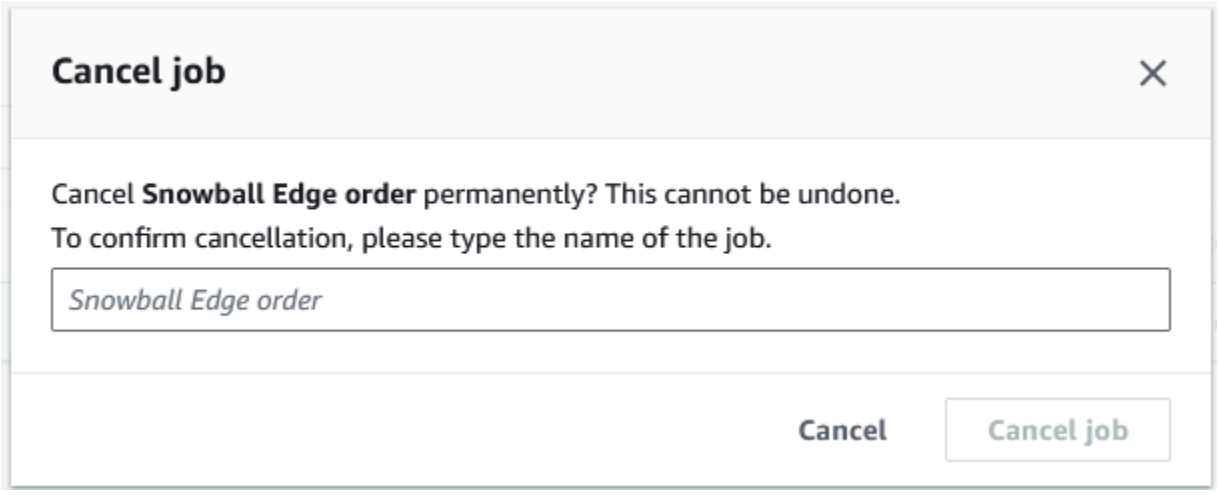
Cancelar un trabajo a través del Consola de administración de la familia de productos Snow de AWS

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.



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 Comprensión de los estados de los AWS Snowcone 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 Mejores prácticas para el AWS Snowcone dispositivo.

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: Uso del AWS Snowball Edge cliente

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.

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 para acceder a él 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 AWS especificaciones del dispositivo Snowcone. Necesitará la siguiente información sobre los dispositivos de la familia Snow:

- Descarga e instalación del cliente de Snowball Edge. Para obtener más información, consulte Uso del AWS Snowball Edge cliente.
- 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 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 AWS Snowcone Especificaciones del dispositivo.

Para desbloquear un dispositivo independiente con el cliente Snowball Edge

1. Busque la dirección IP del Snowcone en la pantalla LCD del dispositivo. 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
```

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.

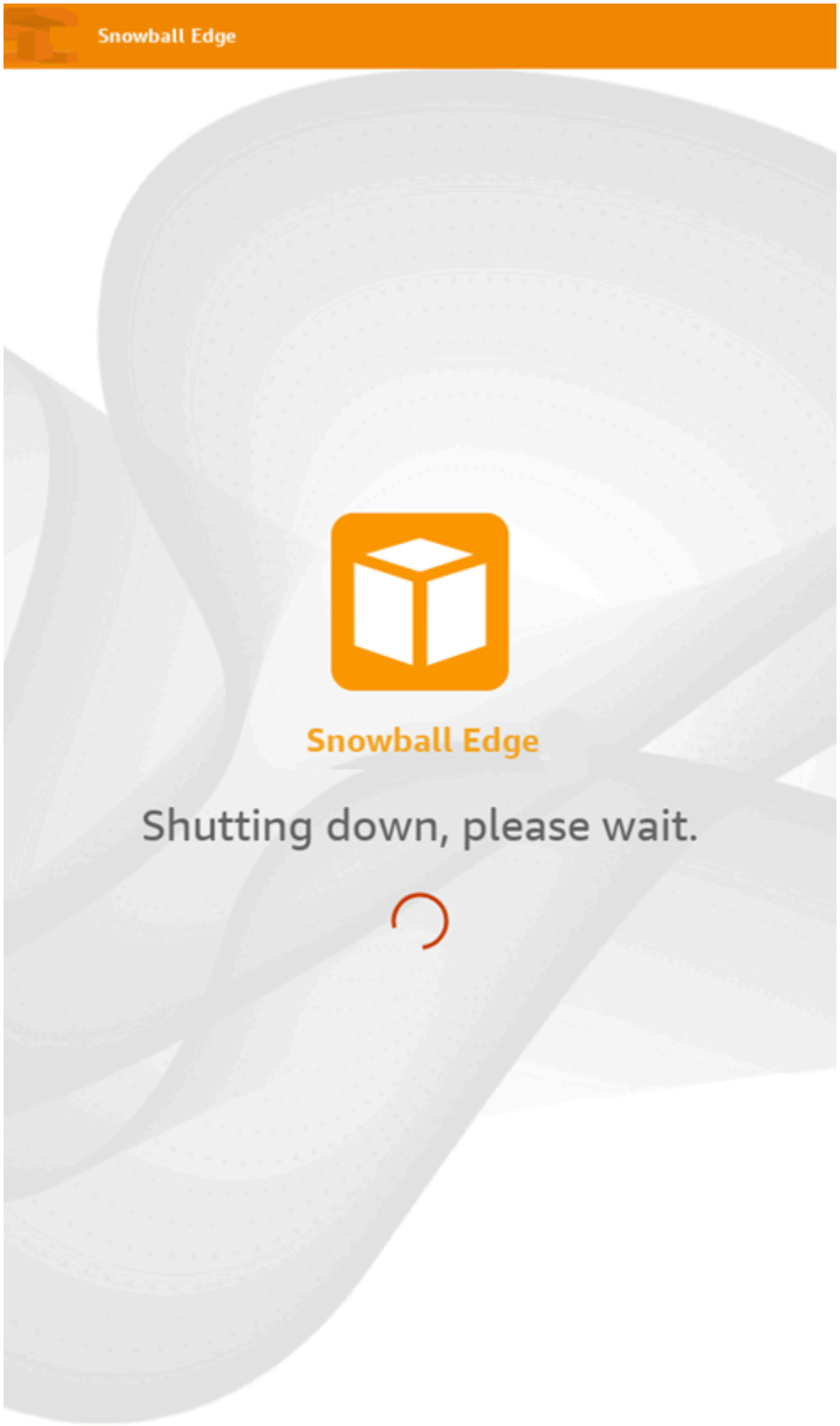
Ahora puede empezar a utilizar el dispositivo de la familia Snow.

Reinicio del dispositivo Snow Family

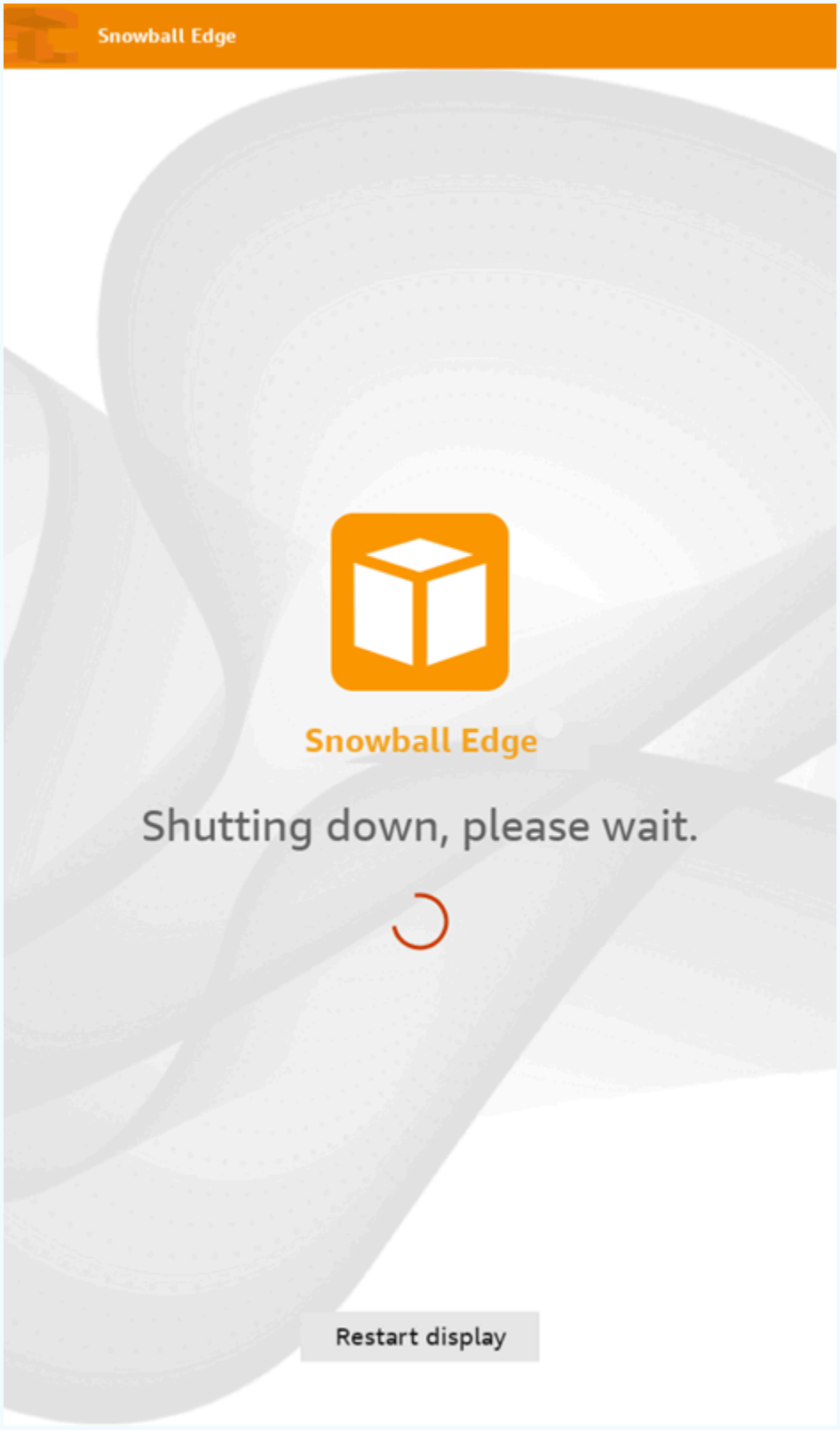
Antes de reiniciar un dispositivo Snow Family, asegúrese de que se hayan detenido todas las transferencias de datos al dispositivo. Si utilizaba la interfaz NFS para transferir datos, desactívela antes de apagar el dispositivo. Para obtener más información, consulte Detener la interfaz NFS.

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 un dispositivo AWS Snowcone.

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 un dispositivo AWS Snowcone.

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.

Tras descargar la AWS OpsHub aplicación e instalarla en un equipo cliente, AWS OpsHub podrá conectarse al AWS Snowcone dispositivo de la misma red, independientemente de si el dispositivo está conectado a través de Wi-Fi o de un cable físico. Luego abres AWS OpsHub y desbloqueas el dispositivo. En ese momento, aparecerá un panel que muestra el dispositivo y sus métricas del sistema. A continuación, puede empezar a implementar sus aplicaciones periféricas o a migrar sus

datos al dispositivo. AWS OpsHub simplifica la transferencia de datos a su dispositivo Snowcone al permitir guardar drag-and-drop archivos o carpetas en el dispositivo. Con AWS OpsHubél, también puede ver fácilmente lo que está almacenado en el dispositivo.

Temas

- Descarga AWS OpsHub para dispositivos de la familia Snow
- Desbloqueo de un dispositivo
- Verificar la firma PGP de AWS OpsHub (opcional)
- Administrar AWS los servicios en tu dispositivo
- Se utiliza DataSync para transferir archivos a AWS
- Administración de sus dispositivos
- 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.

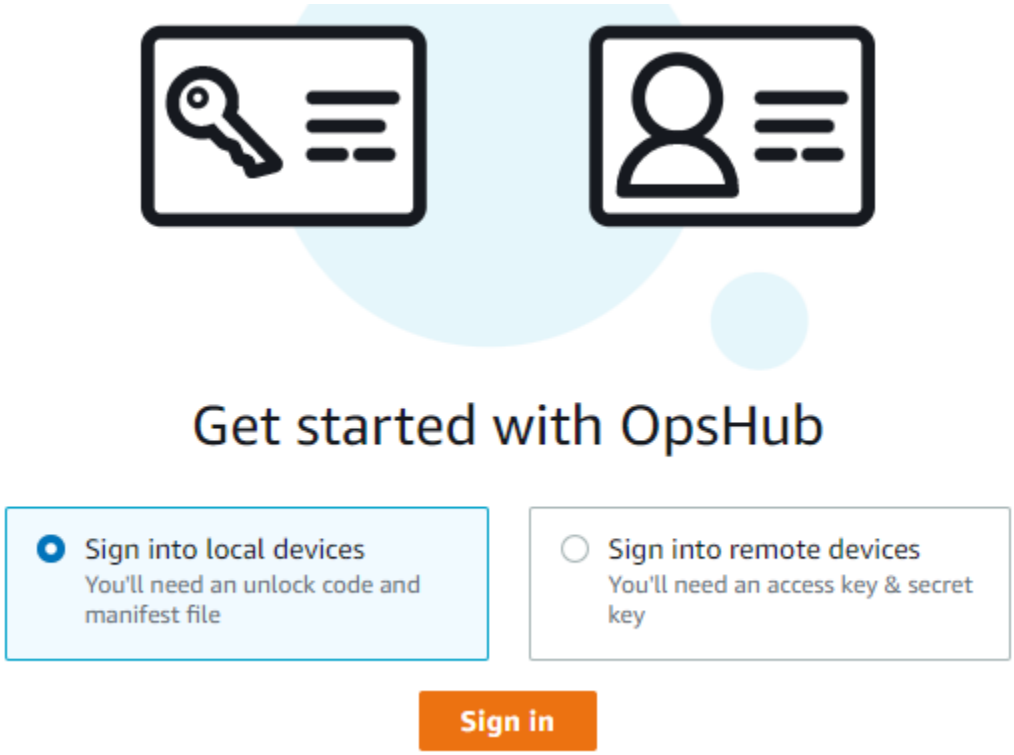
Temas

- Desbloqueo de un dispositivo de forma local
- Desbloqueo de un dispositivo de forma remota

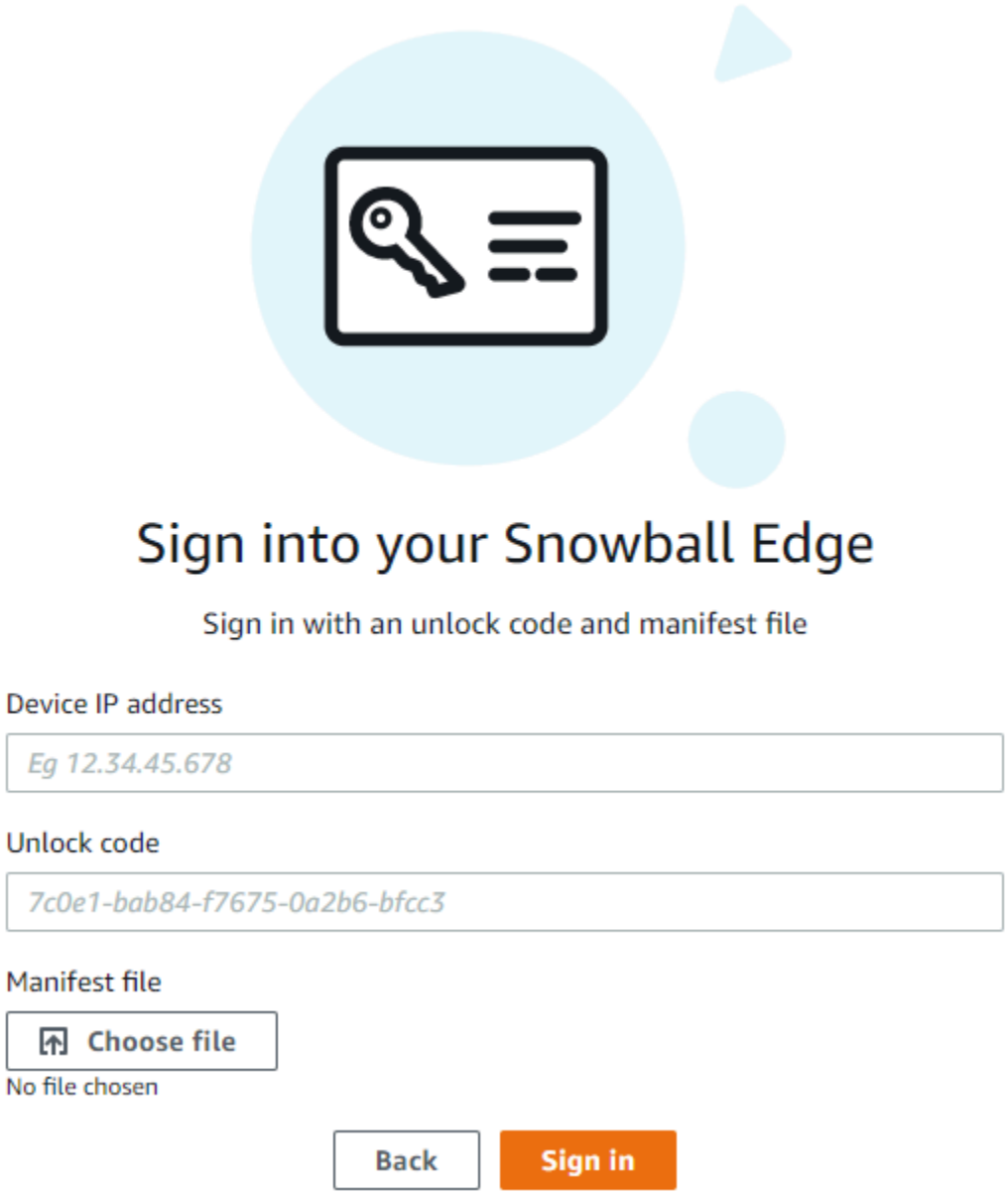
Desbloqueo de un dispositivo de forma local

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.

> **Note**
>
> El espacio de almacenamiento disponible en el dispositivo Snowcone no es preciso hasta que se inicia el servicio NFS. Consulte Administrar la interfaz NFS.

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

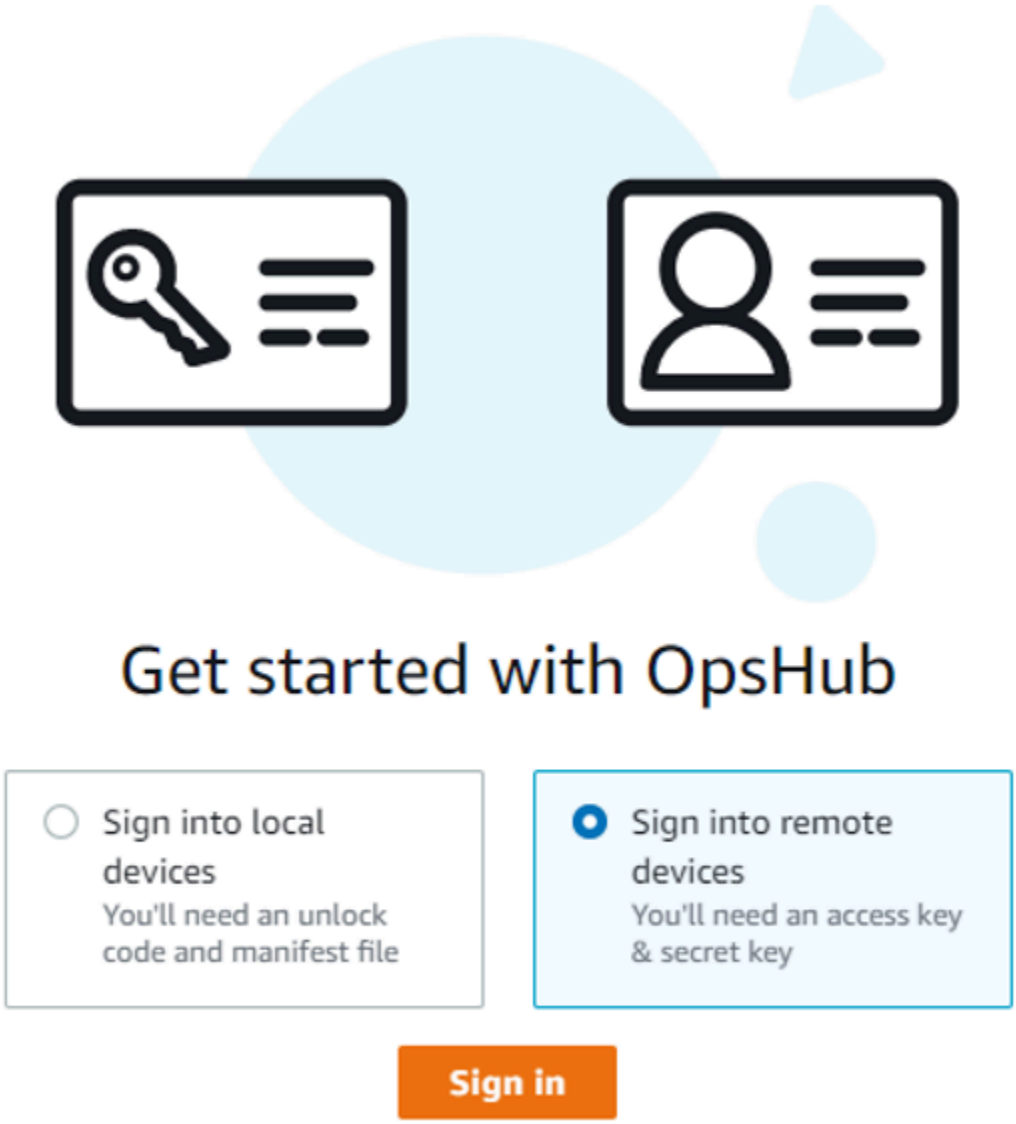
Para desbloquear un dispositivo de la familia Snow, no

Para conectar y desbloquear el dispositivo de forma remota

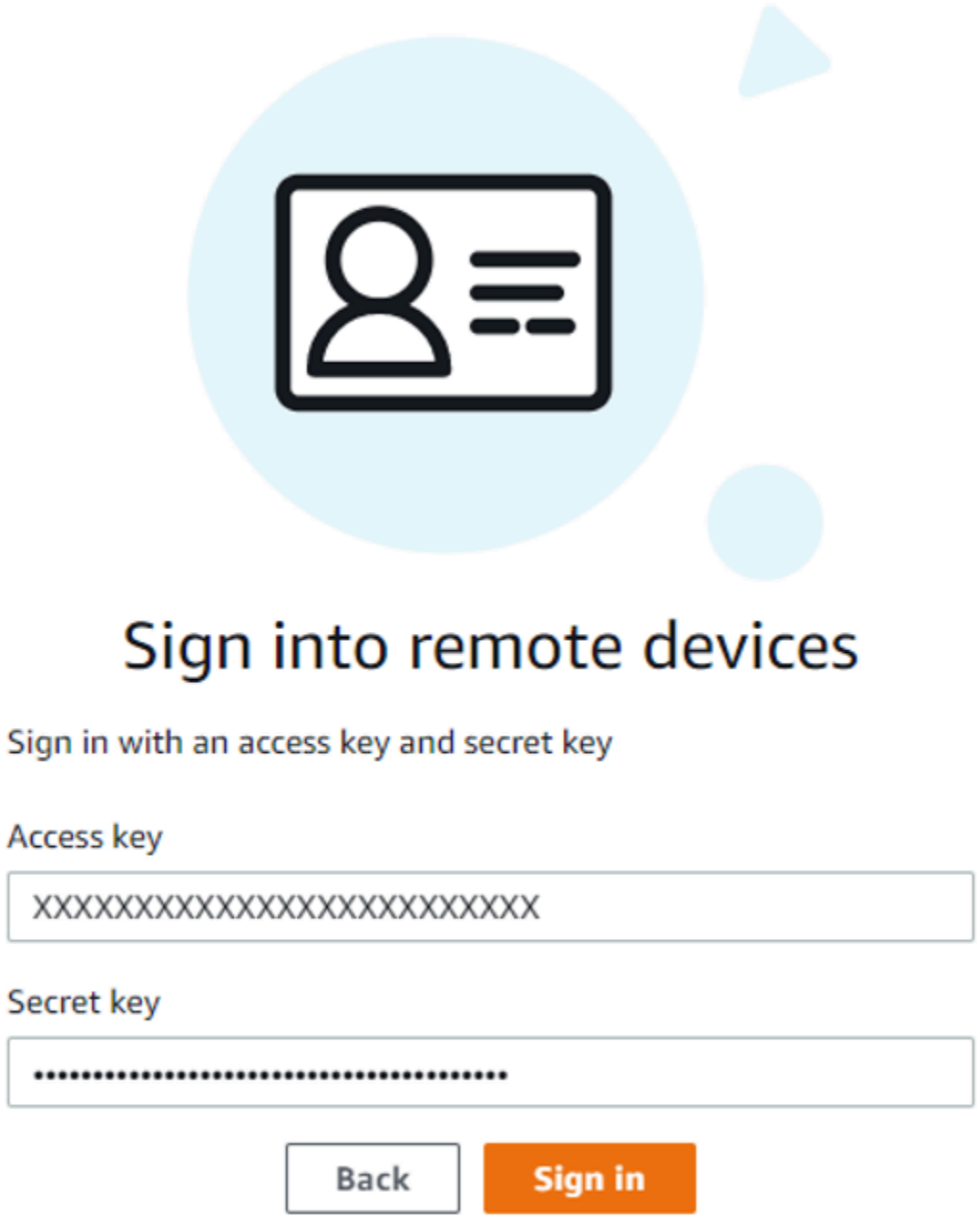
1. Abra la pestaña del dispositivo, localice el cable de alimentación y conecte el dispositivo a una fuente de alimentación.
2. Conecte el dispositivo a la red mediante un cable Ethernet (normalmente un cable RJ45), abra el panel delantero y encienda el dispositivo.

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

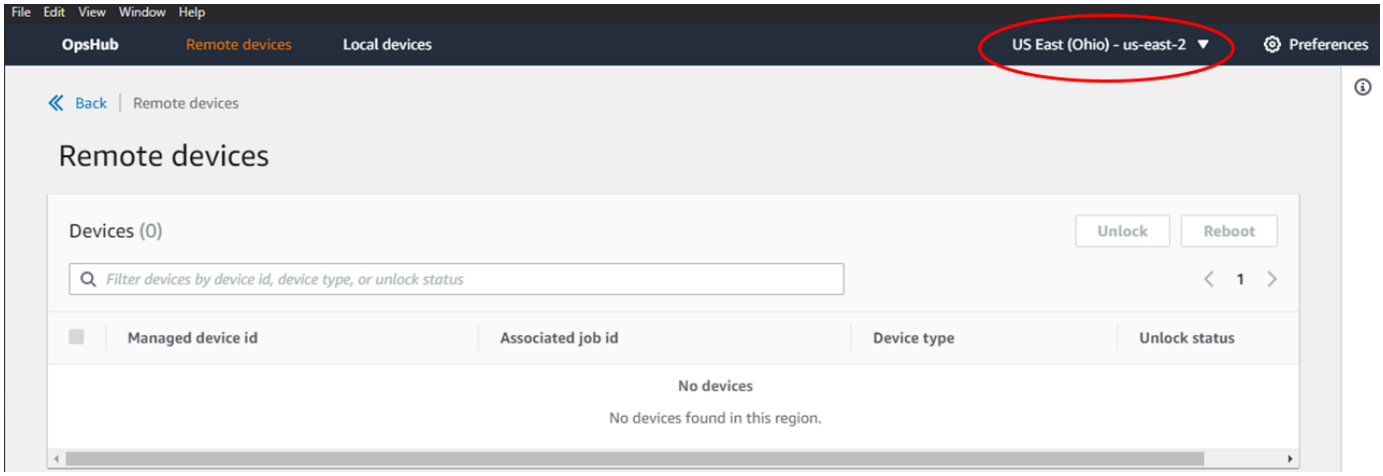
3. Abre la AWS OpsHub aplicación. Si es la primera vez que la utiliza, se le pedirá que seleccione un idioma. A continuación, elija Siguiente.
4. En la OpsHub página Comenzar con, selecciona Iniciar sesión en dispositivos remotos y, a continuación, selecciona Iniciar sesión.



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.

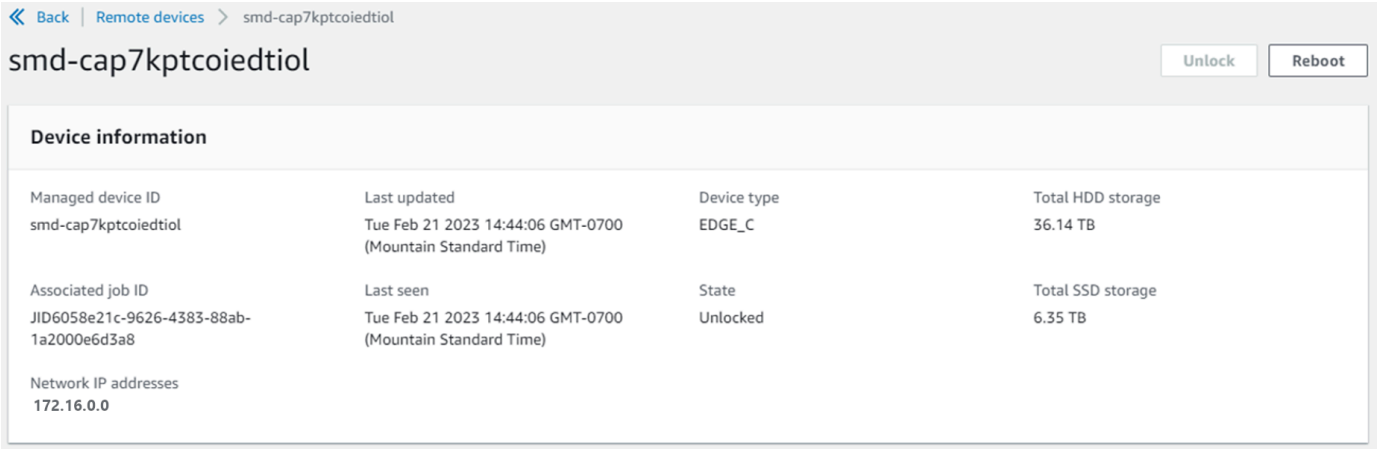


6. En la parte superior de la pestaña Dispositivos remotos, elija la región del dispositivo Snow que desea desbloquear de forma remota.



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.

> **Note**
>
> El espacio de almacenamiento disponible en el dispositivo Snowcone no es preciso hasta que se inicia el servicio NFS. Consulte Administrar la interfaz NFS.



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/ps7Xl3o/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

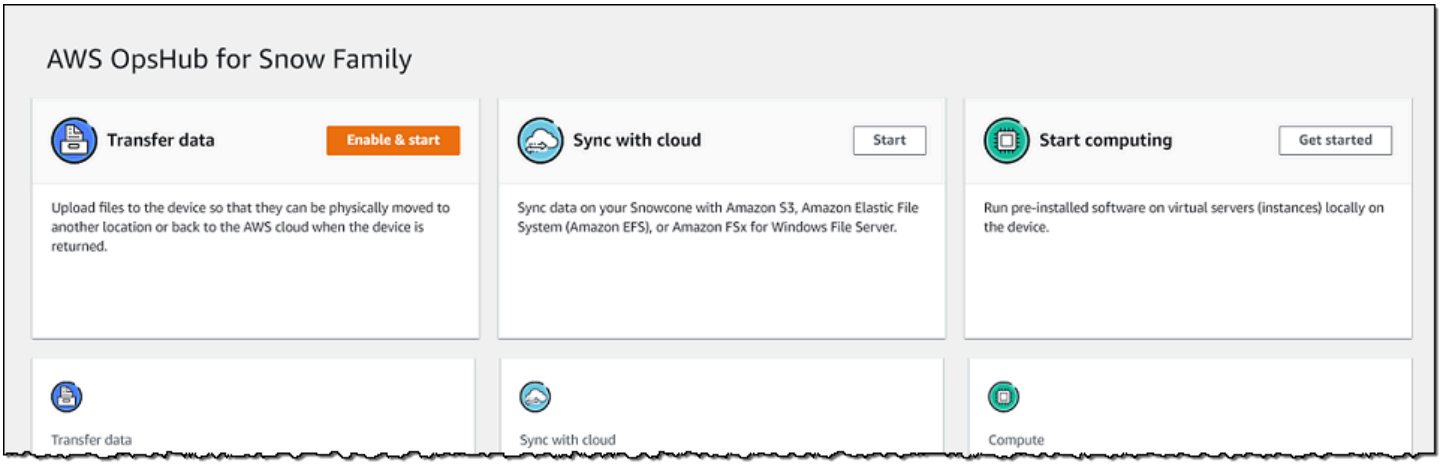
```
gpg: Signature made Mon Dec 21 13:44:47 2020 PST
gpg:                using RSA key 1655BBDE2B770256
gpg: Good signature from "AWS OpsHub for Snow Family <aws-opshub-
signer@amazon.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication 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.
- AWS DataSync—Transfiera una gran cantidad de archivos entre su almacenamiento local y otras Nube de AWS ubicaciones, como sistemas de archivos o Amazon S3.
- 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



Temas

- Uso local de instancias de computación compatibles con Amazon EC2
- 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

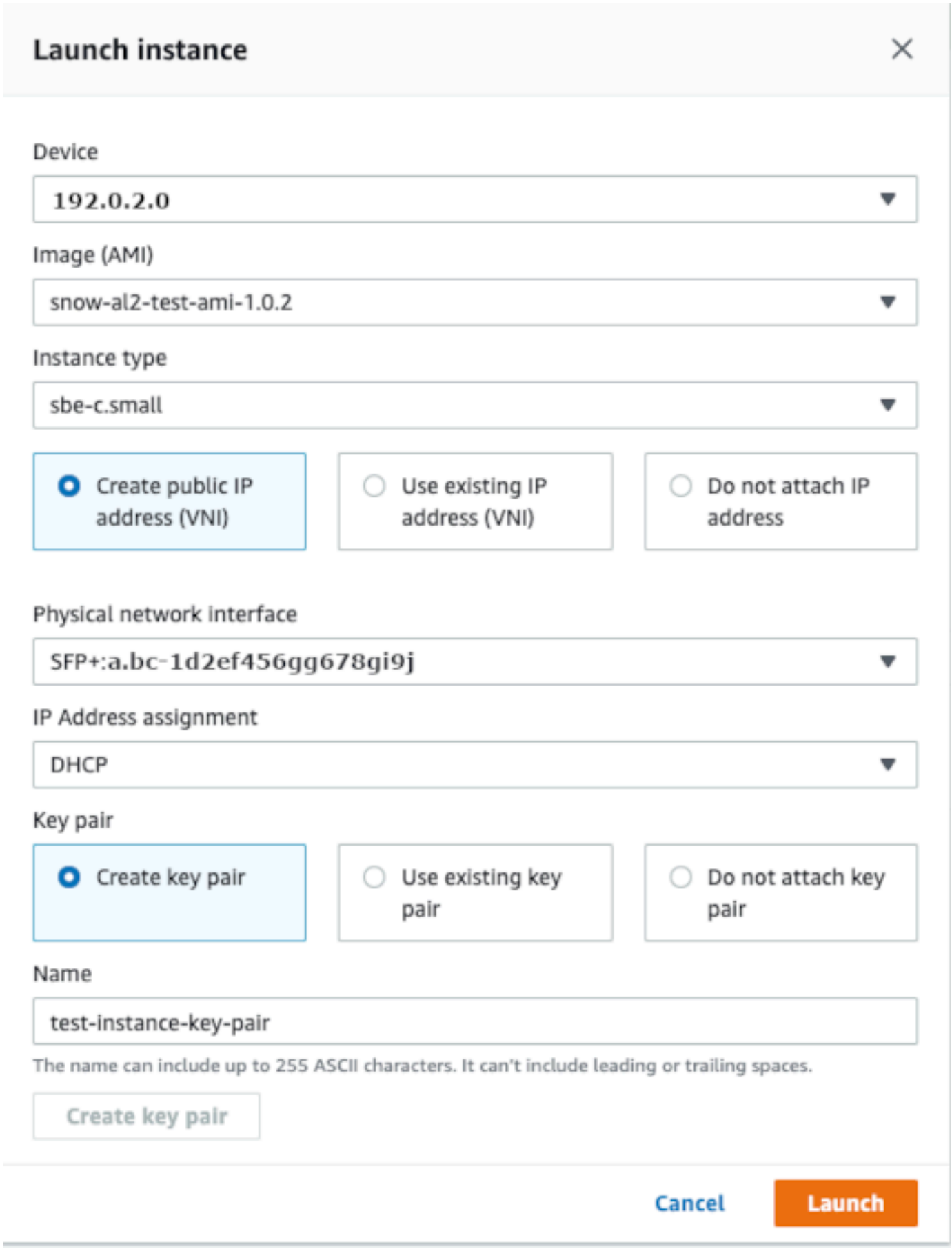
Lanzamiento de una instancia compatible con Amazon EC2

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

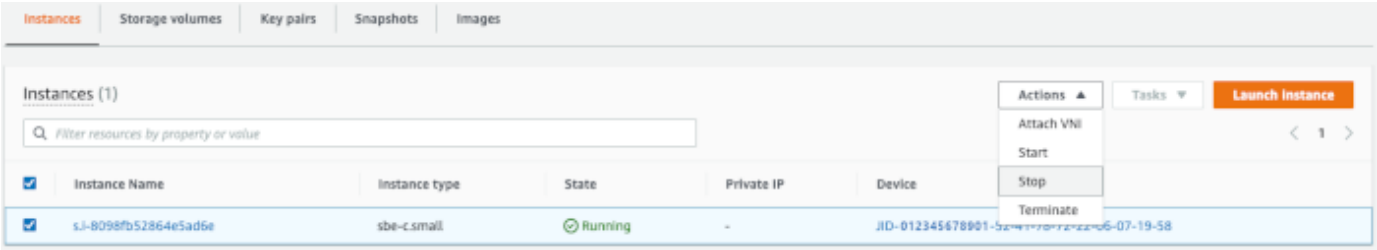
1. Abra la aplicación. AWS OpsHub

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

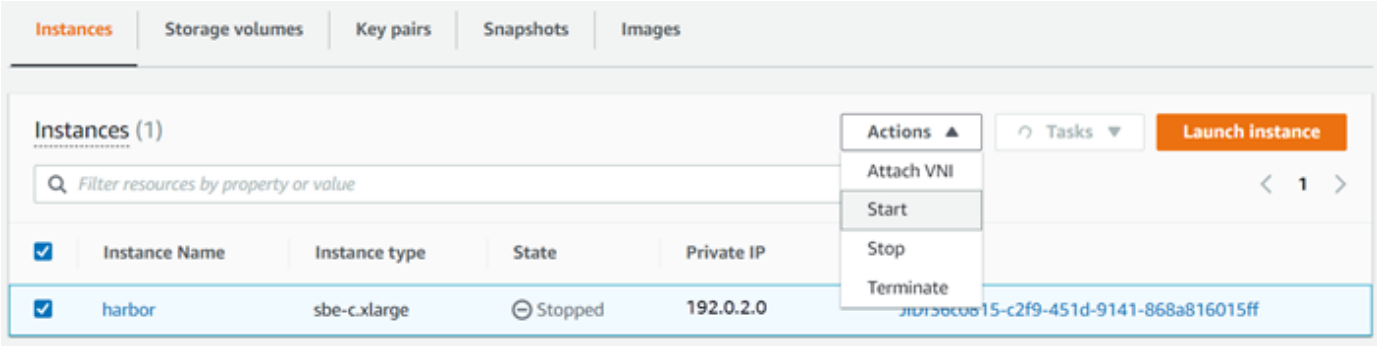
1. Abra la aplicación. AWS OpsHub

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

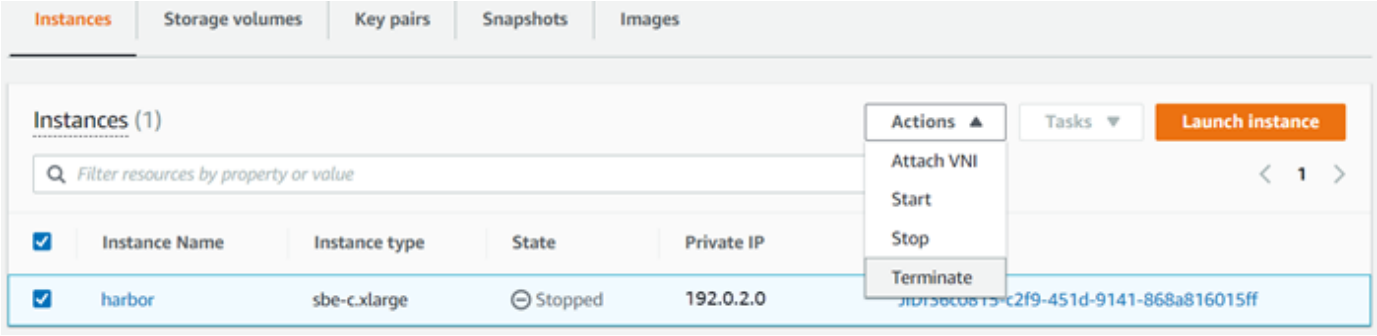
1. Abre Compute en el AWS OpsHub panel de control.
2. En el panel de navegación, elija la página Compute (EC2) y, a continuación, elija la pestaña Pares de claves. Se le redirigirá a la consola de Amazon EC2, donde podrá crear, importar o administrar sus pares de claves.
3. Para obtener instrucciones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

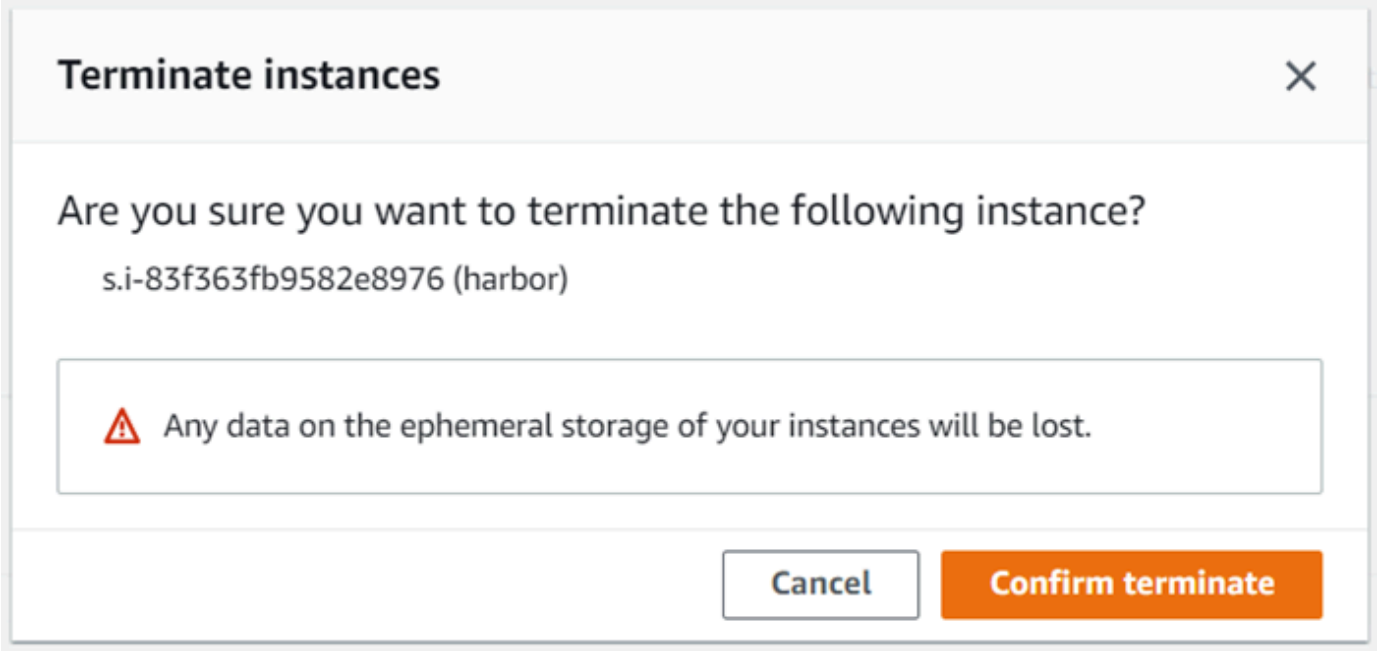
Después de terminar una instancia compatible con Amazon EC2, no puede reiniciarla.

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.

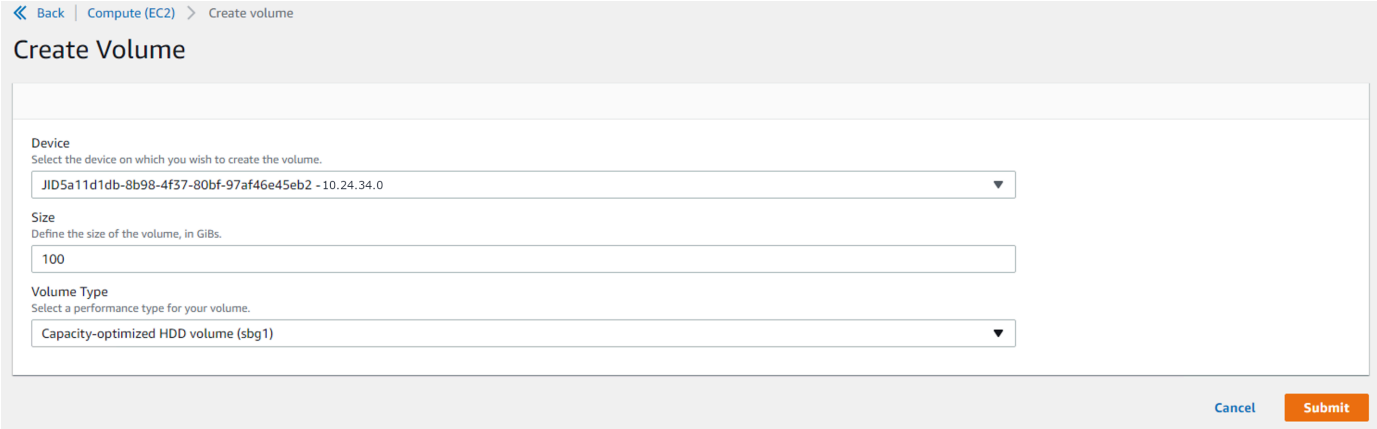
El Estado cambia a Terminando y, a continuación, cambia a Terminado cuando termina.

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

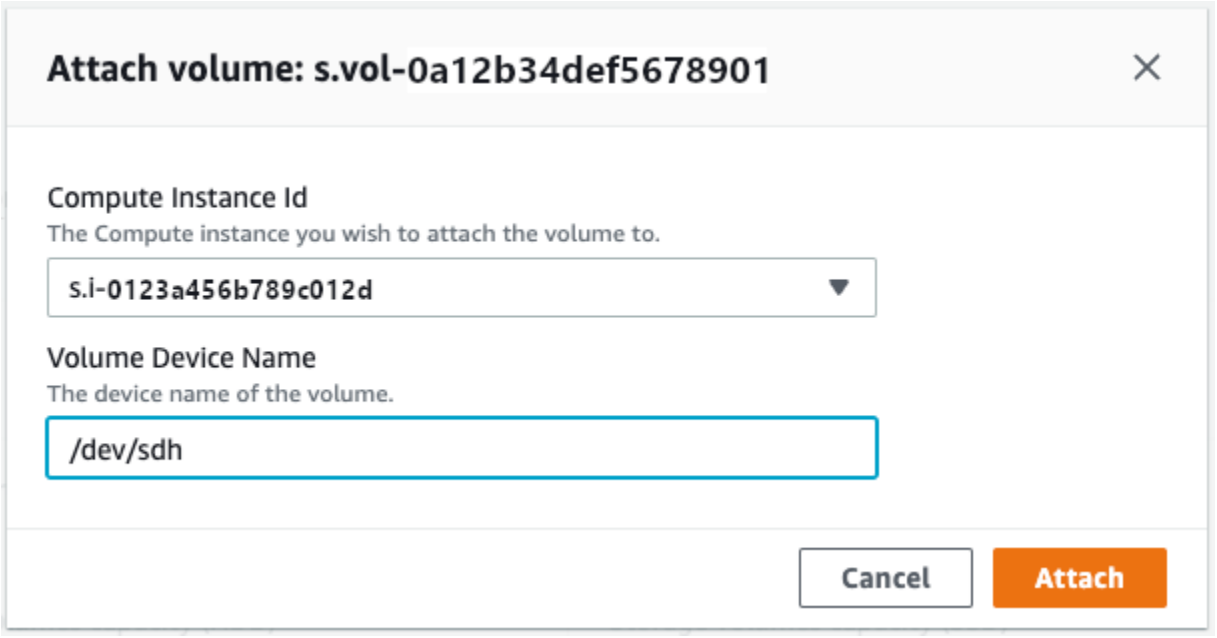
1. Abre la AWS OpsHub aplicación.
2. En la sección Iniciar computación del panel, seleccione Comenzar. O bien, seleccione el menú Servicios en la parte superior y, a continuación, seleccione Compute (EC2) para abrir la página Computación.
3. Seleccione la pestaña Volúmenes de almacenamiento. Si tiene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

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.

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 Cómo AWS funciona Snowcone.

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.

> **Note**
>
> En la página de detalles del dispositivo AWS OpsHub, el espacio de almacenamiento disponible en los dispositivos Snowcone no es preciso hasta que se inicia la interfaz NFS.

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
- Configuración automática de la interfaz NFS
- Configuración manual de la interfaz NFS
- Administración de los puntos finales NFS en el dispositivo de la familia Snow
- Montaje de puntos finales NFS en ordenadores cliente
- Detener la interfaz NFS

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.

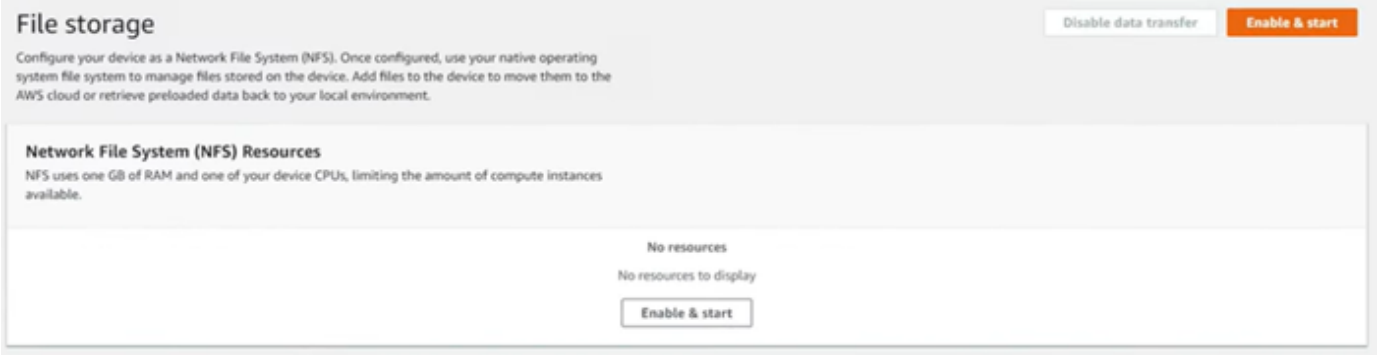
> **Note**
>
> Para activar las funciones de Windows, es posible que tenga que proporcionar un nombre de usuario y una contraseña de administrador para el equipo.

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.

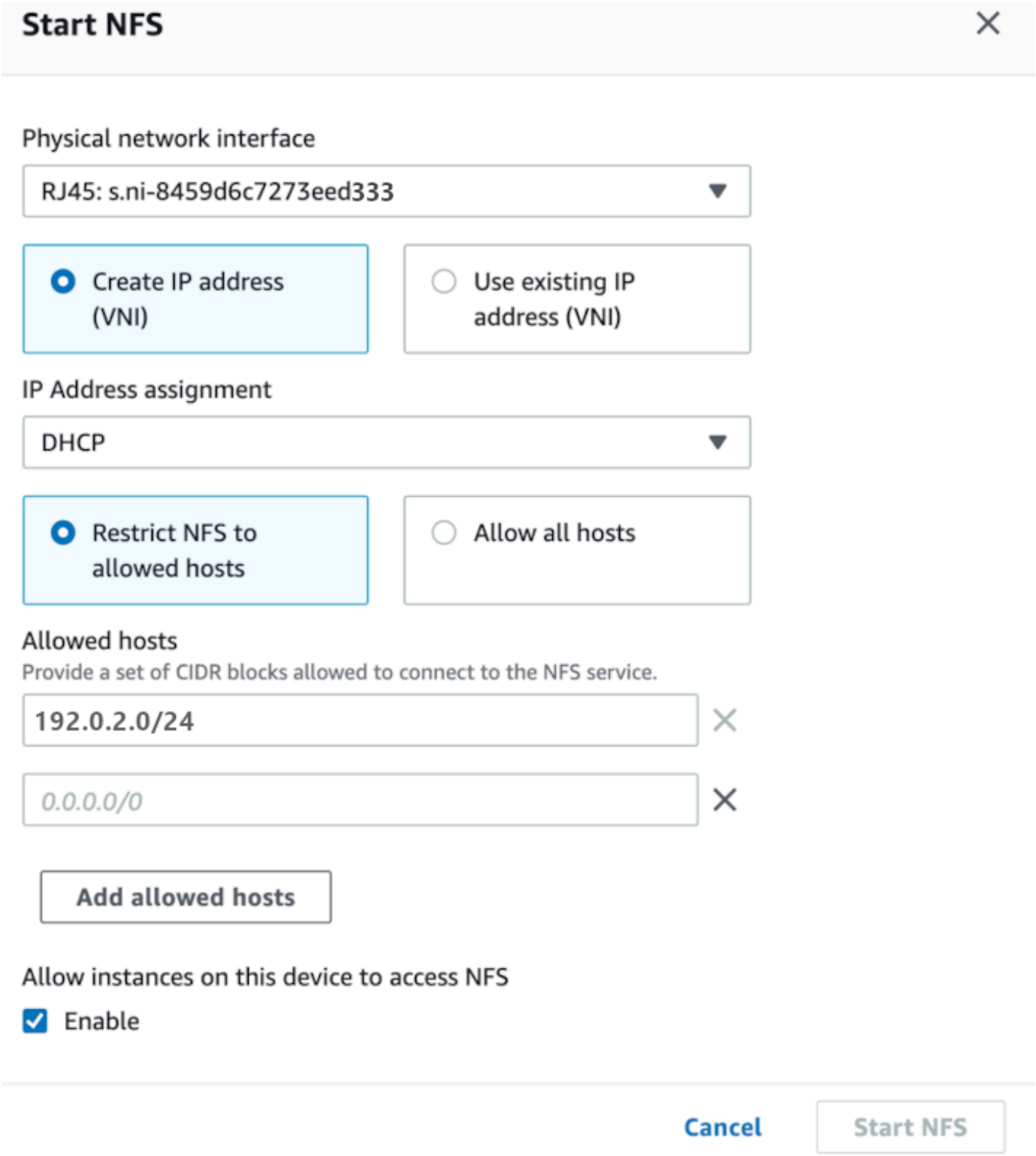
Configuración manual de la interfaz NFS

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.

Se utiliza DataSync para transferir archivos a AWS

Puede usarlo AWS OpsHub para crear un AWS DataSync agente en su dispositivo Snowcone. Puede utilizarlo para transferir archivos entre su dispositivo y Amazon S3, Amazon Elastic File System (Amazon EFS) o FSx for Windows File Server en la Nube de AWS.

AWS DataSync es un servicio de transferencia de datos en línea diseñado para simplificar, automatizar y acelerar la copia de grandes cantidades de datos desde y hacia los servicios de AWS almacenamiento. DataSync copia datos a través de Internet o AWS Direct Connect. Al ser un servicio totalmente gestionado, DataSync elimina gran parte de la necesidad de modificar aplicaciones, desarrollar scripts o gestionar la infraestructura.

DataSync admite la transferencia de datos entre Network File System (NFS) y Amazon EFS, Amazon S3 o Amazon FSx for Windows File Server.

Para obtener información sobre la combinación de ubicaciones de origen y destino que admite AWS DataSync, consulte Trabajar con ubicaciones en la Guía del AWS DataSync usuario.

Snowcone viene con el DataSync agente, que es una máquina virtual (VM) que se utiliza para leer o escribir datos de un sistema de almacenamiento local. Para usarlo DataSync, primero hay que iniciar el agente y, a continuación, ir a la DataSync consola y activarlo. Para obtener más información DataSync, consulte Primeros pasos con AWS DataSync.

Para iniciar el DataSync agente

1. Antes de iniciar el DataSync agente, active NFS en su dispositivo Snowcone. Consulte Configuración automática de la interfaz NFS y Inicio de NFS y restricción del acceso.
2. En el AWS OpsHub panel, seleccione Iniciar en la sección Sincronizar con la nube para abrir el asistente Iniciar el DataSync agente. El formulario Iniciar DataSync agente se rellena con los campos Dirección IP del dispositivo e Interfaz de red física.

3. Elija Crear dirección IP (VNI) para crear una dirección IP virtual 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.

   Si elige Usar la dirección IP existente, elija una interfaz virtual en el cuadro de lista Interfaz de red virtual.
5. Elija Iniciar el agente. Se le redirigirá a la página DataSync de recursos. La dirección IP del agente podría tardar hasta cinco minutos en aparecer.
6. Utilice el icono de copia para copiar el valor de la dirección IP del agente desde el archivo de direcciones IP del agente y seleccione Abrir DataSync consola.

   Esto abre la DataSync consola, donde puede activar el agente y transferir los archivos. El resto de la configuración se realiza en la AWS DataSync consola.

Transferir archivos con DataSync

AWS Snowcone ya ha creado el agente, por lo que solo necesita activarlo, configurar la ubicación de origen y destino, crear una tarea e iniciarla.

Para activar el DataSync agente y usar el DataSync servicio

1. Abra la AWS DataSync consola en https://console.aws.amazon.com/datasync/.
2. En la sección Activación de la página Crear agente, pegue la dirección IP que copió en el cuadro de texto Dirección del agente y elija Obtener clave. El navegador se conecta a la dirección IP y obtiene una clave de activación exclusiva del agente.
3. Una vez activado el agente, configurará el NFS que se ejecuta en su dispositivo Snowcone como ubicación de origen para. DataSync Para obtener instrucciones, consulte Configuración de una ubicación de origen en la Guía del usuario de AWS DataSync .

   > **Note**
   >
   > El DataSync agente que se ejecuta en el dispositivo Snowcone puede transferir archivos a y desde una ubicación accesible en la red.

4. En la página Configurar un destino, elija y configure el destino al que desea transferir archivos. Para obtener instrucciones, consulte Configuración de una ubicación de destino en la Guía del usuario de AWS DataSync .
5. Configure la tarea. Para obtener instrucciones, consulte Configure task settings en la Guía del usuario de AWS DataSync .
6. Revise la configuración y cree la tarea. Para obtener instrucciones, consulte Review your settings and create your task en la Guía del usuario de AWS DataSync .
7. Inicie la tarea y espere a que sus archivos se transfieran. Para obtener instrucciones, consulte Start your task en la Guía del usuario de AWS DataSync .

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
- Cómo obtener actualizaciones para su dispositivo y la AWS OpsHub aplicación
- Administración de perfiles

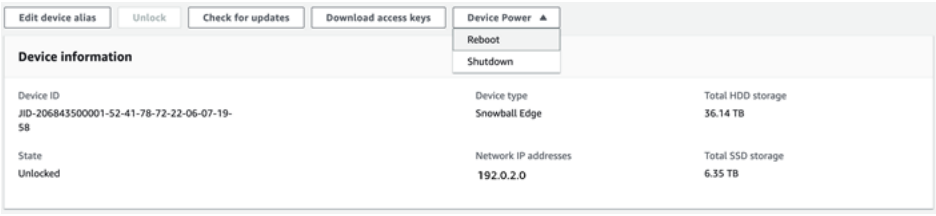
Reinicio del dispositivo

Sigue estos pasos AWS OpsHub para reiniciar tu dispositivo Snow.

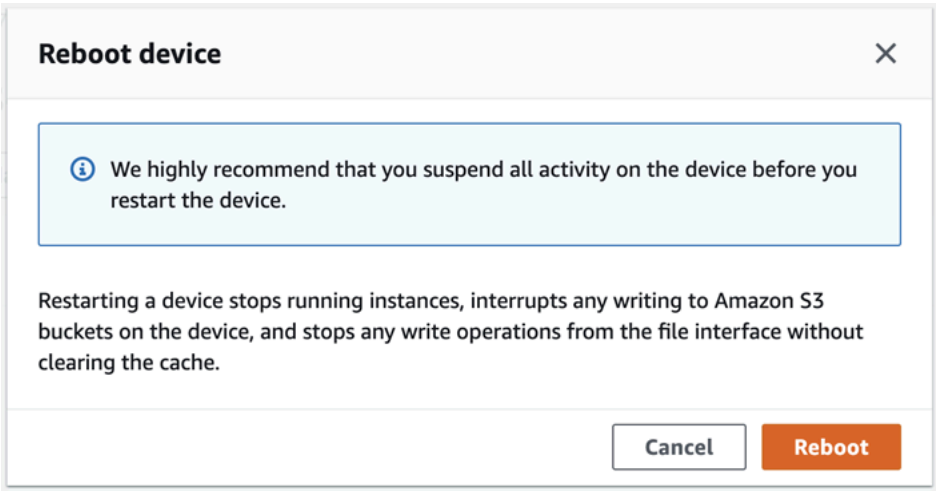
> **Important**
>
> Se recomienda encarecidamente suspender todas las actividades del dispositivo antes de reiniciarlo. Al reiniciar un dispositivo, se detienen las instancias en ejecución e interrumpe cualquier escritura en los buckets de Amazon S3 del dispositivo.

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.



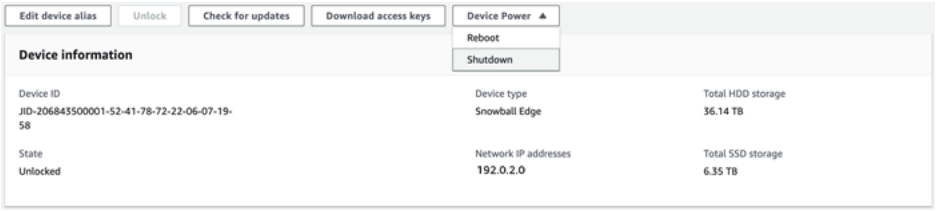
Apagado del dispositivo

Sigue estos pasos AWS OpsHub para apagar tu dispositivo Snow.

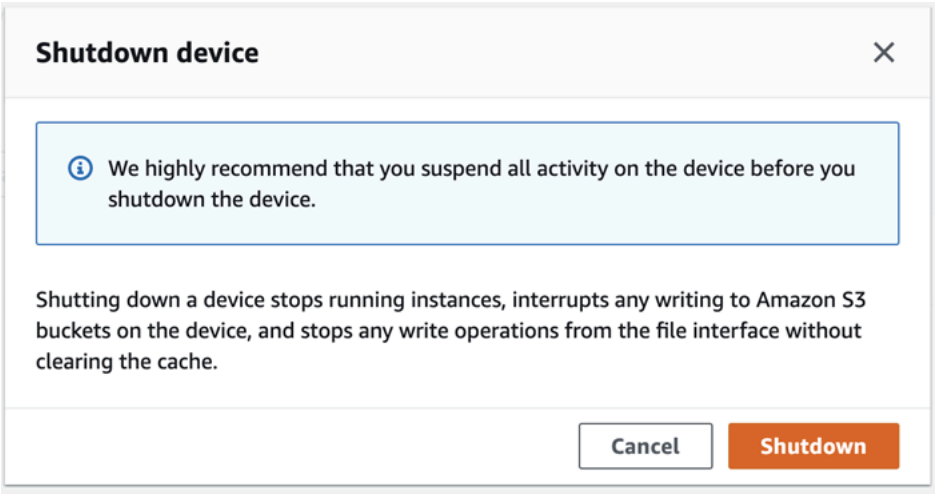
> **Important**
>
> Se recomienda encarecidamente suspender todas las actividades del dispositivo antes de apagarlo. Al apagar un dispositivo, se detienen las instancias en ejecución e interrumpe cualquier escritura en los buckets de Amazon S3 del dispositivo.

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.

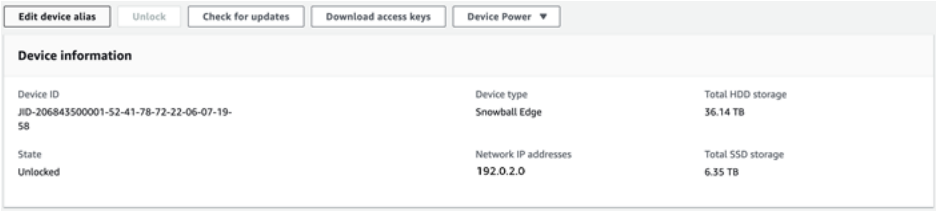


Edición del alias del dispositivo

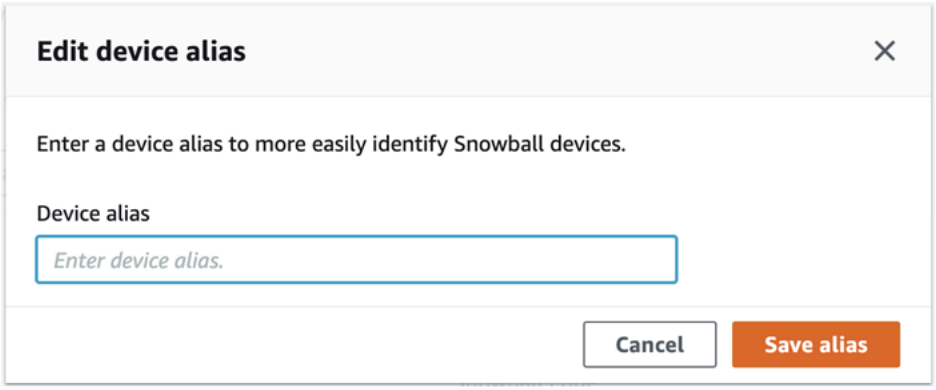
Sigue estos pasos para editar el alias de tu dispositivo utilizando AWS OpsHub.

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.



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.

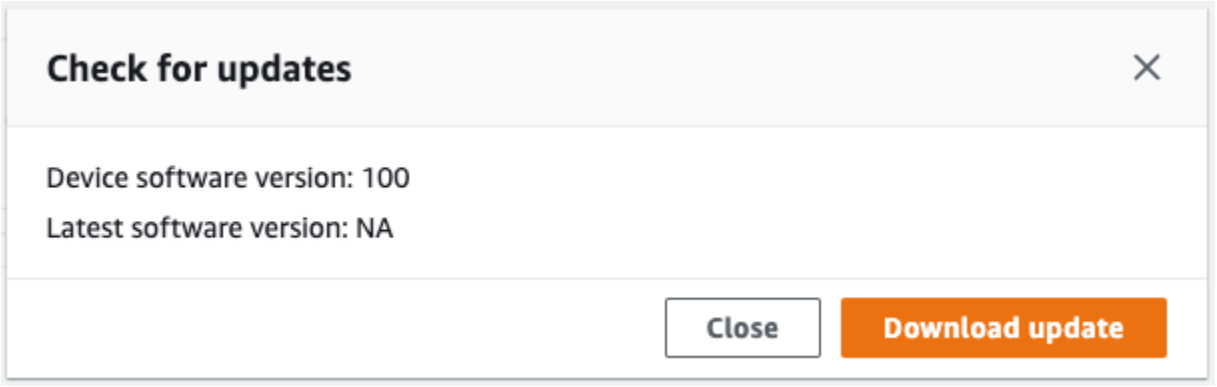
Actualización del dispositivo

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.



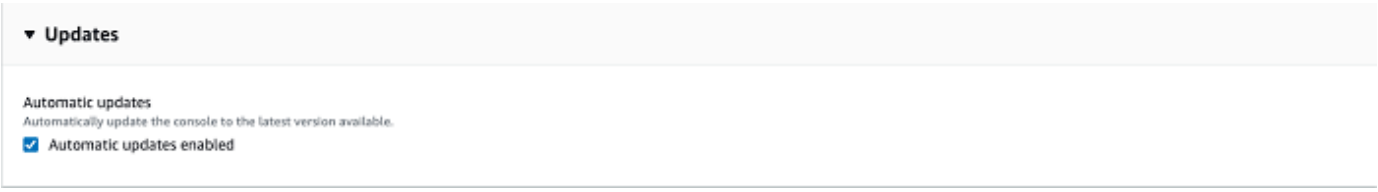
3. Si hay alguna actualización, seleccione Descargar actualización. De lo contrario, seleccione Cerrar.

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.

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.

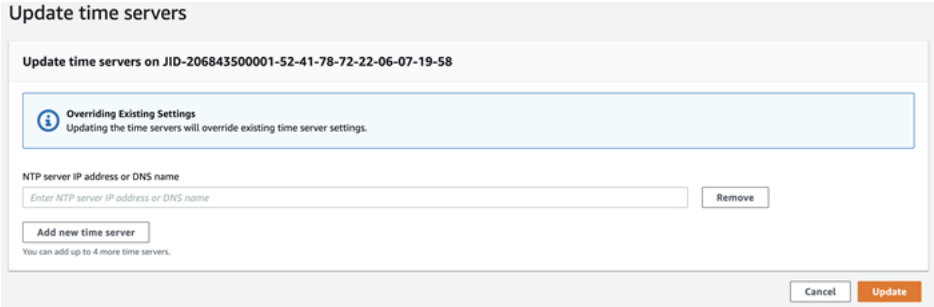
   La tabla Fuentes de tiempo tiene cuatro columnas:

   - 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.



Uso del AWS Snowball Edge cliente

El cliente Snowball Edge es una aplicación de terminal independiente que se ejecuta en el servidor local para desbloquear el AWS Snowcone dispositivo y obtener credenciales, registros e información de estado. Cuando utilice el cliente de Snowball Edge, puede obtener información de soporte adicional si ejecuta el comando `snowballEdge help`.

Al leer y escribir datos en el AWS Snowcone dispositivo, se utiliza la interfaz NFS. También puede utilizar la AWS OpsHub for Snow Family aplicación para gestionar los dispositivos de la familia Snow, incluidos los dispositivos Snowcone. Para obtener más información, consulte Uso AWS OpsHub for Snow Family para administrar dispositivos.

Descarga e instalación del cliente de Snowball Edge

Puede descargar e instalar el cliente de Snowball Edge desde Recursos de AWS Snowball. En esa página, puede encontrar el paquete de instalación correspondiente a su sistema operativo y seguir 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/`. Tenga en cuenta que el cliente de Snowball Edge solo se admite en distribuciones de 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`.

Comandos para el cliente de Snowball Edge

A continuación encontrará información sobre los comandos del cliente de Snowball Edge, incluidos ejemplos de uso y de resultados.

> **Note**
>
> El AWS Snowcone dispositivo utiliza los mismos comandos CLI de Snowball Edge, pero no admite los comandos que se aplican a la agrupación en clústeres.

Temas

- Configuración de un perfil para el cliente de Snowball Edge
- Obtención del código QR para validación por NFC
- Desbloquear un dispositivo AWS Snowcone
- Actualización de un dispositivo Snowcone
- Obtención de credenciales
- Inicio de un servicio en su dispositivo Snowcone
- Detención de un servicio en su dispositivo Snowcone
- Obtención de su certificado para la transferencia de datos
- AWS Snowcone Registros
- Obtención del estado de los dispositivos
- Obtención del estado de los servicios
- Lanzamiento de la AWS DataSync AMI
- Inicio de NFS y restricción del acceso
- Restricción del acceso a recursos compartidos de NFS cuando NFS está en ejecución
- Obtención de la ruta de exportación de un bucket de Amazon S3
- Habilitar la depuración por AWS parte del operador local
- Desactivación de la depuración por parte de operadores locales AWS
- Creación de una interfaz de red directa
- Obtención de información sobre una interfaz de red directa
- Actualización de una interfaz de red directa
- Eliminación de una interfaz de red directa
- Comprobación del estado de las características
- Cambio del estado de las características
- Configuración de servidores de tiempo
- Comprobación de las fuentes de tiempo

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 Obtención de credenciales.

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-.config`.

El punto de conexión es la dirección IP, a la que se añade `https://`. Puede localizar la dirección IP del AWS Snowcone dispositivo en la pantalla LCD del AWS Snowcone dispositivo. La primera vez que el dispositivo AWS Snowcone se conecta a la red, obtiene automáticamente una dirección IP 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 AWS los servicios en AWS Snowcone.

> **Important**
>
> Cualquier persona que pueda obtener acceso al archivo de configuración puede obtener acceso a los datos de su dispositivo Snowcone. 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 Ejemplo de salida

```
Configuration will be stored at home directory\.aws\snowball\config\snowball-.config
Snowcone  Manifest Path: Path/to/manifest/file
```

```
Unlock Code: 29 character unlock code
Default Endpoint: https://192.0.2.0
```

Puede tener varios perfiles si tiene varios trabajos a la vez. 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 para el dispositivo que usará con la aplicación AWS Snowcone Verification App. Puede descargar esta aplicación en la App Store de Apple o en la Google Play Store. 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 Ejemplo de salida

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

Desbloquear un dispositivo AWS Snowcone

Para desbloquear un AWS Snowcone dispositivo independiente, ejecute el `snowballEdge unlock-device` comando. Estos comandos autentican su acceso al AWS Snowcone dispositivo.

Al ejecutar uno de estos comandos de desbloqueo, puede introducir manualmente la ruta al archivo de manifiesto, el código de desbloqueo de 29 caracteres y la dirección IP del dispositivo independiente. Este proceso puede resultar tedioso, por lo que le recomendamos que configure en su lugar el cliente de Snowball Edge. Si ya ha configurado el cliente de Snowball Edge, solo tiene que introducir el comando propiamente dicho sin la ruta al manifiesto, el código de desbloqueo ni la dirección IP.

> **Note**
>
> Para desbloquear el dispositivo asociado a su trabajo, debe estar in situ, conectado a la alimentación eléctrica y a la red y encendido. Además, la pantalla LCD de la parte frontal del AWS Snowcone dispositivo debe indicar que el dispositivo está listo para su uso.

Uso (cliente de Snowball Edge configurado)

```
snowballEdge unlock-device
```

Example

Example Resultados de desbloqueo

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

Actualización de un dispositivo Snowcone

Los siguientes comandos pueden utilizarse para descargar e instalar actualizaciones de un dispositivo Snowcone. Para obtener información sobre los procedimientos que utilizan estos comandos, consulte Actualización de un dispositivo Snowcone .

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

Uso (cliente de Snowball Edge configurado)

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

Example Ejemplo de salida

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

`snowballEdge describe-device-software`: devuelve la versión actual del software del dispositivo. Además, si la actualización se está descargando, también se muestra el estado de la descarga. Si hay una actualización de software en curso, también se muestra el manifiesto de la versión de la actualización y el estado de la instalación. 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 Ejemplo de salida

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

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

Uso (cliente de Snowball Edge configurado)

```
snowballEdge download-updates
```

Example Ejemplo de 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 Snowcone que ya se habían descargado.

Uso (cliente de Snowball Edge configurado)

```
snowballEdge install-updates
```

Example Ejemplo de 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 Ejemplo de 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 Ejemplo de 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 Ejemplo de 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 comandos `snowballEdge list-access-keys` y `snowballEdge get-secret-access-key`, puede obtener sus credenciales locales. Los utilizas para autenticar tus solicitudes cuando utilizas el SDK o con él. AWS CLI AWS Estas credenciales están asociadas exclusivamente con un único trabajo de Snowcone y solo se pueden utilizar en el dispositivo. El dispositivo no tiene ningún permiso de AWS Identity and Access Management (IAM) en la Nube de AWS.

Para obtener más información, consulte Credenciales de AWS y Uso del punto de conexión de Amazon EC2.

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

Uso (cliente de Snowball Edge configurado)

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

Example Ejemplo de salida

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

Uso (cliente de Snowball Edge configurado)

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

Example Ejemplo de salida

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

Inicio de un servicio en su dispositivo Snowcone

Snowcone admite varios servicios, incluidas las instancias de procesamiento, la interfaz de archivos NFS, Amazon EC2 y. AWS DataSync Puede iniciar estos servicios con el comando `snowballEdge start-service`. 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 Ejemplo de 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 Snowcone

Para detener un servicio que se está ejecutando en su dispositivo Snowcone, puede usar el comando `snowballEdge stop-service`. Los servicios de Amazon EC2 no se pueden detener.

> **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.

Uso (cliente de Snowball Edge configurado)

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

Example Ejemplo de salida

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

Obtención de su certificado para la transferencia de datos

Para transferir datos a un dispositivo Snowcone, utilice la interfaz NFS o. AWS DataSync Si desbloquea el dispositivo Snowcone con otra dirección IP, se genera un certificado nuevo y el antiguo ya no se puede utilizar con el punto de conexión. Puede obtener un nuevo certificado actualizado para el dispositivo Snowcone mediante el comando `get-certificate`.

Es posible obtener un listado de estos certificados y descargarlos desde su dispositivo Snowcone con los siguientes comandos:

- `list-certificates`: muestra los nombres de recursos de Amazon (ARN) para los certificados que están disponibles para su uso.

  Uso (cliente de Snowball Edge configurado)

  ```
  snowballEdge list-certificates
  ```

Example Ejemplo de salida

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

- `get-certificate`: obtiene un certificado específico, en función del ARN proporcionado.

  Uso (cliente de Snowball Edge configurado)

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

  Example Ejemplo de salida

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

AWS Snowcone Registros

Al transferir datos entre el centro de datos en las instalaciones y un dispositivo Snowcone, 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 Ejemplo de salida

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

- `get-log`— Descarga una copia de un registro específico del dispositivo Snowcone 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 Ejemplo de salida

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

- `get-support-logs`: descarga una copia de todos los registros de tipo `SUPPORT` del dispositivo Snowcone en la ruta especificada de su servicio.

  Uso (cliente de Snowball Edge configurado)

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

Example Ejemplo de salida

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

> **Important**
>
> Los registros CUSTOMER pueden contener información confidencial sobre sus propios datos. Para proteger esta información potencialmente confidencial, recomendamos encarecidamente eliminar estos registros una vez que haya terminado de usarlos.

Obtención del estado de los dispositivos

Puede determinar el estado y la situación general de sus dispositivos Snowcone con los siguientes comandos del cliente de Snowball Edge:

- `describe-device`

  Uso (cliente de Snowball Edge configurado)

  ```
  snowballEdge describe-device
  ```

  Example Ejemplo de salida

  ```
  {
    "DeviceId" : "JIDbEXAMPLE-7eed-1234-ABCD-7EXAMPLE123c",
    "UnlockStatus" : {
      "State" : "UNLOCKED"
    },
    "ActiveNetworkInterface" : {
      "IpAddress" : "192.168.1.2"
    },
    "PhysicalNetworkInterfaces" : [ {
      "PhysicalNetworkInterfaceId" : "s.ni-8bEXAMPLE5EXAMPLE",
      "PhysicalConnectorType" : "RJ45",
      "IpAddressAssignment" : "DHCP",
  ```

```
    "IpAddress" : "192.168.1.13",
    "Netmask" : "255.255.255.0",
    "DefaultGateway" : "192.168.1.1",
    "MacAddress" : "EX:AM:PL:E0:12:34"
  }, {
    "PhysicalNetworkInterfaceId" : "s.ni-84EXAMPLE3EXAMPLE",
    "PhysicalConnectorType" : "RJ45_2",
    "IpAddressAssignment" : "STATIC",
    "IpAddress" : "0.0.0.0",
    "Netmask" : "0.0.0.0",
    "DefaultGateway" : "192.168.1.1",
    "MacAddress" : "EX:AM:PL:E0:12:34"
  }, {
    "PhysicalNetworkInterfaceId" : "s.ni-87EXAMPLE5EXAMPLE",
    "PhysicalConnectorType" : "WIFI",
    "IpAddressAssignment" : "STATIC",
    "IpAddress" : "0.0.0.0",
    "Netmask" : "0.0.0.0",
    "DefaultGateway" : "192.168.1.1",
    "MacAddress" : "EX:AM:PL:E0:12:34"
  } ],
  "DeviceCapacities" : [ {
    "Name" : "HDD Storage",
    "Unit" : "Byte",
    "Total" : 157242114048,
    "Used" : 81604378624,
    "Available" : 75637735424
  }, {
    "Name" : "SSD Storage",
    "Unit" : "Byte",
    "Total" : 0,
    "Used" : 0,
    "Available" : 0
  }, {
    "Name" : "vCPU",
    "Unit" : "Number",
    "Total" : 3,
    "Used" : 3,
    "Available" : 0
  }, {
    "Name" : "Memory",
    "Unit" : "Byte",
    "Total" : 5368709120,
    "Used" : 5368709120,
```

```
    "Available" : 0
  }, {
    "Name" : "GPU",
    "Unit" : "Number",
    "Total" : 0,
    "Used" : 0,
    "Available" : 0
  } ],
  "DeviceType" : "SNC1_HDD"
}
```

Obtención del estado de los servicios

Puede determinar el estado y la situación general de los servicios que se ejecutan en dispositivos Snowcone 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 Ejemplo de salida

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

- `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.
  - `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 Ejemplo de salida

```
{
"ServiceId" : "ec2",
  "Status" : {
    "State" : "ACTIVE"
  },
"Storage" : {
"TotalSpaceBytes" : 99608745492480,
"FreeSpaceBytes" : 99608744468480
},
"Endpoints" : [ {
"Protocol" : "http",
"Port" : 8080,
"Host" : "192.0.2.0"
}, {
"Protocol" : "https",
"Port" : 8443,
"Host" : "192.0.2.0",
"CertificateAssociation" : {
"CertificateArn" : "arn:aws:snowball-
device:::certificate/6d955EXAMPLEdb71798146EXAMPLE3f0"
}
} ]
}
```

Lanzamiento de la AWS DataSync AMI

Lanza la AWS DataSync AMI en Snowcone.

Uso (cliente de Snowball Edge configurado)

AWS DataSync debe lanzarse con el tipo de `snc1.medium` instancia. El lanzamiento DataSync con un tipo de instancia diferente puede provocar una operación inestable y una posible pérdida de datos. Utilice el comando `describe-images` para buscar la imagen desde la que se va a lanzar una instancia. El resultado es similar al siguiente.

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

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

Example Ejemplo de salida

```
{
    "Reservations": [
        {
            "Instances": [
                {
                    "AmiLaunchIndex": 0,
                    "ImageId": "s.image id",
                    "InstanceId": "s.instance id",
                    "InstanceType": "snc1.medium",
                    "LaunchTime": "2020-03-06T18:58:36.609Z",
                    "PrivateIpAddress": "ip address",
                    "State": {
                        "Code": 16,
                        "Name": "running"
                    },
                    "BlockDeviceMappings": [
```

```
                        {
                            "DeviceName": "/dev/sda",
                            "Ebs": {
                                "AttachTime": "2020-03-06T19:14:21.336Z",
                                "DeleteOnTermination": true,
                                "Status": "attached",
                                "VolumeId": "s.volume id"
                            }
                        }
                    ],
                    "EbsOptimized": false,
                    "EnaSupport": false,
                    "RootDeviceName": "/dev/sda",
                    "SecurityGroups": [
                        {
                            "GroupName": "default",
                            "GroupId": "s.security group id"
                        }
                    ],
                    "SourceDestCheck": false,
                    "CpuOptions": {
                        "CoreCount": 2,
                        "ThreadsPerCore": 1
                    }
                }
            ],
            "ReservationId": "s.r-80c8ee6b041b29eb4"
        },
    ]
}
```

Ejecución de la instancia.

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

Example Ejemplo de salida

```
{
    "Instances": [
        {
            "AmiLaunchIndex": 0,
            "ImageId": "s.ami-0623310b494365cc5",
```

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

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

El espacio de almacenamiento disponible en el dispositivo Snowcone no es preciso hasta que se inicia el servicio NFS.

Puede proporcionar bloques de CIDR para rangos de direcciones IP que puedan montar los recursos compartidos de 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 sus 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
```

Obtención de la ruta de exportación de un bucket de Amazon S3

No hay ningún comando específico de Snowcone para obtener la ruta de exportación de un bucket de Amazon S3. El formato de la ruta de exportación tiene el aspecto siguiente.

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

Habilitar la depuración por AWS parte del operador local

- `enable-local-aws-operator-debugging`— Habilita el dispositivo para la depuración por parte AWS del operador local abriendo el puerto SSH 22.

Uso (cliente de Snowball Edge configurado)

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

Desactivación de la depuración por parte de operadores locales AWS

- `disable-local-aws-operator-debugging`: deshabilita el dispositivo para que un operador local de AWS pueda realizar tareas de depuración en él cerrando el puerto SSH 22. De forma predeterminada, el puerto SSH 22 está cerrado. Cuando el dispositivo Snowcone se apaga o se pasa a un ciclo de alimentación, se desactiva la depuración por parte AWS del operador local.

Uso (cliente de Snowball Edge configurado)

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

Creación de una interfaz de red directa

- `create-direct-network-interface` : Crea una interfaz de red directa (DNI). Crea una interfaz de red directa para utilizarla con instancias de computación de Amazon EC2 de su dispositivo. Puede encontrar las interfaces de red directas disponibles en su dispositivo mediante el comando `describe-direct-network-interfaces`.

Uso (cliente de Snowball Edge configurado)

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

Obtención de información sobre una interfaz de red directa

- `describe-direct-network-interface` : obtiene las interfaces de red directas del dispositivo. Se puede utilizar una interfaz de red directa para configurar las redes para las instancias y los servicios de computación de Amazon EC2 del dispositivo. Puede crear una nueva interfaz de red directa mediante el comando `create-direct-network-interface`.

Uso (cliente de Snowball Edge configurado)

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

Actualización de una interfaz de red directa

- `update-direct-network-interface` : actualiza una interfaz de red directa. Utilice este comando para actualizar una interfaz de red directa que se utilizará con instancias de computación de Amazon EC2 de su dispositivo. Puede encontrar las interfaces de red directas que están disponibles en el dispositivo mediante el comando `describe-direct-network`-interfaces. Al modificar una interfaz de red que está asociada a una instancia de Amazon EC2, primero se desasocia la interfaz.

Uso (cliente de Snowball Edge configurado)

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

Eliminación de una interfaz de red directa

- `delete-direct-network-interface`: elimina una interfaz de red directa que ya no se utiliza. Para eliminar una interfaz de red directa asociada a su instancia de computación de Amazon EC2, primero debe desasociar la interfaz de red directa de su instancia.

Uso (cliente de Snowball Edge configurado)

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

Comprobación del estado de las características

Para ver el estado de las funciones disponibles en su dispositivo AWS Snow Device Management, incluidas las que le permiten gestionar el dispositivo Snowcone y los AWS servicios locales de forma remota, 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
}
```

Cambio del estado de las características

Para cambiar el estado de las funciones disponibles en el AWS Snowcone dispositivo, usa el `set-features` comando. Para activar o desactivar AWS Snow Device Management, lo que le permite gestionar su dispositivo Snowcone y los AWS servicios locales de forma remota, utilice el `--remote-management-state` parámetro. El dispositivo debe estar desbloqueado antes de ejecutar este comando.

Puede configurar Snow Device Management en los siguientes estados:

- `INSTALLED_ONLY`: la característica está instalada pero no habilitada.
- `INSTALLED_AUTOSTART`— La función está habilitada y el dispositivo intenta conectarse a ella Región de AWS cuando está encendida.

> **Note**
>
> El estado `NOT_INSTALLED` solo existe para identificar los dispositivos que no son compatibles con Snow Device Management o que ya estaban sobre el terreno antes de su lanzamiento. No es posible instalar ni desinstalar la característica en dispositivos que ya están implementados. Para utilizar Snow Device Management, debe pedir un dispositivo nuevo con la característica preinstalada.

Uso (cliente de Snowball Edge configurado)

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

Ejemplo de salida

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

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.

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.

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
- Activación de Snow Device Management
- Añadir permisos para Snow Device Management a una función de IAM
- Comandos de la CLI de Snow Device Management

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 especificaciones del AWS Snowcone dispositivo de .
- Desbloquee el dispositivo de la familia Snow. Para obtener más información, consulte un dispositivo localmente.

```
snowballEdge set-features /
  --remote-management-state INSTALLED_AUTOSTART /
  --manifest-file JID1717d8cc-2dc9-4e68-aa46-63a3ad7927d2_manifest.bin /
  --unlock-code 7c0e1-bab84-f7675-0a2b6-f8k33 /
  --endpoint https://192.0.2.0:9091
```

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
- Comprobación del estado de la tarea
- Comprobación de la información del dispositivo
- Comprobación del estado de la instancia compatible con Amazon EC2
- Comprobación de los metadatos de una tarea
- Cancelación de una tarea
- 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 las etiquetas de un dispositivo o de una tarea
- Obtención de una lista de tareas por estado
- Aplicación de etiquetas
- Eliminación de etiquetas

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+d1OKTP9+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
```

Uso de AWS los servicios en AWS Snowcone

A continuación, encontrará una descripción general del AWS Snowcone dispositivo. AWS Snowcone es un dispositivo físicamente robusto protegido por AWS Key Management Service (AWS KMS) que puede utilizar para almacenamiento e informática locales, o para transferir datos entre sus servidores locales y Amazon Simple Storage Service (Amazon S3).

Para obtener información sobre cómo desbloquear un AWS Snowcone dispositivo, consulte. Uso del AWS Snowball Edge cliente

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.

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

Temas

- Uso de instancias de computación compatibles con Amazon EC2
- Uso AWS DataSync para transferir archivos
- Administración de la interfaz NFS
- Uso de AWS IoT Greengrass para ejecutar software preinstalado en instancias compatibles con Amazon EC2
- Puertos necesarios para usar AWS los servicios en un AWS Snowcone dispositivo

Uso de instancias de computación compatibles con Amazon EC2

En este tema, encontrará información general sobre el uso de instancias de computación de Amazon Elastic Compute Cloud (Amazon EC2) en un dispositivo AWS Snowcone . Este tema contiene información conceptual, procedimientos y ejemplos.

> **Note**
>
> Estas funciones no se admiten en Asia Pacífico (Bombay) Región de AWS.

Información general

Puede ejecutar instancias de computación compatibles con Amazon EC2 alojadas en un dispositivo Snowcone utilizando los tipos de instancias compatibles con EC2 admitidas. Al igual que ocurre con sus homólogas basadas en la nube, estas instancias requieren el lanzamiento de imágenes de máquina de Amazon (AMI). Puede elegir la AMI que será la imagen base de una instancia en la nube antes de crear el trabajo de Snowcone. Para obtener información acerca de los tipos de instancia admitidos, consulte Uso de Amazon EC2 en Snowcone .

Si el tipo de trabajo es de computación local, puede crear volúmenes de EBS locales de 8 TiB en total y asociarlos a instancias compatibles con Amazon EC2. Esto permite que las instancias locales compatibles con EC2 obtengan acceso a más capacidad local que el volumen raíz por sí solo. Se trata únicamente de almacenamiento local, por lo que los datos escritos en los volúmenes de EBS se pierden cuando se devuelve el dispositivo, AWS ya que no se pueden importar a Amazon S3.

> **Note**
>
> El servidor de NFS no está disponible para trabajos de computación. Si necesita importar o exportar datos hacia o desde el Nube de AWS, no elija el tipo de trabajo de cómputo local al realizar el pedido.

Para usar una instancia de cómputo en un Snowcone, cree un trabajo para solicitar un dispositivo de la familia Snow y especifique sus AMI. Puede hacerlo desde Consola de administración de la familia de productos Snow de AWS, con o con uno de los AWS SDK. AWS CLI Normalmente, para poder utilizar las instancias, debe cumplir algunos requisitos organizativos previos 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 Snowcone 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 para los AWS SDK. La AWS OpsHub for Snow Family herramienta se utiliza para administrar las AMI, las instancias de cómputo y AWS los servicios. Para obtener más información, consulte Uso AWS OpsHub for Snow Family para administrar dispositivos.

Cuando termines de usar el dispositivo, devuélvelo a AWS. Si el dispositivo se utilizó en un trabajo de importación, los datos transferidos a través de la interfaz NFS se importan a Amazon S3. De lo contrario, llevaremos a cabo un borrado completo del dispositivo cuando se devuelva a 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 Snowcone.
- Los datos de las instancias de computación que se ejecutan en un dispositivo Snowcone no se importan a AWS.

Precios de las instancias de computación en Snowcone

Hay costos adicionales asociados con el uso de instancias de computación. Para más información, consulte Precios de AWS Snowcone.

Requisitos previos

Antes de crear un trabajo, tenga en cuenta la siguiente información:

- Antes de poder añadir cualquier AMI a su trabajo, debe tener una AMI y debe ser un tipo de imagen compatible. Cuenta de AWS Actualmente, las AMI compatibles se basan en los siguientes sistemas operativos:
  - Amazon Linux 2

    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), Ubuntu 20.04 LTS - Focal o Ubuntu 22.04 LTS - Jammy

> **Note**
>
> Ubuntu 16.04 LTS: las imágenes Xenial (HVM) ya no son compatibles con los dispositivos de la familia Snow a través de Amazon EC2 VM Import/Export AWS Marketplace, pero siguen siendo compatibles con su uso en dispositivos de la familia Snow a través de Amazon EC2 VM Import/Export y ejecutándose localmente en las AMI.

Puede obtener estas imágenes de AWS Marketplace.

Antes de agregar cualquier AMI a su solicitud de creación de trabajo, asegúrese de que tiene una o más AMI compatibles en su Cuenta de AWS.

- Todas las AMI deben residir en Amazon Elastic Block Store (Amazon EBS) y tener un solo volumen.
- Si tiene previsto conectarse a instancias de computación que se ejecutan en un dispositivo Snowcone, debe usar Secure Shell (SSH). Para ello, primero debe agregar el par de claves.

Creación de un trabajo con instancias de computación

En esta sección, creará su primer trabajo de instancia de computación.

> **Important**
>
> Tenga en cuenta lo siguiente antes de crear el trabajo:
>
> - Si va a utilizar una AMI de AWS Marketplace, asegúrese de que tiene un código de producto y un código de operación de uso compatibles. Para obtener más información, consulte Comprobar los códigos de producto y de opciones de uso de las AMI AWS Marketplace.
> - 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 configurar SSH para que se conecte a la instancia después de lanzar dicha instancia en el dispositivo Snowcone, debe realizar primero el siguiente procedimiento.
> - No se admite el uso de AMI cifradas o volúmenes de Amazon EBS cifrados en AWS Snowcone los dispositivos.

Comprobar los códigos de producto y de opciones de uso de las AMI AWS Marketplace

Antes de comenzar el proceso de añadir una AMI AWS Marketplace a su dispositivo de la familia Snow, asegúrese de que el producto y los códigos de uso de la AMI sean compatibles con su dispositivo 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 disponible, independientemente de su ubicación.
3. En el panel de navegación, elija AMIs.
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, para ver una lista de todas las AMI de Linux proporcionadas por AWS, seleccione Imágenes públicas. Después, utilice las opciones de búsqueda para acotar aún más 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. Vuelva a elegir la barra de búsqueda para elegir Platform (Plataforma), luego el operador = y, por último, el sistema operativo en la lista proporcionada.

   (Consola antigua) Elija la barra Search (Búsqueda) y, en el menú, elija Owner (Propietario) y, a continuación, el valor Amazon images (Imágenes de Amazon). Vuelva a elegir la barra Search (Búsqueda) para seleccionar Platform (Plataforma) y, a continuación, elija el sistema operativo en la lista proporcionada.

   > **Note**
   >
   > AWS Marketplace Entre las AMI de aws-marketplace se incluye 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.

> **Note**
>
> El código de producto avyfzznywektkgl5qv5f57ska es compatible en todas las regiones.

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. Para todas las regiones, asegúrese de que el código de operación de uso sea. RunInstances

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.

Configurar una AMI de forma que utilice SSH para conectarse a las instancias de computación lanzadas en el dispositivo

Si desea utilizar Secure Shell (SSH) para conectarse a las instancias de computación de los dispositivos Snowcone, 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.

Cómo poner una clave SSH en una AMI

1. Lance una nueva instancia en la imagen HVM Nube de AWS basada en la familia Amazon Linux 2 for Snow, CentOS 7 (x86_64), con actualizaciones, o Ubuntu 16.04 LTS, Xenial (HVM).

   Al lanzar la instancia, es conveniente que se asegure de que el espacio de almacenamiento que asigne a la instancia sea adecuado para el uso que se le dará en el dispositivo Snowcone. 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 la instancia de computación en un dispositivo Snowcone, consulte AWS Snowcone cuotas .
2. Instale y configure las aplicaciones que desea ejecutar en el dispositivo Snowcone 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 Snowcone. 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 usar la Consola de administración de la familia de productos Snow de AWS, siga las instrucciones que se indican en Introducción.

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 snowballEdge create-job --job-type IMPORT --resources '{"S3Resources":
[{"BucketArn":"arn:aws:s3:::bucket-name"}],"Ec2AmiResources":
[{"AmiId":"ami-12345678"}]}' --description Example --address-
id ADIEXAMPLE60-1234-1234-5678-41fEXAMPLE57  --kms-key-arn arn:aws:kms:us-
west-2:012345678901:key/eEXAMPLE-1234-1234-5678-5b4EXAMPLE8e --role-
arn arn:aws:iam::012345678901:role/snowball-local-s3-lambda-us-west-2-role --snowball-
capacity-preference T100 --shipping-option SECOND_DAY --snowball-type SNOWCONE
```

Cuando llegue el dispositivo y lo desbloquee, tendrá que utilizar el cliente de Snowball Edge para obtener las 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.

Los dispositivos Snowcone admiten ocho DNI por instancia compatible con EC2, con un máximo de 8 por dispositivo.

Temas

- Requisitos previos
- Configuración de una interfaz de red virtual (VNI)
- Configuración de una interfaz de red directa (DNI)

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 Snowcone.
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-01234567890123456
 --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
```

Comandos adicionales

Para ver todos los comandos disponibles para AWS Snowcone los dispositivos, consulte Uso del cliente de Snowball Edge.

Conexión a las instancias de computación de un dispositivo Snowcone mediante SSH

Si desea utilizar SSH para conectarse a las instancias de computación de un dispositivo Snowcone, debe proporcionar la clave SSH a la AMI antes de crear el trabajo. Si necesita más información sobre ese procedimiento, consulte Configurar una AMI de forma que utilice SSH para conectarse a las instancias de computación lanzadas en el dispositivo. Si no ha seguido ese procedimiento, no podrá utilizar SSH para conectarse a las instancias.

Para conectarse a la instancia con SSH

1. Asegúrese de que el dispositivo está encendido, conectado a la red y desbloqueado.
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.

Comandos del cliente de Snowcone 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 Snowcone. Para

obtener más información acerca de cómo utilizar el cliente de Snowball Edge (por ejemplo, cómo iniciar y detener servicios con él), consulte Uso del AWS Snowball Edge cliente.

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 Snowcone dispositivo, consulte. AWS CLI Comandos compatibles con Amazon EC2 compatibles con un Snowcone

> **Note**
>
> Los comandos relacionados con los clústeres no son compatibles y devolverán un error.

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 Snowcone dispositivo una vez desbloqueado, puede crear una configuración de lanzamiento. Para ello, utilice el comando `snowballEdge create-autostart-configuration`, cuyo uso se muestra a continuación.

Uso

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

Actualización de una configuración de lanzamiento para iniciar automáticamente instancias compatibles con EC2

Para actualizar una configuración de lanzamiento existente en su dispositivo Snowcone, 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]]
                                           [--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 está en uso, utilice el comando `snowballEdge delete-autostart-configuration`. Puede ver su uso 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 Snowcone, utilice el comando `describe-autostart-configurations`. Puede ver su uso a continuación.

Uso

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

Creación de una interfaz de red virtual

Para ejecutar una instancia de procesamiento en su Snowcone o iniciar la interfaz NFS en su Snowcone, primero debe crear una interfaz de red virtual (VNIC). Cada dispositivo Snowcone tiene tres interfaces de red (NIC), los controladores de interfaz de red física del dispositivo. Son los puertos RJ45 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"
  }
}
```

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"
  },{
    "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"
  }
]
```

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 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
- Ejemplos de recuperación de metadatos de instancia mediante IMDSv1 e IMDSv2

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 punto de conexión compatible con Amazon EC2

A continuación, encontrará información general sobre el punto de conexión compatible con Amazon Elastic Compute Cloud (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.

Temas

- Especificar el punto final compatible con Amazon EC2 como punto final AWS CLI
- Características de Amazon EC2 no compatibles con Snowcone
- AWS CLI Comandos compatibles con Amazon EC2 compatibles con un Snowcone
- Operaciones de la API de Amazon EC2 admitidas

Especificar el punto final compatible con Amazon EC2 como punto final AWS CLI

Cuando utiliza el comando AWS CLI para enviar un comando al AWS Snowcone dispositivo, puede especificar que el punto final sea el punto final 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. El cifrado está protegido con un certificado generado por el dispositivo Snowcone 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.

Para asociar el certificado al punto de conexión compatible con Amazon EC2

1. Conecte el dispositivo Snowcone 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 Snowcone.
4. Ejecute el comando `snowballEdge get-certificate` en el terminal. Para obtener más información acerca de este comando, consulte Obtención de su certificado para la transferencia de datos.
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.snowcone.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.

Características de Amazon EC2 no compatibles con Snowcone

El punto de conexión compatible con Amazon EC2 le permite administrar mediante programación las AMI y las instancias de computación de los dispositivos Snowcone con operaciones de la API compatibles con Amazon EC2. Sin embargo, no todas las características y operaciones de la API pueden utilizarse con dispositivos Snowcone.

No se admite ninguna característica o acción que no se indique explícitamente en esta guía. Por ejemplo, las siguientes acciones de Amazon EC2 no se pueden usar con Snowcone:

- create-nat-gateway
- create-key-pair

AWS CLI Comandos compatibles con Amazon EC2 compatibles con un Snowcone

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 Snowcone

A continuación, encontrará una descripción del subconjunto de AWS CLI comandos y opciones de Amazon EC2 compatibles con los dispositivos Snowcone. 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: adjunta un volumen de Amazon EBS a una instancia detenida o en ejecución del AWS Snowcone 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 Amazon EC2 de destino.
  - --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 su uso con un dispositivo Snowcone. 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 Snow.
  - --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 AWS Snowcone 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"
            }
         ]
      }
   ]
}
```

- [--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 de Amazon EC2. Para obtener más información, consulte Especificar el punto final compatible con Amazon EC2 como punto final 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 de Amazon EC2. Para obtener más información, consulte Especificar el punto final compatible con Amazon EC2 como punto final 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
- create-security-group— Crea un grupo de seguridad en el dispositivo Snowcone. 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 adjuntar a una instancia del dispositivo. AWS Snowcone
  - [--size`value`]: 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 de Amazon EC2. Para obtener

más información, consulte Especificar el punto final compatible con Amazon EC2 como punto final 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 de Amazon EC2.
- 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 disponibles se agregan al dispositivo Snowcone al crear el trabajo.
  - --image-id: el ID de AMI de Snowcone 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-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 de Amazon EC2. Para obtener más información, consulte Especificar el punto final compatible con Amazon EC2 como punto final 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 de Amazon EC2. Para obtener más información, consulte Especificar el punto final compatible con Amazon EC2 como punto final 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 de Amazon EC2. Para obtener más información, consulte Especificar el punto final compatible con Amazon EC2 como punto final 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 de Amazon EC2. Para obtener

más información, consulte Especificar el punto final compatible con Amazon EC2 como punto final 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 mediante un ID de AMI de Snowcone para una AMI.

> **Note**
>
> Se puede tardar hasta una hora y media en lanzar instancias de computación en un dispositivo Snowcone, en función del 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 Snowcone 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.

- 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.

Operaciones de la API de Amazon EC2 admitidas

A continuación, encontrará las operaciones de la API de Amazon EC2 que puede utilizar con un dispositivo Snowcone, con enlaces a sus descripciones en la Referencia de la API de Amazon EC2.Las llamadas a la API de Amazon EC2 requieren la firma 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.

- 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 su uso con un dispositivo Snowcone. 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 Snowcone. 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`
- 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**
>
> Se puede tardar hasta una hora y media en lanzar instancias de computación en un dispositivo Snowcone, en función del 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 Snowcone dispositivo mediante plantillas de lanzamiento y comandos de configuración de lanzamiento del

cliente Snowball Edge. Si una instancia sale, el inicio automático la iniciará, pero si elimina la instancia o actualiza la configuración de inicio automático de la instancia, el inicio automático iniciará una nueva instancia.

Una plantilla de lanzamiento contiene la información de configuración necesaria para crear una instancia compatible con Amazon EC2 en su dispositivo Snowcone. 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 el dispositivo Snowcone.

Cuando utiliza configuraciones de inicio automático en su dispositivo Snowcone, debe configurar los parámetros con los que desea que se inicie su instancia compatible con Amazon EC2. Una vez configurado el dispositivo Snowcone, 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 posteriores de las instancias (tras un reinicio planificado o imprevisto) se producen automáticamente una vez desbloqueado el dispositivo. AWS Snowcone

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 lanzar automáticamente instancias compatibles con Amazon EC2 en el dispositivo Snowcone, siga estos pasos:

1. Cuando pidas tu AWS Snowcone dispositivo, crea una tarea para solicitar un dispositivo de la familia Snow con instancias de cómputo. Para obtener más información, consulte Creación de un trabajo con instancias de computación.
2. Tras recibir el dispositivo Snowcone, desbloquéelo.
3. Utilice el comando `aws ec2 create-launch-template` de la API de EC2 para crear una plantilla de lanzamiento. Para obtener más información, consulte Lista de comandos de la AWS CLI compatibles con Amazon EC2 admitidos en un dispositivo Snowcone .

> **Note**
>
> El punto de conexión de Amazon EC2 es el punto de conexión del dispositivo.

4. Utilice el comando `snowballEdge create-autostart-configuration` del cliente de Snowball Edge para enlazar su plantilla de lanzamiento 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. Reinicia y desbloquea AWS Snowcone 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 Snowcone.

Para ver el estado de las instancias en ejecución, use el comando `describe-autostart-configurations` de la API de EC2.

> **Note**
>
> No existe una consola ni una API de administración de AWS Snowball trabajos que permita lanzar plantillas. Puede utilizar los comandos de la CLI de EC2 y del cliente de Snowball Edge para iniciar automáticamente instancias compatibles con EC2 en su dispositivo AWS Snowcone .

Uso del almacenamiento en bloques con sus instancias compatibles con Amazon EC2

El almacenamiento en bloque en Snowcone le permite agregar o eliminar almacenamiento en bloque 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 de EC2. Estos son algunos de los comandos admitidos: `attach-volume`, `create-volume`, `delete-volume`, `detach-volume` y `describe-volumes`. Para obtener más información sobre estos comandos,

consulte Lista de comandos de la AWS CLI compatibles con Amazon EC2 admitidos en un dispositivo Snowcone .

> **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 AWS Snowcone y los volúmenes de Amazon EBS en la nube:

- Los volúmenes de Amazon EBS solo están disponibles para las instancias compatibles con EC2 que se ejecutan en el AWS Snowcone 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`.
- Los volúmenes raíz de 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 8 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 Snowcone . Sin embargo, la capacidad total del volumen de Amazon EBS está limitada por el espacio disponible en el AWS Snowcone dispositivo.

Grupos de seguridad en dispositivos Snow

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 los 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 Snowcone son similares a los grupos de seguridad de la Nube de AWS. Las nubes virtuales privadas (VPC) no se admiten en los dispositivos Snowcone.

En la siguiente tabla, puede ver las demás diferencias que existen entre los grupos de seguridad de Snowcone y los grupos de seguridad de la VPC de EC2:

- Cada dispositivo Snowcone 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 Snowcone . Para obtener más información acerca de las operaciones de API permitidas, consulte Operaciones de la API de 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. Snowcone 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 un dispositivo Snowcone

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.
`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.

Datos	Descripción
userData	Scripts de intérprete de comandos para enviar instrucciones a una instancia en el momento del lanzamiento.

Categorías de datos dinámicos de instancia admitidos en un dispositivo Snowcone

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.

Modificación de los datos de usuario en las instancias de computación de Snowcone

Se pueden usar datos de usuario con scripts de intérprete de comandos en instancias de computación de un dispositivo Snowcone. 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 las instancias de computación que se están ejecutando en un dispositivo Snowcone. Para obtener más información sobre cómo trabajar con AWS CLI comandos, consulta la Referencia de AWS CLI comandos.

Solución de problemas de las instancias de computación en dispositivos Snowcone

A continuación, encontrará sugerencias para solucionar problemas de los trabajos de Snowcone con instancias de computación.

Temas

- La interfaz de red virtual tiene una dirección IP de 0.0.0.0
- Snowcone 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 RJ45 incorrecta. El dispositivo Snowcone tiene dos interfaces RJ45; es posible que esté especificando una interfaz física incorrecta

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.

Snowcone se bloquea al lanzar una instancia de computación grande

Puede parecer que el dispositivo SnowconeEdge 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. Puede comprobar el estado de sus instancias mediante el AWS CLI comando `aws ec2 describe-instances` run en el punto de conexión HTTP o HTTPS de Amazon EC2 en Snowcone.

La instancia tiene un volumen raíz

Las instancias tienen una volumen raíz por diseño. Todas las instancias sbe tienen un único volumen raíz.

Para obtener información adicional sobre cómo agregar volúmenes adicionales, consulte https://docs.aws.amazon.com/snowball/latest/snowcone-guide/snowcone-snowcone-ebs.html

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 AWS DataSync para transferir archivos

AWS DataSync es un servicio de transferencia de datos en línea que simplifica, automatiza y acelera la copia de grandes cantidades de datos hacia y desde los servicios de AWS almacenamiento a través de Internet o. AWS Direct Connect DataSync el agente viene preinstalado en su dispositivo Snowcone. Puede transferir datos entre el dispositivo y los buckets de Amazon S3, Amazon EFS y Amazon FSx for Windows File Server. AWS DataSync gestiona automáticamente los archivos y objetos en movimiento, programa las transferencias de datos, supervisa el progreso de las transferencias, cifra, verifica las transferencias de datos y notifica a los clientes cualquier problema.

Antes de iniciar el DataSync agente, active el Sistema de archivos de red (NFS) en su dispositivo Snowcone. Consulte Configuración automática de la interfaz NFS y Inicio de NFS y restricción del acceso.

El DataSync agente viene preinstalado en el dispositivo Snowcone como AMI durante la preparación del trabajo en Snowcone. Para transferir datos en línea AWS, conecte el dispositivo Snowcone a la

red externa y utilice AWS OpsHub la CLI para iniciar la DataSync AMI del agente. Active el DataSync agente en la consola de AWS administración o utilice la CLI y configure la tarea de transferencia de datos en línea entre el almacén NFS de Snowcone y Amazon S3, Amazon EFS o Amazon FSx for Windows File Server.

Puedes usar la opción de AWS DataSync correr en Snowcone para lo siguiente:

- Aplicaciones de computación periférica, para recopilar datos, procesarlos para obtener información inmediata y, luego, transferirlos en línea a AWS.
- Transfiera los datos que generan continuamente los sensores o las máquinas AWS en línea a una fábrica o a otros lugares periféricos.
- Distribuya contenido multimedia, científico o de otro tipo en línea desde los servicios de AWS almacenamiento a sus socios y clientes.
- Agregue contenido transfiriendo contenido multimedia, científico o de otro tipo en línea desde sus ubicaciones periféricas a AWS.
- Asegúrese de utilizar una dirección IP estática para el VNI del DataSync agente. El uso de DHCP puede causar problemas, ya que cualquier dispositivo que se reinicie puede significar que se está utilizando una dirección IP diferente, lo que obliga a volver a configurar tanto el DataSync agente como la activación en la nube. DataSync AWS
- Para usar el agente Datasync en Snowcone, debe asegurarse de que las entradas «AllowedHosts» incluyan la dirección IP del DataSync agente en la configuración de NFS en Snowcone. Esto puede requerir que detenga y reinicie el servicio NFS en Snowcone para habilitar DataSync el agente.
- Siempre que detenga el servicio NFS, también debe detener el DataSync agente. Nota: Si detiene el servicio NFS que permite el agente que aparece en la lista, el DataSync agente de Datasync dejará de funcionar.
- Comprobar las cuotas de tareas de AWS DataSync para ver el número máximo de archivos por tarea para un dispositivo Snowcone. Si supera el límite de 200 000 archivos, la DataSync tarea notificará un error de asignación de memoria e interrumpirá la ejecución.

Para flujos de trabajo de procesamiento perimetral o transferencia de datos únicos o para flujos de trabajo de Snowcone en ubicaciones perimetrales sin un enlace de red de área amplia (WAN) o un ancho de banda WAN inadecuado, debe devolver el dispositivo Snowcone AWS para completar la transferencia de datos.

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.

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 Cómo AWS funciona Snowcone.

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.

> **Note**
>
> El espacio de almacenamiento disponible en el dispositivo Snowcone no es preciso hasta que se inicia el servicio NFS.

También puede configurar y administrar la interfaz NFS con una herramienta de interfaz gráfica AWS OpsHub de usuario. Para obtener más información, consulte para la transferencia de archivos sin conexión.

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.

Puertos necesarios para usar AWS los servicios en un AWS Snowcone dispositivo

Para que AWS los servicios funcionen correctamente en un AWS Snowcone dispositivo, 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	SSH	Comprobación de estado del dispositivo y de SSH de EC2
2049	NFS	Punto de conexión NFS
8008	HTTP	Punto de conexión HTTP de EC2
8243	HTTPS	Punto de conexión HTTPS de EC2
9091	HTTP	Punto de conexión para la administración de dispositivos

Devolución del dispositivo Snowcone

Cuando haya terminado de transferir datos al dispositivo Snowcone, debe prepararlo para su devolución a AWS. Antes de continuar, asegúrese de que se hayan detenido todas las transferencias de datos al dispositivo.

Cuando haya finalizado toda comunicación con el dispositivo, solo tiene que apagarlo pulsando el botón de encendido. El dispositivo tarda unos 20 segundos en apagarse.

Desconexión del dispositivo Snowcone

Desconecte los cables del dispositivo Snowcone. Cuando aparece la etiqueta de envío de devolución en la pantalla de tinta electrónica de la parte superior del dispositivo, este queda listo para devolverlo. Para saber cuál es el transportista de la región, consulte Consideraciones de envío para AWS Snowcone.

Consideración específica del tipo de trabajo

Important

Si va a importar datos, no elimine las copias locales de los datos transferidos hasta que la importación AWS se haya realizado correctamente al final del proceso y pueda comprobar los resultados de la transferencia de datos.

Note

Cuando devuelvas el dispositivo Snow para importarlo a Amazon S3, AWS empezará a ingerir los datos tras comprobar que el dispositivo no ha sido manipulado y que se encuentra en buen estado. Si no desea que los datos del dispositivo se transfieran a su bucket de S3 de destino, puede 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 obtener información sobre cómo enviar el dispositivo, consulte Consideraciones de envío para AWS Snowcone.

Protección de los datos de su dispositivo

Tenga en cuenta las siguientes recomendaciones para ayudar a proteger los datos AWS Snowcone del dispositivo.

Temas

- Protegiendo su AWS Snowcone
- Validación de etiquetas NFC

Protegiendo su AWS Snowcone

A continuación se indican algunos puntos de seguridad que le recomendamos que tenga en cuenta al utilizar Snowcone, además de información de alto nivel sobre otras precauciones de seguridad que adoptamos cuando llega un dispositivo AWS para su procesamiento.

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. Aunque cada dispositivo Snowcone es compacto y robusto, las condiciones meteorológicas adversas pueden deteriorar hasta 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**
>
> El dispositivo Snowcone es 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 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. Snowcone usa varias capas de seguridad diseñadas para proteger sus datos, incluidos mecanismos de cierre a prueba de manipulación, cifrado de 256 bits y un TPM estándar del sector diseñado para garantizar la seguridad y la cadena de custodia completa de sus datos.
- Una vez procesado y verificado el trabajo de transferencia de datos, AWS realiza un borrado por software del dispositivo Snowcone siguiendo las directrices del Instituto Nacional de Estándares y Tecnología (NIST) para la desinfección de los medios.

Validación de etiquetas NFC

AWS Snowcone los dispositivos tienen etiquetas NFC integradas. Puede escanear estas etiquetas con la aplicación Edge Verification App, 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. Para obtener más información, consulte Obtención del código QR para validación por NFC.

En el siguiente procedimiento se describe cómo validar las etiquetas NFC de un dispositivo Snowcone. Antes de empezar, asegúrese de haber realizado los cinco primeros pasos siguientes del ejercicio de introducción:

1. Creación de su primer trabajo. Para obtener más información, consulte Crear una tarea para solicitar un dispositivo de la familia Snow.
2. Recepción del dispositivo.
3. Conexión a la red local.
4. Obtención de las credenciales y herramientas. Para obtener más información, consulte Obtención de credenciales.
5. Descarga e instalación del cliente de Snowball Edge. Para obtener más información, consulte Uso del AWS Snowball Edge cliente.

Para validar las etiquetas NFC de un dispositivo AWS Snowcone

1. Ejecute el comando `snowballEdge get-app-qr-code` del cliente de Snowball Edge. 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. Para escanear las etiquetas NFC con su teléfono, descargue e instale la aplicación Snowcone Verification App. Descargue la aplicación desde la Google Play Store si va a utilizar un dispositivo Android.
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:

- Descargue la aplicación en otro teléfono e inténtelo de nuevo.
- 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.

Comprensión de los estados de los AWS Snowcone trabajos

Al crear un AWS Snowcone trabajo, pasa por los estados del trabajo y el estado se muestra en el. Consola de administración de la familia de productos Snow de AWS

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.

> **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 su AWS Snow Family trabajo y eliminar los datos del dispositivo.

AWS Snowcone estados de trabajo del dispositivo

Estado del trabajo	Significado
Trabajo creado	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	AWS está preparando un dispositivo para su trabajo.
Preparando el envío	AWS se está preparando para enviarle un dispositivo.
En tránsito hacia usted	El dispositivo se ha enviado a la dirección proporcionada al crear el trabajo.

Estado del trabajo	Significado
Entregado a usted	El dispositivo ha llegado a la dirección proporcionada al crear el trabajo.
En tránsito a AWS	Has devuelto el dispositivo a AWS.
En las instalaciones de clasificación	El dispositivo para este trabajo se encuentra en nuestras instalaciones de clasificación interna. Cualquier procesamiento adicional para los trabajos de importación en Amazon S3 empezará pronto, normalmente en un plazo de dos días.
En AWS	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	AWS está importando sus datos a Amazon S3.
Completado	El trabajo o una parte de él se ha completado correctamente.
Cancelado	El trabajo se ha cancelado.

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"
	}

Comprensión del proceso AWS Snowcone de pedido

Hay dos opciones a la hora de pedir un dispositivo AWS Snowcone. Puede realizar el pedido a través de la Consola de administración de la familia de productos Snow de AWS o puede utilizar la API de administración de trabajos (JMAPI).

Descripción del proceso de envío

En esta sección encontrarás información sobre cómo se gestiona el envío de un AWS Snowcone dispositivo y una lista de los dispositivos Regiones de AWS compatibles. Para obtener más información acerca de las regiones y los puntos de conexión admitidos, consulte Puntos de conexión y cuotas de AWS Snow Family en la Referencia general de AWS. La velocidad de envío que elija para un trabajo se aplica tanto al envío como a la recepción del dispositivo Snowcone utilizados para ese trabajo. Para obtener más información sobre los cargos de envío, consulte Precios de AWS Snowcone.

> **Note**
>
> Los dispositivos Snowcone solo se pueden usar para importar o exportar datos en la región de AWS en la que se pidieron.

Devolución de un dispositivo Snowcone

La etiqueta de envío a portes pagados de la pantalla de tinta electrónica contiene la dirección correcta a la que hay que devolver el dispositivo. Para obtener información acerca de cómo devolver el dispositivo Snowcone, consulte Transportistas. El dispositivo Snowcone se entrega a una instalación de AWS clasificación y se envía al centro de AWS datos. El transportista de su región le proporcionará un servicio de seguimiento del paquete. Puede realizar el seguimiento de los cambios de estado del trabajo desde la Consola de administración de la familia de productos Snow de AWS.

> **Important**
>
> A menos que se indique lo contrario personalmente AWS, no pegue una etiqueta de envío independiente en el dispositivo Snowcone. Utilice siempre la etiqueta de envío que se muestra en la pantalla de tinta electrónica del dispositivo.

Uso del AWS Management Console

Puede pedir un dispositivo Snowcone utilizando la Consola de administración de la familia de productos Snow de AWS.

Pedido del dispositivo Snowcone desde la consola

Para obtener instrucciones paso a paso sobre cómo pedir un Snowcone con AWS Snowball la consola, consulte. Introducción

Uso de las API de administración de trabajos

La API de administración de trabajos (JMAPI) proporciona acceso mediante programación a la misma funcionalidad disponible en la Consola de administración de la familia de productos Snow de AWS. Esto le permite automatizar la funcionalidad de trabajos. Con la JMAPI, puede ver el estado de los trabajos, crearlos, descargar el archivo de manifiesto y el código de desbloqueo y ver los informes de finalización de los trabajos. Como las llamadas se realizan a través de la API, puede integrarlas en una aplicación personalizada o en un front end web.

Temas

- Usos comunes de JMAPI
- Cadenas obligatorias de JMAPI
- Puntos de conexión de MAPI
- Comandos de la CLI de JMAPI
- Ejemplos

Usos comunes de JMAPI

- Automatizar el pedido de dispositivos Snowcone
- Descargar el archivo de manifiesto
- Descargar el archivo de desbloqueo
- Mostrar una lista de los trabajos actuales de Snowcone
- Descargar el informe de finalización de trabajos de Snowcone

Cadenas obligatorias de JMAPI

Al realizar un pedido a través de la API de administración de trabajos, debe utilizar los siguientes parámetros obligatorios, que se muestran con ejemplos.

```
--job-type
--resources
--address-id
--region
--role-arn
--kms-key-arn
--shipping-option
--device-type
--description
```

Puntos de conexión de MAPI

Punto de conexión de la API

Para realizar llamadas a cada punto de conexión, se debe utilizar el formato `snowballEdge.region.amazonaws.com`. A continuación, se muestran algunos ejemplos para ayudarlo entender comprender el desglose del punto de conexión.

Example

Región	Punto de conexión
Este de EE. UU. (Norte de Virginia)	snowball.us-east-1.amazonaws.com
Oeste de EE. UU. (Oregón)	snowball.us-west-2.amazonaws.com

Comandos de la CLI de JMAPI

CLI de administración de trabajos

Las siguientes son las llamadas a la CLI que puede realizar en la API de administración de trabajos.

Comando	Ejemplo
Hacer un listado de trabajos	`aws snowball list-jobs`
Describir trabajo	`aws snowball describe-job --job-id [JOB ID]`
Describir direcciones	`aws snowball describe-address --address-id`
Crear dirección	`aws snowball create-address --cli-input-json file://create-address.json`
Crear trabajo	`aws snowball create-job --cli-input-json file://create-job.json`
Cancelar trabajo	`aws snowball cancel-job --job-id [JOB ID]`

Ejemplos

A continuación, se muestran algunos ejemplos de comandos que utilizan la API de administración de trabajos.

Ejemplo de JSON de KMS

El siguiente ejemplo de JSON es un archivo JSON con el formato correcto para usar el archivo de política de AWS KMS .

```
{
    "KeyMetadata": {
        "Origin": "AWS_KMS",
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "Description": "",
        "KeyManager": "CUSTOMER",
        "Enabled": true,
        "KeyUsage": "ENCRYPT_DECRYPT",
        "KeyState": "Enabled",
```

```
        "CreationDate": 1502910355.475,
        "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "AWSAccountId": "111122223333"
    }
}
```

Ejemplo de creación de una dirección

En los ejemplos siguientes se muestra el formato que tendría el comando para crear la dirección y cuál es la respuesta cuando se ejecuta correctamente.

```
aws snowball create-address --address "Name=Bob,Company=AWS,Street1=1234 Fake
 St.,City=All,StateOrProvince=Any,Country=US,PostalCode=12345,PhoneNumber=1234567890"
```

Ejemplo de salida

```
{
    "AddressId": "ADID3be640c8-1111-1111-1111-917f201ffa42"
}
```

Ejemplo de creación de un trabajo

El comando siguiente muestra un ejemplo de comando para ejecutar el comando `create-job`.

```
aws snowball create-job --job-type IMPORT --resources file://path/to/resources.json
 --address-id ADID3be640c8-1111-1111-1111-917f201ffa42 --region us-east-1 --role-
arn arn:aws:iam::123456789123:role/example_role --kms-key-arn arn:aws:kms:us-
west-2:000000000000:key/Example --snowball-capacity-preference T14 --device-
configuration file://path/to/configuration.json --shipping-option SECOND_DAY --
snowball-type SNC1_SSD
```

El comando `create-job` anterior creará un trabajo de importación en la región us-east-1 con un dispositivo Snowcone tipo SNC1_SSD con preferencia de capacidad T14 y con la opción de envío SECOND_DAY.

Exportación de una AMI para utilizarla con trabajos de Amazon EC2

En esta sección se proporciona información general sobre cómo exportar su imagen de máquina de Amazon (AMI) para utilizarla con instancias informáticas compatibles con Amazon EC2 en un AWS Snowcone dispositivo.

Temas

- Configuración de una AMI de forma que utilice SSH para conectarse a instancias de computación lanzadas en el dispositivo
- Creación de un trabajo en la consola
- Creación de un trabajo en la CLI de AWS

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 Snowcone, 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 Snowcone.

Cómo poner una clave SSH en una AMI

1. Lance una nueva instancia en el Nube de AWS uso de una imagen AMI compatible (consultehttps://docs.aws.amazon.com/snowball/latest/developer-guide/using-ami.html).

   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 Snowcone. 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 almacén de instancias de computación en un dispositivo Snowcone, consulte “ec2-snowcone-limits”.

2. Instale y configure las aplicaciones que desea ejecutar en el dispositivo Snowcone 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 Snowcone. 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 con respaldo de Amazon EBS.
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 una tarea 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. Al llegar a la página Step 3: Give job details del asistente de creación de trabajos, agregue los siguientes pasos adicionales.

1. Elija Enable compute with EC2.
2. Elija Add an AMI.
3. Se abre un cuadro de diálogo. 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.

Creación de un trabajo en la CLI de AWS

También puede crear su trabajo con AWS Command Line Interface (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::123456789012:role/snowcone-import-snowcone-role --shipping-
option SECOND_DAY --snowball-type SNC1_HDD --snowball-capacity-preference T8
 --device-configuration '{"SnowconeDeviceConfiguration":{"WirelessConnection":
 {"IsWifiEnabled": false}}}'
```

Cuando llegue el dispositivo y lo desbloquee, tendrá que utilizar el cliente de Snowball Edge para obtener las credenciales locales. Para obtener más información, consulte Obtención de credenciales.

Consideraciones de envío para AWS Snowcone

A continuación, encontrarás información sobre cómo se gestiona el envío de un AWS Snowcone dispositivo y una lista en la Región de AWS que se muestran todos los dispositivos compatibles. La tarifa de envío que elijas para un trabajo se aplica tanto al envío como a la recepción del AWS Snowcone dispositivo utilizado para ese trabajo. Para obtener más información sobre los cargos de envío, consulte Precios de AWS Snowcone.

Temas

- Preparar un AWS Snowcone dispositivo para su envío
- Restricciones de envío en función de la región
- Envío de un AWS Snowcone dispositivo

Al crear un trabajo para pedir un dispositivo de la familia Snow, se especifica la dirección y la velocidad de envío. Esta velocidad de envío no indica cuánto tardarás en recibir el AWS Snowcone dispositivo a partir del día en que creaste el trabajo. Solo muestra el tiempo que el dispositivo está en tránsito desde AWS tu dirección de envío. Este tiempo no incluye el tiempo dedicado al procesamiento, que depende de diversos factores, como el tipo de trabajo (las exportaciones suelen tardar más que las importaciones). Además, los transportistas suelen recoger los AWS Snowcone dispositivos salientes solo una vez al día. Así pues, el procesamiento antes del envío puede durar un día o más.

> **Note**
>
> Los dispositivos de la familia Snow solo se pueden devolver al mismo Región de AWS lugar donde se solicitaron. Algunas AWS regiones admiten el envío de los dispositivos de la familia Snow a un país diferente al país desde el que se realizó el pedido. Para obtener más información, consulte Restricciones de envío en función de la región.

Preparar un AWS Snowcone dispositivo para su envío

A continuación se explica cómo preparar un dispositivo Snowcone para devolverlo a AWS.

Para preparar un AWS Snowcone dispositivo para su envío

1. Asegúrese de haber terminado de transferir todos los datos de este trabajo al AWS Snowcone dispositivo o desde él. Desbloquee el dispositivo.
2. Pulse el botón de encendido de la parte frontal del dispositivo, situado cerca de los indicadores luminosos, frente a los puertos de red. El dispositivo tarda unos 20 segundos en apagarse.

   Si ha apagado y desconectado el dispositivo Snowcone y la información de envío no aparece en la pantalla de tinta electrónica después de un minuto aproximadamente, consulte Solución de problemas con la devolución de dispositivos Snow Family.

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 la Región de AWS que se encuentran sus datos. Los dispositivos Snow Family no se envían entre distintos países internacionales; 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.

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.

Envío de un AWS Snowcone dispositivo

La etiqueta de envío a portes pagados de la pantalla de tinta electrónica contiene la dirección correcta a la que hay que devolver el dispositivo AWS Snowcone . Para obtener información sobre cómo devolver AWS Snowcone el dispositivo, consultethe section called “Transportistas”. El AWS Snowcone dispositivo se entrega a una instalación AWS de clasificación y se envía al centro AWS de datos. El transportista de su región le proporcionará un servicio de seguimiento del paquete. Puede realizar un seguimiento de los cambios de estado de su trabajo mediante el Consola de administración de la familia de productos Snow de AWS.

Si ha apagado y desconectado el dispositivo Snowcone y la información de envío no aparece en la pantalla de tinta electrónica después de un minuto aproximadamente, consulte Solución de problemas con la devolución de dispositivos Snow Family.

Transportistas

Cuando crea un trabajo para solicitar un dispositivo de la familia Snow, proporciona la dirección a la que desea que se envíe el AWS Snowcone dispositivo. El transportista que opera en tu región se encarga del envío de AWS los AWS Snowcone dispositivos desde y hacia ti AWS. Cuando se envía un AWS Snowcone dispositivo, recibes un número de seguimiento. Encontrará el número de seguimiento de cada trabajo y un enlace al sitio web de seguimiento en el panel de trabajos de la Consola de administración de la familia de productos Snow de AWS, o bien mediante llamadas de API a la API de administración de trabajos.

La siguiente es la lista de operadores compatibles con AWS Snowcone los dispositivos por región:

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

AWS Snowcone Recogidas en Canadá, la UE, Sudáfrica y EE. UU.

En Canadá, la UE, Sudáfrica y EE. UU., ten en cuenta la siguiente información para que UPS recoja un AWS Snowcone dispositivo:

- Haz los arreglos necesarios para que UPS recoja el AWS Snowcone dispositivo programando una recogida directamente con UPS, o lleva el 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 correcta para devolver el AWS Snowcone dispositivo.
- El AWS Snowcone dispositivo se entrega a una instalación de AWS clasificación y se envía al centro de AWS datos. UPS proporciona automáticamente un número de seguimiento para su envío.

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

AWS Snowcone Recogidas en Brasil

En Brasil, debe tener en cuenta la siguiente información relativa a la recogida de dispositivos Snowcone por parte de UPS:

- Cuando esté preparado para devolver un dispositivo Snowcone, llame al 0800-770-9035 para concertar la recogida con UPS.
- Snowcone 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 Snowcone. Confirme con el departamento fiscal cuál de los documentos siguientes es necesario en su país, en función de su registro 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 Snowcone camionetas en Israel

En Israel, organiza la recogida contactando AWS por correo electrónico a snowball-shipping@amazon.com. Escriba Snowcone Pickup Request en el asunto e incluya esta información:

- ID de trabajo: el ID del trabajo asociado al dispositivo Snow que va a devolver. Puede encontrar el ID del trabajo en Consola de administración de la familia de productos Snow de AWS.
- Dirección de recogida: la dirección donde se recogerá el dispositivo.
- Fecha de recogida: el día más próximo 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 el servicio de envío, Kuehne + Nagel, puede utilizar si es necesario para obtener información sobre la recogida.

Pronto recibirás un correo electrónico de seguimiento AWS Support con información sobre la recogida de tu dispositivo en la dirección que has indicado. Prepare el dispositivo para su envío y prepárese para la recogida, normalmente antes de las 12:00 (hora local). Consulte Preparar un AWS Snowcone dispositivo para su envío.

AWS Snowcone Recogidas en el Reino Unido

En el Reino Unido, ten en cuenta la siguiente información para que UPS recoja un AWS Snowcone dispositivo.

- Puedes hacer los arreglos para que UPS recoja el AWS Snowcone dispositivo programando directamente la recogida con UPS, o bien llevas el 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 Snowcone dispositivo.
- El AWS Snowcone 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 Snowcone dispositivo. Utilice siempre la etiqueta de envío que se muestra en la pantalla de tinta electrónica del dispositivo.

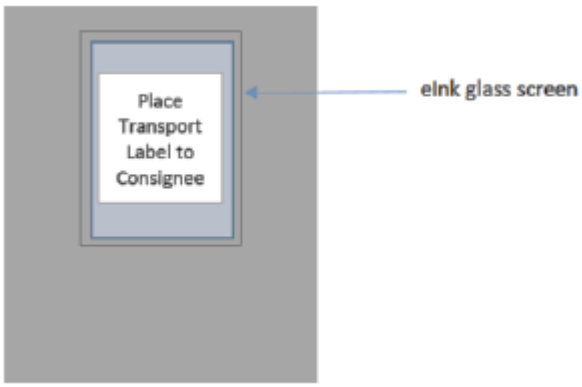
Los servicios de UPS para los productos Snow Family son nacionales únicamente dentro de un país.

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 Snowcone Recogidas en Australia

En Australia, si vas a devolver un AWS Snowcone 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.



Si no ha recibido una etiqueta de devolución con su dispositivo Snow, envíe un correo electrónico a knau.snowball_return@kuehne-nagel.com e indique el número de serie del dispositivo o su número de referencia.

Example where to locate tracking number and serial number

Para organizar la devolución del dispositivo Snow, envíe un correo electrónico a knau.snowball_return@kuehne-nagel.com con la siguiente información:

- Su nombre
- Número de seguimiento (se muestra en azul)
- Número de serie del dispositivo (se muestra en rojo)
- Dirección de recogida completa
- Persona de contacto en el momento de la recogida
- Número de teléfono de contacto en el momento de la recogida
- Fecha de recogida
- Periodo de recogida (plazo mínimo de 3 horas dentro del horario laboral)

> **Note**
>
> El día y la hora de recogida deben ser un día hábil dentro del horario laboral
> El equipo de Kuehne + Nagel responderá para confirmar la recepción de la solicitud de recogida.

AWS Snowcone Recogidas en la India

En la India, Blue Dart recogerá el dispositivo Snowcone. Cuando esté listo para devolver el dispositivo Snowcone, apáguelo y prepárelo para el envío de 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 del trabajo asociado al dispositivo Snowcone que desea devolver a AWS.
- AWS ID de cuenta: 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 desea que se recoja el dispositivo Snowcone.
- Latest Pickup Time: la hora más tardía del día (en hora local) a la que desea que se recoja el dispositivo Snowcone.
- Special Instructions (opcional): instrucciones especiales para recoger el dispositivo Snowcone, incluidos los datos de contacto para coordinar la recogida.

El equipo de Snowcone organiza la recogida con Blue Dart y le envía un correo electrónico de confirmación. Blue Dart le proporciona una etiqueta de envío de papel y recogerá el dispositivo Snowcone.

> **Important**
>
> Si utiliza un dispositivo Snowcone en la India, recuerde presentar todos los documentos fiscales en su estado.

AWS Snowcone Recogidas en Corea del Sur

En Corea del Sur, Kuehne + Nagel gestiona sus 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 Snowcone al que desea que se devuelva. AWS
- Dirección de recogida: la dirección donde se recogerá el dispositivo.
- Fecha de recogida: el día más próximo en el que le gustaría que se recogiera el 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.

En breve, recibirá un correo electrónico de seguimiento AWS Support con información sobre la recogida de su dispositivo en la dirección que ha indicado. Prepare el dispositivo para su envío (consulte Preparar un AWS Snowcone dispositivo para su envío) y prepárese para la recogida, normalmente entre las 13:00 y las 15:00 horas (hora local).

AWS Snowcone Recogidas 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 Snowcone en el asunto para que podamos programar la recogida para usted. En el cuerpo del mensaje, incluya la siguiente información:

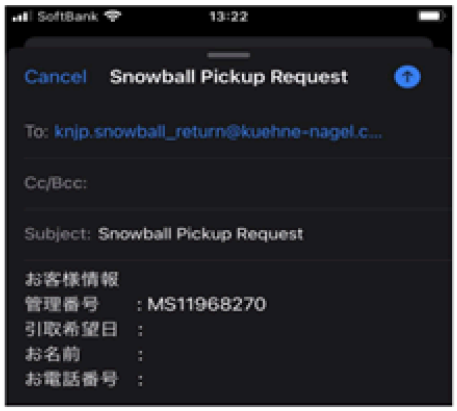
- ID del trabajo
- AWS ID de cuenta
- Nombre del contacto
- Número de teléfono del contacto
- Dirección de correo electrónico del contacto
- El día que desea que se recoja el dispositivo.
- Hora de recogida preferida más temprana
- Última hora de recogida preferida
- Dirección de recogida

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

S.F. Express AWS entregará el dispositivo. Utilice el número de seguimiento de S.F. Express del envío de devolución para saber cuándo se completó la entrega.

AWS Snowcone Recogidas en Indonesia, Japón y Singapur

En Indonesia, Japón y Singapur, 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.



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 Snowcone Las velocidades de envío son las siguientes:

- Australia, Indonesia, Japón, Singapur 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. Normalmente, los dispositivos Snowcone que se envían con la modalidad urgente tardan alrededor de un día en entregarse. 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.
- India: al realizar envíos dentro de la India, AWS Snowcone los dispositivos se envían en un plazo de 7 días laborables a partir de la AWS recepción de todos los documentos fiscales relacionados.

- Israel: cuando se realizan envíos en Israel, tiene acceso al envío el mismo día.
- Estados Unidos de América (EE. UU.) y Canadá: para los envíos dentro de los Estados Unidos o Canadá, dispone de opciones de envío en 24 o 48 horas.
- Reino Unido: si realiza envíos dentro del Reino Unido, tiene acceso al envío exprés. Normalmente, los dispositivos Snowcone 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.

Actualización del software en dispositivos Snowcone

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 Snowcone 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 los servicios que se ejecutan en el dispositivo y reiniciarlo una vez finalizada la actualización.

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
- Descarga de actualizaciones
- Instalación de actualizaciones
- Actualización del certificado SSL
- Actualización de las AMI de Amazon Linux 2 en los dispositivos Snow Family

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 Snowcone 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 AWS 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 Snowball Edge.

Ahora que ha completado estas tareas, puede descargar e instalar las actualizaciones para los dispositivos Snowcone.

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 de su dispositivo

Snowcone, consulte `configure-auto-update-strategy` en Actualización de un dispositivo Snowcone.

> **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
> ```

Cómo comprobar si hay actualizaciones de software disponibles para Snowcone y descargarlas

1. Abra una ventana de terminal y utilice el comando `describe-device` para asegurarse de que el dispositivo Snowcone está desbloqueado. Si el dispositivo está bloqueado, utilice el comando `unlock-device` para desbloquearlo. Para obtener más información, consulte Desbloquear el dispositivo 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
   ```

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.

> **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 Snowcone está desbloqueado. Si el dispositivo está bloqueado, utilice el comando

`unlock-device` para desbloquearlo. Para obtener más información, consulte Desbloquear un dispositivo de la familia Snow.

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 Snowcone. 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. Para obtener más información sobre cómo reiniciar el dispositivo, consulte Reiniciar el dispositivo de la . Para obtener más información sobre cómo desbloquear el dispositivo, consulte Cómo .
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 Snowcone, así como la versión actual instalada en el dispositivo.

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.

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 Edge.

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
```

Mejores prácticas para el AWS Snowcone dispositivo

Para obtener el máximo beneficio y satisfacción con su AWS Snowcone dispositivo, le recomendamos que siga estas prácticas recomendadas.

Temas

- Seguridad
- Network
- Administración de recursos
- Administración de instancias compatibles con EC2

Seguridad

- Si observas algo sospechoso en el AWS Snowcone dispositivo, no lo conectes a la red interna. En su lugar, contacte con AWS Support y se le enviará un nuevo dispositivo AWS Snowcone .
- 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 por separado ayuda a evitar que personas no autorizadas accedan al AWS Snowcone 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 Snowcone dispositivo a las personas que tienen acceso a los archivos guardados en el servidor y también a la dirección de correo electrónico del usuario.
- Las credenciales que se muestran al ejecutar el comando `snowballEdge list-access-keys` del cliente de Snowball Edge seguido de `snowballEdge get-secret-access-key` son un par de claves: una clave de acceso y una clave secreta. Estas claves solo están asociadas al trabajo y a los recursos locales del dispositivo. No se corresponden con la tuya Cuenta de AWS ni con ninguna otra Cuenta de AWS. Si intenta utilizar estas claves para acceder a los servicios y recursos del Nube de AWS, no lo conseguirán, ya que solo funcionan para los recursos locales asociados a su trabajo.
- Puede restringir el acceso a recursos compartidos NFS. Para obtener más detalles, consulte Restricción del acceso a recursos compartidos de NFS cuando NFS está en ejecución.
- Al apagar o apagar y encender un dispositivo Snowcone, este pasa a un estado bloqueado.

Network

- Te recomendamos que solo utilices un método para leer y escribir datos en un depósito local de un AWS Snowcone dispositivo a la vez. El uso de

  El montaje en NFS y DataSync en el mismo bucket de S3 al mismo tiempo puede provocar conflictos de lectura y escritura.
- Para evitar que tus datos se dañen, no desconectes un AWS Snowcone dispositivo ni cambies su configuración de red mientras los transfieres.
- Los archivos deben encontrarse en un estado estático mientras se escriben en el dispositivo. Modificar archivos mientras se están escribiendo puede dar lugar a conflictos de lectura/escritura.
- Para obtener más información sobre cómo mejorar el rendimiento del AWS Snowcone dispositivo, consultaDesempeño de Snowcone.

Administración de recursos

- Los cinco días gratuitos para realizar la transferencia de datos local comienzan el día siguiente a la llegada del AWS Snowcone dispositivo a su centro de datos.

Administración de instancias compatibles con EC2

Para evitar la eliminación accidental de las instancias compatibles con Amazon EC2 que crea en su dispositivo AWS Snowcone , 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.

Desempeño de Snowcone

En la siguiente tabla se describe cómo la velocidad de transferencia de la red afecta al tiempo que se tarda en llenar un AWS Snowcone servidor con datos.

Velocidad (MB/s)	Tiempo de transferencia de 8 TB	Tiempo de transferencia de 4 TB
100	21,17 horas	10,59 horas
60	36,57 horas	18,29 horas
30	68,57 horas	34,29 horas
10	210,29 horas	105,15 horas

AWS Snowcone cuotas

A continuación, encontrará información sobre las cuotas de uso de su dispositivo Snowcone.

Almacenamiento en disco de Snowcone

Internamente, su dispositivo Snowcone contiene 8 TB o 14 TB de almacenamiento en disco que puede utilizar con el servicio interno de Sistema de archivos de red (NFS) o con instancias locales compatibles con Amazon EC2 mediante una presentación de volumen local de Amazon Elastic Block Store (Amazon EBS). Puede usar este almacenamiento para NFS o para Amazon EBS, pero no para ambos. Puede asignar el almacenamiento en función de su caso de uso. Tenga en cuenta que el almacenamiento se preasigna al realizar el pedido de Snowcone.

Almacenamiento de trabajos de computación

Si el tipo de trabajo es computación local, puede crear un total de 8 TB o 14 TB de volúmenes locales de Amazon EBS y adjuntarlos a instancias compatibles con Amazon EC2. El uso de volúmenes de Amazon EBS permite que las instancias locales de Amazon EC2 obtengan acceso a más capacidad local que el volumen raíz por sí solo. Como se trata únicamente de almacenamiento local, los datos escritos en los volúmenes de Amazon EBS se pierden cuando el dispositivo se devuelve a AWS , ya que no se pueden importar a Amazon S3.

Temas

- Cuotas de recursos de computación
- Limitaciones para el envío de un dispositivo Snowcone
- Limitaciones relativas al procesamiento de dispositivos Snowcone devueltos para importación
- Disponible Regiones de AWS

Cuotas de recursos de computación

Cuotas de almacenamiento de los recursos de computación disponibles para los dispositivos Snowcone

En la siguiente tabla se describen los recursos de computación disponibles para los dispositivos Snowcone y sus cuotas de almacenamiento.

Tipo de instancia	Núcleos de CPU virtual	Memoria (GiB)	Cuota
`snc1.micro`	1	1	2
`snc1.small`	1	2	2
`snc1.medium`	2	4	1

Cuotas de capacidad de imagen de máquina de Amazon (AMI) y Amazon EC2 para los dispositivos Snowcone

En la siguiente tabla se describen las cuotas de capacidad de las AMI y de las instancias compatibles con Amazon EC2 para un dispositivo Snowcone.

Amazon EC2	Tamaño
AMI compatibles con Amazon EC2	125 GB (el tamaño combinado de todas las AMI utilizadas en el trabajo de un cliente)
Instancias compatibles con Amazon EC2	150 GB (representa el espacio disponible para los volúmenes de almacenamiento de respaldo de las instancias)

Limitaciones para el envío de un dispositivo Snowcone

Las siguientes son las limitaciones para el envío de un dispositivo Snowcone:

- AWS no enviará un dispositivo Snowcone a un apartado de correos.
- No se permite mover un dispositivo Snowcone a una dirección fuera del país especificado al crear el trabajo, y constituye una infracción de los Términos de servicio de AWS .

Para obtener más información sobre el envío, consulte Consideraciones de envío para AWS Snowcone.

Limitaciones relativas al procesamiento de dispositivos Snowcone devueltos para importación

Para importar sus datos al Nube de AWS, el dispositivo Snowcone debe cumplir los siguientes requisitos:

- La seguridad del dispositivo Snowcone no debe haberse visto comprometida. Excepto para abrir las puertas de las partes delantera y trasera, no abra el dispositivo Snowcone por ningún motivo.
- El dispositivo no debe presentar daños físicos. Para evitar daños, cierre las dos puertas del dispositivo Snowcone y presione hasta que los pestillos emitan un clic audible.
- A menos que se proporcione una etiqueta de envío AWS, la pantalla de tinta electrónica del dispositivo Snowcone debe estar visible y debe mostrar la etiqueta de devolución que se generó automáticamente al terminar de transferir los datos al dispositivo Snowcone.

> **Note**
>
> Todos los dispositivos Snowcone devueltos que no cumplan estos requisitos se borrarán y no se llevará a cabo ningún trabajo con ellos.

Disponible Regiones de AWS

Para obtener información sobre los puntos de enlace Regiones de AWS y los puntos de conexión compatibles, consulte los puntos de conexión y las cuotas de la familia AWS Snow en. Referencia general de AWS

Solución de problemas de Snowcone

Esta sección proporciona orientación e información sobre el AWS Snowcone dispositivo o el servicio para solucionar algunos de los problemas encontrados.

Temas

- Solución de problemas de las instancias de computación
- Solución de problemas de red
- Solución de problemas de instancias compatibles con Amazon EC2 en Datasync
- Solución de problemas de transferencia de datos
- Solución de problemas con la devolución de dispositivos Snow Family

Solución de problemas de las instancias de computación

La solución de problemas de las instancias de computación se documenta aquí.

Solución de problemas de red

La dirección IP es 0.0.0.0

Está conectado a la red y a los cables de alimentación, pero la dirección IP del dispositivo muestra 0.0.0.0

Acción que debe ejecutarse

Compruebe que el cableado entre el dispositivo Snowcone y los dispositivos de red es correcto.

Si el dispositivo sigue sin mostrar una dirección IP, compruebe si el router tiene problemas relacionados con un mal funcionamiento o una configuración que puedan provocar un error de configuración IP.

Si la red no tiene DHCP habilitado, asegúrese de configurar una IP estática en el dispositivo usando la opción STATIC de la pantalla de Snowcone y programando el dispositivo con la dirección IP estática adecuada.

No se puede desbloquear el dispositivo

No puede desbloquear el dispositivo mediante el OpsHub cliente Snowball Edge.

Acción que debe ejecutarse

Asegúrese de que el cliente esté en la misma subred y en la misma red que el dispositivo AWS Snowcone .

Si el Snowcone tiene varias asignaciones de direcciones IP (por ejemplo, WiFi y Ethernet), asegúrese de utilizar la misma dirección IP para conectarse si varios clientes están intentando responder a Snowcone. Tenga en cuenta que solo puede utilizar una interfaz cada vez.

Si los pasos anteriores no funcionan, asegúrese de AWS Support proporcionar los registros del dispositivo. Utilice el cliente Snowball Edge y el comando: SnowballEdge get-support-logs

Solución de problemas de instancias compatibles con Amazon EC2 en Datasync

Error: no se pudo lanzar la instancia

Snowcone no tiene capacidad suficiente para lanzar la instancia para esta solicitud.

Acción que debe ejecutarse

Los requisitos para ejecutarse DataSync en un AWS Snowcone dispositivo como agente utilizan la instancia predeterminada snc1.medium, que proporciona 2 núcleos de CPU y 4 GiB de memoria. Asegúrese de disponer de recursos suficientes en el dispositivo Snowcone para aprovisionar la nueva solicitud de lanzamiento de instancia compatible con Amazon EC2.

Solución de problemas de transferencia de datos

Acceso denegado por el servidor

Error: mount.nfs: acceso denegado por el servidor durante el montaje de 192.168.1.214

Acción que debe ejecutarse

Si configuró NFS mediante una configuración rápida, de forma predeterminada solo su sistema tendrá acceso a la transferencia de archivos a este dispositivo. Si desea permitir que otros hosts carguen datos en el dispositivo Snowcone, deshabilite el servicio NFS y vuelva a habilitarlo con la lista de direcciones IP que desea permitir en la configuración de NFS.

La conexión agota el tiempo de espera durante la transferencia de datos

Se agota el tiempo de espera de la conexión al intentar transferir datos a AWS Snowcone través de la interfaz Amazon S3 (vía AWS CLI).

Motivo de este comportamiento esperado

El AWS Snowcone dispositivo solo admite transferencias a través del soporte NFS para transferencias fuera de línea y AWS DataSync transferencias en línea; actualmente, la interfaz Amazon S3 no es compatible. Esto explicaría por qué se agotan los tiempos de espera cuando se conecta mediante la AWS CLI.

Spawn Showmount ENOENT

Error: Error no detectado: genera showmount ENOENT. Es una abreviatura de Error NO ENTry (o Error NO ENTity) y, de hecho, se puede usar para algo más que archivos/directorios.

Acción que debe ejecutarse

Este error se produce si el cliente de NFS no se está ejecutando en la estación de trabajo. Si el servicio NFS no se inició antes de configurar NFS AWS OpsHub, es posible que aparezca este error.

En un cliente Windows, puede realizar los siguientes pasos para comprobar si el servicio NFS se está ejecutando:

1. En el equipo cliente, abra Inicio, elija Panel de control y elija Programas.
2. Elija Activar o desactivar las características de Windows.
3. En Servicios para NFS, elija Cliente para NFS y elija Aceptar. Referencia: Montaje de NFS en un cliente de Windows

Este error también puede producirse si hay un firewall/antivirus entre la estación de trabajo en ejecución AWS OpsHub y el dispositivo que pueda bloquear la conexión.

Desde la estación de trabajo, ejecute el comando telnet a la dirección IP del AWS Snowcone dispositivo en el puerto NFS número 2049 para comprobar si la conexión se ha establecido correctamente.

Solución de problemas con la devolución de dispositivos Snow Family

En ocasiones, después de apagar el dispositivo Snow Family como preparación para su devolución, la información de envío de la devolución no aparece en la pantalla de tinta electrónica.

Acción que debe ejecutarse

1. Inicie sesión en. Consola de administración de la familia de productos Snow de AWS
2. Vea el trabajo del dispositivo.
3. En la sección Detalles, en la sección Return shipping label, seleccione To view and print your return label follow this link.
4. Imprima la etiqueta y péguela al dispositivo.
5. Devuelva el dispositivo según las instrucciones que se indican en Devolución de un dispositivo Snowcone.

Referencia de la API de administración de trabajos

- Referencia de la API de administración de trabajos
  - Acciones
  - Tipos de datos
  - Parámetros comunes
  - Errores comunes

Historial de documentos para la guía AWS Snowcone del usuario

En la siguiente tabla se describe la documentación de esta versión de AWS Snowcone.

- Versión de la API: la más reciente
- Última actualización de la documentación: 25 de agosto de 2023

Cambio	Descripción	Fecha
Incluya AMI personalizadas al solicitar dispositivos	Las imágenes personalizadas de Amazon Machine ahora se pueden precargar al solicitar AWS Snow Family trabajos. Para obtener más información, consulte Uso de Amazon EC2 en Snowcone.	15 de noviembre de 2023
Nuevo compatible Región de AWS	AWS Snowcone Los dispositivos SSD ya están disponibles en Israel (Tel Aviv) Región de AWS. Se ha agregado información de recogida para esta región. Para obtener más información, consulte Puntos de conexión y cuotas de AWS Snow Family en la Referencia general de AWS. Para obtener información sobre el envío, consulte Consideraciones de envío para AWS Snowcone.	25 de agosto de 2023
Nuevo Región de AWS compatible	Los dispositivos Snowcone ya están disponibles en Europa (París). Región de AWS Para	29 de junio de 2022

	obtener más información, consulte Puntos de conexión y cuotas de AWS Snow Family en la Referencia general de AWS. Para obtener informaci ón sobre el envío, consulte Consideraciones de envío para AWS Snowcone.	
Nuevas sugerencias para la solución de problemas de Snowcone	AWS Snowcone Se agregó una sección de consejos para la solución de problemas similar a Snowball Edge. Para ver la nueva sección agregada, consulte Solución de problemas de Snowcone.	15 de abril de 2022
Nuevo compatible Región de AWS	AWS Snowcone ahora está disponible en las regiones de Asia Pacífico (Bombay) y Brasil. Se ha agregado información de recogida para la UE, Canadá, Singapur y Brasil. Para obtener más información, consulte Puntos de conexión y cuotas de AWS Snow Family en la Referencia general de AWS.	23 de febrero de 2022
Nuevo Región de AWS compatible	AWS Snowcone ya está disponible en la región de Europa (Londres). Para obtener más información, consulte Puntos de conexión y cuotas de AWS Snow Family en la Referencia general de AWS.	5 de enero de 2022

Compatibilidad con la configuración de servidor de Network Time Protocol (NTP)	Ahora, los dispositivos Snowcone admiten la configuración de servidores externos de Network Time Protocol (NTP).	16 de noviembre de 2021
Nuevo Región de AWS compatible	AWS Snowcone La SSD ya está disponible en las regiones EE.UU. Oeste (Norte de California), EE.UU. Este (Ohio), Asia Pacífico (Singapur), Asia Pacífico (Tokio) y Asia Pacífico (Sídney). Para obtener más información, consulte Puntos de conexión y cuotas de AWS Snow Family en la Referencia general de AWS.	3 de noviembre de 2021
Nuevo Región de AWS compatible	AWS Snowcone ahora está disponible en las regiones EE.UU. Oeste (Norte de California), EE.UU. Este (Ohio) y Sudamérica (São Paulo). Para obtener más información, consulte Puntos de conexión y cuotas de AWS Snow Family en la Referencia general de AWS.	29 de septiembre de 2021

Nuevo Región de AWS compatible	AWS Snowcone ahora está disponible en las regiones de Asia Pacífico (Singapur) y Asia Pacífico (Tokio). Para obtener más información, consulte Puntos de conexión y cuotas de AWS Snow Family en la Referencia general de AWS.	26 de agosto de 2021
Posibilidad de exportar datos sin conexión desde Amazon S3 mediante dispositivos Snowcone	Ahora puede solicitar AWS la exportación de sus datos de Amazon S3 transfiriéndolos a dispositivos Snowcone, que luego se envían físicamente a su ubicación. Para obtener más información, consulte Cómo funcionan los trabajos de importación y exportación.	4 de agosto de 2021
Presentamos AWS Snow Device Management	Snow Device Managemen t le permite administrar su AWS Snowcone dispositivo y AWS los servicios locales de forma remota. Todos los dispositivos Snowcone son compatibles con la administr ación de dispositivos Snow y viene preinstalada en los nuevos dispositivos en la mayoría de los lugares donde Regiones de AWS Snowcone está disponible. Para obtener más información, consulte Uso AWS Snow Device Management para administrar dispositivos.	4 de agosto de 2021

Nuevo Región de AWS compatible	AWS Snowcone ya está disponible en la región de Canadá (centro). Para obtener más información, consulte Puntos de conexión y cuotas de AWS Snow Family en la Referencia general de AWS.	28 de abril de 2021
Nuevo Región de AWS compatible	AWS Snowcone ya está disponible en la región Asia-Pacífico (Sídney). Para obtener más información, consulte Puntos de conexión y cuotas de AWS Snow Family en la Referencia general de AWS.	24 de marzo de 2021
Compatibilidad con la interfaz de red directa	AWS Snowcone ahora agrega la configuración de interfaz de red directa (DNI), una función de red avanzada que permite casos de uso como las transmisiones de multidifusión, el enrutamie nto y el equilibrio de carga. Para obtener más información, consulte Network Configura tion for Compute Instances.	12 de enero de 2021
Nuevo compatible Región de AWS	AWS Snowcone ya está disponible en la región de Europa (Fráncfort). Para obtener más información, consulte Puntos de conexión y cuotas de AWS Snow Family en la Referencia general de AWS.	18 de noviembre de 2020

Nuevo Región de AWS compatible	AWS Snowcone ya está disponible en la región de Europa (Irlanda). Para obtener más información, consulte Puntos de conexión y cuotas de AWS Snow Family en la Referencia general de AWS.	16 de septiembre de 2020
Presentamos AWS Snowcone	AWS Snowcone es un dispositivo portátil, robusto y seguro para la computación perimetral y la transferencia de datos. Puede usarlo AWS Snowcone para recopilar, procesar y transferir datos AWS, ya sea sin conexión (enviando el dispositivo a AWS) o en línea AWS DataSync. Para obtener más información, consulte ¿Qué es AWS Snowcone?	17 de junio de 2020

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.