aws

Guía del usuario

Amazon EBS

Amazon EBS: Guía del usuario

Table of Contents

¿Qué es Amazon Elastic Block Store?

Amazon Elastic Block Store (Amazon EBS) proporciona recursos de almacenamiento en bloque de alto rendimiento y escalables que se pueden utilizar con instancias de Amazon Elastic Compute Cloud (Amazon EC2). Con Amazon Elastic Block Store, puede crear y administrar los siguientes recursos de almacenamiento en bloque:

- Volúmenes de Amazon EBS: son volúmenes de almacenamiento que se adjuntan a las instancias de Amazon EC2. Después de asociar un volumen a una instancia, puede usarlo de la misma forma en que usaría cualquier otro disco duro local conectado a un ordenador, por ejemplo, para almacenar archivos o instalar aplicaciones.
- Instantáneas de Amazon EBS: son copias de seguridad puntuales de los volúmenes de Amazon EBS que persisten independientemente del volumen en sí. Puede crear instantáneas para hacer una copia de seguridad de los datos en sus volúmenes de Amazon EBS. A continuación, podrá restaurar volúmenes nuevos a partir de esas instantáneas en cualquier momento.

Temas

Características de Amazon EBS

Amazon EBS ofrece las siguientes características y beneficios:

- Varios tipos de volúmenes: Amazon EBS ofrece varios tipos de volúmenes que le permiten optimizar el rendimiento y el coste del almacenamiento para una amplia gama de aplicaciones. Los tipos de volumen se dividen en dos categorías principales: almacenamiento basado en SSD para cargas de trabajo transaccionales y almacenamiento basado en HDD para cargas de trabajo de rendimiento intensivo.
- Escalabilidad: puede crear volúmenes de Amazon EBS con especificaciones de capacidad y rendimiento que se adapten a sus necesidades. A medida que cambien sus necesidades, puede utilizar las operaciones de volúmenes elásticos para aumentar la capacidad o ajustar el rendimiento de forma dinámica, sin tiempo de inactividad.

- Copia de seguridad y recuperación: utilice instantáneas de Amazon EBS para hacer una copia de seguridad de los datos almacenados en sus volúmenes. A continuación, puede utilizar esas instantáneas para restaurar los volúmenes al instante o para migrar datos entre cuentas de AWS, zonas de disponibilidad o regiones de AWS.
- Protección de datos: utilice el cifrado de Amazon EBS para cifrar los volúmenes de Amazon EBS y las instantáneas de Amazon EBS. Las operaciones de cifrado se producen en los servidores que alojan instancias de Amazon EC2, lo que garantiza la seguridad tanto de los datos en reposo como de los datos en tránsito entre la instancia, el volumen asociado y las instantáneas posteriores.
- Disponibilidad y durabilidad de los datos: los volúmenes de io2 Block Express ofrecen una durabilidad del 99,999 % con una tasa de errores anual del 0,001 %. Otros tipos de volumen ofrecen una durabilidad de 99,8 % - 99,9 %, con una tasa anual de errores de 0,1 % - 0,2 %. Además, los datos de los volúmenes de se replican de manera automática en varios servidores de una zona de disponibilidad para evitar la pérdida de datos debido a un error de alguno de los componentes únicos.
- Archivado de datos: EBS Snapshots Archive proporciona un nivel de almacenamiento de bajo costo para archivar copias completas y puntuales de las instantáneas de EBS que debe retener durante 90 días o más por motivos normativos y de cumplimiento, o para futuras versiones de proyectos.

Servicios relacionados

Amazon EBS es compatible con los siguientes servicios:

- Amazon Elastic Compute Cloud: un servicio que le permite iniciar y administrar máquinas virtuales (instancias de Amazon EC2) en la nube de AWS. Puede asociar volúmenes de EBS a esas instancias y usarlos de la misma forma en que usaría un disco duro local, por ejemplo, para almacenar archivos o instalar aplicaciones. Para obtener más información, consulte ¿Qué es Amazon EC2?
- AWS Key Management Service: un servicio administrado que le permite crear y administrar claves criptográficas. Puede utilizar claves criptográficas de AWS KMS para cifrar los datos almacenados en los volúmenes de Amazon EBS y en las instantáneas de Amazon EBS. Para obtener más información, consulte Cómo Amazon EBS usa AWS KMS.
- Amazon Data Lifecycle Manager: un servicio administrado que permite automatizar la creación, retención y eliminación de instantáneas de EBS y de AMI respaldadas por EBS. Puede utilizar Amazon Data Lifecycle Manager para automatizar las copias de seguridad de los volúmenes de

Amazon EBS y las instancias Amazon EC2. Para obtener más información, consulte Administrador de vida útil de datos de Amazon.

- API directas de EBS: servicio que le permite crear instantáneas de EBS, escribir datos directamente en las instantáneas, leer datos en las instantáneas e identificar las diferencias o los cambios entre dos instantáneas. Para obtener más información, consulte Usar las API directas de EBS para acceder al contenido de una instantánea de EBS.
- Papelera de reciclaje: servicio de recuperación de datos que le permite restaurar instantáneas de Amazon EBS y AMI basadas en EBS que se han eliminado por accidente. Para obtener más información, consulte Papelera de reciclaje.

Acceso a Amazon EBS

Puede crear y administrar los recursos de Amazon EBS desde cualquiera de las siguientes interfaces:

Consola de Amazon EC2

Una interfaz web para crear y administrar volúmenes e instantáneas. Si se registró con una cuenta de AWS, podrá acceder a la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.

AWS Command Line Interface

Una herramienta de línea de comandos que le permite administrar los recursos de Amazon EBS mediante el intérprete de comandos de la línea de comandos. Es compatible con Windows, Mac y Linux. Para obtener más información, consulte la Guía del usuario de AWS Command Line Interface y la Referencia de comandos de AWS CLI.

AWS Tools for PowerShell

Un conjunto de módulos de PowerShell que le permiten llevar a cabo operaciones mediante script en sus recursos de Amazon EBS desde la línea de comandos de PowerShell. Para obtener más información, consulte la Guía del usuario de AWS Tools for Windows PowerShell y la Referencia de Cmdlet de AWS Tools for PowerShell.

AWS CloudFormation

Un servicio totalmente administrado de AWS que le permite crear plantillas JSON o YAML reutilizables que describan sus recursos de AWS y que luego aprovisiona y configura

esos recursos en su nombre. Para más información, consulte la Guía del usuario de AWS CloudFormation.

API de consulta de Amazon EC2

La API de consulta de Amazon EC2 proporciona solicitudes de HTTP o HTTPS que utilizan el verbo HTTP `GET` o `POST` y un parámetro de consulta llamado `Action`. Para obtener más información, consulte Referencia de las API de Amazon EC2.

SDK de AWS

API específicas del lenguaje que le permiten crear aplicaciones que estén integradas con los servicios de AWS. AWS Los SDK están disponibles para varios lenguajes de programación populares. Para obtener más información, consulte Herramientas para crear en AWS.

Precios

Con Amazon EBS, paga únicamente por lo que aprovisiona. Para obtener más información, consulte Precios Amazon EBS.

Configuración de Amazon EBS

Complete las tareas de esta sección para configurar el trabajo con recursos de Amazon EBS.

Tareas

- Inscríbase en un Cuenta de AWS
- Creación de un usuario con acceso administrativo
- (Opcional) Creación y uso de una clave gestionada por el cliente para el cifrado de Amazon EBS
- (Opcional) Habilitación del bloqueo del acceso público de las instantáneas de Amazon EBS

Inscríbase en un Cuenta de AWS

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

Para suscribirte a una Cuenta de AWS

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

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

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

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

Creación de un usuario con acceso administrativo

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

Proteja su Usuario raíz de la cuenta de AWS

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

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

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

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

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

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

Iniciar sesión como usuario con acceso de administrador

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

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

Concesión de acceso a usuarios adicionales

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

Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

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

(Opcional) Creación y uso de una clave gestionada por el cliente para el cifrado de Amazon EBS

El cifrado de Amazon EBS es una solución de cifrado que utiliza claves AWS KMS criptográficas para cifrar los volúmenes de Amazon EBS y las instantáneas de Amazon EBS. Amazon EBS crea automáticamente una clave de KMS AWS administrada única para el cifrado de Amazon EBS en cada región. Esta clave KMS tiene el alias `aws/ebs`. No puede rotar la clave KMS predeterminada ni administrar sus permisos. Para obtener más flexibilidad y control sobre la clave de KMS utilizada para el cifrado de Amazon EBS, podría considerar la posibilidad de crear y usar una clave administrada por el cliente.

Creación y uso de una clave administrada por el cliente para el cifrado de Amazon EBS

1. Cree una clave de KMS de cifrado simétrica.
2. Seleccione la clave de KMS como clave predeterminada de KMS para el cifrado de Amazon EBS.
3. Otorgue permiso a los usuarios para usar la clave de KMS para el cifrado de Amazon EBS.

(Opcional) Habilitación del bloqueo del acceso público de las instantáneas de Amazon EBS

Para impedir que sus instantáneas se compartan públicamente, puede habilitar el bloqueo del acceso público de las instantáneas. Tras habilitar el bloqueo del acceso público de las instantáneas de una región, se bloquea automáticamente cualquier intento de compartir públicamente las instantáneas en esa región. Esto puede ser de ayuda para mejorar la seguridad de sus instantáneas y para proteger sus datos contra el acceso no autorizado o no intencionado.

Para obtener más información, consulte Bloqueo del acceso público de las instantáneas.

Console

Habilitación del bloqueo del acceso público para las instantáneas

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Panel de EC2 y, a continuación, en Atributos de la cuenta (a la derecha), elija Protección y seguridad de datos.
3. En la sección Bloquear el acceso público de las instantáneas de EBS, seleccione Administrar.
4. Seleccione Bloquear acceso público y, a continuación, elija una de las siguientes opciones:
   - Bloquear todo el uso compartido: para bloquear todo el uso compartido público de sus instantáneas. Los usuarios de la cuenta no pueden solicitar un nuevo uso compartido público. Además, las instantáneas que ya se compartieron públicamente se consideran privadas y dejan de ser de acceso público.
   - Bloquear el nuevo uso compartido público: para bloquear solo el uso compartido público nuevo de sus instantáneas. Los usuarios de la cuenta no pueden solicitar un nuevo uso compartido público. Sin embargo, las instantáneas que ya se compartieron públicamente seguirán siendo de acceso público.
5. Elija Actualizar.

AWS CLI

Habilitación del bloqueo del acceso público para las instantáneas

Utilice el comando enable-snapshot-block-public-access. En `--state`, especifique uno de los siguientes valores:

- `block-all-sharing`: para bloquear todo el uso compartido público de sus instantáneas. Los usuarios de la cuenta no pueden solicitar un nuevo uso compartido público. Además, las instantáneas que ya se compartieron públicamente se consideran privadas y dejan de ser de acceso público.
- `block-new-sharing`: para bloquear solo el nuevo uso compartido público de sus instantáneas. Los usuarios de la cuenta no pueden solicitar un nuevo uso compartido público. Sin embargo, las instantáneas que ya se compartieron públicamente seguirán siendo de acceso público.

```
aws ec2 enable-snapshot-block-public-access --state block-all-sharing|block-new-sharing
```

Volúmenes de Amazon EBS

Un volumen de Amazon EBS es un dispositivo de almacenamiento de nivel de bloque duradero que se puede adjuntar a sus instancias. Después de asociar un volumen a una instancia, puede usarlo como cualquier otro disco duro físico. Los volúmenes de EBS son flexibles. En el caso de los volúmenes de la generación actual adjuntados a los tipos de instancias de la generación actual, puede aumentar el tamaño de forma dinámica, modificar la capacidad de IOPS provisionadas y cambiar el tipo de volumen de los volúmenes de producción activos.

Puede usar volúmenes de EBS como almacenamiento principal de los datos que requieren actualizaciones frecuentes, como la unidad del sistema de una instancia o el almacenamiento de una aplicación de base de datos. También se pueden utilizar con las aplicaciones de uso intensivo que realicen exploraciones de discos continuas. Los volúmenes de EBS persisten, independientemente de la vida de ejecución de una instancia EC2.

También puede asociar varios volúmenes de EBS a una sola instancia. El volumen y la instancia deben estar dentro de la misma zona de disponibilidad. Dependiendo del volumen y los tipos de instancia, puede utilizar Multi-Attach para montar un volumen en varias instancias al mismo tiempo.

Amazon EBS ofrece los siguientes tipos de volúmenes: SSD de uso general (`gp2` y `gp3`), SSD de IOPS provisionadas (`io1` e `io2`), HDD con rendimiento optimizado (`st1`), HDD en frío (`sc1`) y magnéticos (`standard`). Se diferencian en las características de rendimiento y en el precio, y permiten adaptar el rendimiento y el costo del almacenamiento a las necesidades de las aplicaciones. Para obtener más información, consulte Tipos de volúmenes de Amazon EBS.

Su cuenta tiene un límite en el espacio total de almacenamiento disponible. Para obtener más información sobre estos límites y sobre cómo solicitar un incremento, consulte Puntos de conexión y cuotas de Amazon EBS.

Para obtener más información sobre los precios, consulte Precios de Amazon EBS.

Contenido

- Ciclo de vida del volumen de Amazon EBS
- Reemplazar un volumen Amazon EBS con una instantánea anterior
- Monitoreo de los volúmenes de Amazon EBS
- Pruebas de fallos en Amazon EBS

Beneficios de utilizar volúmenes de EBS

Los volúmenes de EBS proporcionan beneficios que no proporcionan los volúmenes de almacenamiento de instancias.

Ventajas

- Disponibilidad de datos
- Persistencia de datos
- Cifrado de datos
- Seguridad de los datos
- Instantáneas
- Flexibilidad

Disponibilidad de datos

Cuando se crea un volumen de EBS, se replica automáticamente dentro de su zona de disponibilidad para evitar la pérdida de datos por errores en cualquiera de los componentes del hardware. Puede asociar un volumen de EBS a cualquier instancia EC2 en la misma zona de disponibilidad. Después de adjuntar un volumen, este aparece como dispositivo de bloques nativo, similar a un disco duro u otro dispositivo físico. En ese punto, la instancia puede interactuar con el volumen tal y como lo haría con una unidad local. Puede conectarse a la instancia y formatear el volumen de EBS con un sistema de archivos, como `Ext4` para una instancia de Linux o `NTFS` para una instancia de Windows y, a continuación, instalar aplicaciones.

Si adjunta varios volúmenes a un dispositivo que ha nombrado, puede distribuir los datos entre los volúmenes para un mayor rendimiento y velocidad de E/S.

Puede adjuntar volúmenes de EBS `io1` e `io2` a un máximo de 16 instancias basadas en Nitro. Para obtener más información, consulte Asociar un volumen a varias instancias con Amazon EBS Multi-Attach. De lo contrario, puede asociar un volumen de EBS a una única instancia.

Puede obtener datos de monitorización para los volúmenes de EBS, incluidos los volúmenes de dispositivo raíz para instancias respaldadas por EBS, sin cargo adicional. Para obtener más información sobre las métricas de monitorización, consulte CloudWatch Métricas de Amazon para Amazon EBS. Para obtener información sobre cómo realizar un seguimiento del estado de los volúmenes, consulte Amazon EventBridge para Amazon EBS.

Persistencia de datos

Un volumen de EBS es un almacenamiento fuera de la instancia que puede persistir independientemente de la duración de esta. Seguirá pagando por el uso del volumen mientras persistan los datos.

Los volúmenes de EBS que están asociados a una instancia en ejecución se pueden desconectar automáticamente de la instancia con sus datos intactos cuando se termina la instancia si desactiva la casilla de verificación Delete on Termination (Eliminar al terminar) al configurar los volúmenes de EBS para su instancia en la consola de EC2. A continuación, el volumen se puede volver a adjuntar a una nueva instancia, permitiendo una recuperación rápida. Si la casilla de verificación Delete on Termination (Eliminar al terminar) está marcada, los volúmenes se eliminarán al terminar la instancia EC2. Si utiliza una instancia respaldada por EBS puede detener y reiniciar dicha instancia sin que ello afecte a los datos almacenados en el volumen adjunto. El volumen permanece adjunto durante todo el ciclo de detención e inicio. Esto le permite procesar y almacenar los datos en el volumen de forma indefinida, utilizando solo los recursos de procesamiento y almacenamiento cuando sea preciso. Los datos persisten en el volumen hasta que este se elimine explícitamente. El almacenamiento en bloques físicos utilizado por los volúmenes de EBS eliminados se sobrescribe con ceros o datos criptográficos pseudoaleatorios antes de asignarlo a un nuevo volumen. Si trabaja con información confidencial, debería plantearse cifrar los datos manualmente o almacenarlos en un volumen protegido por Cifrado de Amazon EBS. Para obtener más información, consulte Cifrado de Amazon EBS.

De forma predeterminada, el volumen raíz de EBS que se crea y adjunta a una instancia durante el lanzamiento se elimina cuando se termina dicha instancia. Puede modificar este comportamiento cambiando el valor de la marca `DeleteOnTermination` a `false` al lanzar la instancia. Este valor modificado hace que el volumen persista incluso después de terminarse la instancia y le permite adjuntar el volumen a otra instancia.

De forma predeterminada, los volúmenes de EBS adicionales que se crean y adjuntan a una instancia durante el lanzamiento no se eliminan cuando se termina dicha instancia. Puede modificar este comportamiento cambiando el valor de la marca `DeleteOnTermination` a `true` al lanzar la

instancia. La modificación de este valor provoca que los volúmenes se eliminen cuando la instancia termina.

Cifrado de datos

Para un cifrado de datos simplificado, puede crear volúmenes de EBS cifrados con la característica Cifrado de Amazon EBS. Todos los tipos de volúmenes de EBS admiten el cifrado. Puede utilizar volúmenes de EBS cifrados para cumplir una amplia gama de requisitos de cifrado para datos y aplicaciones regulados o auditados. data-at-rest El cifrado de Amazon EBS utiliza algoritmos Advanced Encryption Standard de 256 bits (AES-256) y una infraestructura de claves administrada por Amazon. El cifrado se produce en el servidor que aloja la instancia de EC2 y proporciona el cifrado data-in-transit desde la instancia de EC2 al almacenamiento de Amazon EBS. Para obtener más información, consulte Cifrado de Amazon EBS.

El cifrado de Amazon EBS AWS KMS keys se utiliza al crear volúmenes cifrados y cualquier instantánea creada a partir de sus volúmenes cifrados. La primera vez que crea un volumen de EBS cifrado en una región, se crea automáticamente una clave de KMS AWS administrada predeterminada. Esta clave se utilizará en el cifrado de Amazon EBS a menos que cree y utilice una clave administrada por el cliente. Crear su propia clave administrada por el cliente le ofrece una mayor flexibilidad, incluida la opción de crear, rotar, deshabilitar y definir los controles de acceso y auditar las claves de cifrado utilizadas para proteger los datos. Para obtener más información, consulte la Guía para desarrolladores de AWS Key Management Service.

Seguridad de los datos

Los volúmenes de Amazon EBS se presentan como dispositivos de bloques sin formatear y sin procesar. Estos dispositivos son dispositivos lógicos que se crean en la infraestructura de EBS, y el servicio Amazon EBS garantiza que los dispositivos estén vacíos de forma lógica (es decir, los bloques sin procesar se establecen en cero o contienen datos criptográficamente pseudoaleatorios) antes de cualquier uso o reutilización por parte de un cliente.

Si tiene procedimientos que requieren que todos los datos se borren mediante un método específico, ya sea después o antes de su uso (o ambos), como los que se detallan en DoD 5220.22-M (National Industrial Security Program Operating Manual) o NIST 800-88 (Guidelines for Media Sanitization), puede hacerlo en Amazon EBS. Esa actividad de bloques se reflejará en los medios de almacenamiento subyacentes del servicio Amazon EBS.

Instantáneas

Amazon EBS ofrece la posibilidad de crear instantáneas (copias de seguridad) de cualquier volumen de EBS y guardar una copia de los datos del volumen en Amazon S3, donde se almacena de forma redundante en varias zonas de disponibilidad. No es necesario adjuntar el volumen a una instancia en ejecución para tomar una instantánea. Mientras siga grabando datos en un volumen, puede crear periódicamente una instantánea del volumen para usarla como referencia para nuevos volúmenes. Estas instantáneas se pueden utilizar para crear varios volúmenes de EBS nuevos o mover volúmenes por diferentes zonas de disponibilidad. Las instantáneas de volúmenes de EBS cifrados se cifran automáticamente.

Cuando se crea un nuevo volumen de EBS a partir de una instantánea, es una copia exacta del volumen original en el momento en que se tomó la instantánea. Los volúmenes EBS que se crean a partir de instantáneas cifradas se cifran automáticamente. De manera opcional, si se especifica una zona de disponibilidad distinta, puede usar esta funcionalidad un volumen duplicado en dicha zona. Las instantáneas se pueden compartir con AWS cuentas específicas o hacerse públicas. Cuando crea instantáneas, se le cobran cargos en Amazon S3 en función del tamaño de los datos a los que se les hace una copia de seguridad en lugar del tamaño del volumen de origen. Las instantáneas posteriores del mismo volumen son instantáneas progresivas. Incluyen solo los datos nuevos y modificados escritos en el volumen desde que se creó la última instantánea, y solo se le cobrará por esos datos.

Las instantáneas son backups incrementales, lo que significa que solo se guardan los bloques del volumen que han cambiado después de la instantánea más reciente. Si tiene un volumen con 100 GiB de datos pero solo 5 GiB han cambiado desde su última instantánea, solo se graban en Amazon S3 los 5 GiB de datos que se han modificado. Aunque las instantáneas se guarden de forma incremental, su proceso de eliminación está diseñado para que solo tenga que retener la instantánea más reciente.

Para ayudarle a categorizar y a administrar los volúmenes y las instantáneas, puede etiquetarlas con los metadatos que elija.

Para hacer copias de seguridad de los volúmenes de forma automática, puede usar Amazon Data Lifecycle Manager o AWS Backup.

Flexibilidad

Los volúmenes de EBS admiten cambios de configuración activos mientras se encuentran en producción. Puede modificar el tipo de volumen, el tamaño del volumen y la capacidad de IOPS sin

interrupciones del servicio. Para obtener más información, consulte Modificación de un volumen mediante Volúmenes elásticos de Amazon EBS.

Tipos de volúmenes de Amazon EBS

Amazon EBS proporciona los siguientes tipos de volúmenes, que difieren en cuanto a rendimiento y precio, para que pueda adaptar el rendimiento y el costo del almacenamiento a las necesidades de las aplicaciones.

> **Important**
>
> Existen varios factores que pueden afectar al rendimiento de los volúmenes de EBS, como la configuración de la instancia, las características de E/S o la demanda de la carga de trabajo. Para utilizar completamente las IOPS aprovisionadas en un volumen de EBS, utilice instancias optimizadas para EBS. Para obtener más información sobre cómo obtener el máximo rendimiento de los volúmenes de EBS, consulte Rendimiento del volumen de Amazon EBS.

Para obtener más información sobre los precios, consulte Precios de Amazon EBS.

Tipos de volúmenes

- Volúmenes en unidades de estado sólido (SSD)
- Volúmenes de unidades de disco duro (HDD)
- Volúmenes de generaciones anteriores

Volúmenes en unidades de estado sólido (SSD)

Volúmenes respaldados por SSD, optimizados para cargas de trabajo de transacciones que impliquen operaciones de lectura/escritura frecuentes de pequeño tamaño de E/S, en las que el atributo de rendimiento dominante es IOPS. Los tipos de volumen respaldados por SSD incluyen SSD de uso general y SSD de IOPS aprovisionadas. A continuación se presenta un resumen de los casos de uso y las características de los volúmenes respaldados por SSD.

	Volúmenes SSD de uso general		volúmenes Provisioned IOPS SSD	
Tipo de volumen	gp3	gp2	io2 Block Express [3]	io1
Durabilidad	99,8 % - 99,9 % de durabilidad (0,1 % - 0,2 % tasa anual de errores)		99,999 % de durabilidad (0,001 % tasa anual de errores)	99,8 % - 99,9 % de durabilidad (0,1 % - 0,2 % tasa anual de errores)
Casos de uso	• Cargas de trabajo transaccionales • Escritorios virtuales • Bases de datos de tamaño mediano y una sola instancia • Aplicaciones interactivas de baja latencia • Volúmenes de arranque • Entornos de desarrollo y pruebas		Cargas de trabajo que requieren lo siguiente: • Latencia inferior a milisegundos • Rendimiento de IOPS sostenido • Más de 64 000 IOPS o 1000 MiB/s de rendimiento	• Cargas de trabajo que requieren un rendimiento sostenido de IOPS o más de 16,000 IOPS • Cargas de trabajo de bases de datos con uso intensivo de operaciones de E/S
Tamaño del volumen	1 GiB - 16 TiB		4 GiB - 64 TiB [4]	4 GiB - 16 TiB
Máximo de IOPS por volumen	16 000 (E/S de 64 KiB)	16 000 (E/S de 16 KiB)	256 000 (E/S de 16 KiB) [5]	64 000 (E/S de 16 KiB)
Rendimiento máximo	1000 MiB/s	250 MiB/s [1]	4000 MiB/s	1000 MiB/s [2]

	Volúmenes SSD de uso general		volúmenes Provisioned IOPS SSD	
por volumen				
Amazon EBS Multi-attach	No compatible		Compatible	
Reservas de NVMe	No compatible		Compatible	No compatible
Volumen de arranque	Compatible			

[1] El límite de rendimiento está comprendido entre 128 MiB/s y 250 MiB/s, en función del tamaño del volumen. Para obtener más información, consulte Rendimiento del volumen gp2. Es posible que los volúmenes creados antes del 3 de diciembre de 2018 que no se hayan modificado desde su creación no alcancen el máximo rendimiento a menos que modifique el volumen.

[2] Para lograr el rendimiento máximo de 1000 MiB/s, el volumen debe aprovisionarse con 64 000 IOPS y debe estar asociado a una instancia creada en Nitro System. Es posible que los volúmenes creados antes del 6 de diciembre de 2017 que no se hayan modificado desde su creación no alcancen el máximo rendimiento a menos que modifique el volumen.

[3] Todos los volúmenes `io2` creados después del 21 de noviembre de 2023 son volúmenes `io2` Block Express. Los volúmenes `io2` creados antes del 21 de noviembre de 2023 se pueden convertir en volúmenes `io2` Block Express; para ello, modifique las IOPS o el tamaño del volumen.

Solo se pueden conectar [4] volúmenes de más de 16 TiB a las instancias integradas en el sistema Nitro.

Solo se pueden conectar [5] volúmenes de más de 64 000 IOPS a instancias integradas en el sistema Nitro. Se pueden conectar volúmenes de hasta 64 000 IOPS a instancias que no sean de Nitro, pero solo pueden alcanzar hasta 32 000 IOPS.

Para obtener más información acerca de los tipos de volumen basados en SSD, consulte lo siguiente:

- Volúmenes SSD de uso general
- volúmenes Provisioned IOPS SSD

Volúmenes de unidades de disco duro (HDD)

Los volúmenes respaldados por HDD están optimizados para grandes cargas de trabajo de streaming en las que el atributo de desempeño dominante es el rendimiento. Los tipos de volumen de HDD incluyen HDD de rendimiento optimizado y HDD en frío. A continuación se presenta un resumen de los casos de uso y las características de los volúmenes respaldados por HDD.

	Volúmenes de HDD con rendimiento optimizado	Volúmenes de HDD en frío
Tipo de volumen	`st1`	`sc1`
Durabilidad	99,8 % - 99,9 % de durabilidad (0,1 % - 0,2 % tasa anual de errores)	
Casos de uso	• Big data • Data warehouses • Procesamiento de registros	• Almacenamiento orientado al rendimiento para datos a los que se accede con poca frecuencia • Escenarios en los que es important e el costo de almacenamiento más bajo
Tamaño del volumen	125 GiB - 16 TiB	
IOPS máximo por volumen (E/S de 1 MiB)	500	250
Rendimiento máximo por volumen	500 MiB/s	250 MiB/s

	Volúmenes de HDD con rendimiento optimizado	Volúmenes de HDD en frío
Amazon EBS Multi-attach	No compatible	
Volumen de arranque	No compatible	

Para obtener más información acerca de los volúmenes de unidades de disco duro (HDD), consulte Volúmenes de HDD con rendimiento optimizado y de HDD en frío.

Volúmenes de generaciones anteriores

Los volúmenes magnéticos (`standard`) son volúmenes de generaciones anteriores respaldados por unidades magnéticas. Son perfectos para utilizarse para cargas de trabajo con conjuntos de datos pequeños en los que se accede a la información con poca frecuencia y el rendimiento no tiene una importancia primordial. Estos volúmenes ofrecen aproximadamente un promedio de 100 IOPS, con una capacidad de ráfaga de hasta cientos de IOPS, y su tamaño puede variar entre 1 GiB y 1 TiB.

> **Tip**
>
> Los volúmenes magnéticos son un tipo de volumen de generaciones anteriores. Si necesita un rendimiento o una uniformidad del rendimiento superior a los que proporcionan los volúmenes de generaciones anteriores, le recomendamos que use uno de los tipos de volumen nuevos.

En la siguiente tabla se describen los tipos de volúmenes de EBS de generaciones anteriores.

	Magnético
Tipo de volumen	`standard`
Casos de uso	Cargas de trabajo en las que el acceso a los datos es infrecuente
Tamaño del volumen	1 GiB-1 TiB

	Magnético
Máximo de IOPS por volumen	40-200
Rendimiento máximo por volumen	40-90 MiB/s
Volumen de arranque	Compatible

Para obtener más información, consulte Volumen de generaciones anteriores.

Volúmenes SSD de uso general

Los volúmenes SSD de uso general (gp2 y gp3) están respaldados por unidades de estado sólido (SSD). Combinan precio y rendimiento para una gran variedad de cargas de trabajo transacciones. Estos incluyen escritorios virtuales, bases de datos de tamaño mediano y una sola instancia, aplicaciones interactivas sensibles a la latencia, entornos de desarrollo y pruebas, y volúmenes de arranque. Recomendamos estos volúmenes para la mayoría de las cargas de trabajo.

Amazon EBS ofrece los siguientes tipos de volúmenes SSD de uso general:

Tipos

- Volúmenes de SSD de uso general (gp3)
- Volúmenes de SSD de uso general (gp2)

Volúmenes de SSD de uso general (gp3)

Los volúmenes SSD de uso general (gp3) son la última generación de volúmenes SSD de uso general y el volumen SSD de menor costo que ofrece Amazon EBS. Este tipo de volumen ayuda a que la mayoría de las aplicaciones obtengan el equilibrio adecuado entre precio y rendimiento. También lo ayuda a aumentar el rendimiento del volumen independientemente de su tamaño. Esto significa que puede aprovisionar el rendimiento necesario sin necesidad de aprovisionar capacidad de almacenamiento de bloques adicional. Además, los volúmenes gp3 ofrecen un precio por GiB un 20 % más bajo que los volúmenes SSD de uso general (gp2).

Los volúmenes gp3 ofrecen una latencia de milisegundos de un solo dígito y una durabilidad de volumen del 99,8 al 99,9 por ciento, con una tasa de errores anual (AFR) no superior al 0,2 por ciento, lo que se traduce en un máximo de dos fallos de volumen por cada 1000 volúmenes en

ejecución durante un período de un año. AWS diseña los volúmenes gp3 para ofrecer el rendimiento previsto el 99 por ciento de las veces.

Contenido

Rendimiento del volumen gp3

> **Tip**
>
> Los volúmenes gp3 no utilizan el rendimiento por ráfagas. Pueden mantener indefinidamente sus máximos rendimiento e IOPS aprovisionadas.

Rendimiento de IOPS

Los volúmenes gp3 ofrecen un rendimiento de IOPS de referencia constante de 3000 IOPS, que se incluye en el precio del almacenamiento. Puede aprovisionar IOPS adicionales (hasta un máximo de 16 000) por un costo adicional a razón de 500 IOPS por GiB del tamaño del volumen. Se puede aprovisionar el máximo de IOPS para volúmenes de 32 GiB o más grandes (500 IOPS por GiB × 32 GiB = 16 000 IOPS).

Rendimiento

Los volúmenes gp3 ofrecen un rendimiento de referencia constante de 125 MiB/s, que se incluye en el precio del almacenamiento. Puede aprovisionar rendimiento adicional (hasta un máximo de 1000 MiB/s) por un costo adicional a razón de 0,25 MiB/s por IOPS aprovisionadas. Se puede aprovisionar el rendimiento máximo a 4000 IOPS o más y a 8 GiB o más (4000 IOPS × 0,25 MiB/s por IOPS = 1000 MiB/s).

Tamaño del volumen gp3

El tamaño de un volumen gp3 puede variar entre 1 GiB y 16 TiB.

Migrar a gp3 desde gp2

Si en la actualidad utiliza volúmenes gp2, puede migrar sus volúmenes a gp3 mediante operaciones de Modificación de un volumen mediante Volúmenes elásticos de Amazon EBS. Puede utilizar

las operaciones de Amazon EBS Elastic Volumes para modificar el tipo de volumen, las IOPS y el rendimiento de los volúmenes existentes sin interrumpir las instancias de Amazon EC2. Cuando se utiliza la consola para crear un volumen o una AMI a partir de una instantánea, el volumen SSD de uso general gp3 es la opción predeterminada para el tipo de volumen. En otros casos, gp2 es la opción predeterminada. En estos casos, puede seleccionar gp3 como tipo de volumen en lugar de usar gp2.

Para saber cuánto puede ahorrar gracias a la migración de sus volúmenes gp2 a gp3, utilice la calculadora de ahorro de costos de migración de gp2 a gp3 de Amazon EBS.

Volúmenes de SSD de uso general (gp2)

Ofrecen almacenamiento económico que resulta ideal para una gran variedad de cargas de trabajo transaccionales. En los volúmenes gp2 el rendimiento aumenta con el tamaño del volumen.

> **Tip**
>
> Los volúmenes gp3 son la última generación de volúmenes SSD de uso general. Ofrecen una escala de rendimiento más predecible y precios que son hasta un 20 % más bajos que en el caso de los volúmenes gp2. Para obtener más información, consulte Volúmenes de SSD de uso general (gp3).
> Para saber cuánto puede ahorrar gracias a la migración de sus volúmenes gp2 a gp3, utilice la calculadora de ahorro de costos de migración de gp2 a gp3 de Amazon EBS.

gp2los volúmenes ofrecen una latencia de milisegundos de un solo dígito y una durabilidad de volumen del 99,8 al 99,9 por ciento, con una tasa de errores anual (AFR) no superior al 0,2 por ciento, lo que se traduce en un máximo de dos errores de volumen por cada 1000 volúmenes en funcionamiento durante un período de un año. AWS diseña los gp2 volúmenes para ofrecer el rendimiento previsto el 99 por ciento de las veces.

Contenido

Rendimiento del volumen **gp2**

Rendimiento de IOPS

El rendimiento de IOPS de referencia aumenta de forma lineal entre un mínimo de 100 y un máximo de 16 000 a razón de 3 IOPS por GiB del tamaño del volumen. El rendimiento de IOPS se aprovisiona de la siguiente manera:

- Los volúmenes de 33,33 GiB o menores se aprovisionan con un mínimo de 100 IOPS.
- Los volúmenes de más de 33,33 GiB se aprovisionan con 3 IOPS por GiB del tamaño del volumen hasta un máximo de 16 000 IOPS, que se alcanza a los 5334 GiB (3 X 5334).
- Los volúmenes de 5334 GiB o mayores se aprovisionan con 16 000 IOPS.

Los volúmenes gp2 de menos de 1 TiB (y que se aprovisionan con menos de 3000 IOPS) pueden ampliarse hasta 3000 IOPS cuando sea necesario durante un periodo prolongado. La capacidad de ampliarse de un volumen se rige por los créditos de E/S. Cuando la demanda de E/S es mayor que el rendimiento de referencia, el volumen gasta créditos de E/S para alcanzar el nivel de rendimiento requerido (hasta 3000 IOPS). En una transmisión por ráfagas, los créditos de E/S no se acumulan y se gastan a la tasa de IOPS que se utiliza por encima de la IOPS de referencia (tasa de gasto = IOPS de ráfaga - IOPS de referencia). Cuantos más créditos de E/S acumule un volumen, más tiempo podrá mantener el rendimiento por ráfagas. Puede calcular la duración de las ráfagas de la siguiente manera:

$$\text{Burst duration} = \frac{\text{(I/O credit balance)}}{\text{(Burst IOPS) - (Baseline IOPS)}}$$

Cuando la demanda de E/S cae al nivel de rendimiento de referencia o uno inferior, el volumen comienza a obtener créditos de E/S a una velocidad de 3 créditos de E/S por GiB del tamaño del volumen por segundo. Los volúmenes tienen un límite de acumulación de créditos de E/S de 5,4 millones de créditos de E/S, suficiente para mantener el rendimiento por ráfagas máximo de 3000 IOPS durante al menos 30 minutos.

> **Note**
>
> Cada volumen recibe un saldo inicial de 5,4 millones de créditos de E/S, lo que proporciona un ciclo de arranque inicial rápido para los volúmenes de arranque y una buena experiencia de arranque para otras aplicaciones.

En la siguiente tabla se muestra una lista de ejemplos de tamaños de volumen y el rendimiento de referencia asociado a cada uno de ellos, la duración de la ráfaga (cuando se comienza con 5,4 millones de créditos de E/S) y el tiempo necesario para rellenar un saldo vacío de créditos de E/S.

Tamaño del volumen (GiB)	Rendimiento de referencia (IOPS)	Duración de la ráfaga a 3000 IOPS (segundos)	Tiempo para recargar un saldo de créditos vacío (segundos)
1 a 33,33	100	1,862	54,000
100	300	2000	18 000
334 (tamaño mínimo para máximo rendimiento)	1002	2703	5389
750	2250	7200	2400
1000	3,000	N/A*	N/A*
5334 (tamaño mínimo para máximo de IOPS) y más	16,000	N/A*	N/A*

* El rendimiento de la línea de base del volumen excede el rendimiento por ráfagas máximo.

Puedes monitorizar el saldo de créditos de E/S de un volumen mediante la `BurstBalance` métrica Amazon EBS de Amazon. CloudWatch Esta métrica muestra el porcentaje de créditos de E/S de gp2restante. Para obtener más información, consulte Características de E/S de Amazon EBS y monitoreo. Puede establecer una alarma que lo notifica cuando el valor de `BurstBalance` cae a un cierto nivel. Para obtener más información, consulte Creación CloudWatch de alarmas.

Rendimiento

El rendimiento los volúmenes gp2 está comprendido entre 128 MiB/s y 250 MiB/s, en función del tamaño del volumen. El rendimiento se aprovisiona de la siguiente manera:

- Los volúmenes de 170 GiB o menos ofrecen un rendimiento máximo de 128 MiB/s.

- Los volúmenes más grandes de 170 GiB pero más pequeños de 334 GiB pueden ampliarse y ofrecer un rendimiento máximo de 250 MiB/s.
- Los volúmenes de 334 GiB o más ofrecen 250 MiB/s.

El rendimiento de un volumen gp2 se puede calcular con la siguiente fórmula, hasta el límite de rendimiento de 250 MiB/s:

```
Throughput in MiB/s = IOPS performance × I/O size in KiB / 1,024
```

Tamaño del volumen **gp2**

El tamaño de un volumen gp2 puede variar de 1 GiB a 16 TiB. Tenga en cuenta que el rendimiento del volumen aumenta de forma lineal con el tamaño del volumen.

volúmenes Provisioned IOPS SSD

Los volúmenes SSD de IOPS aprovisionadas están respaldados por unidades de estado sólido (SSD). Son los volúmenes de almacenamiento de Amazon EBS de mayor rendimiento y están diseñados para cargas de trabajo críticas con uso intensivo de IOPS y rendimiento que requieren baja latencia. Los volúmenes SSD de IOPS aprovisionadas ofrecen su rendimiento de IOPS aprovisionadas el 99,9 por ciento del tiempo.

Amazon EBS ofrece dos tipos de volúmenes SSD de IOPS aprovisionadas:

- Volúmenes SSD de IOPS aprovisionadas (io2) Block Express
- Volúmenes SSD de IOPS aprovisionadas (io1)

Volúmenes SSD de IOPS aprovisionadas (**io2**) Block Express

Los volúmenes io2 Block Express están basados en la siguiente generación de arquitectura de servidores de almacenamiento de Amazon EBS. Se ha diseñado con el fin de satisfacer los requisitos de rendimiento de las aplicaciones intensivas de E/S más exigentes que se ejecutan en las instancias creadas en Nitro System. Con la mayor durabilidad y la latencia más baja, Block Express es ideal para ejecutar cargas de trabajo críticas y de rendimiento intensivo, como Oracle, SAP HANA, Microsoft SQL Server y SAS Analytics.

La arquitectura de Block Express aumenta el rendimiento y la escala de los volúmenes io2. Los servidores de Block Express se comunican con las instancias creadas en Nitro System mediante

el protocolo de red Scalable Reliable Datagram (SRD). Esta interfaz se implementa en la Tarjeta Nitro exclusiva para la función de Amazon EBS E/S en el hardware host de la instancia. Minimiza el retraso de E/S y la variación de latencia (fluctuación de red), lo que proporciona un rendimiento más rápido y uniforme para sus aplicaciones.

Los volúmenes `io2` Block Express están diseñados para ofrecer una durabilidad del volumen del 99,999 por ciento con una tasa anual de errores (AFR) no superior al 0,001 por ciento, lo que se traduce en un solo error de volumen por cada 100 000 volúmenes en ejecución durante un periodo de un año. `io2` Los volúmenes Block Express son adecuados para las cargas de trabajo que se benefician de un único volumen que proporciona latencia inferior a milisegundos, admite un mayor rendimiento e IOPS más altas y una mayor capacidad que los volúmenes gp3.

Los volúmenes SSD de IOPS aprovisionadas (`io2`) Block Express ofrecen su rendimiento de IOPS aprovisionadas el 99,9 por ciento del tiempo.

Los volúmenes `io2` Block Express son compatibles con todas las instancias creadas en Nitro System. Para obtener más información, consulte Volúmenes de `io2` Block Express.

Temas

- Consideraciones
- Rendimiento

Consideraciones

- Los volúmenes `io2` Block Express están disponibles en las regiones siguientes: Este de EE. UU. (Ohio), Este de EE. UU. (Norte de Virginia), Oeste de EE. UU. (Norte de California), Oeste de EE. UU. (Oregón), Asia-Pacífico (Hong Kong), Asia-Pacífico (Bombay) Asia Pacífico (Seúl), Asia Pacífico (Singapur), Asia Pacífico (Sídney), Asia Pacífico (Tokio), Canadá (centro), Europa (Fráncfort), Europa (Irlanda), Europa (Londres), Europa (Estocolmo) y Medio Oriente (Baréin).
- Todos los volúmenes `io2` creados después del 21 de noviembre de 2023 son volúmenes `io2` Block Express. Los volúmenes `io2` creados antes del 21 de noviembre de 2023 se pueden convertir en volúmenes `io2` Block Express; para ello, modifique las IOPS o el tamaño del volumen.
- Las instancias creadas en Nitro System se pueden asociar a volúmenes de hasta 64 TiB de tamaño. Se pueden asociar otros tipos de instancias a volúmenes de hasta 16 TiB de tamaño.
- Las instancias creadas en Nitro System se pueden asociar a volúmenes aprovisionados con hasta 256 000 IOPS. Se pueden asociar otros tipos de instancias a volúmenes aprovisionados con hasta 64 000 IOPS, pero pueden lograr hasta 32 000 IOPS.

- Para crear un volumen `io2` cifrado que tenga un tamaño superior a 16 TiB o una cantidad de IOPS superior a 64 000 a partir de una instantánea no cifrada o de una instantánea cifrada compartida, debe hacer lo siguiente:
  1. Crear una copia cifrada de esa instantánea en su cuenta.
  2. Utilizar la copia de esa instantánea para crear el volumen.

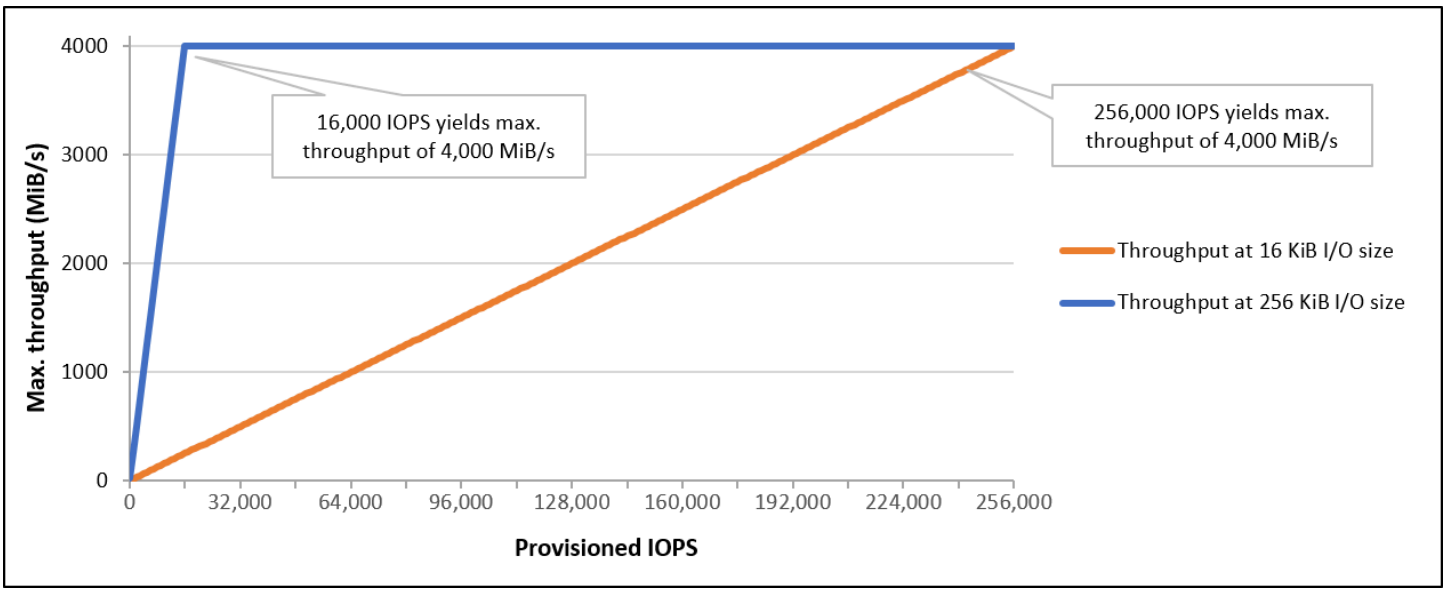
Rendimiento

Con los volúmenes `io2` Block Express, puede aprovisionar volúmenes con las siguientes características:

- Latencia media por debajo de milisegundos
- Capacidad de almacenamiento de hasta 64 TiB (65 536 GiB)
- IOPS provisionadas hasta 256 000, con una relación IOPS: GIB de 1000:1. Las IOPS máximas se pueden aprovisionar con volúmenes de 256 GiB y más grandes (1000 IOPS × 256 GiB = 256 000 IOPS).

> **Note**
>
> Puede alcanzar hasta 256 000 IOPS con instancias creadas en Nitro System. En otras instancias, puede lograr un rendimiento de hasta 32 000 IOPS.

- Rendimiento de volumen de hasta 4000 MiB/s. El rendimiento se escala de manera proporcional hasta 0,256 MiB/s por IOPS provisionadas. El rendimiento máximo se puede lograr a 16 000 IOPS o superior.



Volúmenes SSD de IOPS aprovisionadas (**`io1`**)

Los volúmenes SSD de IOPS aprovisionadas (`io1`) están diseñados para satisfacer las necesidades de las cargas de trabajo con uso intensivo de operaciones de E/S, en especial las cargas de trabajo de bases de datos, que son sensibles al rendimiento y a la consistencia del almacenamiento. Los volúmenes de SSD de IOPS provisionadas utilizan una velocidad de IOPS consistente que usted especifica al momento de crear el volumen. Amazon EBS ofrece rendimiento aprovisionado el 99,9 % del tiempo.

Los volúmenes `io1` están diseñados para ofrecer una durabilidad del volumen del 99,8 por ciento al 99,9 por ciento con una tasa anual de errores (AFR) no superior al 0,2 por ciento, lo que se traduce en un máximo de dos errores de volumen por cada 1000 volúmenes en ejecución durante un periodo de un año.

Los volúmenes `io1` están disponibles para todos los tipos de instancias de Amazon EC2.

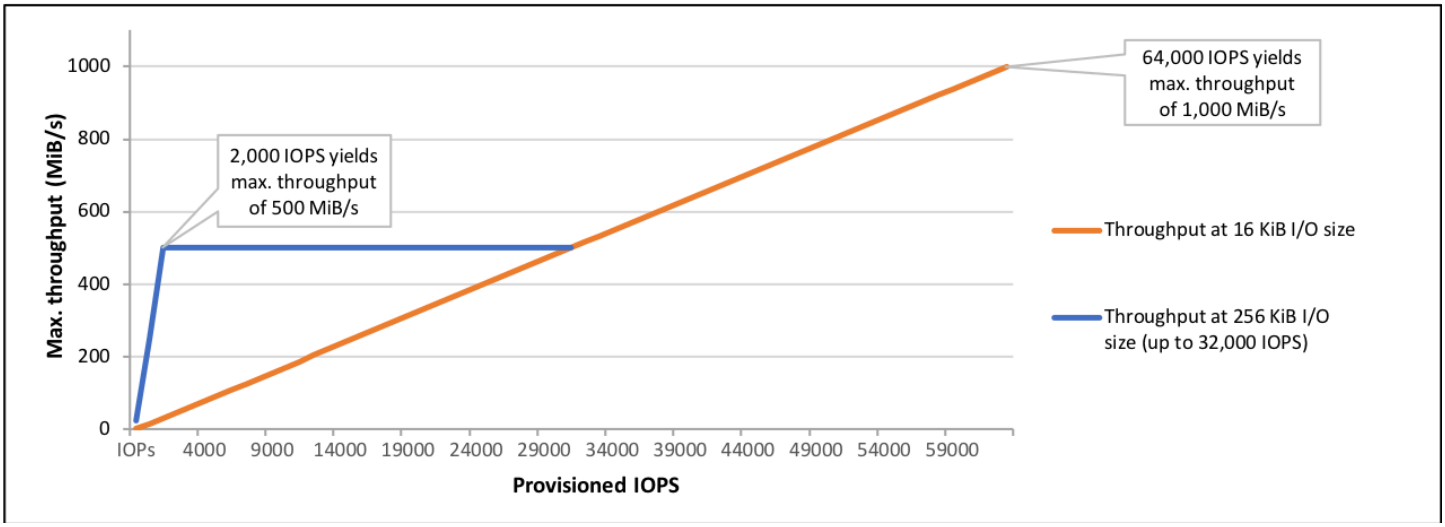
Rendimiento

Los volúmenes `io1` pueden variar entre 4 GiB y 16 TiB y se puede aprovisionar desde 100 IOPS hasta 64 000 IOPS por volumen. La relación máxima de IOPS provisionadas en relación con el tamaño de volumen solicitado (en GiB) es de 50:1. Por ejemplo, un volumen `io1` de 100 GiB se puede aprovisionar con hasta 5000 IOPS.

Se puede aprovisionar el máximo de IOPS para volúmenes de 1280 GiB o más (50 × 1280 GiB = 64 000 IOPS).

- Los volúmenes `io1` provisionados con hasta 32 000 IOPS admiten un tamaño de E/S máximo de 256 KiB y proporcionan un rendimiento de hasta 500 MiB/s. Con el tamaño máximo de E/S, el rendimiento máximo se alcanza a las 2000 IOPS.
- Los volúmenes `io1` aprovisionados con más de 32 000 IOPS (hasta el máximo de 64 000 IOPS) generan un aumento lineal del rendimiento a una velocidad de 16 KiB por IOPS aprovisionada. Por ejemplo, un volumen aprovisionado con 48.000 IOPS puede admitir hasta 750 MiB/s de rendimiento (16 KiB por IOPS provisionadas × 48 000 IOPS provisionadas = 750 MiB/s).
- Para lograr el rendimiento máximo de 1000 MiB/s, un volumen debe aprovisionarse con 64 000 IOPS (16 KiB por IOPS provisionadas × 64 000 IOPS provisionadas = 1000 MiB/s).
- Puede alcanzar hasta 64 000 IOPS solo en instancias creadas en Nitro System. En otras instancias, puede lograr un rendimiento de hasta 32 000 IOPS.

En el siguiente gráfico se ilustran estas características de rendimiento:



La experiencia de latencia por E/S depende de las IOPS provisionadas y del perfil de la carga de trabajo. Para obtener la mejor experiencia de latencia de E/S, asegúrese de aprovisionar IOPS para satisfacer el perfil de E/S de su carga de trabajo.

Volúmenes de HDD con rendimiento optimizado y de HDD en frío

Los volúmenes respaldados por unidades de disco duro proporcionados por Amazon EBS se clasifican en estas categorías:

- HDD con rendimiento optimizado: HDD de bajo costo diseñado para cargas de trabajo de rendimiento intensivo a las que se accede con frecuencia.

- HDD en frío: el diseño de HDD de más bajo costo destinado a cargas de trabajo a las que se accede con menos frecuencia.

Temas

Limitaciones en cuanto al rendimiento por instancia

El rendimiento de los volúmenes `st1` y `sc1` está determinado siempre por el valor menor entre los siguientes:

- Límites de rendimiento del volumen
- Límites de rendimiento de la instancia

Al igual que para todos los volúmenes de Amazon EBS, le recomendamos que seleccione una instancia de EC2 adecuada y optimizada para EBS a fin de evitar atascos en la red.

Volúmenes de HDD con rendimiento optimizado

Los volúmenes de HDD con rendimiento optimizado (`st1`) proporcionan almacenamiento magnético de bajo costo que define el desempeño en términos de rendimiento y no de IOPS. Este tipo de volumen es idóneo para grandes cargas de trabajo secuenciales como Amazon EMR, ETL, data warehouses y procesamiento de registros. No se admiten volúmenes de arranque `st1`.

Los volúmenes de HDD con rendimiento optimizado (`st1`), aunque son similares a los volúmenes de HDD en frío (`sc1`), están diseñados para admitir datos a los que se accede con frecuencia.

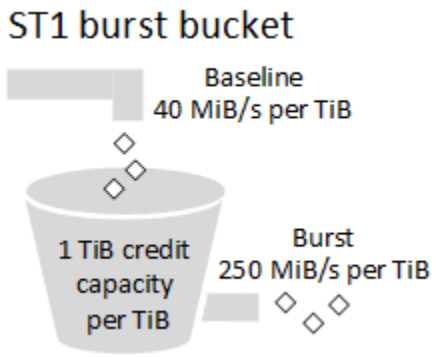
Este tipo de volumen está optimizado para cargas de trabajo que impliquen grandes E/S secuenciales, por lo que recomendamos que los clientes con cargas de trabajo que realicen pequeñas E/S aleatorias utilicen gp2. Para obtener más información, consulte Ineficiencia de operaciones de lectura/escritura pequeñas en HDD.

Los volúmenes de HDD con rendimiento optimizado (`st1`) que se adjuntan a las instancias optimizadas para EBS están diseñados para ofrecer un rendimiento uniforme, por lo que ofrecen, al menos, el 90 % del rendimiento esperado el 99 % del tiempo en un año determinado.

Créditos y rendimiento por ráfagas

Al igual que `gp2`, `st1` ofrece un rendimiento basado en un modelo de bucket por ráfaga. El tamaño del volumen determina el rendimiento de referencia del volumen, que es la velocidad a la que el volumen acumula créditos de rendimiento. El tamaño del volumen también determina el rendimiento de ráfaga del volumen, que es la velocidad a la que puede utilizar los créditos disponibles. Los volúmenes grandes presentan un rendimiento de referencia y de ráfaga superior. Cuantos más créditos tiene el volumen, más tiempo puede realizar E/S en el nivel de ráfaga.

En el siguiente diagrama se muestra el comportamiento del bucket por ráfaga de `st1`.



El rendimiento disponible de un volumen `st1`, que está sujeto a los límites del rendimiento y de los créditos de rendimiento, se expresa mediante la siguiente fórmula:

```
(Volume size) × (Credit accumulation rate per TiB) = Throughput
```

Para un volumen `st1` de 1 TiB, el rendimiento de ráfaga está limitado a 250 MiB/s, el bucket se rellena con créditos a 40 MiB/s y puede albergar hasta 1 TiB de créditos.

Los volúmenes más grandes amplían estos límites linealmente, limitándose el rendimiento a un máximo de 500 MiB/s. Una vez que se agota el bucket, el rendimiento se limita a la velocidad de referencia de 40 MiB/s por TiB.

En los tamaños de volumen que van de 0,125 a 16 TiB, el rendimiento de referencia varía entre 5 MiB/s y un máximo de 500 MiB/s, el cual se alcanza a 12,5 TiB del siguiente modo:

```
            40 MiB/s
12.5 TiB × ---------- = 500 MiB/s
```

```
              1 TiB
```

El rendimiento de ráfaga varía de 31 MiB/s al límite de 500 MiB/s, el cual se alcanza a 2 TiB del modo siguiente:

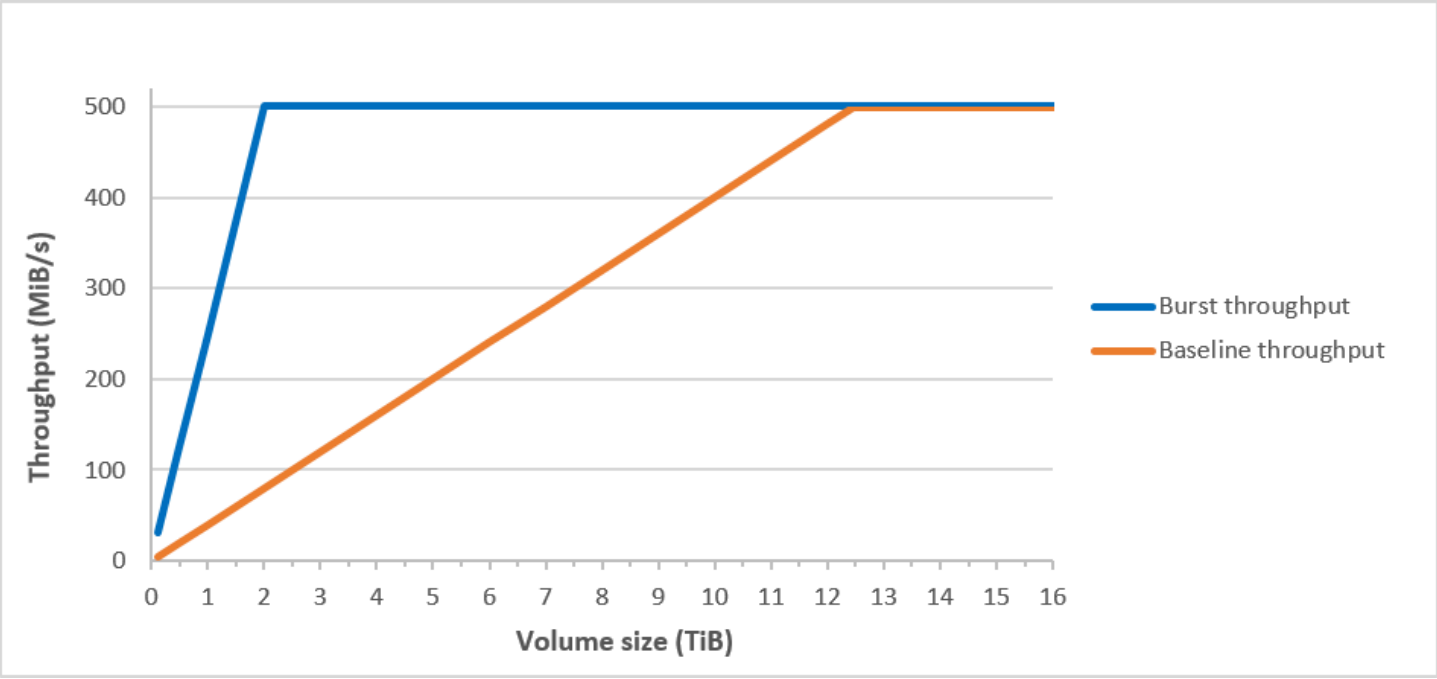
```
         250 MiB/s
2 TiB × ---------- = 500 MiB/s
          1 TiB
```

En la siguiente tabla se muestra el rango completo de valores de rendimiento de referencia y de ráfaga para `st1`:

Tamaño del volumen (TiB)	Rendimiento de referencia de ST1 (MiB/s)	Rendimiento de ráfaga de ST1 (MiB/s)
0.125	5	31
0,5	20	125
1	40	250
2	80	500
3	120	500
4	160	500
5	200	500
6	240	500
7	280	500
8	320	500
9	360	500
10	400	500
11	440	500

Tamaño del volumen (TiB)	Rendimiento de referencia de ST1 (MiB/s)	Rendimiento de ráfaga de ST1 (MiB/s)
12	480	500
12,5	500	500
13	500	500
14	500	500
15	500	500
16	500	500

El siguiente diagrama ilustra los valores de la tabla:



> **Note**
>
> Cuando se crea una instantánea de un volumen de HDD con rendimiento optimizado (`st1`), el rendimiento puede caer hasta el valor de base de referencia del volumen mientras la instantánea está en curso.

Para obtener información sobre el uso de CloudWatch métricas y alarmas para monitorizar el saldo acumulado, consulte Supervisar el balance del bucket de ráfagas para los volúmenes.

Volúmenes de HDD en frío

Los volúmenes de HDD en frío (`sc1`) proporcionan almacenamiento magnético de bajo costo que define el desempeño en términos de rendimiento y no de IOPS. Con un límite de rendimiento inferior al de `st1`, `sc1` es ideal para grandes cargas de trabajo secuenciales de datos inactivos. Si requiere un acceso poco frecuente a los datos y busca ahorrar costos, `sc1` proporciona un almacenamiento de bloques económico. No se admiten volúmenes de arranque `sc1`.

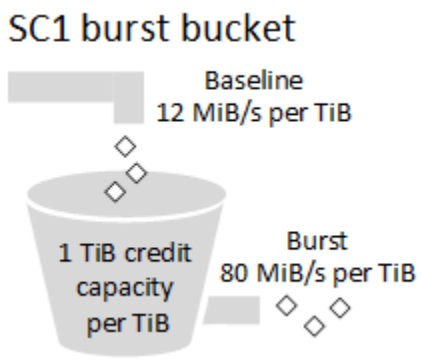
Los volúmenes de HDD en frío (`sc1`), aunque son similares a los volúmenes de HDD con rendimiento optimizado (`st1`), están diseñados para admitir datos a los que se accede con poca frecuencia.

> **Note**
>
> Este tipo de volumen está optimizado para cargas de trabajo que impliquen grandes E/S secuenciales, por lo que recomendamos que los clientes con cargas de trabajo que realicen pequeñas E/S aleatorias utilicen gp2. Para obtener más información, consulte Ineficiencia de operaciones de lectura/escritura pequeñas en HDD.

Los volúmenes de HDD en frío (`sc1`) que se adjuntan a las instancias optimizadas para EBS están diseñados para ofrecer un rendimiento uniforme, por lo que ofrecen, al menos, el 90 % del rendimiento esperado el 99 % del tiempo en un año determinado.

Créditos y rendimiento por ráfagas

Al igual que gp2, `sc1` ofrece un rendimiento basado en un modelo de bucket por ráfaga. El tamaño del volumen determina el rendimiento de referencia del volumen, que es la velocidad a la que el volumen acumula créditos de rendimiento. El tamaño del volumen también determina el rendimiento de ráfaga del volumen, que es la velocidad a la que puede utilizar los créditos disponibles. Los volúmenes grandes presentan un rendimiento de referencia y de ráfaga superior. Cuantos más créditos tiene el volumen, más tiempo puede realizar E/S en el nivel de ráfaga.



El rendimiento disponible de un volumen `sc1`, que está sujeto a los límites del rendimiento y de los créditos de rendimiento, se expresa mediante la siguiente fórmula:

```
(Volume size) × (Credit accumulation rate per TiB) = Throughput
```

Para un volumen `sc1` de 1 TiB, el rendimiento de ráfaga está limitado a 80 MiB/s, el bucket se rellena con créditos a 12 MiB/s y puede albergar hasta 1 TiB de créditos.

Los volúmenes más grandes amplían estos límites linealmente, y tienen un rendimiento limitado a un máximo de 250 MiB/s. Una vez que se agota el bucket, el rendimiento se limita a la velocidad de referencia de 12 MiB/s por TiB.

En los tamaños de volumen de 0,125 a 16 TiB, el rendimiento de referencia varía entre 1,5 MiB y el máximo de 192 MiB/s, el cual se alcanza a 16 TiB del modo siguiente:

```
           12 MiB/s
16 TiB × ---------- = 192 MiB/s
            1 TiB
```

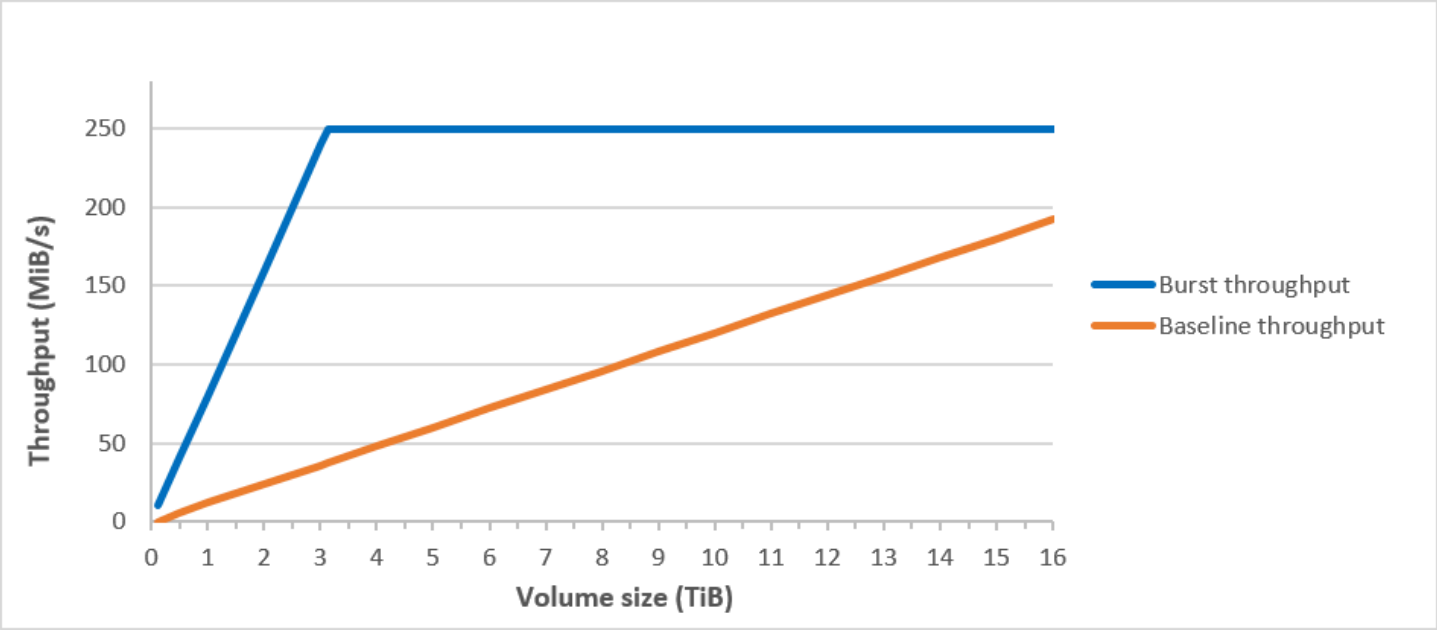
El rendimiento de ráfaga varía entre 10 MiB/s y el límite de 250 MiB/s, el cual se alcanza a 3,125 TiB del siguiente modo:

```
             80 MiB/s
3.125 TiB × ---------- = 250 MiB/s
              1 TiB
```

En la siguiente tabla se muestra el rango íntegro de valores de rendimiento de referencia y de ráfaga para `sc1`:

Tamaño del volumen (TiB)	Rendimiento de referencia de SC1 (MiB/s)	Rendimiento de ráfaga de SC1 (MiB/s)
0.125	1.5	10
0,5	6	40
1	12	80
2	24	160
3	36	240
3125	37,5	250
4	48	250
5	60	250
6	72	250
7	84	250
8	96	250
9	108	250
10	120	250
11	132	250
12	144	250
13	156	250
14	168	250
15	180	250
16	192	250

El siguiente diagrama ilustra los valores de la tabla:



> **Note**
>
> Cuando se crea una instantánea de un volumen de HDD en frío (`sc1`), el rendimiento puede caer hasta el valor de base de referencia del volumen mientras la instantánea está en curso.

Para obtener información sobre el uso de CloudWatch métricas y alarmas para monitorizar el saldo de la cubeta acumulada, consulteSupervisar el balance del bucket de ráfagas para los volúmenes.

Consideraciones sobre el rendimiento cuando se utilizan volúmenes HDD

Para un rendimiento óptimo a la hora de utilizar volúmenes HDD, planifique sus cargas de trabajo teniendo en cuenta las siguientes consideraciones.

Comparación de los volúmenes de HDD con rendimiento optimizado y de HDD en frío

El tamaño de los buckets de `st1` y `sc1` varía en función del tamaño del volumen, y un bucket completo contiene suficientes tokens para un análisis de volumen completo. Sin embargo, los volúmenes `st1` y `sc1` más grandes tardan más tiempo en completar el análisis de volumen debido a los límites de rendimiento por instancia y por volumen. Los volúmenes adjuntos a instancias más pequeñas están restringidos según el rendimiento por instancia en lugar de los límites de rendimiento de `st1` o `sc1`.

Tanto `st1` como `sc1` están diseñados para ofrecer una uniformidad del 90 % del rendimiento de ráfaga el 99 % del tiempo. Los periodos que no cumplen estas convenciones se distribuyen de manera prácticamente uniforme, por lo que se alcanza el 99 % del rendimiento total previsto cada hora.

En general, los tiempos de análisis se expresan mediante esta fórmula:

```
 Volume size
------------ = Scan time
 Throughput
```

Por ejemplo, si se tienen en cuenta las garantías sobre consistencia del rendimiento y otras optimizaciones, cabe esperar que un cliente de `st1` con un volumen de 5 TiB realice un análisis de volumen completo en un tiempo de entre 2,91 y 3,27 horas.

- Tiempo óptimo de análisis

```
   5 TiB            5 TiB
----------- = ------------------ = 10,486 seconds = 2.91 hours
 500 MiB/s     0.00047684 TiB/s
```

- Tiempo máximo de análisis

```
  2.91 hours
-------------- = 3.27 hours
 (0.90)(0.99) <-- From expected performance of 90% of burst 99% of the time
```

Del mismo modo, cabe esperar que un cliente de `sc1` con un volumen de 5 TiB realice un análisis de volumen completo en un tiempo de entre 5,83 y 6,54 horas.

- Tiempo óptimo de análisis

```
   5 TiB             5 TiB
----------- = ------------------- = 20972 seconds = 5.83 hours
 250 MiB/s     0.000238418 TiB/s
```

- Tiempo máximo de análisis

```
  5.83 hours
```

```
-------------- = 6.54 hours
 (0.90)(0.99)
```

En la tabla siguiente se muestran los tiempos de análisis ideales para volúmenes de diversos tamaños, presumiendo buckets íntegros y un rendimiento de las instancias suficiente.

Tamaño del volumen (TiB)	Tiempo de análisis con ráfaga de ST1 (horas)*	Tiempo de análisis con ráfaga de SC1 (horas)*
1	1,17	3,64
2	1,17	3,64
3	1,75	3,64
4	2,33	4,66
5	2,91	5,83
6	3,50	6,99
7	4,08	8,16
8	4,66	9,32
9	5,24	10,49
10	5,83	11,65
11	6,41	12,82
12	6,99	13,98
13	7,57	15,15
14	8,16	16,31
15	8,74	17,48
16	9,32	18,64

* Estos tiempos de análisis presuponen una profundidad de la cola media (redondeada al siguiente número entero) de cuatro o más al completar 1 MiB de E/S secuencial.

Por lo tanto, si tiene una carga de trabajo orientada al rendimiento que necesite realizar análisis rápidamente (hasta 500 MiB/s) o que requiera varios análisis de volumen completos al día, utilice `st1`. Si está optimizando costos, el acceso a los datos es relativamente poco frecuente y no necesita un rendimiento de análisis de más de 250 MiB/s, entonces utilice `sc1`.

Ineficiencia de operaciones de lectura/escritura pequeñas en HDD

El modelo de rendimiento de los volúmenes `st1` y `sc1` está optimizado para E/S secuenciales, lo que favorece las cargas de trabajo de alto rendimiento, ofrece un rendimiento aceptable para cargas de trabajo con IOPS y rendimiento mixtos y desfavorece las cargas de trabajo con E/S pequeñas y aleatorias.

Por ejemplo, una solicitud de E/S de 1 MiB o menos cuenta como un crédito de E/S de 1 MiB. Sin embargo, si las E/S son secuenciales, se fusionan en bloques de E/S de 1 MiB cuentan como un solo crédito de E/S de 1 MiB.

Supervisar el balance del bucket de ráfagas para los volúmenes

Puede supervisar el nivel de los cubos de ráfaga `st1` y los `sc1` volúmenes mediante la `BurstBalance` métrica de Amazon EBS disponible en Amazon CloudWatch. Esta métrica muestra los créditos de rendimiento de `st1` y `sc1` que quedan en el bucket por ráfaga. Para obtener más información sobre la `BurstBalance` métrica y otras métricas relacionadas con la E/S, consulte. Características de E/S de Amazon EBS y monitoreo CloudWatch también le permite configurar una alarma que le notifica cuando el `BurstBalance` valor cae a un nivel determinado. Para obtener más información, consulte Creación de CloudWatch alarmas.

Restricciones de tamaño y configuración de un volumen de EBS

El tamaño de un volumen de Amazon EBS está limitado por la física y la aritmética del almacenamiento de datos en bloques, así como por las decisiones de implementación de los diseñadores de sistemas operativos (OS) y sistemas de archivos. AWS impone límites adicionales al tamaño del volumen para garantizar la fiabilidad de sus servicios.

En las siguientes secciones se describen los factores más importantes que limitan el tamaño utilizable de un volumen de EBS y se ofrecen recomendaciones para configurar los volúmenes de EBS.

Contenido

Capacidad de almacenamiento

En la tabla siguiente se resumen las capacidades de almacenamiento teóricas e implementadas de los sistemas de archivos más conocidos en Amazon EBS, bajo el supuesto de un tamaño de bloque de 4 096 bytes.

Esquema de partición	Máx. bloques direccionables	Tamaño máx. teórico (bloques x tamaño de bloque)	Tamaño máx. implementado Ext4*	Tamaño máx. implementado XFS**	Tamaño máx. implementado NTFS	Máx. compatible con EBS
MBR	2^{32}	2 TiB	2 TiB	2 TiB	2 TiB	2 TiB
GPT	2^{64}	64 ZiB	1 EiB = 1024^2 TiB (50 TiB certificados en RHEL7)	500 TiB (certificado en RHEL7)	256 TiB	64 TiB †

* https://ext4.wiki.kernel.org/index.php/Ext4_Howto y https://access.redhat.com/solutions/1532

** https://access.redhat.com/solutions/1532

† Los volúmenes `io2` Block Express admiten hasta 64 TiB para las particiones GPT. Para obtener más información, consulte Volúmenes SSD de IOPS aprovisionadas (`io2`) Block Express.

Limitaciones del servicio

Amazon EBS extrae el almacenamiento distribuido masivamente de un centro de datos en discos duros virtuales. Para un sistema operativo instalado en una instancia EC2, un volumen de EBS adjunto parece un disco duro físico que contiene sectores de disco de 512 bytes. El sistema operativo administra la asignación de bloques de datos (o clústeres) en los sectores virtuales mediante sus utilidades de administración del almacenamiento. La asignación sigue un esquema de creación de particiones del volumen, como un registro de arranque maestro (MBR) o una tabla de particiones GUID (GPT), y está dentro de las posibilidades del sistema de archivos instalado (ext4, NTFS, etc.).

EBS no es consciente de los datos contenidos en sus sectores de disco virtuales; se limita a garantizar la integridad de los sectores. Esto significa que AWS las acciones y las acciones del sistema operativo son independientes entre sí. Cuando seleccione un tamaño de volumen, considere las posibilidades y los límites de ambos, como en los casos siguientes:

- EBS admite actualmente un tamaño de volumen máximo de 64 TiB. Esto significa que puede crear un volumen de EBS tan grande como 64 TiB, pero el reconocimiento por parte del sistema operativo de esa capacidad depende de sus propias características de diseño y de la partición del volumen.
- Los volúmenes de arranque deben utilizar el esquema de partición MBR o GPT. La AMI desde la que inicia una instancia determina el modo de arranque y posteriormente, el esquema de partición utilizado para el volumen de arranque.

  Con el MBR, los volúmenes de arranque están limitados a un tamaño de 2 TiB.

  Con GPT, los volúmenes de arranque pueden tener un tamaño de hasta 64 TiB cuando se utilizan con el modo de arranque GRUB2 (Linux) o UEFI (Windows).

  Para obtener más información, consulte Cómo hacer que un volumen de Amazon EBS esté disponible para su uso.
- Los volúmenes de Windows que no son de arranque de 2 TiB (2048 GiB) o más deben utilizar una tabla de particiones GPT para acceder a todo el volumen.

Esquemas de partición

Entre los impactos restantes, el esquema de partición determina cuántos bloques de datos lógicos se pueden abordar de forma única en un solo volumen. Para obtener más información, consulte

Tamaños de los bloques de datos. Los esquemas de particiones comunes que se utilizan son el registro de arranque maestro (MBR) y la tabla de partición GUID (GPT). Las principales diferencias entre estos esquemas se resumen a continuación.

MBR

MBR utiliza una estructura de datos de 32 bits para almacenar direcciones de bloques. Esto significa que cada bloque de datos se asigna a uno de los 2^{32} enteros posibles. El tamaño máximo direccionable máximo de un volumen se indica mediante la siguiente fórmula:

$$2^{32} \times \text{Block size}$$

El tamaño de los bloques de los volúmenes MBR está convencionalmente limitado a 512 bytes. Por consiguiente:

$$2^{32} \times 512 \text{ bytes} = 2 \text{ TiB}$$

Las soluciones de ingeniería destinadas a aumentar este límite de 2 TiB para los volúmenes MBR no han tenido una gran aceptación en el sector. En consecuencia, Linux y Windows nunca detectan que un volumen MBR sea superior a 2 TiB, incluso AWS si muestran que su tamaño es mayor.

GPT

GPT utiliza una estructura de datos de 64 bits para almacenar direcciones de bloques. Esto significa que cada bloque de datos se asigna a uno de los 2^{64} enteros posibles. El tamaño máximo direccionable máximo de un volumen se indica mediante la siguiente fórmula:

$$2^{64} \times \text{Block size}$$

El tamaño de los bloques de los volúmenes GPT está normalmente limitado a 4096 bytes. Por consiguiente:

$$\begin{aligned} & 2^{64} \times 4{,}096 \text{ bytes} \\ &= 2^{64} \times 2^{12} \text{ bytes} \\ &= 2^{70} \times 2^{6} \text{ bytes} \\ &= 64 \text{ ZiB} \end{aligned}$$

Los sistemas de computación reales no admiten nada que esté cercano a este máximo teórico. El tamaño del sistema de archivos implementado está actualmente limitado a 50 TiB para ext4 y 256 TiB para NTFS.

Tamaños de los bloques de datos

El almacenamiento de datos en un disco duro moderno se administra mediante la direccionabilidad por bloques lógicos, una capa de abstracción que permite al sistema operativo leer y escribir datos en bloques lógicos teniendo poca información sobre el hardware subyacente. El sistema operativo se basa en el dispositivo de almacenamiento para asignar los bloques a sus sectores físicos. EBS publica sus sectores de 512 bytes en el sistema operativo, el cual lee y escribe datos en el disco con la ayuda de bloques de datos que son un múltiplo del tamaño del sector.

El tamaño predeterminado del sector para los bloques de datos lógicos está actualmente en 4096 bytes (4 KiB). Dado que algunas cargas de trabajo se benefician de un tamaño de bloque más pequeño o más grande, los sistemas de archivos admiten tamaños de bloques no predeterminados que se pueden especificar durante el formato. Los casos en los que deben utilizarse tamaños de bloques de datos que no son los tamaños predeterminados no entran dentro de este tema, pero la elección del tamaño de los bloques repercute sobre la capacidad de almacenamiento del volumen. En la tabla siguiente se muestra la capacidad de almacenamiento en función del tamaño de los bloques:

Tamaño del bloque	Tamaño máx. del volumen
4 KiB (valor predeterminado)	16 TiB
8 KiB	32 TiB
16 KiB	64 TiB
32 KiB	128 TiB
64 KiB (máximo)	256 TiB

El límite impuesto por EBS sobre el tamaño del volumen (64 TiB) es actualmente el mismo que el tamaño máximo permitido por los bloques de datos de 16 KiB.

Amazon EBS y NVMe

Los volúmenes de EBS se exponen como dispositivos de bloque NVMe en las instancias creadas en Nitro System.

Las guía de rendimiento de EBS indicadas en los detalles del producto Amazon EBS son válidas, independientemente de la interfaz del dispositivo de bloques.

instancias de Linux

Los nombres de dispositivo son `/dev/nvme0n1`, `/dev/nvme1n1` y así sucesivamente. Los nombres de dispositivos que especifica en un mapeo de dispositivos de bloques se cambian por los nombres de dispositivos NVMe (`/dev/nvme[0-26]n1`). El controlador de dispositivo de bloques puede asignar nombres de dispositivos NVMe en un orden distinto al especificado para los volúmenes del mapeo del dispositivo de bloques.

instancias de Windows

Cuando adjunta un volumen a su instancia, incluye un nombre de dispositivo para el volumen. Amazon EC2 utiliza este nombre del dispositivo. El controlador del dispositivo de bloques de la instancia asigna el nombre del volumen real al montar el volumen, y el nombre asignado puede diferir del que utiliza Amazon EC2.

Contenido

Instalar o actualizar el controlador NVMe

Para obtener acceso a los volúmenes NVMe, deben estar instalados los controladores NVMe. Las instancias pueden admitir volúmenes de EBS NVMe, volúmenes de almacén de instancias NVMe, ambos tipos de volúmenes NVMe o ningún volumen NVMe. Para obtener más información, consulte Resumen de las características de redes y almacenamiento.

instancias de Linux

Las siguientes AMI incluyen los controladores NVMe necesarios:

- Amazon Linux 2

- Amazon Linux AMI 2018.03
- Ubuntu 14.04 o versiones posteriores con el kernel `linux-aws`

> **Note**
>
> AWS Los tipos de instancias basados en Graviton requieren Ubuntu 18.04 o posterior con kernel `linux-aws`

- Red Hat Enterprise Linux 6.5 o versiones posteriores
- Red Hat Enterprise Linux 7.4 o versiones posteriores
- SUSE Linux Enterprise Server 12 SP2 o versiones posteriores
- CentOS 7.4.1708 o versiones posteriores
- FreeBSD 11.1 o versiones posteriores
- Debian GNU/Linux 9 o versiones posteriores

Para confirmar que su instancia tiene el controlador NVMe

Puede confirmar que la instancia tiene el controlador NVMe mediante el siguiente comando.

- Amazon Linux, RHEL, CentOS y SUSE Linux Enterprise Server

```
$ modinfo nvme
```

  Si la instancia tiene el controlador NVMe, el comando devuelve información sobre el controlador.

- Amazon Linux 2 y Ubuntu

```
$ ls /sys/module/ | grep nvme
```

  Si la instancia tiene el controlador NVMe, el comando devuelve los controladores instalados.

Para actualizar el controlador NVMe

Si la instancia tiene el controlador NVMe, puede actualizar el controlador a la versión más reciente mediante el procedimiento siguiente.

1. Conéctese a la instancia.

2. Actualice la caché del paquete para obtener las actualizaciones necesarias del paquete que se indican a continuación.

   - En Amazon Linux 2, Amazon Linux, CentOS y Red Hat Enterprise Linux:

     ```
     [ec2-user ~]$ sudo yum update -y
     ```

   - En Ubuntu y Debian:

     ```
     [ec2-user ~]$ sudo apt-get update -y
     ```

3. Ubuntu 16.04 y versiones posteriores incluyen el paquete `linux-aws`, que contiene los controladores NVMe y ENA necesarios para las instancias basadas en Nitro. Actualice el paquete `linux-aws` para recibir la última versión tal como se indica a continuación:

   ```
   [ec2-user ~]$ sudo apt-get install --only-upgrade -y linux-aws
   ```

   Para Ubuntu 14.04, puede instalar el último paquete `linux-aws` del modo siguiente:

   ```
   [ec2-user ~]$ sudo apt-get install linux-aws
   ```

4. Reinicie la instancia para cargar la última versión de kernel.

   ```
   sudo reboot
   ```

5. Vuelva a conectarse a su instancia una vez que se haya reiniciado.

instancias de Windows

Las AMI de AWS Windows para Windows Server 2008 R2 y versiones posteriores incluyen el AWS controlador NVMe. Si no utiliza las últimas AMI de AWS Windows proporcionadas por Amazon, consulte Instalación o actualización de los controladores AWS NVMe mediante PowerShell la Guía del usuario de Amazon EC2.

Identificar el dispositivo EBS

EBS utiliza la virtualización de E/S de raíz única (SR-IOV) para proporcionar asociaciones de volumen en instancias basadas en Nitro mediante la especificación NVMe. Estos dispositivos se basan en los controladores NVMe estándar del sistema operativo. Por lo general, estos controladores detectan los dispositivos conectados durante el arranque de la instancia y crean nodos de dispositivo

basados en el orden en el que responden los dispositivos, no en cómo se especifican los dispositivos en la asignación de dispositivos de bloques.

instancias de Linux

En Linux, los nombres de dispositivo NVMe siguen el patrón `/dev/nvme<x>n<y>`, donde **<x>** es el orden de enumeración y, para EBS, **<y>** es 1. A veces, los dispositivos pueden responder a la búsqueda con un orden distinto en los siguientes inicios de instancia, lo que provoca un cambio del nombre del dispositivo. Además, el nombre de dispositivo asignado por el controlador de dispositivo de bloques puede ser diferente del nombre especificado en la asignación de dispositivos de bloques.

Le recomendamos que utilice identificadores estables para sus volúmenes EBS dentro de su instancia, como uno de los siguientes:

- Para las instancias basadas en Nitro, los mapeos de dispositivos de bloques que se especifican en la consola Amazon EC2 cuando está conectando un volumen de EBS o durante las llamadas a la API `AttachVolume` o `RunInstances` se capturan en el campo de datos específico del proveedor de la identificación del controlador NVMe. Con AMI Amazon Linux de versiones posteriores a la 2017.09.01, proporcionamos una regla `udev` que lee estos datos y crea un enlace simbólico al mapeo de dispositivos de bloques.
- El ID de volumen de EBS y el punto de montaje son estables entre los cambios de estado de instancia. El nombre de dispositivo NVMe puede cambiar en función del orden en el que respondan los dispositivos durante el arranque de la instancia. Se recomienda utilizar el ID de volumen de EBS y el punto de montaje para una identificación de dispositivo coherente.
- Los volúmenes EBS de NVMe disponen de un ID de volumen de EBS establecido como número de serie en la identificación del dispositivo. Utilice el comando `lsblk -o +SERIAL` para enumerar el número de serie.
- El formato del nombre del dispositivo NVMe puede variar en función de si el volumen de EBS se adjuntó durante o después del lanzamiento de la instancia. Los nombres de dispositivos NVMe para los volúmenes adjuntos después del lanzamiento de la instancia incluyen el prefijo `/dev/`, mientras que los nombres de dispositivos NVMe para los volúmenes adjuntos durante el lanzamiento de la instancia no incluyen el prefijo `/dev/`. Si utiliza una AMI de Amazon Linux o FreeBSD, utilice el comando `sudo ebsnvme-id /dev/nvme0n1 -u` para obtener un nombre de dispositivo NVMe coherente. Para otras distribuciones, utilice el comando `sudo nvme id-ctrl -v /dev/nvme0n1` para determinar el nombre del dispositivo NVMe.
- Cuando se le da formato a un dispositivo, se genera un UUID que se conserva durante la vida útil del sistema de archivos. Se puede especificar una etiqueta de dispositivo al mismo tiempo. Para

obtener más información, consulte Cómo hacer que un volumen de Amazon EBS esté disponible para su uso y Arranque desde un volumen incorrecto.

AMI de Amazon Linux

Con la AMI de Amazon Linux 2017.09.01 o posterior (incluido Amazon Linux 2), puede ejecutar el comando ebsnvme-id como se indica a continuación para mapear el nombre del dispositivo NVMe a un ID de volumen y un nombre de dispositivo:

En el ejemplo siguiente se muestra el comando y el resultado de un volumen adjunto durante el lanzamiento de la instancia. Tenga en cuenta que el nombre del dispositivo NVMe no incluye el prefijo `/dev/`.

```
[ec2-user ~]$ sudo /sbin/ebsnvme-id /dev/nvme0n1
Volume ID: vol-01324f611e2463981
sda
```

En el siguiente ejemplo se muestra el comando y el resultado de un volumen adjunto después del lanzamiento de la instancia. Tenga en cuenta que el nombre del dispositivo NVMe incluye el prefijo `/dev/`.

```
[ec2-user ~]$ sudo /sbin/ebsnvme-id /dev/nvme1n1
Volume ID: vol-064784f1011136656
/dev/sdf
```

Amazon Linux también crea un enlace simbólico desde el nombre del dispositivo en el mapeo de dispositivos de bloques (por ejemplo, `/dev/sdf`) al nombre del dispositivo NVMe.

AMI de FreeBSD

A partir de FreeBSD 12.2-RELEASE, puede ejecutar el comando ebsnvme-id como se muestra arriba. Pase el nombre del dispositivo NVMe (por ejemplo, `nvme0`) o el dispositivo de disco (por ejemplo, `nvd0` o `nda0`). FreeBSD también crea enlaces simbólicos a los dispositivos de disco (por ejemplo, `/dev/aws/disk/ebs/`*`volume_id`*).

Otras AMI de Linux

Con una versión del kernel 4.2 o posterior, puede ejecutar el comando nvme id-ctrl como se indica a continuación para mapear un dispositivo NVMe a un ID de volumen. En primer lugar, instale el paquete de línea de comandos de NVMe, `nvme-cli`, mediante las herramientas de administración

de paquetes de la distribución de Linux. Para obtener instrucciones de descarga e instalación para otras distribuciones, consulte la documentación específica de su distribución.

En el siguiente ejemplo se obtiene el ID de volumen y el nombre del dispositivo NVMe de un volumen que se adjuntó durante el lanzamiento de la instancia. Tenga en cuenta que el nombre del dispositivo NVMe no incluye el prefijo `/dev/`. El nombre del dispositivo está disponible a través de la extensión específica del proveedor del controlador NVMe (bytes 384:4095 de la identificación del controlador):

```
[ec2-user ~]$ sudo nvme id-ctrl -v /dev/nvme0n1
NVME Identify Controller:
vid     : 0x1d0f
ssvid   : 0x1d0f
sn      : vol01234567890abcdef
mn      : Amazon Elastic Block Store
...
0000: 2f 64 65 76 2f 73 64 6a 20 20 20 20 20 20 20 20 "sda..."
```

En el siguiente ejemplo se obtiene el ID de volumen y el nombre del dispositivo NVMe de un volumen que se adjuntó después del lanzamiento de la instancia. Tenga en cuenta que el nombre del dispositivo NVMe incluye el prefijo `/dev/`.

```
[ec2-user ~]$ sudo nvme id-ctrl -v /dev/nvme1n1
NVME Identify Controller:
vid     : 0x1d0f
ssvid   : 0x1d0f
sn      : volabcdef01234567890
mn      : Amazon Elastic Block Store
...
0000: 2f 64 65 76 2f 73 64 6a 20 20 20 20 20 20 20 20 "/dev/sdf..."
```

El comando lsblk muestra los dispositivos disponibles y sus puntos de montaje (cuando corresponda). Esto le ayuda a determinar el nombre de dispositivo correcto que debe usar. En este ejemplo, `/dev/nvme0n1p1` se monta en el dispositivo raíz y `/dev/nvme1n1` se adjunta pero no se monta.

```
[ec2-user ~]$ lsblk
NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme1n1       259:3   0  100G  0 disk
nvme0n1       259:0   0    8G  0 disk
  nvme0n1p1   259:1   0    8G  0 part /
```

```
nvme0n1p128 259:2   0    1M  0 part
```

instancias de Windows

También puede ejecutar el comando **ebsnvme-id** para asignar el número de disco del dispositivo NVMe a un ID de volumen EBS y a un nombre de dispositivo. De forma predeterminada, todos los dispositivos NVMe de EBS se enumeran. Puede pasar un número de disco para enumerar información de un dispositivo concreto. La `ebsnvme-id` herramienta se incluye en las últimas AMI de Windows Server AWS proporcionadas en. `C:\PROGRAMDATA\AMAZON\Tools`

A partir del paquete de controladores AWS NVMe, `1.5.0,` el paquete de controladores instala la última versión de la `ebsnvme-id` herramienta. La versión más reciente solo está disponible en el paquete de controladores. El enlace de descarga independiente de la herramienta `ebsnvme-id` ya no recibirá actualizaciones. La última versión disponible a través del enlace independiente es `1.1.0`, que puede descargar con el enlace ebsnvme-id.zip y extraer el contenido en su instancia de Amazon EC2 para obtener acceso a `ebsnvme-id.exe`.

```
PS C:\Users\Administrator\Desktop> ebsnvme-id.exe
Disk Number: 0
Volume ID: vol-0d6d7ee9f6e471a7f
Device Name: sda1

Disk Number: 1
Volume ID: vol-03a26248ff39b57cf
Device Name: xvdd

Disk Number: 2
Volume ID: vol-038bd1c629aa125e6
Device Name: xvde

Disk Number: 3
Volume ID: vol-034f9d29ec0b64c89
Device Name: xvdb

Disk Number: 4
Volume ID: vol-03e2dbe464b66f0a1
Device Name: xvdc
PS C:\Users\Administrator\Desktop> ebsnvme-id.exe 4
Disk Number: 4
Volume ID: vol-03e2dbe464b66f0a1
Device Name: xvdc
```

Utilizar volúmenes EBS de NVMe

Para formatear y montar un volumen de EBS de NVMe, consulte Cómo hacer que un volumen de Amazon EBS esté disponible para su uso.

instancias de Linux

Si utiliza el kernel de Linux 4.2 o posterior, todos los cambios que realiza en el tamaño de un volumen de EBS de NVMe se reflejan automáticamente en la instancia. Para los kernels de Linux anteriores, es posible que tenga que separar y adjuntar el volumen de EBS o reiniciar la instancia para que se refleje el cambio de tamaño. Con una versión del kernel de Linux 3.19 o posterior, puede utilizar el comando hdparm como se indica a continuación para forzar un nuevo análisis del dispositivo NVMe:

```
[ec2-user ~]$ sudo hdparm -z /dev/nvme1n1
```

Cuando se desconecta un volumen EBS de NVMe, las instancias no tienen la oportunidad de vaciar las cachés ni los metadatos del sistema de archivos antes de que se separe el volumen. Por tanto, antes de separar un volumen de EBS de NVMe, primero debe sincronizarlo y desmontarlo. Si el volumen no consigue desconectarse, puede intentar un comando `force-detach` como se describe en Cómo separar un volumen de Amazon EBS de una instancia.

instancias de Windows

Las AMI de AWS Windows más recientes contienen el controlador AWS NVMe que requieren los tipos de instancias que exponen los volúmenes de EBS como dispositivos de bloques de NVMe. No obstante, si cambia el tamaño del volumen raíz en un sistema Windows, debe volver a analizar el volumen para que este campo se refleje en la instancia. Si lanzaste la instancia desde una AMI diferente, es posible que no contenga el controlador AWS NVMe necesario. Si la instancia no tiene el controlador AWS NVMe más reciente, debe instalarlo. Para obtener más información, consulte controladores NVMe de AWS en instancias de Windows.

Tiempo de espera de las operaciones de E/S

La mayoría de los sistemas operativos especifican un tiempo de espera para las operaciones de E/S enviadas a los dispositivos NVMe.

instancias de Linux

En Linux, los volúmenes EBS conectados a instancias basadas en Nitro utilizan el controlador predeterminado de NVMe proporcionado por el sistema operativo. La mayoría de los sistemas operativos especifican un tiempo de espera para las operaciones de E/S enviadas a los dispositivos NVMe. El tiempo de espera predeterminado es 30 segundos y se puede cambiar mediante el parámetro de arranque `nvme_core.io_timeout`. En la mayoría de los kernels de Linux anteriores a la versión 4.6, este parámetro es `nvme.io_timeout`.

Si la latencia de E/S supera el valor de este parámetro de tiempo de espera, se produce un error de E/S en el controlador NVMe de Linux y se devuelve un error al sistema de archivos o a la aplicación. Según la operación de E/S, el sistema de archivos o aplicación puede recuperar el error. En algunos casos, el sistema de archivos puede volverse a montar como de solo lectura.

Para obtener una experiencia similar a los volúmenes de EBS asociados a instancias Xen, recomendamos establecer `nvme_core.io_timeout` en el máximo valor posible. Para los kernels actuales, el máximo es 4294967295, mientras que para los kernels anteriores el máximo es 255. En función de la versión de Linux, el tiempo de espera ya podría estar definido en el valor máximo admitido. Por ejemplo, el tiempo de espera se define en 4294967295 de forma predeterminada para la AMI de Amazon Linux 2017.09.01 y versiones posteriores.

Puede verificar el valor máximo de la distribución de Linux mediante la escritura de un valor superior al máximo sugerido en `/sys/module/nvme_core/parameters/io_timeout` y la comprobación del error Numerical result out of range cuando intente guardar el archivo.

instancias de Windows

En Windows, el tiempo de espera predeterminado es de 60 segundos y el máximo de 255 segundos. Se puede modificar el valor del registro de la clase de disco `TimeoutValue` mediante el procedimiento descrito en el artículo Registry Entries for SCSI Miniport Drivers.

Abort command

El comando `Abort` es un comando de administración de NVMe que se emite para anular un comando específico que se envió anteriormente al controlador. El controlador de dispositivos suele emitir este comando para los dispositivos de almacenamiento que han superado el límite de tiempo de espera de la operación de E/S. Los tipos de instancias de Amazon EC2 que admiten el comando `Abort` de forma predeterminada, anularán un comando específico que se envió anteriormente al controlador del dispositivo de Amazon EBS adjunto al que se emite un comando `Abort`.

Los siguientes tipos de instancias admiten el comando `Abort` para todos los volúmenes de Amazon EBS adjuntos de forma predeterminada: `R5b`, `R6i`, `M6i`, `M6a`, `C6gn`, `C6i`, `X2gd`, `X2iezn`, `Im4gn`, `Is4gen`.

Otros tipos de instancias no realizan ninguna acción cuando se emiten los comandos `Abort` para los volúmenes de Amazon EBS adjuntos.

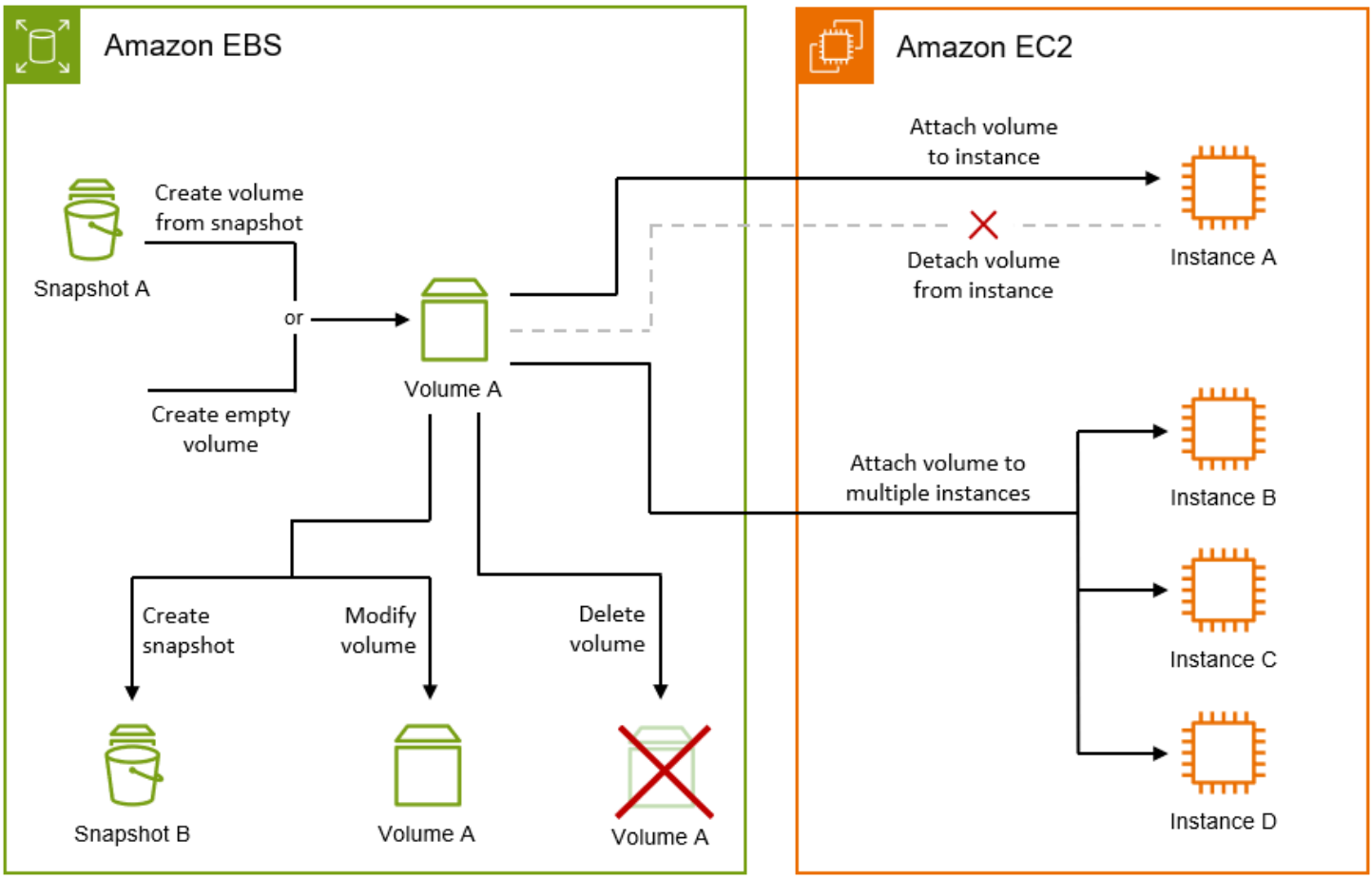
Los dispositivos de Amazon EBS con la versión del dispositivo NVMe `1.4` o una superior admiten el comando `Abort`.

Para obtener más información, consulte la sección 5.1 Abort command (5.1 Abortar comando) de la NVM Express Base Specification (Especificación de base de NVM Express).

Ciclo de vida del volumen de Amazon EBS

El ciclo de vida de un volumen de Amazon EBS comienza con el proceso de creación. Puede crear un volumen a partir de una instantánea de Amazon EBS o puede crear un volumen vacío. Antes de poder usar el volumen, debe asociarlo a una o más instancias de Amazon EC2 que se encuentren en la misma zona de disponibilidad que el volumen. También puede asociar varios volúmenes a una instancia. Si es necesario, también puede separar un volumen de una instancia y asociarlo a otra. Si sus requisitos de almacenamiento cambian, puede modificar el tamaño o el rendimiento del volumen en cualquier momento. Puede crear point-in-time copias de seguridad de sus volúmenes mediante la creación de instantáneas de Amazon EBS. Si ya no necesita un volumen, puede eliminarlo para que deje de incurrir en costes de almacenamiento relacionados.

La siguiente imagen muestra las acciones que puede realizar en los volúmenes como parte de su ciclo de vida.



También hay tareas para las que debe conectarse a la instancia y ejecutar un comando del sistema operativo. Por ejemplo, formatear el volumen, montarlo, administrar las particiones y ver el espacio libre en disco.

Tareas

- Creación de un volumen de Amazon EBS.
- Adjunte un volumen de Amazon EBS a una instancia.
- Asociar un volumen a varias instancias con Amazon EBS Multi-Attach
- Cómo hacer que un volumen de Amazon EBS esté disponible para su uso
- Visualización de información acerca de un volumen de Amazon EBS
- Modificación de un volumen mediante Volúmenes elásticos de Amazon EBS
- Cómo separar un volumen de Amazon EBS de una instancia
- Eliminar un volumen Amazon EBS

Creación de un volumen de Amazon EBS.

Puede crear un volumen de Amazon EBS y, a continuación, adjuntarlo a cualquier instancia de EC2 en la misma zona de disponibilidad. Si crea un volumen de EBS cifrado, solo puede adjuntarlo a los tipos de instancia admitidos. Para obtener más información, consulte Tipos de instancias admitidas.

Si va a crear un volumen para un escenario de almacenamiento de alto rendimiento, debe asegurarse de utilizar un volumen de SSD de IOPS provisionadas (`io1` o `io2`) y adjuntarlo a una instancia que disponga de ancho de banda suficiente para admitir la aplicación, como, por ejemplo, una instancia optimizada para EBS. El mismo consejo es aplicable a los volúmenes de HDD con rendimiento optimizado (`st1`) y de HDD en frío (`sc1`).

> **Note**
>
> Si crea un volumen para utilizarlo con una instancia de Windows y es mayor que 2048 GiB (o es un volumen menor que 2048 GiB pero es posible que aumentase más tarde), asegúrese de configurar el volumen para utilizar tablas de particiones GPT. Para obtener más información, consulte Compatibilidad con Windows para discos duros de más de 2 TB..

Los volúmenes de EBS nuevos disponen de su máximo rendimiento en cuanto están disponibles y no es necesario inicializarlos (proceso que antes se denominaba precalentamiento). No obstante, debe inicializar los bloques de almacenamiento en los volúmenes creados a partir de instantáneas (extraídas de Amazon S3 y grabadas en el volumen) para poder obtener acceso al bloque. Esta acción preliminar lleva tiempo y puede provocar un aumento considerable de la latencia de una operación de E/S la primera vez que se obtiene acceso a cada bloque. El rendimiento del volumen se alcanza después de descargar todos los bloques y de escribirlos en el volumen. Para la mayoría de las aplicaciones, la amortización de este costo a lo largo de la vida útil del volumen es aceptable. Para evitar este impacto inicial en el rendimiento en un entorno de producción, puede forzar la inicialización inmediata de todo el volumen o habilitar la restauración rápida de instantáneas. Para obtener más información, consulte Inicializar de volúmenes de Amazon EBS.

Métodos de creación de un volumen

- Cree y asocie volúmenes de EBS al lanzar instancias especificando una asignación de dispositivos de bloques. Para obtener más información, consulte Cómo iniciar una instancia con el nuevo asistente de inicialización de instancias y asignación de dispositivos de bloques.

- Puede crear un volumen de EBS vacío y asociarlo a una instancia en ejecución. Para obtener más información, consulte Crear un volumen vacío más abajo.
- Cree un volumen de EBS a partir de una instantánea creada anteriormente y asócielo a una instancia en ejecución. Para obtener más información, consulte Creación de un volumen desde una instantánea más abajo.

Temas

Crear un volumen vacío

Los volúmenes vacíos reciben su máximo rendimiento en el momento en que están disponibles y no requieren inicialización.

Puede crear un volumen de EBS vacío utilizando alguno de los métodos siguientes.

Console

Para crear un volumen de EBS vacío con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Volumes (Volúmenes).
3. Seleccione Create volume (Crear volumen).
4. En Volume type (Tipo de volumen), elija el tipo de volumen que desea crear. Para obtener más información, consulte Tipos de volúmenes de Amazon EBS.

   El volumen SSD de uso general `gp3` es la opción predeterminada.
5. En Tamaño, ingrese el tamaño del volumen en GiB. Para obtener más información, consulte Restricciones de tamaño y configuración de un volumen de EBS.
6. (Solo para `io1`, `io2` y `gp3`) En IOPS, ingrese el número máximo de operaciones de entrada/salida por segundo (IOPS) que debe proporcionar el volumen.
7. (Solo `gp3`) En Throughput (Rendimiento), ingrese el rendimiento que debe proporcionar el volumen, en MiB/s.

8. En Availability Zone (Zona de disponibilidad), seleccione la zona de disponibilidad en la que desea crear el volumen. Un volumen solo se puede adjuntar a una instancia que se encuentre en la misma zona de disponibilidad.
9. En Snapshot ID (ID de instantánea), conserve el valor predeterminado (Don't create volume from a snapshot [No crear volumen desde una instantánea]).
10. (Solo `io1` e `io2`) A fin de habilitar el volumen para Amazon EBS Multi-Attach, seleccione Enable Multi-Attach (Habilitar Multi-Attach). Para obtener más información, consulte Asociar un volumen a varias instancias con Amazon EBS Multi-Attach.
11. Configure el estado de cifrado del volumen.

    Si la cuenta está habilitada para el cifrado de forma predeterminada, el cifrado se habilita automáticamente y no puede desactivarlo. Puede elegir la clave de KMS que se utilizará para cifrar el volumen.

    Si la cuenta no está habilitada para el cifrado de forma predeterminada, el cifrado es opcional. Para cifrar el volumen, en Encryption (Cifrado), elija Encrypt this volume (Cifrar este volumen) y, a continuación, seleccione la clave de KMS que se utilizará para cifrar el volumen.

    > **Note**
    >
    > Los volúmenes cifrados solo se pueden adjuntar a instancias que admitan el cifrado de Amazon EBS. Para obtener más información, consulte Cifrado de Amazon EBS.

12. (Opcional) Para asignar etiquetas personalizadas al volumen, en la sección Etiquetas, elija Agregar etiqueta y, a continuación, ingrese un par de clave y valor de la etiqueta.
13. Seleccione Create volume (Crear volumen).

    > **Note**
    >
    > El volumen está listo para su uso cuando Volume state (Estado de volumen) está available (disponible).

14. Para utilizar el volumen, adjúntelo a una instancia. Para obtener más información, consulte Adjunte un volumen de Amazon EBS a una instancia..

AWS CLI

Para crear un volumen de EBS vacío mediante el AWS CLI

Utilice el comando create-volume.

El volumen está listo para utilizar cuando `state` es `available`.

Tools for Windows PowerShell

Para crear un volumen de EBS vacío mediante las herramientas de Windows PowerShell

Utilice el comando New-EC2Volume.

El volumen está listo para utilizar cuando `state` es `available`.

Creación de un volumen desde una instantánea

Los volúmenes creados a partir de instantáneas se cargan lentamente en segundo plano. Esto significa que no es necesario esperar a que todos los datos se transfieran desde Amazon S3 hasta el volumen de EBS antes de que la instancia pueda comenzar a acceder a un volumen adjunto y a todos sus datos. Si la instancia obtiene acceso a datos que aún no se han cargado, el volumen descarga inmediatamente los datos solicitados de Amazon S3 y, a continuación, continúa cargando el resto de los datos del volumen en segundo plano. El rendimiento del volumen se alcanza después de descargar todos los bloques y de escribirlos en el volumen. Para evitar el impacto inicial en el rendimiento en un entorno de producción, consulte Inicializar de volúmenes de Amazon EBS.

Los nuevos volúmenes EBS que se crean a partir de instantáneas cifradas se cifran automáticamente. También puede cifrar un volumen on-the-fly mientras lo restaura a partir de una instantánea no cifrada. Los volúmenes cifrados solo pueden asociarse a los tipos de instancias que admiten el cifrado de EBS. Para obtener más información, consulte Tipos de instancias admitidas.

Puede crear un volumen a partir de una instantánea utilizando alguno de los métodos siguientes.

Console

Para crear un volumen de EBS a partir de una instantánea con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Volumes (Volúmenes).

3. Seleccione Create volume (Crear volumen).
4. En Volume type (Tipo de volumen), elija el tipo de volumen que desea crear. Para obtener más información, consulte Tipos de volúmenes de Amazon EBS.

   El volumen SSD de uso general `gp3` es la opción predeterminada.
5. En Tamaño, ingrese el tamaño del volumen en GiB. Para obtener más información, consulte Restricciones de tamaño y configuración de un volumen de EBS.
6. (Solo para `io1`, `io2` y `gp3`) En IOPS, ingrese el número máximo de operaciones de entrada/salida por segundo (IOPS) que debe proporcionar el volumen.
7. (Solo `gp3`) En Throughput (Rendimiento), ingrese el rendimiento que debe proporcionar el volumen, en MiB/s.
8. En Availability Zone (Zona de disponibilidad), seleccione la zona de disponibilidad en la que desea crear el volumen. Un volumen solo se puede adjuntar a instancias que se encuentren en la misma zona de disponibilidad.
9. Para Snapshot ID (ID de instantánea), seleccione la instantánea desde la que desea crear el volumen.
10. Configure el estado de cifrado del volumen.

    Si la instantánea seleccionada está cifrada o si la cuenta está habilitada para el cifrado de forma predeterminada, el cifrado se habilita automáticamente y no puede desactivarlo. Puede elegir la clave de KMS que se utilizará para cifrar el volumen.

    Si la instantánea seleccionada no está cifrada y la cuenta no está habilitada para el cifrado de forma predeterminada, el cifrado es opcional. Para cifrar el volumen, en Encryption (Cifrado), elija Encrypt this volume (Cifrar este volumen) y, a continuación, seleccione la clave de KMS que se utilizará para cifrar el volumen.

    > **Note**
    >
    > Los volúmenes cifrados solo se pueden adjuntar a instancias que admitan el cifrado de Amazon EBS. Para obtener más información, consulte Cifrado de Amazon EBS.
11. (Opcional) Para asignar etiquetas personalizadas al volumen, en la sección Etiquetas, elija Agregar etiqueta y, a continuación, ingrese un par de clave y valor de la etiqueta.
12. Elija Create volume (Crear volumen).

> **Note**
>
> El volumen está listo para su uso cuando Volume state (Estado de volumen) está available (disponible).

13. Para utilizar el volumen, adjúntelo a una instancia. Para obtener más información, consulte Adjunte un volumen de Amazon EBS a una instancia..

AWS CLI

Para crear un volumen de EBS a partir de una instantánea mediante el AWS CLI

Utilice el comando create-volume.

El volumen está listo para utilizar cuando `state` es `available`.

Tools for Windows PowerShell

Para crear un volumen de EBS a partir de una instantánea mediante las herramientas de Windows PowerShell

Utilice el comando New-EC2Volume.

El volumen está listo para utilizar cuando `state` es `available`.

Adjunte un volumen de Amazon EBS a una instancia.

Puede asociar un volumen de EBS disponible a una de las instancias que se encuentre en la misma zona de disponibilidad que el volumen.

Para obtener información sobre cómo agregar volúmenes de EBS a la instancia en el inicio, consulte Asignación de dispositivos de bloques de instancias.

Consideraciones

- Determine cuántos volúmenes puede adjuntar a una instancia. La cantidad máxima de volúmenes de Amazon EBS que puede adjuntar a una instancia depende del tipo y tamaño de la instancia. Para obtener más información, consulte Límites de volumen de instancia.
- Determine si puede adjuntar el volumen a varias instancias y habilitar Multi-Attach. Para obtener más información, consulte Asociar un volumen a varias instancias con Amazon EBS Multi-Attach.

- Si un volumen está cifrado, solo puede adjuntarse a una instancia que admita el cifrado de Amazon EBS. Para obtener más información, consulte Tipos de instancias admitidas.
- Si un volumen tiene un código de AWS Marketplace producto:
  - El volumen solo puede adjuntarse a una instancia detenida.
  - Debe estar suscrito al AWS Marketplace código que figura en el volumen.
  - La configuración de la instancia, como su tipo y sistema operativo, debe ser compatible con ese AWS Marketplace código específico. Por ejemplo, no puede tomar un volumen de una instancia de Windows y adjuntarlo a una instancia de Linux.
  - AWS Marketplace los códigos de producto se copian del volumen a la instancia.

Puede adjuntar un volumen a una instancia mediante alguno de los métodos siguientes.

Console

Para adjuntar un volumen de EBS a una instancia con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Volumes (Volúmenes).
3. Seleccione el volumen que desea adjuntar y elija Actions (Acciones), Attach Volume (Adjuntar volumen).

   > **Note**
   >
   > Puede adjuntar solo los volúmenes que se encuentran en el estado `Available`.

4. En Instance (Instancia), ingrese el ID de la instancia o selecciónela de la lista de opciones.

   > **Note**
   >
   > - El volumen debe estar adjunto a una instancia en la misma zona de disponibilidad.
   > - Si un volumen está cifrado, solo puede adjuntarse a tipos de instancia que admitan el cifrado de Amazon EBS. Para obtener más información, consulte Cifrado de Amazon EBS.

5. Para el nombre del dispositivo, realice una de las siguientes acciones:

- Para un volumen raíz, seleccione el nombre de dispositivo necesario en la sección Reservado para el volumen raíz de la lista. Normalmente, `/dev/sda1` o `/dev/xvda` para instancias de Linux, según la AMI, o `/dev/sda1` para instancias de Windows.
- Para los volúmenes de datos, seleccione un nombre de dispositivo disponible en la sección Recomendado para volúmenes de datos de la lista.
- Para usar un nombre de dispositivo personalizado, seleccione Especificar un nombre de dispositivo personalizado y, a continuación, introduzca el nombre del dispositivo que se va a usar.

Amazon EC2 utiliza este nombre del dispositivo. El controlador del dispositivo de bloques de la instancia puede asignar un nombre de dispositivo diferente al montar el volumen. Para obtener más información, consulta los nombres de los dispositivos en las instancias de Linux o los nombres de los dispositivos en las instancias de Windows.

6. Elija Attach volume (Asociar volumen).
7. Conéctese a la instancia y monte el volumen. Para obtener más información, consulte Cómo hacer que un volumen de Amazon EBS esté disponible para su uso.

AWS CLI

Para adjuntar un volumen de EBS a una instancia mediante el AWS CLI

Utilice el comando attach-volume.

Tools for Windows PowerShell

Para adjuntar un volumen de EBS a una instancia mediante las Herramientas de Windows PowerShell

Utilice el comando Add-EC2Volume.

> **Note**
>
> - Si intenta adjuntar una cantidad de volúmenes que supere el límite de volumen del tipo de instancia, se producirá un error en la solicitud. Para obtener más información, consulte Límites de volumen de instancia.

- En algunas situaciones, puede suceder que un volumen que no es el volumen adjunto a `/dev/xvda` o `/dev/sda` se ha convertido en el volumen raíz de la instancia. Esto puede suceder cuando se ha adjuntado el volumen raíz de otra instancia o un volumen creado a partir de una instantánea de un volumen raíz, a una instancia que ya tiene un volumen raíz. Para obtener más información, consulte Arranque desde un volumen incorrecto.

Asociar un volumen a varias instancias con Amazon EBS Multi-Attach

Amazon EBS Multi-Attach le permite adjuntar un único volumen de SSD de IOPS provisionadas (`io1` o `io2`) a varias instancias que se encuentren en la misma zona de disponibilidad. Puede asociar varios volúmenes habilitados para Multi-Attach a una instancia o a un conjunto de instancias. Cada instancia a la que se asocia el volumen tiene permiso completo de lectura y escritura en el volumen compartido. Multi-Attach le permite conseguir una mayor disponibilidad de las aplicaciones que administran operaciones de escritura simultáneas.

Contenido

Condiciones y limitaciones

- Los volúmenes habilitados para Multi-Attach se pueden asociar a un máximo de 16 instancias creadas en Nitro System que se encuentran en la misma zona de disponibilidad.
- Las instancias de Linux admiten volúmenes habilitados `io1` y `io2` de Multi-Attach. Las instancias de Windows solo admiten volúmenes habilitados `io2` de Multi-Attach.
- La cantidad máxima de volúmenes de Amazon EBS que puede adjuntar a una instancia depende del tipo y tamaño de la instancia. Para obtener más información, consulte Límites de volumen de instancia.
- Multi-Attach es compatible exclusivamente en volúmenes de SSD de IOPS aprovisionadas (`io1` y `io2`).

- La asociación múltiple para volúmenes `io1` solo está disponible en las siguientes regiones: Este de EE. UU. (Norte de Virginia), Oeste de EE. UU. (Oregón) y Asia-Pacífico (Seúl).

  La asociación múltiple para `io2` está disponible en todas las regiones que admiten `io2`.

  > **Note**
  >
  > Para obtener un rendimiento, una coherencia y una durabilidad mejores a un costo menor, le recomendamos que utilice volúmenes `io2`.

- Los volúmenes `io1` con la asociación múltiple habilitada no son compatibles con las instancias basadas en Nitro System que solo admiten el protocolo de red Scalable Reliable Datagram (SRD). Para utilizar la asociación múltiple con estos tipos de instancias, debe utilizar volúmenes `io2` Block Express.
- Los sistemas de archivos estándar, como XFS y EXT4, no están diseñados para obtener acceso simultáneamente por varios servidores como, por ejemplo, instancias EC2. Puede utilizar un sistema de archivos agrupados en clústeres para garantizar la resiliencia y la fiabilidad de los datos para las cargas de trabajo de producción.
- Los volúmenes `io2` habilitados para Multi-Attach son compatibles con el aislamiento de E/S. Los protocolos de aislamiento de E/S controlan el acceso de escritura en un entorno de almacenamiento compartido para mantener la coherencia de los datos. Las aplicaciones deben proporcionar un orden de escritura para las instancias asociadas a fin de mantener la coherencia de los datos. Para obtener más información, consulte Reservas de NVMe.

  Los volúmenes `io1` habilitados para Multi-Attach no son compatibles con el aislamiento de E/S.
- Los volúmenes habilitados para Multi-Attach no se pueden crear como volúmenes de arranque.
- Los volúmenes habilitados para Multi-Attach se pueden conectar a un mapeo de dispositivo de bloque por instancia.
- La conexión múltiple no se puede habilitar durante el lanzamiento de la instancia mediante la consola RunInstances o la API de Amazon EC2.
- Los volúmenes habilitados para Multi-Attach que tienen un problema en la capa de infraestructura de Amazon EBS no están disponibles para todas las instancias asociadas. Es posible que los problemas en la capa de red o de Amazon EC2 solo afecten a algunas instancias asociadas.
- En la tabla siguiente, se muestra la compatibilidad de la modificación de volúmenes para los volúmenes `io1` e `io2` habilitados para Multi-Attach después de la creación.

	io2 Volúmenes de	**io1**Volúmenes de
Modificar tipo de volumen	✗	✗
Modificar tamaño de volumen	✓	✗
Modificar las IOPS provisionadas	✓	✗
Habilitar Multi-Attach	✓ *	✗
Deshabilitar Multi-Attach	✓ *	✗

* No puede habilitar o deshabilitar Multi-Attach mientras el volumen está asociado a una instancia.

Rendimiento

Cada instancia asociada puede ampliar su rendimiento de IOPS máximo hasta el rendimiento máximo aprovisionado del volumen. Sin embargo, el rendimiento acumulado de todas las instancias asociadas no puede ser superior el rendimiento máximo aprovisionado del volumen. Si la demanda de IOPS de las instancias asociadas es mayor que las IOPS provisionadas del volumen, el volumen no superará su rendimiento aprovisionado.

Digamos, por ejemplo, que crea un volumen `io2` habilitado para Multi-Attach con `80,000` IOPS aprovisionadas y lo asocia a una instancia `m7g.large` que soporta hasta `40,000` IOPS, y una instancia `r7g.12xlarge` que soporta hasta `60,000` IOPS. Cada instancia puede ampliar su IOPS máxima, ya que es menor que las IOPS aprovisionadas del volumen de `80,000`. Sin embargo, si ambas instancias aumentan su E/S en el volumen simultáneamente, sus IOPS combinadas no pueden exceder el rendimiento aprovisionado del volumen de IOPS `80,000`.

Para lograr un rendimiento constante, se recomienda equilibrar la E/S obtenida de las instancias asociadas en todos los sectores de un volumen habilitado para Multi-Attach.

Trabajar con Multi-Attach

Los volúmenes habilitados para Multi-Attach se pueden administrar prácticamente del mismo modo que administraría cualquier otro volumen de Amazon EBS. Sin embargo, para utilizar la funcionalidad Multi-Attach, debe habilitarla para el volumen. Cuando se crea un nuevo volumen, Multi-Attach está deshabilitado de forma predeterminada.

Contenido

Habilitar Multi-Attach

Puede habilitar Multi-Attach durante la creación de volúmenes. Utilice alguno de los métodos siguientes.

Console

Para habilitar Multi-Attach durante la creación de un volumen

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Volumes (Volúmenes).
3. Seleccione Create volume (Crear volumen).
4. En Tipo de volumen, elija SSD de IOPS aprovisionadas (**`io1`**) o SSD de IOPS aprovisionadas (**`io2`**).
5. En Size (Tamaño) e IOPS, elija el tamaño de volumen requerido y el número de IOPS que desea aprovisionar.
6. En Availability Zone (Zona de disponibilidad), elija la misma Zona de disponibilidad en la que se encuentran las instancias.
7. En Amazon EBS Multi-Attach, elija Enable Multi-Attach (Habilitar Multi-Attach).

8. (Opcional) En Snapshot ID (ID de instantánea), elija la instantánea desde la que desea crear el volumen.
9. Configure el estado de cifrado del volumen.

   Si la instantánea seleccionada está cifrada o si la cuenta está habilitada para el cifrado de forma predeterminada, el cifrado se habilita automáticamente y no puede desactivarlo. Puede elegir la clave de KMS que se utilizará para cifrar el volumen.

   Si la instantánea seleccionada no está cifrada y la cuenta no está habilitada para el cifrado de forma predeterminada, el cifrado es opcional. Para cifrar el volumen, en Encryption (Cifrado), elija Encrypt this volume (Cifrar este volumen) y, a continuación, seleccione la clave de KMS que se utilizará para cifrar el volumen.

   > **Note**
   >
   > Solo puede adjuntar volúmenes cifrados a instancias que admitan el cifrado de Amazon EBS. Para obtener más información, consulte Cifrado de Amazon EBS.

10. (Opcional) Para asignar etiquetas personalizadas al volumen, en la sección Etiquetas, elija Agregar etiqueta y, a continuación, ingrese un par de clave y valor de la etiqueta.
11. Seleccione Create volume (Crear volumen).

Command line

Para habilitar Multi-Attach durante la creación de un volumen

Utilice el comando create-volume y especifique el parámetro `--multi-attach-enabled`.

```
$ C:\> aws ec2 create-volume --volume-type io2 --multi-attach-enabled --size 100 --
iops 2000 --region us-west-2 --availability-zone us-west-2b
```

También puede habilitar Multi-Attach para volúmenes `io2` una vez creados, solo si no están asociados a ninguna instancia.

> **Note**
>
> No puede habilitar Multi-Attach para `io1` volúmenes después de su creación.

Utilice uno de los siguientes métodos para habilitar Multi-Attach para un volumen `io2` después de su creación.

Console

Para habilitar Multi-Attach después de la creación

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Volumes (Volúmenes).
3. Seleccione el volumen y elija Actions (Acciones), Modify volume (Modificar volumen).
4. En Amazon EBS Multi-Attach, elija Enable Multi-Attach (Habilitar Multi-Attach).
5. Elija Modify.

Command line

Para habilitar Multi-Attach después de la creación

Utilice el comando Modificar volumen y especifique el parámetro `--multi-attach-enabled`.

```
$ C:\> aws ec2 modify-volume --volume-id vol-1234567890abcdef0 --multi-attach-
enabled
```

Deshabilitar Multi-Attach

Puede deshabilitar Multi-Attach para un volumen `io2` solo si está conectado a no más de una instancia.

> **Note**
>
> No puede deshabilitar Multi-Attach para volúmenes `io1` después de la creación.

Utilice uno de los métodos siguientes para deshabilitar Multi-Attach para un volumen `io2`.

Console

Para deshabilitar Multi-Attach después de la creación

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.

2. En el panel de navegación, elija Volumes (Volúmenes).
3. Seleccione el volumen y elija Actions (Acciones), Modify volume (Modificar volumen).
4. En Amazon EBS Multi-Attach, cancele la selección de Enable Multi-Attach (Habilitar Multi-Attach).
5. Elija Modify.

Command line

Para deshabilitar Multi-Attach después de la creación

Utilice el comando Modificar volumen y especifique el parámetro `-no-multi-attach-enabled`.

```
$ C:\> aws ec2 modify-volume --volume-id vol-1234567890abcdef0 --no-multi-attach-enabled
```

Asociar un volumen a instancias

Un volumen habilitado para Multi-Attach se asocia a una instancia de la misma forma que asocia cualquier otro volumen de EBS. Para obtener más información, consulte Adjunte un volumen de Amazon EBS a una instancia..

Eliminar al terminar

Los volúmenes habilitados para Multi-Attach se eliminan al terminar si se termina la última instancia asociada y si esa instancia está configurada para eliminar el volumen al terminar. Si el volumen está asociado a varias instancias que tienen diferentes configuraciones de eliminación al terminar en sus asignaciones de dispositivos de bloque de volumen, la configuración de asignación de dispositivos de bloque de la última instancia asociada determina el comportamiento de eliminación al terminar.

Para garantizar el comportamiento previsto de eliminar al terminar, habilite o deshabilite la opción de eliminar al terminar para todas las instancias a las que está asociado el volumen.

De forma predeterminada, cuando se asocia un volumen a una instancia, la configuración de eliminación al terminar para la asignación de dispositivos de bloque se establece en false. Si desea activar la eliminación al terminar para un volumen habilitado para Multi-Attach, modifique la asignación de dispositivos de bloque.

Si desea que el volumen se elimine al terminar las instancias asociadas, habilite la eliminación al terminar en la asignación de dispositivos de bloque para todas las instancias asociadas. Si desea conservar el volumen una vez terminadas las instancias asociadas, deshabilite la eliminación al terminar en la asignación de dispositivos de bloque para todas las instancias asociadas. Para obtener más información, consulte Conservación de los datos cuando se termina una instancia.

Puede modificar la configuración de eliminación al terminar en el momento de lanzar la instancia o una vez que se ha lanzado. Si habilita o deshabilita la eliminación al terminar durante el lanzamiento de la instancia, la configuración solo se aplica a los volúmenes que se asocian durante el lanzamiento. Si asocia un volumen a una instancia una vez lanzada, debe establecer explícitamente el comportamiento de eliminación al terminar para ese volumen.

Solo puede modificar la configuración de eliminación al terminar de la instancia mediante las herramientas de línea de comandos.

Para modificar la configuración de eliminación al terminar para una instancia existente

Utilice el comando modify-instance-attribute y especifique el atributo `DeleteOnTermination` en la `--block-device-mappings option`.

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --block-device-mappings file://mapping.json
```

En `mapping.json`, especifique lo siguiente.

```
[
  {
    "DeviceName": "/dev/sdf",
    "Ebs": {
      "DeleteOnTermination": true|false
    }
  }
]
```

Supervisar un volumen habilitado para Multi-Attach

Puede monitorizar un volumen con conexión múltiple mediante CloudWatch las métricas de los volúmenes de Amazon EBS. Para obtener más información, consulte CloudWatch Métricas de Amazon para Amazon EBS.

Se agregan los datos de todas las instancias asociadas. No se pueden monitorear las métricas de instancias asociadas individuales.

Precios y facturación

El uso de Amazon EBS Multi-Attach no tiene costos adicionales. Se le cobrarán los cargos estándar que se aplican a los volúmenes de SSD de IOPS provisionadas (`io1` e `io2`). Para obtener más información, consulte Precios Amazon EBS.

Reservas de NVMe

Los volúmenes `io2` habilitados para Multi-Attach admiten reservas de NVMe, que son un conjunto de protocolos de protección de almacenamiento estándar del sector. Estos protocolos le permiten crear y gestionar reservas que controlan y coordinan el acceso desde varias instancias a un volumen compartido. Las aplicaciones de almacenamiento compartido utilizan las reservas para garantizar la coherencia de datos.

Temas

- Requisitos
- Habilitación de la compatibilidad con las reservas de NVMe
- Comandos de reserva NVMe compatibles
- Precios

Requisitos

Las reservas de NVMe solo son compatibles con volúmenes `io2` habilitados para Multi-Attach. Los volúmenes habilitados para Multi-Attach se pueden asociar unicamente a instancias creadas en Nitro System.

Las reservas de NVMe son compatibles con los siguientes sistemas operativos:

- SUSE Linux Enterprise 12 SP3 y versiones posteriores
- RHEL 8.3 y versiones posteriores
- Amazon Linux 2 y versiones posteriores
- Windows Server 2016 y versiones posteriores

> **Note**
>
> En el caso de las AMI de Windows Server compatibles con fecha del 13 de septiembre de 2023 y versiones posteriores, se incluyen los controladores NVMe necesarios. Para las AMI anteriores, debe actualizar a la versión 1.5.0 o posterior del controlador NVMe. Para obtener más información, consulte controladores NVMe de AWS en instancias de Windows.

Si utiliza EC2launch v2 para iniciar los discos, debe actualizarlos a la versión 2.0.1521 o posterior. Para obtener más información, consulte Configuración de una instancia de Windows con EC2Launch v2.

Habilitación de la compatibilidad con las reservas de NVMe

La compatibilidad con las reservas de NVMe está habilitada de forma predeterminada para todos los volúmenes `io2` habilitados para Multi-Attach creados después del 18 de septiembre de 2023.

Para habilitar la compatibilidad con las reservas de NVMe para los volúmenes `io2` existentes creados antes del 18 de septiembre de 2023, debe separar todas las instancias del volumen y, a continuación, volver a conectar las instancias necesarias. Todos los adjuntos que se realicen después de separar todas las instancias tendrán habilitadas las reservas de NVMe.

Comandos de reserva NVMe compatibles

Amazon EBS es compatible con los siguientes comandos de reserva de NVMe:

Registro de reservas

Registra, anula o reemplaza una clave de reserva. Se utiliza una clave de registro para identificar y autenticar una instancia. El registro de una clave de reserva con un volumen crea una asociación entre la instancia y el volumen. Debe registrar la instancia con el volumen antes de que esa instancia pueda adquirir una reserva.

Adquirir una reserva

Adquiere una reserva de un volumen, anula una reserva de un espacio de nombres y anula una reserva de un volumen. Se pueden adquirir los siguientes tipos de reservas:

- Reserva de escritura exclusiva
- Reserva de acceso exclusivo
- Reserva de escritura exclusiva: solo para inscritos

- Reserva de acceso exclusivo:solo para inscritos
- Reserva de escritura exclusiva: todos los inscritos
- Reserva de acceso exclusivo: todos los inscritos

Liberación de reserva

Libera o anula una reserva mantenida en un volumen.

Informe de reservas

Describe el estado de registro y reserva de un volumen.

Precios

El uso y la habilitación de Multi-Attach no tiene costos adicionales.

Cómo hacer que un volumen de Amazon EBS esté disponible para su uso

Tras asociar un volumen Amazon EBS a la instancia, queda expuesto como dispositivo de bloques. Puede formatear el volumen con cualquier sistema de archivos y, a continuación, montarlo. Tras hacer que el volumen de EBS esté disponible para su uso, puede obtener acceso a él del mismo modo que obtiene acceso a cualquier otro volumen. Cualquier dato grabado en este sistema de archivos se graba en el volumen de EBS y es transparente a las aplicaciones que utilizan este dispositivo.

Puede tomar instantáneas del volumen de EBS con fines de backup o para usarlos como referencia a la hora de crear otro volumen. Para obtener más información, consulte Instantáneas de Amazon EBS.

Si el volumen de EBS que se está preparando para el uso tiene más de 2 TiB, se debe utilizar un esquema de particiones GPT para acceder a todo el volumen. Para obtener más información, consulte Restricciones de tamaño y configuración de un volumen de EBS.

instancias de Linux

Dar formato y montar un volumen asociado

Suponga que tiene una instancia EC2 con un volumen EBS para dispositivo raíz, `/dev/xvda` y que acaba de asociar un volumen EBS vacío a la instancia utilizando `/dev/sdf`. Utilice el procedimiento siguiente para hacer que el volumen recién asociado esté disponible para utilizar.

Para dar formato y montar un volumen de EBS en Linux

1. Conéctese a la instancia mediante SSH. Para obtener más información, consulte Conexión con la instancia de Linux.
2. El dispositivo podría estar asociado a la instancia con un nombre distinto al que especificó en el mapeo de dispositivos de bloques. Para obtener más información, consulte nombres de dispositivos en instancias de Linux. Utilice el comando lsblk para ver los dispositivos de disco disponibles y sus puntos de montaje (si procede) para ayudarle a determinar el nombre de dispositivo correcto que debe emplear. El resultado de lsblk elimina el prefijo `/dev/` de las rutas completas del dispositivo.

   A continuación se muestra un ejemplo de resultado para una instancia creada en Nitro System que expone los volúmenes de EBS como dispositivos de bloques NVMe. El dispositivo raíz es `/dev/nvme0n1`, que tiene dos particiones denominadas `nvme0n1p1` y `nvme0n1p128`. El volumen adjunto es `/dev/nvme1n1`, que no tiene particiones ni se ha montado aún.

   ```
   [ec2-user ~]$ lsblk
   NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
   nvme1n1       259:0    0  10G  0 disk
   nvme0n1       259:1    0   8G  0 disk
   -nvme0n1p1    259:2    0   8G  0 part /
   -nvme0n1p128  259:3    0   1M  0 part
   ```

   El siguiente es un resultado de ejemplo para una instancia T2. El dispositivo raíz es `/dev/xvda`, que tiene una partición denominada `xvda1`. El volumen adjunto es `/dev/xvdf`, que no tiene particiones ni se ha montado aún.

   ```
   [ec2-user ~]$ lsblk
   NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
   xvda    202:0    0    8G  0 disk
   -xvda1  202:1    0    8G  0 part /
   xvdf    202:80   0   10G  0 disk
   ```
3. Determine si se hay un sistema de archivos en el volumen. Los volúmenes nuevos son dispositivos de bloques sin procesar, por lo que debe crear un sistema de archivos en ellos para poder montarlos y utilizarlos. Los volúmenes que se crearon a partir de instantáneas suelen contar ya con un sistema de archivos; si crea un nuevo sistema de archivos sobre uno existente, se sobrescribirán los datos.

Utilice uno o ambos de los métodos siguientes para determinar si hay un sistema de archivos en el volumen:

- Utilice el comando file -s para obtener información sobre un dispositivo específico como, por ejemplo, su tipo de sistema de archivos. Si el resultado solo muestra `data`, como en el siguiente ejemplo, no hay ningún sistema de archivos en el dispositivo

```
[ec2-user ~]$ sudo file -s /dev/xvdf
/dev/xvdf: data
```

  Si el dispositivo tiene un sistema de archivos, el comando muestra información acerca del tipo de sistema de archivos. Por ejemplo, el resultado siguiente muestra un dispositivo raíz con el sistema de archivos XFS.

```
[ec2-user ~]$ sudo file -s /dev/xvda1
/dev/xvda1: SGI XFS filesystem data (blksz 4096, inosz 512, v2 dirs)
```

- Utilice el comando lsblk -f para obtener información sobre todos los dispositivos asociados a la instancia.

```
[ec2-user ~]$ sudo lsblk -f
```

  Por ejemplo, el siguiente resultado muestra que hay tres dispositivos asociados a las instancias—nvme1n1, nvme0n1 y nvme2n1. La primera columna enumera los dispositivos y sus particiones. La columna FSTYPE muestra el tipo de sistema de archivos para cada dispositivo. Si la columna está vacía para un dispositivo específico, significa que el dispositivo no tiene un sistema de archivos. En este caso, el dispositivo nvme1n1 y la partición nvme0n1p1 en el dispositivo nvme0n1 se formatean con el sistema de archivos XFS, mientras que el dispositivo nvme2n1 y la partición nvme0n1p128 en el dispositivo nvme0n1 no tiene sistemas de archivos.

```
NAME  FSTYPE LABEL UUID      MOUNTPOINT
nvme1n1         xfs  7f939f28-6dcc-4315-8c42-6806080b94dd
nvme0n1
##nvme0n1p1 xfs     / 90e29211-2de8-4967-b0fb-16f51a6e464c         /
##nvme0n1p128
nvme2n1
```

Si el resultado de estos comandos muestra que no hay ningún sistema de archivos en el dispositivo, debe crear uno.

4. (Condicional) Si descubrió que existe un sistema de archivos en el dispositivo en el paso anterior, omita este paso. Si tiene un volumen vacío, utilice el comando mkfs -t para crear un sistema de archivos en el volumen.

   > **Warning**
   >
   > No utilice este comando si está montando un volumen que ya tiene datos (por ejemplo, un volumen que se creó a partir de una instantánea). De lo contrario, formateará el volumen y se eliminarán los datos existentes.

   ```
   [ec2-user ~]$ sudo mkfs -t xfs /dev/xvdf
   ```

   Si recibe un error que indica que no se encuentra `mkfs.xfs`, utilice el comando siguiente para instalar las herramientas XFS y, a continuación, repita el comando anterior:

   ```
   [ec2-user ~]$ sudo yum install xfsprogs
   ```

5. Utilice el comando mkdir para crear un directorio para el punto de montaje del volumen. El punto de montaje es el lugar en el que se ubica el volumen en el árbol del sistema de archivos y donde se leen y escriben los archivos después de montar el volumen. El siguiente ejemplo crea un directorio denominado `/data`.

   ```
   [ec2-user ~]$ sudo mkdir /data
   ```

6. Monte el volumen o partición en el directorio del punto de montaje que creó en el paso anterior.

   Si el volumen no tiene particiones, utilice el siguiente comando y especifique el nombre del dispositivo para montar todo el volumen.

   ```
   [ec2-user ~]$ sudo mount /dev/xvdf /data
   ```

   Si el volumen tiene particiones, utilice el siguiente comando y especifique el nombre de la partición para montar una partición.

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /data
```

7. Revise los permisos del archivo del montaje del nuevo volumen para asegurarse de que los usuarios y las aplicaciones puedan escribir en el volumen. Para obtener más información sobre los permisos de archivos, consulte File security en The Linux Documentation Project.
8. El punto de montaje no se preserva automáticamente después de reiniciar la instancia. Para montar automáticamente este volumen de EBS después del reinicio, consulte Montar automáticamente un volumen asociado después del reinicio.

Montar automáticamente un volumen asociado después del reinicio

Para montar un volumen de EBS asociado en cada reinicio del sistema, añada una entrada para el dispositivo en el archivo `/etc/fstab`.

Puede utilizar el nombre de dispositivo, por ejemplo `/dev/xvdf`, en `/etc/fstab`, pero recomendamos utilizar el identificador universal único (UUID) de 128 bits del dispositivo. Los nombres de dispositivo pueden cambiar, pero el UUID persiste durante la vida útil de la partición. Utilizando el UUID, reduce las posibilidades de que el sistema no se pueda arrancar tras una reconfiguración del hardware. Para obtener más información, consulte Identificar el dispositivo EBS.

Montar automáticamente un volumen asociado después del reinicio

1. (Opcional) Cree una copia de seguridad del archivo `/etc/fstab` que pueda utilizar si destruye o elimina accidentalmente este archivo al editarlo.

```
[ec2-user ~]$ sudo cp /etc/fstab /etc/fstab.orig
```

2. Ejecute el comando blkid para encontrar el UUID del dispositivo. Tome nota del UUID del dispositivo que desea montar después del reinicio. Lo necesitará en el siguiente paso.

   Por ejemplo, el siguiente comando muestra que hay dos dispositivos montados en la instancia y muestra los UUID de ambos dispositivos.

```
[ec2-user ~]$ sudo blkid
/dev/xvda1: LABEL="/" UUID="ca774df7-756d-4261-a3f1-76038323e572" TYPE="xfs"
 PARTLABEL="Linux" PARTUUID="02dcd367-e87c-4f2e-9a72-a3cf8f299c10"
/dev/xvdf: UUID="aebf131c-6957-451e-8d34-ec978d9581ae" TYPE="xfs"
```

En Ubuntu 18.04 use el comando lsblk.

```
[ec2-user ~]$ sudo lsblk -o +UUID
```

3. Abra el archivo `/etc/fstab` con cualquier editor de texto (como nano o vim).

```
[ec2-user ~]$ sudo vim /etc/fstab
```

4. Añada la siguiente entrada a `/etc/fstab` para montar el dispositivo en el punto de montaje especificado. Los campos son el valor UUID devuelto por blkid (o lsblk para Ubuntu 18.04), el punto de montaje, el sistema de archivos y las opciones de montaje del sistema de archivos recomendadas. Para obtener más información acerca de los campos obligatorios, ejecute `man fstab` para abrir el manual fstab.

   En el siguiente ejemplo, montamos el dispositivo con UUID `aebf131c-6957-451e-8d34-ec978d9581ae` al punto de montaje `/data` y usamos el sistema de archivos `xfs`. También usamos los marcadores `defaults` y `nofail`. Especificamos `0` para evitar que el sistema de archivos sea volcado, y especificamos 2 para indicar que es un dispositivo no raíz.

```
UUID=aebf131c-6957-451e-8d34-ec978d9581ae  /data  xfs  defaults,nofail  0  2
```

> **Note**
>
> Si en algún momento arranca la instancia sin este volumen asociado (por ejemplo, después de mover el volumen a otra instancia), la opción de montaje `nofail` permite a la instancia arrancar incluso si hay errores al montar el volumen. Los derivados de Debian, incluidas las versiones de Ubuntu anteriores a la 16.04, también deben añadir la opción de montaje `nobootwait`.

5. Para verificar que la entrada funciona, ejecute los siguientes comandos para desmontar el dispositivo y, a continuación, monte todos los sistemas de archivos en `/etc/fstab`. Si no hay ningún error, el archivo `/etc/fstab` está correcto y el sistema de archivos se montará automáticamente después de su reinicio.

```
[ec2-user ~]$ sudo umount /data
[ec2-user ~]$ sudo mount -a
```

Si recibe un mensaje de error, solucione los errores en el archivo.

> **Warning**
>
> Los errores del archivo `/etc/fstab` pueden impedir el arranque del sistema. No apague un sistema que presente errores en el archivo `/etc/fstab`.

Si no está seguro de cómo corregir errores en `/etc/fstab` y creó un archivo de copia de seguridad en el primer paso de este procedimiento, puede restaurarlo desde su archivo de copia de seguridad utilizando el comando siguiente.

```
[ec2-user ~]$ sudo mv /etc/fstab.orig /etc/fstab
```

instancias de Windows

Utilice uno de los siguientes métodos para que un volumen esté disponible en una instancia de Windows.

PowerShell

Hacer que todos los volúmenes de EBS con particiones sin procesar estén disponibles para su uso con Windows PowerShell

1. Inicie sesión en la instancia de Windows mediante el Escritorio remoto. Para obtener más información, consulte Conexión con su instancia de Windows.
2. En la barra de tareas, abra el menú Inicio y seleccione Windows. PowerShell
3. Utilice la serie de PowerShell comandos de Windows proporcionada en el cuadro de diálogo abierto PowerShell . El script realiza las siguientes acciones de manera predeterminada:

    1. Detiene el servicio ShellHWDetection.
    2. Enumera los discos en los que el estilo de partición es sin procesar.
    3. Crea una nueva partición que abarca el tamaño máximo que admitirán el disco y el tipo de partición.
    4. Asigna una letra disponible a la unidad de disco.

5. Formatea el sistema de archivos como NTFS con la etiqueta del sistema de archivos especificada.
6. Vuelve a iniciar el servicio ShellHWDetection.

```
Stop-Service -Name ShellHWDetection
Get-Disk | Where PartitionStyle -eq 'raw' | Initialize-Disk -PartitionStyle MBR
 -PassThru | New-Partition -AssignDriveLetter -UseMaximumSize | Format-Volume -
FileSystem NTFS -NewFileSystemLabel "Volume Label" -Confirm:$false
Start-Service -Name ShellHWDetection
```

DiskPart command line tool

Para hacer que un volumen de EBS esté disponible para su uso con la herramienta de línea de DiskPart comandos

1. Inicie sesión en la instancia de Windows mediante el Escritorio remoto. Para obtener más información, consulte Conexión con su instancia de Windows.
2. Determine el número del disco que desea que esté disponible:
   1. Abra el menú Inicio y seleccione Windows PowerShell.
   2. Utilice cmdlet `Get-Disk` para recuperar una lista de los discos disponibles.
   3. En la salida del comando, fíjese en el Number (Número) correspondiente al disco que quiere que esté disponible.
3. Cree un archivo de script para ejecutar DiskPart comandos:
   1. Abra el menú Inicio y seleccione Explorador de archivos.
   2. Desplácese hasta un directorio, como por ejemplo C:\, para almacenar el archivo de script.
   3. Elija un espacio vacío, o haga clic en él con el botón derecho, dentro de la carpeta para abrir el cuadro de diálogo, coloque el cursor sobre Nuevo para acceder al menú contextual, y luego elija Documento de texto.
   4. Utilice `diskpart.txt` como nombre del archivo de texto.
4. Agregue los siguientes comandos al archivo de script. Es posible que tenga que modificar el número de disco, el tipo de partición, la etiqueta del volumen y la letra de la unidad. El script realiza las siguientes acciones de manera predeterminada:

1. Selecciona el disco 1 para su modificación.
2. Configura el volumen para que utilice la estructura de partición MBR (registro de arranque maestro).
3. Formatea el volumen como volumen NTFS.
4. Establece la etiqueta del volumen.
5. Asigna una letra de unidad al volumen.

> **Warning**
>
> Si va a montar un volumen que ya contiene datos, no reformatee el volumen, ya que esta acción eliminaría dichos datos.

```
select disk 1
attributes disk clear readonly
online disk noerr
convert mbr
create partition primary
format quick fs=ntfs label="volume_label"
assign letter="drive_letter"
```

Para obtener más información, consulte DiskPart Sintaxis y parámetros.

5. Abra un símbolo del sistema, desplácese hasta la carpeta en la que está el script y ejecute el siguiente comando para que un volumen esté disponible para su uso en el disco especificado:

```
C:\> diskpart /s diskpart.txt
```

Disk Management utility

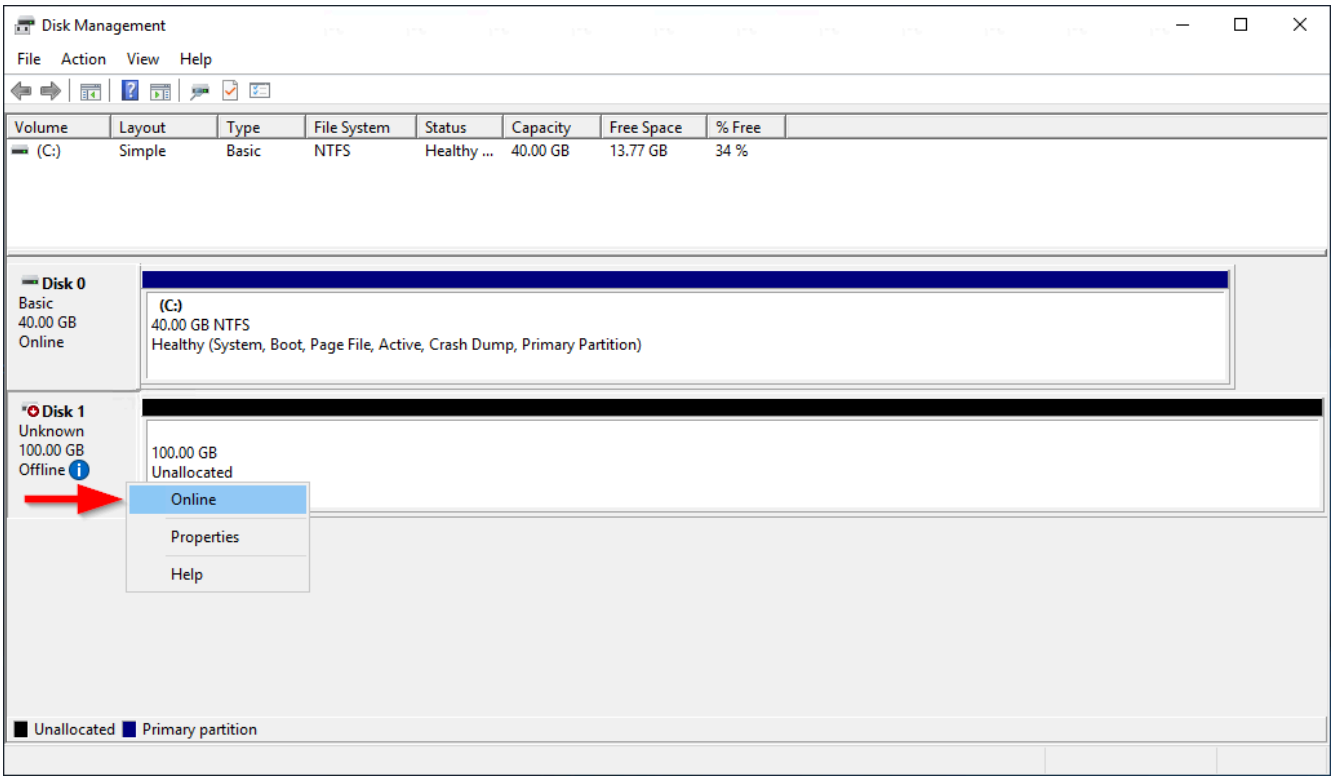
Para conseguir que un volumen de EBS esté disponible para su uso mediante la utilidad Administración de discos

1. Inicie sesión en la instancia de Windows mediante el Escritorio remoto. Para obtener más información, consulte Conexión con su instancia de Windows.

2. Inicie la utilidad de Administración de discos. En la barra de tareas, abra el menú contextual (haga clic con el botón derecho) del logotipo de Windows y elija Administración de discos.

> **Note**
>
> En Windows Server 2008, elija Inicio, Herramientas administrativas, Administración de equipos, Administración de discos.

3. Conecte el volumen. En el panel inferior, abra el menú contextual (con el botón derecho del ratón) del panel izquierdo del volumen de EBS. Elija En línea.

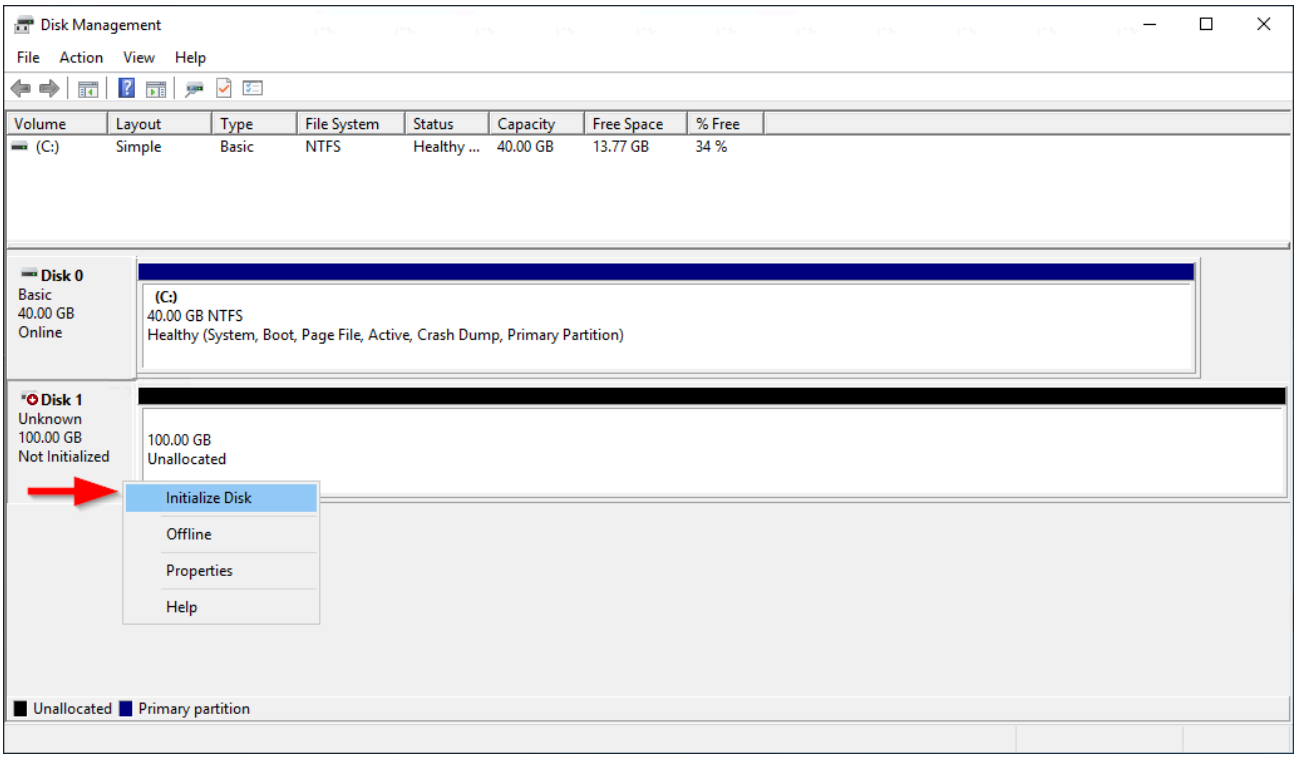


4. (Condicional) Si el disco no se ha inicializado, es necesario inicializarlo para poder utilizarlo. Si el disco ya se inicializó, omita este paso.

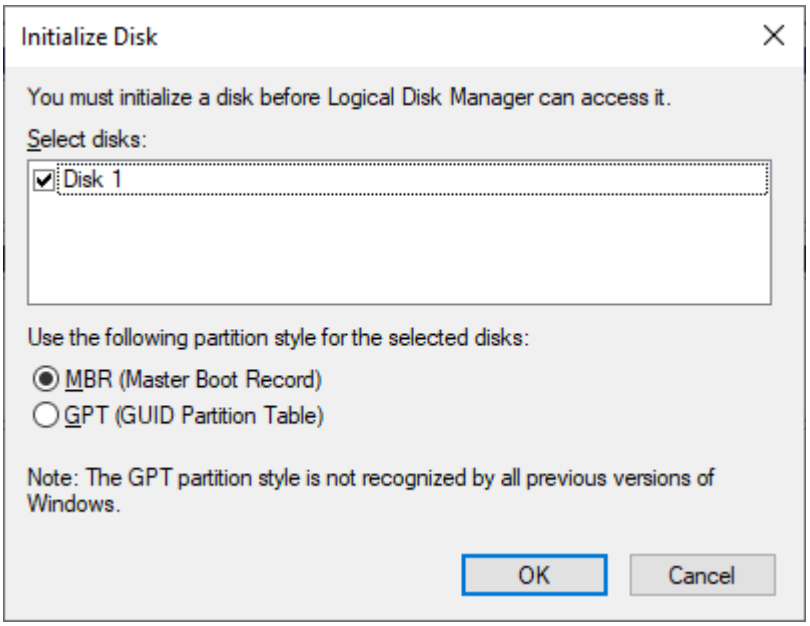
> **Warning**
>
> Si va a montar un volumen que ya contiene datos (por ejemplo, un conjunto de datos públicos o un volumen que ha creado a partir de una instantánea), no reformatee el volumen, ya que esta acción eliminaría dichos datos.

Si no se ha inicializado el disco, hágalo de la siguiente manera:

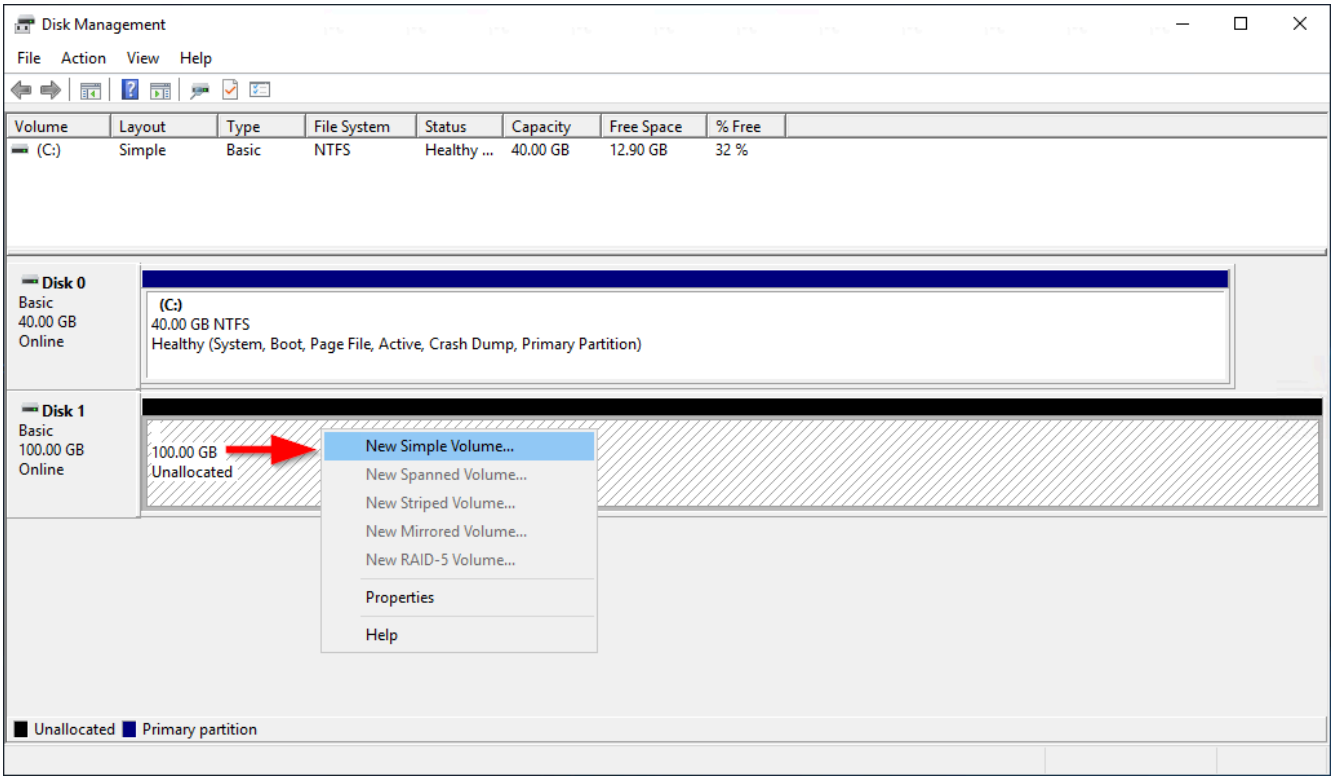
1. Abra el menú contextual (haga clic con el botón derecho) del panel izquierdo correspondiente al disco y elija Inicializar disco.



2. En el cuadro de diálogo Inicializar disco, seleccione un estilo de partición y elija Aceptar.

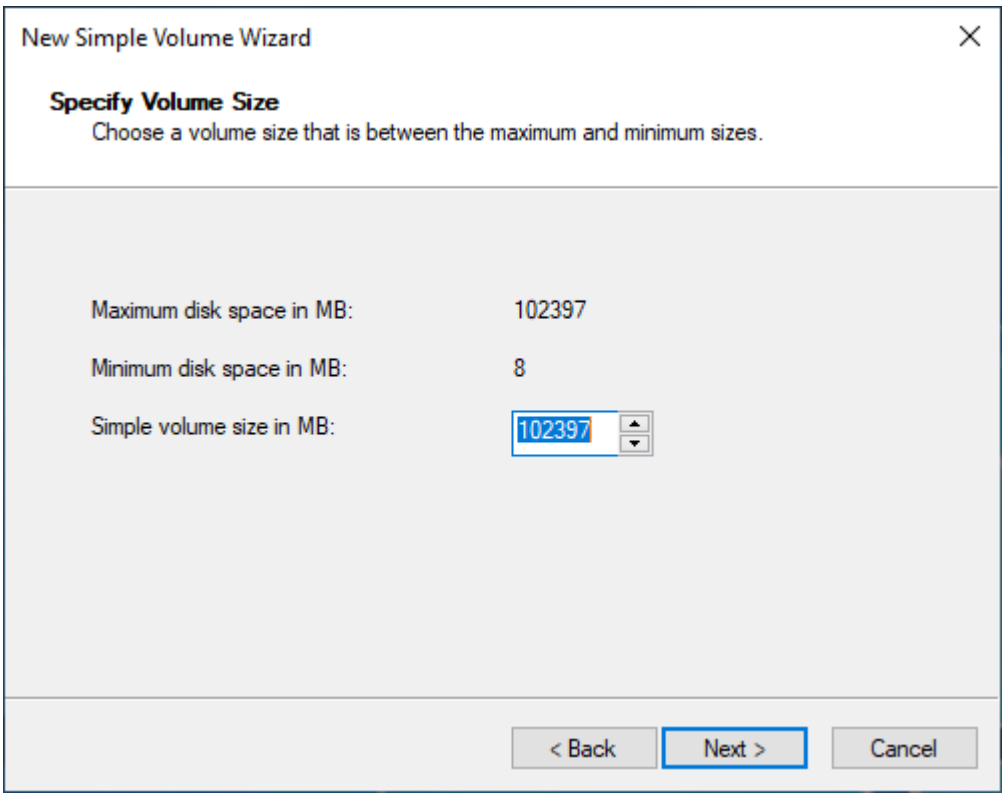


5. Abra el menú contextual (haga clic con el botón derecho) del panel derecho correspondiente al disco y elija Nuevo volumen simple.

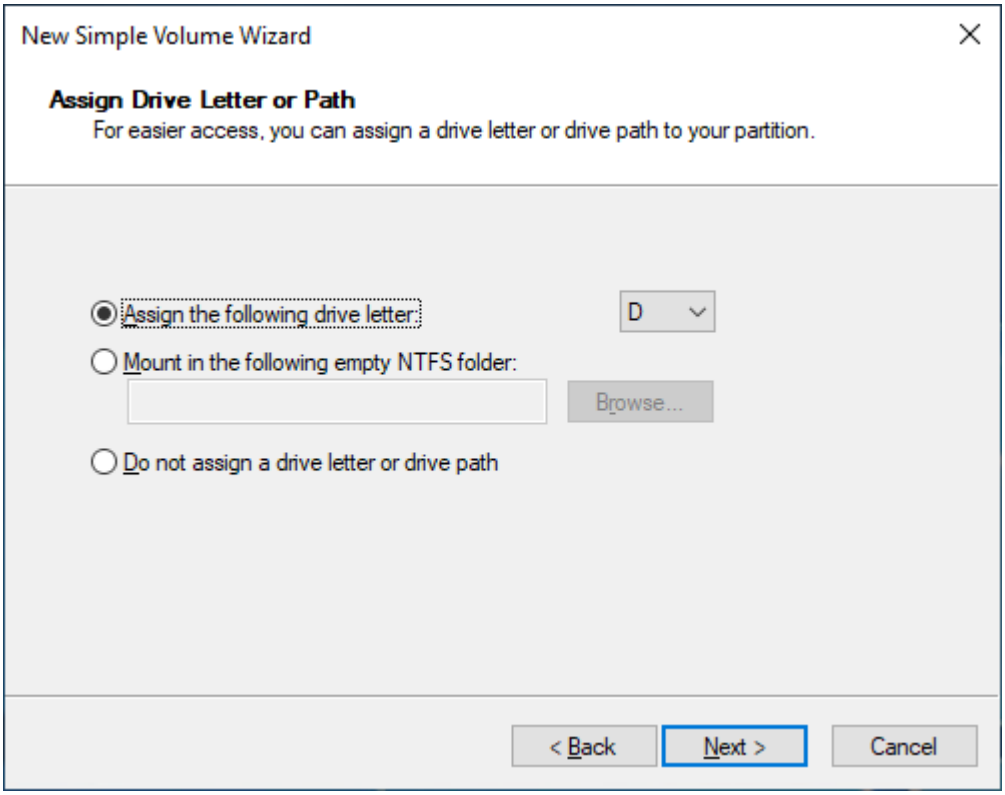


6. En el Asistente para nuevo volumen simple, elija Siguiente.

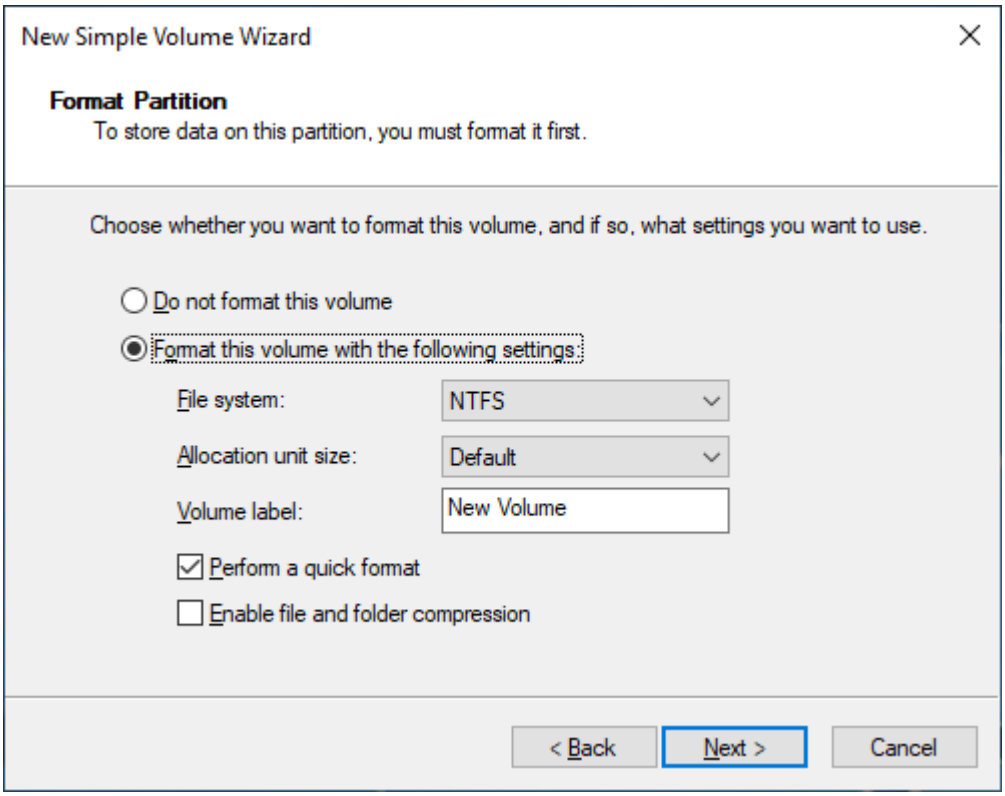
7. Si desea cambiar el valor máximo predeterminado, especifique el Tamaño del volumen simple en MB y luego elija Siguiente.



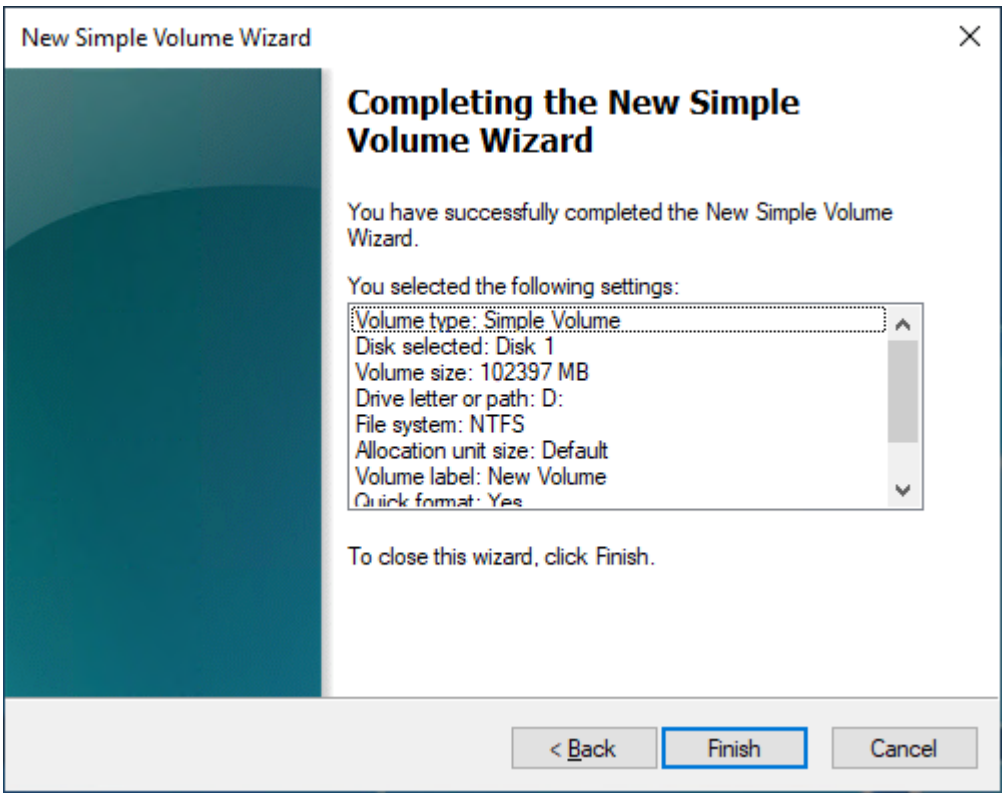
8. Especifique la letra de unidad que prefiera, si es necesario, en el menú desplegable Asignar la letra de unidad siguiente, y luego elija Siguiente.



9. Especifique una Etiqueta del volumen, ajuste la configuración predeterminada según sea necesario y luego elija Siguiente.



10. Revise la configuración y luego elija Finalizar para aplicar las modificaciones y cerrar el Asistente para nuevo volumen simple.



Visualización de información acerca de un volumen de Amazon EBS

Puede ver información descriptiva sobre sus volúmenes de EBS. Por ejemplo, puede ver información sobre todos los volúmenes de una región específica o puede ver información detallada acerca de un volumen concreto, incluidos el tamaño, el tipo de volumen, si está cifrado o no, la clave de KMS utilizada para cifrar el volumen y la instancia específica a la que está asociado el volumen.

Desde el sistema operativo de la instancia puede obtener información adicional sobre sus volúmenes de EBS, como la cantidad de espacio disponible en el disco.

Temas

- Ver la información del volumen
- Estados del volumen
- Visualización de métricas de volumen
- Ver espacio libre en disco

Ver la información del volumen

Puede ver información acerca de un volumen utilizando alguno de los métodos siguientes.

Console

Para ver información acerca de un volumen con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Volumes (Volúmenes).
3. Para reducir la lista, puede filtrar los volúmenes mediante etiquetas y atributos de volumen. Elija el campo de filtro, seleccione una etiqueta o un atributo de volumen y, a continuación, seleccione el valor del filtro.
4. Para ver más información acerca de un volumen, elija el ID.

Para ver qué volúmenes de EBS están asociados a una instancia mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instancias.
3. Seleccione la instancia.
4. En la pestaña Storage (Almacenamiento), la sección Block devices (Dispositivos de bloques) enumera los volúmenes adjuntos a la instancia. Para ver información acerca de un volumen específico, elija el ID en la columna Volume ID (ID de volumen).

Amazon EC2 Global View

Puede utilizar Amazon EC2 Global View a fin de ver los volúmenes en todas las regiones para las que se encuentra habilitada su cuenta de AWS . Para obtener más información, consulte Amazon EC2 Global View.

AWS CLI

Para ver información sobre un volumen de EBS mediante el AWS CLI

Utilice el comando describe-volumes.

Tools for Windows PowerShell

Para ver información sobre un volumen de EBS mediante las Herramientas de Windows PowerShell

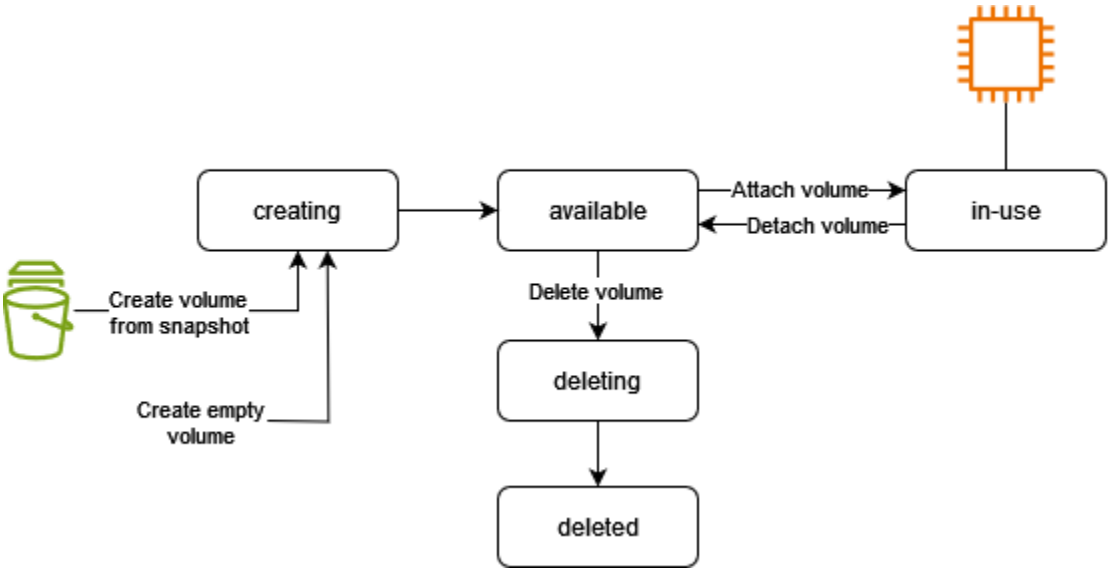
Utilice el comando Get-EC2Volume.

Estados del volumen

El estado del volumen describe la disponibilidad de un volumen de Amazon EBS. Puede ver el estado del volumen en la columna Estado de la página Volúmenes de la consola o mediante el comando AWS CLI describe-volumes.

Un volumen de Amazon EBS pasa por diferentes estados desde que se lo crea hasta que se lo elimina.

La siguiente ilustración muestra las transiciones entre los estados de un volumen. Puede crear un volumen a partir de una instantánea de Amazon EBS o puede crear un volumen vacío. Cuando crea una volumen, este pasa al estado `creating`. Una vez que el volumen está listo para usarse, entra en el estado `available`. Puede adjuntar un volumen disponible a una instancia que se encuentre en la misma zona de disponibilidad que el volumen. Debe separar el volumen para poder asociarlo a otra instancia o eliminarlo. Puede eliminar un volumen cuando ya no lo necesite.



En la siguiente tabla se indican los estados de un volumen.

Estado	Descripción
`creating`	Se está creando el volumen.
`available`	El volumen no está asociado a una instancia.

Estado	Descripción
`in-use`	El volumen está asociado a una instancia.
`deleting`	Se está eliminando el volumen.
`deleted`	Se ha eliminado el volumen.
`error`	Ha ocurrido un error con el hardware subyacente relacionado con el volumen de EBS y es imposible recuperar los datos asociados con el volumen. Para obtener información acerca de cómo restaurar el volumen o recuperar los datos del volumen, vea Mi volumen EBS tiene un estado de “error”.

Visualización de métricas de volumen

Puede obtener información adicional sobre sus volúmenes de EBS en Amazon CloudWatch. Para obtener más información, consulte CloudWatch Métricas de Amazon para Amazon EBS.

Ver espacio libre en disco

instancias de Linux

Desde el sistema operativo Linux de la instancia puede obtener información adicional sobre sus volúmenes de EBS, como la cantidad de espacio disponible en el disco. Por ejemplo, use el siguiente comando:

```
[ec2-user ~]$ df -hT /dev/xvda1
Filesystem     Type      Size  Used Avail Use% Mounted on
/dev/xvda1     xfs       8.0G  1.2G  6.9G  15% /
```

> **Tip**
>
> También puede usar el CloudWatch agente para recopilar métricas de uso del espacio en disco de una instancia de Amazon EC2 sin conectarse a la instancia. Para obtener más información, consulte Creación del archivo de configuración del CloudWatch agente e Instalación del CloudWatch agente en la Guía del CloudWatch usuario de Amazon. Si necesita supervisar el uso del espacio en disco para varias instancias, puede instalar y configurar el CloudWatch agente en esas instancias mediante Systems Manager. Para

obtener más información, consulte Instalación del CloudWatch agente mediante Systems Manager.

Para obtener información sobre cómo ver el espacio libre en disco en una instancia de Windows, consulte Ver el espacio libre en disco en la Guía del usuario de Amazon EC2.

instancias de Windows

Desde el sistema operativo Windows de la instancia puede obtener información adicional sobre sus volúmenes de EBS, como la cantidad de espacio disponible en el disco. Puede ver, por ejemplo, el espacio libre en disco abriendo el explorador de archivos y seleccionando Este equipo.

También puede ver el espacio libre en el disco con el siguiente comando `dir` y consultando la última línea del resultado:

```
C:\> dir C:
 Volume in drive C has no label.
 Volume Serial Number is 68C3-8081

 Directory of C:\

03/25/2018  02:10 AM    <DIR>          .
03/25/2018  02:10 AM    <DIR>          ..
03/25/2018  03:47 AM    <DIR>          Contacts
03/25/2018  03:47 AM    <DIR>          Desktop
03/25/2018  03:47 AM    <DIR>          Documents
03/25/2018  03:47 AM    <DIR>          Downloads
03/25/2018  03:47 AM    <DIR>          Favorites
03/25/2018  03:47 AM    <DIR>          Links
03/25/2018  03:47 AM    <DIR>          Music
03/25/2018  03:47 AM    <DIR>          Pictures
03/25/2018  03:47 AM    <DIR>          Saved Games
03/25/2018  03:47 AM    <DIR>          Searches
03/25/2018  03:47 AM    <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)  18,113,662,976 bytes free
```

También puede ver el espacio libre en el disco con el siguiente comando `fsutil`:

```
C:\> fsutil volume diskfree C:
```

```
Total # of free bytes        : 18113204224
Total # of bytes             : 32210153472
Total # of avail free bytes  : 18113204224
```

> **Tip**
>
> También puede usar el CloudWatch agente para recopilar métricas de uso del espacio en disco de una instancia de Amazon EC2 sin conectarse a la instancia. Para obtener más información, consulte Creación del archivo de configuración del CloudWatch agente e Instalación del CloudWatch agente en la Guía del CloudWatch usuario de Amazon. Si necesita supervisar el uso del espacio en disco para varias instancias, puede instalar y configurar el CloudWatch agente en esas instancias mediante Systems Manager. Para obtener más información, consulte Instalación del CloudWatch agente mediante Systems Manager.

Para obtener información sobre cómo ver el espacio libre en disco en una instancia de Linux, consulte Ver el espacio libre en disco en la Guía del usuario de Amazon EC2.

Modificación de un volumen mediante Volúmenes elásticos de Amazon EBS

Con los volúmenes elásticos de Amazon EBS puede aumentar el tamaño del volumen, cambiar el tipo de volumen o ajustar el rendimiento de sus volúmenes de EBS. Si su instancia admite volúmenes elásticos, puede realizar estas operaciones sin desconectar el volumen ni reiniciar la instancia. Esto permite seguir usando la aplicación mientras se aplican los cambios.

No se aplica ningún cargo por modificar la configuración de un volumen. El precio de la nueva configuración de volumen se le cobrará después de que comience una modificación del volumen. Para obtener más información, consulte la Página de precios de Amazon EBS.

Contenido

Requisitos para las modificaciones del volumen de EBS

Los siguientes requisitos y limitaciones se aplican al modificar un volumen de Amazon EBS. Para obtener más información sobre los requisitos generales de los volúmenes de EBS, consulte Restricciones de tamaño y configuración de un volumen de EBS.

Temas

- Tipos de instancias admitidos
- Sistema operativo
- Limitaciones

Tipos de instancias admitidos

Los volúmenes elásticos se admiten en las siguientes instancias:

- Todas las instancias de la generación actual
- Las siguientes instancias de generación anterior: C1, C3, C4, G2, I2, M1, M3, M4, R3 y R4

Si su tipo de instancia no admite volúmenes estáticos, consulte Modificar un volumen de EBS si no se admiten volúmenes elásticos.

Sistema operativo

Se aplican los siguientes requisitos del sistema operativo:

Linux

Las AMI de Linux requieren una tabla de partición GUID (GPT) y GRUB 2 para volúmenes de arranque de 2 TiB (2048 GiB) o más. Muchas AMI de Linux aún emplean en la actualidad un esquema de partición MBR que solo admite tamaños de volúmenes de arranque de un máximo de 2 TiB. Si su instancia no arranca con un volumen de arranque superior a 2 TiB, la AMI que use puede estar limitada a un tamaño de volumen de arranque inferior a 2 TiB. Los volúmenes sin arranque no tienen esta limitación en las instancias de Linux. Para conocer los requisitos que afectan a los volúmenes de Windows, consulte Requisitos para los volúmenes de Windows en la Guía del usuario de Amazon EC2.

Antes de intentar cambiar el tamaño de un volumen de arranque más allá de los 2 TiB, puede ejecutar el siguiente comando en la instancia para determinar si el volumen está usando una partición MBR o GPT:

```
[ec2-user ~]$ sudo gdisk -l /dev/xvda
```

Una instancia de Amazon Linux con partición GPT devuelve la siguiente información:

```
GPT fdisk (gdisk) version 0.8.10

  Partition table scan:
    MBR: protective
    BSD: not present
    APM: not present
    GPT: present

  Found valid GPT with protective MBR; using GPT.
```

Una instancia de SUSE con partición MBR devuelve la siguiente información:

```
GPT fdisk (gdisk) version 0.8.8

  Partition table scan:
    MBR: MBR only
    BSD: not present
    APM: not present
    GPT: not present
```

Windows

De forma predeterminada, Windows inicializa los volúmenes con una tabla de partición MBR (registro de arranque maestro). Dado que MBR admite solo volúmenes cuyo tamaño sea inferior a 2 TiB (2048 GiB), Windows le impide que cambie el tamaño de los volúmenes MBR más allá de este límite. En dicho caso, la opción Extender volumen se deshabilita en la utilidad Administración de discos de Windows. Si utiliza AWS Management Console o AWS CLI para crear un volumen particionado en MBR que supere el límite de tamaño, Windows no podrá detectar ni utilizar el espacio adicional. Para conocer los requisitos que afectan a los volúmenes de Linux, consulte Requisitos para los volúmenes de Linux en la Guía del usuario de Amazon EC2.

Para superar este límite, puede crear un volumen nuevo, más grande, con una tabla de partición GUID (GPT) y copiar en ella los datos del volumen MBR original.

Para crear un volumen GPT

1. Cree un volumen nuevo y vacío que tenga el tamaño deseado en la zona de disponibilidad de la instancia EC2 y asócielo a su instancia.

   > **Note**
   >
   > El nuevo volumen no tiene que ser un volumen restaurado a partir de una instantánea.

2. Inicie sesión en su sistema Windows y abra Administración de discos (diskmgmt.exe).
3. Abra el menú contextual del disco nuevo (haga clic con el botón derecho) y elija En línea.
4. En la ventana Inicializar disco seleccione el disco nuevo y elija GPT (Tabla de particiones GUID), Aceptar.
5. Cuando haya acabado la inicialización, copie los datos del volumen original en el volumen nuevo con una herramienta como robocopy o teracopy.
6. En Administración de discos cambie las letras de las unidades por los valores adecuados y desconecte el volumen antiguo.
7. En la consola de Amazon EC2 separe el volumen antiguo de la instancia, rearranque la instancia para verificar que funcione bien y elimine el antiguo volumen.

Limitaciones

- Existen límites para el máximo de almacenamiento agregado que se puede solicitar en todas las modificaciones de volumen. Para obtener más información, consulte Service Quotas de Amazon EBS en Referencia general de Amazon Web Services.
- Después de modificar un volumen, debe esperar como mínimo seis horas y asegurarse de que el estado del volumen sea `in-use` o `available` antes de poder modificarlo.
- La modificación de un volumen de EBS puede tardar entre varios minutos a varias horas, dependiendo de los cambios que se han realizado en la configuración. Por lo general, un volumen de EBS de 1 TiB puede tardar hasta seis horas en modificarse. Sin embargo, el mismo volumen puede tardar 24 horas o más en otras situaciones. El tiempo que tardan los volúmenes en modificarse no siempre se escala linealmente. Por lo tanto, un volumen más grande puede llevar menos tiempo y un volumen más pequeño puede tardar más.
- Si el volumen se conectó antes del 3 de noviembre de 2016 23:40 UTC, debe inicializar la compatibilidad con volúmenes estáticos. Para obtener más información, consulte Inicializar la compatibilidad con volúmenes estáticos.

- Si recibe un mensaje de error al intentar modificar a un volumen de EBS, o si está modificando un volumen de EBS adjunto a un tipo de instancia de generación anterior, ejecute uno de los pasos siguientes:
  - Para un volumen que no es raíz, separe el volumen de la instancia, aplique las modificaciones y, a continuación, vuelva a adjuntar el volumen.
  - Para un volumen raíz, detenga la instancia, aplique las modificaciones y, a continuación, reinicie la instancia.
- Se aumenta el tiempo de modificación para los volúmenes que no están completamente inicializados. Para obtener más información, consulte Inicializar de volúmenes de Amazon EBS.
- El nuevo tamaño del volumen no puede exceder la capacidad admitida de su sistema de archivos y su esquema de partición. Para obtener más información, consulte Restricciones de tamaño y configuración de un volumen de EBS.
- Si modifica el tipo de volumen de un volumen, el tamaño y el rendimiento deben encontrarse dentro de los límites del tipo de volumen de destino. Para obtener más información, consulte Tipos de volúmenes de Amazon EBS
- No puede reducir el tamaño de un volumen de EBS. No obstante, se puede crear un volumen más pequeño y, a continuación, migrar los datos a él mediante una herramienta de nivel de aplicación como rsync (instancias de Linux) o robocopy (instancias de Windows).
- Después de aprovisionar más de 32 000 IOPS en un volumen `io1` o `io2` existente, es posible que deba desconectar y volver a adjuntar el volumen, o bien, reiniciar la instancia para ver todas las mejoras de rendimiento.
- Los volúmenes `io2` asociados a instancias basadas en Nitro System admiten tamaños de hasta 64 TiB e IOPS de hasta 256 000 IOPS. Los volúmenes `io2` asociados a otras instancias admiten tamaños de hasta 16 TiB e IOPS de hasta 64 000, pero solo pueden lograr rendimiento de hasta 32 000 IOPS.
- No puede modificar el tipo de volumen de los volúmenes `io2` habilitados para Multi-Attach.
- No puede modificar el tipo, ni el tamaño ni las IOPS provisionadas de los volúmenes `io1` habilitados para Multi-Attach.
- Un volumen raíz de tipo `io1`,`io2`,`gp2`,`gp3` o `standard` no se puede modificar como un volumen `st1` o `sc1`, incluso si está separado de la instancia.
- Mientras las instancias `m3.medium` son totalmente compatibles con la modificación de volúmenes, es posible que las instancias `m3.large`, `m3.xlarge` y `m3.2xlarge` no admitan todas las características de la modificación de volúmenes.

Solicitar modificaciones a los volúmenes de EBS

Con los volúmenes elásticos, puede, de manera dinámica, aumentar el tamaño, aumentar o disminuir el rendimiento y cambiar el tipo de volumen de sus volúmenes de Amazon EBS sin desconectarlos.

Utilice el siguiente proceso al modificar un volumen:

1. (Opcional) Antes de modificar un volumen que contenga datos valiosos, una práctica recomendada consiste en crear una instantánea del volumen por si más adelante fuera necesario revertir los cambios. Para obtener más información, consulte Crear instantáneas de Amazon EBS.
2. Solicite la modificación del volumen.
3. Monitorice el progreso de la modificación del volumen. Para obtener más información, consulte Monitoreo del progreso de las modificaciones del volumen de EBS.
4. Si se ha modificado el tamaño del volumen, amplíe el sistema de archivos del volumen para aprovechar el aumento en la capacidad de almacenamiento. Para obtener más información, consulte Ampliación de un sistema de archivos después de cambiar el tamaño de un volumen de EBS.

Contenido

Modificación de un volumen de EBS mediante volúmenes elásticos

Consideraciones

Tenga en cuenta lo siguiente cuando modifique volúmenes :

- Después de modificar un volumen, debe esperar como mínimo seis horas y asegurarse de que el estado del volumen sea `in-use` o `available` antes de poder modificarlo.
- La modificación de un volumen de EBS puede tardar entre varios minutos a varias horas, dependiendo de los cambios que se han realizado en la configuración. Por lo general, un volumen de EBS de 1 TiB puede tardar hasta seis horas en modificarse. Sin embargo, el mismo volumen puede tardar 24 horas o más en otras situaciones. El tiempo que tardan los volúmenes en modificarse no siempre se escala linealmente. Por lo tanto, un volumen más grande puede llevar menos tiempo y un volumen más pequeño puede tardar más.

- No puede cancelar una solicitud de modificación de volumen después de enviarla.
- Solo puede aumentar el tamaño del volumen. No puede reducir el tamaño del volumen.
- Puede aumentar o disminuir el rendimiento del volumen.
- Si no cambia el tipo del volumen, las modificaciones de su tamaño y rendimiento deben estar dentro de los límites del tipo de volumen actual. Si cambia el tipo de volumen, las modificaciones de su tamaño y rendimiento deben estar dentro de los límites del tipo de volumen de destino.
- Si cambia el tipo de volumen de gp2 a gp3, y no especifica el rendimiento de IOPS ni el rendimiento, Amazon EBS aprovisiona automáticamente un rendimiento equivalente al del volumen gp2 de origen o del rendimiento de gp3 de referencia, lo que sea mayor.

  Por ejemplo, si modifica un volumen gp2 de 500 GiB con rendimiento de 250 MiB/s y 1500 IOPS para gp3 sin especificar el rendimiento de IOPS ni el rendimiento, Amazon EBS aprovisiona automáticamente el volumen gp3 con 3000 IOPS (IOPS de gp3 de referencia) y 250 MiB/s (para que coincida con el rendimiento del volumen gp2 de origen).

Para modificar un volumen de EBS, utilice alguno de los métodos siguientes.

Console

Para modificar un volumen de EBS con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Volumes (Volúmenes).
3. Seleccione el volumen que desea modificar y elija Actions (Acciones), Modify volume (Modificar volumen).
4. La pantalla Modify Volume (Modificar volumen) muestra el ID de volumen y la configuración del volumen actual, incluido el tipo, el tamaño, las IOPS y el rendimiento. Especifique los nuevos valores de configuración del siguiente modo:
   - Para modificar el tipo, elija un valor para Volume Type (Tipo de volumen).
   - Para modificar el tamaño, escriba un nuevo valor para Tamaño.
   - (Solo para gp3, io1 y io2) A fin de modificar las IOPS, ingrese un nuevo valor para IOPS.
   - (Solo para gp3) A fin de modificar el rendimiento, ingrese un nuevo valor para Throughput (Rendimiento).
5. Una vez que haya completado el cambio de configuración del volumen, seleccione Modificar. Cuando reciba la pregunta de confirmación, elija Modificar.

6.

> **Important**
>
> Si aumentó el tamaño del volumen, también debe ampliar la partición del volumen para utilizar la capacidad de almacenamiento adicional. Para obtener más información, consulte Ampliación de un sistema de archivos después de cambiar el tamaño de un volumen de EBS.

7. (Solo instancias de Windows) Si aumenta el tamaño de un volumen NVMe en una instancia que no tiene los controladores AWS NVMe, debe reiniciar la instancia para que Windows pueda ver el nuevo tamaño del volumen. Para obtener más información sobre la instalación de los controladores AWS NVMe, consulte Controladores AWS NVMe para instancias de Windows.

AWS CLI

Para modificar un volumen de EBS mediante AWS CLI

Utilice el comando modify-volume para modificar una o varias opciones de configuración de un volumen. Por ejemplo, si tiene un volumen de tipo gp2 con un tamaño de 100 GiB, el siguiente comando cambia su configuración a un volumen de tipo io1 con 10 000 IOPS y un tamaño de 200 GiB.

```
aws ec2 modify-volume --volume-type io1 --iops 10000 --size 200 --volume-
id vol-11111111111111111
```

A continuación, se muestra un ejemplo de la salida:

```
{
    "VolumeModification": {
        "TargetSize": 200,
        "TargetVolumeType": "io1",
        "ModificationState": "modifying",
        "VolumeId": "vol-11111111111111111",
        "TargetIops": 10000,
        "StartTime": "2017-01-19T22:21:02.959Z",
        "Progress": 0,
        "OriginalVolumeType": "gp2",
        "OriginalIops": 300,
        "OriginalSize": 100
```

```
    }
}
```

> **Important**
>
> Si aumentó el tamaño del volumen, también debe ampliar la partición del volumen para utilizar la capacidad de almacenamiento adicional. Para obtener más información, consulte Ampliación de un sistema de archivos después de cambiar el tamaño de un volumen de EBS.

Inicializar la compatibilidad de volúmenes elásticos (si es necesario)

Para poder modificar un volumen que estuvo adjunto a una instancia antes del 3 de noviembre de 2016 23:40 UTC, debe inicializar la compatibilidad de la modificación de volúmenes ejecutando una de las acciones siguientes:

- Separar y adjuntar el volumen.
- Detenga e inicie la instancia.

Realice uno de los siguientes procedimientos para determinar si sus instancias están listas para la modificación de volúmenes.

Console

Para determinar si sus instancias están listas mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instances (Instancia[s]).
3. Elija el icono Show/Hide Columns (Mostrar/ocultar columnas) (el engranaje). Seleccione la columna de atributo Launch time (Hora de lanzamiento) y, a continuación, elija Confirm (Confirmar).
4. Ordene la lista de instancias por la columna Launch Time (Hora de lanzamiento). Para cada instancia iniciada antes de la fecha límite, elija la pestaña Storage (Almacenamiento) y marque la columna Attachment time (Hora de conexión) para ver cuándo se asociaron sus volúmenes.

AWS CLI

Para determinar si sus instancias están listas mediante la CLI

Use el siguiente comando describe-instances para averiguar si el volumen se conectó antes del 3 de noviembre de 2016 23:40 UTC.

```
aws ec2 describe-instances --query "Reservations[*].Instances[*].
[InstanceId,LaunchTime<='2016-11-01',BlockDeviceMappings[*]
[Ebs.AttachTime<='2016-11-01']]" --output text
```

La primera línea del resultado de cada instancia muestra su ID y si sus volúmenes se conectaron antes de la fecha límite o no (True o False). La primera línea va seguida de una o varias líneas que muestran si cada volumen de EBS se conectó antes de la fecha límite o no (True o False). En la salida del ejemplo siguiente debe inicializar la modificación de volumen de la primera instancia porque comenzó antes de la fecha límite y su volumen raíz se adjuntó antes de dicha fecha. Las demás instancias están listas porque se iniciaron después de la fecha límite.

```
i-e905622e              True
True
i-719f99a8              False
True
i-006b02c1b78381e57     False
False
False
i-e3d172ed              False
True
```

Modificar un volumen de EBS si no se admiten volúmenes elásticos

Si utiliza un tipo de instancia admitido, puede usar volúmenes estáticos para modificar de manera dinámica el tamaño, el rendimiento y el tipo de volumen de sus volúmenes de Amazon EBS sin desconectarlos.

Si no puede usar volúmenes estáticos, pero necesita modificar el volumen raíz (arranque), debe detener la instancia, modificar el volumen y, a continuación, reiniciar la instancia.

Una vez iniciada la instancia, puede comprobar el tamaño del sistema de archivos para ver si la instancia reconoce el mayor espacio del volumen. En Linux, utilice el comando df -h para comprobar el tamaño del sistema de archivos.

```
[ec2-user ~]$ df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/xvda1            7.9G  943M  6.9G  12% /
tmpfs                 1.9G     0  1.9G   0% /dev/shm
```

Si el tamaño no refleja el nuevo volumen ampliado, debe ampliar el sistema de archivos de su dispositivo de forma que la instancia pueda usar el nuevo espacio. Para obtener más información, consulte Ampliación de un sistema de archivos después de cambiar el tamaño de un volumen de EBS.

Con las instancias de Windows, puede que deba poner el volumen en línea para usarlo. Para obtener más información, consulte Cómo hacer que un volumen de Amazon EBS esté disponible para su uso. No es necesario que reformatee el volumen.

Monitoreo del progreso de las modificaciones del volumen de EBS

Cuando modifica un volumen de EBS, este pasa por una serie de estados. El volumen pasa al estado `modifying`, al estado `optimizing` y, finalmente, al estado `completed`. En este punto, el volumen está listo para ser modificado.

> **Note**
>
> En raras ocasiones, un AWS fallo transitorio puede provocar un `failed` estado. Esto no es una indicación del estado del volumen; simplemente indica que la modificación del volumen ha devuelto un error. Si esto sucede, vuelva a intentar la modificación del volumen.

Mientras el volumen está en el estado `optimizing`, el rendimiento del volumen estará entre las especificaciones de las configuraciones de origen y de destino. El rendimiento transitorio del volumen no estará por debajo del rendimiento del volumen de origen. Si está reduciendo las IOPS, el rendimiento transitorio del volumen no estará por debajo del rendimiento del volumen de destino.

Los cambios de modificación del volumen se aplican del modo siguiente:

- Los cambios de tamaño suelen tardar unos segundos en completarse y en tener efecto después de que el volumen pasa al estado `Optimizing`.
- Los cambios en el rendimiento (IOPS) pueden tardar de varios minutos a varias horas en completarse y dependen del cambio que se ha realizado en la configuración.

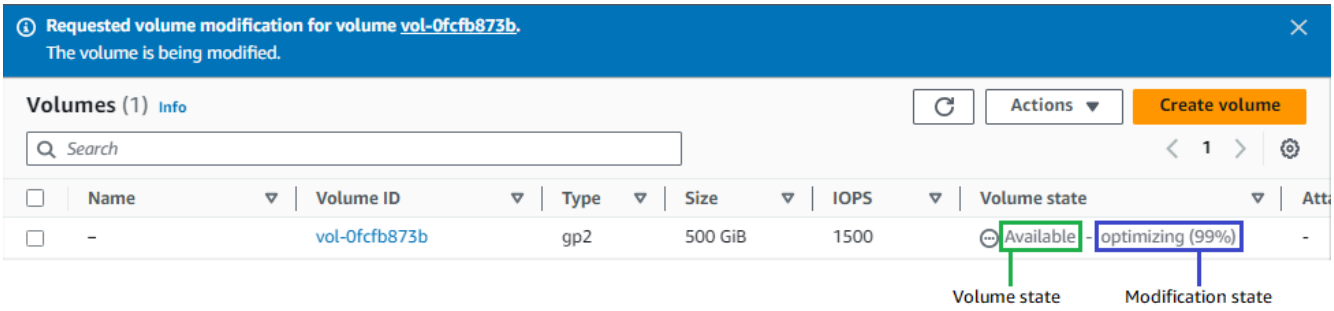
- En algunos casos, pueden pasar más de 24 horas para que una nueva configuración surta efecto, como cuando el volumen no se ha inicializado completamente. Normalmente, un volumen de 1 TiB completamente utilizado tarda unas 6 horas en migrar a una nueva configuración de rendimiento.

Para monitorear el progreso de la modificación de un volumen, use alguno de los métodos siguientes.

Console

Para monitorear el progreso de una modificación con la consola de Amazon EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Volumes (Volúmenes).
3. Seleccione el volumen.
4. La columna Estado del volumen y el campo Estado del volumen de la pestaña Detalles contienen información en el siguiente formato: *Estado del volumen* - *Estado de la modificación* (*Progreso de la modificación* %). La siguiente imagen muestra los estados de volumen y modificación del volumen.



Los posibles estados de volumen son `creating`, `available`, `in-use`, `deleting`, `deleted` y `error`.

Los posibles estados de modificación son `modifying`, `optimizing` y `completed`.

Una vez finalizada la modificación, solo se muestra el estado del volumen. El estado y el progreso de la modificación ya no se muestran.

AWS CLI

Para supervisar el progreso de una modificación mediante el AWS CLI

Utilice el comando describe-volumes-modifications para ver el progreso de una o varias modificaciones del volumen. En el siguiente ejemplo se describen las modificaciones de dos volúmenes.

```
aws ec2 describe-volumes-modifications --volume-
ids vol-1111111111111111 vol-2222222222222222
```

En el siguiente resultado de ejemplo, las modificaciones del volumen siguen estando en el estado `modifying`. El progreso se indica como porcentaje.

```
{
    "VolumesModifications": [
        {
            "TargetSize": 200,
            "TargetVolumeType": "io1",
            "ModificationState": "modifying",
            "VolumeId": "vol-1111111111111111",
            "TargetIops": 10000,
            "StartTime": "2017-01-19T22:21:02.959Z",
            "Progress": 0,
            "OriginalVolumeType": "gp2",
            "OriginalIops": 300,
            "OriginalSize": 100
        },
        {
            "TargetSize": 2000,
            "TargetVolumeType": "sc1",
            "ModificationState": "modifying",
            "VolumeId": "vol-2222222222222222",
            "StartTime": "2017-01-19T22:23:22.158Z",
            "Progress": 0,
            "OriginalVolumeType": "gp2",
            "OriginalIops": 300,
            "OriginalSize": 1000
        }
    ]
}
```

El siguiente ejemplo describe todos los volúmenes con estado de modificación `optimizing` o `completed`, y, a continuación, filtra y da formato a los resultados para mostrar solo aquellas modificaciones iniciadas el día 1 de febrero de 2017 o después:

```
aws ec2 describe-volumes-modifications --filters Name=modification-
state,Values="optimizing","completed" --query "VolumesModifications[?
StartTime>='2017-02-01'].{ID:VolumeId,STATE:ModificationState}"
```

A continuación, se muestra un resultado de ejemplo con información sobre dos volúmenes:

```
[
    {
        "STATE": "optimizing",
        "ID": "vol-06397e7a0eEXAMPLE"
    },
    {
        "STATE": "completed",
        "ID": "vol-ba74e18c2aEXAMPLE"
    }
]
```

CloudWatch Events console

Con CloudWatch Events, puede crear una regla de notificación para los eventos de modificación de volumen. Puede utilizar la regla para generar un mensaje de notificación con Amazon SNS o para invocar una función Lambda en respuesta a los eventos coincidentes. Los eventos se emiten en la medida de lo posible.

Para supervisar el progreso de una modificación mediante CloudWatch Events

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. Elija Events (Eventos), Create rule (Crear regla).
3. Para Build event pattern to match events by service (Crear patrón de eventos para buscar eventos coincidentes por servicio), elija Custom event pattern (Patrón de eventos personalizado).
4. En Build custom event pattern (Crear patrón de eventos personalizado), sustituya el contenido por lo siguiente y elija Save (Guardar).

```
{
  "source": [
    "aws.ec2"
  ],
  "detail-type": [
```

```
    "EBS Volume Notification"
  ],
  "detail": {
    "event": [
      "modifyVolume"
    ]
  }
}
```

A continuación se muestran datos de evento de ejemplo:

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Volume Notification",
   "source": "aws.ec2",
   "account": "012345678901",
   "time": "2017-01-12T21:09:07Z",
   "region": "us-east-1",
   "resources": [
      "arn:aws:ec2:us-east-1:012345678901:volume/vol-03a55cf56513fa1b6"
   ],
   "detail": {
      "result": "optimizing",
      "cause": "",
      "event": "modifyVolume",
      "request-id": "01234567-0123-0123-0123-0123456789ab"
   }
}
```

Ampliación de un sistema de archivos después de cambiar el tamaño de un volumen de EBS

Después de aumentar el tamaño de un volumen de EBS, debe ampliar las particiones y el sistema de archivos en el nuevo tamaño más grande. Puede hacerlo en cuanto el volumen pase al estado `optimizing`.

Antes de empezar

- Cree una instantánea del volumen por si más adelante es necesario revertir los cambios. Para obtener más información, consulte Crear instantáneas de Amazon EBS.

- Confirme que la modificación del volumen se realizó correctamente y que se encuentra en el estado `optimizing` o `completed`. Para obtener más información, consulte Monitoreo del progreso de las modificaciones del volumen de EBS.
- Asegúrese de que el volumen esté adjunto a la instancia y de que esté formateado y montado. Para obtener más información, consulte Dar formato y montar un volumen asociado.
- (Solamente instancias de Linux) Si utiliza volúmenes lógicos en el volumen de Amazon EBS, debe usar el Administrador de volúmenes lógicos (LVM) para extender el volumen lógico. Para obtener instrucciones sobre cómo hacerlo, consulte la sección Ampliar el volumen lógico en la sección ¿Cómo se crea un volumen lógico LVM en un volumen completo de EBS? AWS Artículo del Knowledge Center.

instancias de Linux

> **Note**
>
> En el siguiente tema, obtendrá información sobre el proceso de ampliación de los sistemas de archivos XFS y Ext4 para Linux. Para obtener información sobre cómo ampliar un sistema de archivos diferente, consulte su documentación.

Antes de extender un sistema de archivos en Linux, debe extender la partición, en caso de que su volumen tenga una.

Amplíe el sistema de archivos de los volúmenes de EBS.

Utilice el siguiente procedimiento para ampliar el sistema de archivos de un volumen redimensionado.

Tenga en cuenta que los nombres de los dispositivos y las particiones difieren para las instancias de Xen y las instancias creadas en Nitro System. Para determinar si su instancia está basada en Xen o en Nitro, use el comando de AWS CLI describe-instance-types de la siguiente manera:

```
[ec2-user ~]$ aws ec2 describe-instance-types --instance-type instance_type --query
 "InstanceTypes[].Hypervisor"
```

`nitro` indica que su instancia está basada en Nitro. `xen` o `xen-on-nitro` indica que su instancia está basada en Xen.

Para ampliar el sistema de archivos de los volúmenes de EBS

1. Conéctese a la instancia.
2. Cambie el tamaño de la partición, en caso de ser necesario. Para ello:

   a. Compruebe si el volumen tiene una partición. Utilice el comando lsblk.

      Nitro instance example

      En el siguiente resultado de ejemplo, el volumen raíz (`nvme0n1`) tiene dos particiones (`nvme0n1p1` y `nvme0n1p128`), mientras que el volumen adicional (`nvme1n1`) no tiene particiones.

```
[ec2-user ~]$ sudo lsblk
NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme1n1       259:0    0  30G  0 disk /data
nvme0n1       259:1    0  16G  0 disk
##nvme0n1p1   259:2    0   8G  0 part /
##nvme0n1p128 259:3    0   1M  0 part
```

      Xen instance example

      En el siguiente resultado de ejemplo, el volumen raíz (`xvda`) tiene una partición (`xvda1`), mientras que el volumen adicional (`xvdf`) no tiene particiones.

```
[ec2-user ~]$ sudo lsblk
NAME    MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvda    202:0    0  16G  0 disk
##xvda1 202:1    0   8G  0 part /
xvdf    202:80   0  24G  0 disk
```

   Si el volumen tiene una partición, continúe el procedimiento desde el paso siguiente (2b). Si el volumen no tiene particiones, omita los pasos 2b, 2c y 2d, y continúe el procedimiento desde el paso 3.

   > **Consejo para la solución de problemas**
   >
   > Si no ve el volumen en la salida del comando, asegúrese de que el volumen esté adjunto a la instancia, y que esté formateado y montado.

b. Compruebe si es necesario ampliar la partición. En la salida del comando lsblk del paso anterior, compare el tamaño de la partición y el tamaño del volumen.

   Si el tamaño de la partición es menor que el tamaño del volumen, continúe con el siguiente paso. Si el tamaño de la partición es igual al tamaño del volumen, no se puede ampliar la partición.

   > **Consejo para la solución de problemas**
   >
   > Si el volumen sigue reflejando el tamaño original, confirme que la modificación del volumen se realizó correctamente.

c. Amplíe la partición. Utilice el comando growpart y especifique la partición que se ampliará.

   Nitro instance example

   Por ejemplo, para ampliar una partición denominada `nvme0n1p1`, utilice el siguiente comando.

   > **Important**
   >
   > Observe el espacio entre el nombre del dispositivo (`nvme0n1`) y el número de partición (1).

   ```
   [ec2-user ~]$ sudo growpart /dev/nvme0n1 1
   ```

   Xen instance example

   Por ejemplo, para ampliar una partición denominada `xvda1`, utilice el siguiente comando.

   > **Important**
   >
   > Observe el espacio entre el nombre del dispositivo (`xvda`) y el número de partición (1).

```
[ec2-user ~]$ sudo growpart /dev/xvda 1
```

Consejos para la solución de problemas

- `mkdir: cannot create directory ‘/tmp/growpart.31171’: No space left on device FAILED: failed to make temp dir`: indica que no hay suficiente espacio libre en disco en el volumen para que growpart cree el directorio temporal que necesita para cambiar el tamaño. Libere espacio en el disco e inténtelo de nuevo.
- `must supply partition-number`: indica que especificó una partición incorrecta. Utilice el comando lsblk para confirmar el nombre de la partición y asegúrese de escribir un espacio entre el nombre del dispositivo y el número de partición.
- `NOCHANGE: partition 1 is size 16773087. it cannot be grown`: indica que la partición ya amplía todo el volumen y no se puede ampliar. Confirme que la modificación del volumen se haya realizado correctamente.

d. Compruebe que la partición se haya ampliado. Utilice el comando lsblk. El tamaño de la partición ahora debe ser igual al tamaño del volumen.

Nitro instance example

En el siguiente resultado de ejemplo se muestra que el volumen (`nvme0n1`) y la partición (`nvme0n1p1`) tienen el mismo tamaño (`16 GB`).

```
[ec2-user ~]$ sudo lsblk
NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme1n1       259:0    0  30G  0 disk /data
nvme0n1       259:1    0  16G  0 disk
##nvme0n1p1   259:2    0  16G  0 part /
##nvme0n1p128 259:3    0   1M  0 part
```

Xen instance example

En el siguiente resultado de ejemplo se muestra que el volumen (`xvda`) y la partición (`xvda1`) tienen el mismo tamaño (`16 GB`).

```
[ec2-user ~]$ sudo lsblk
NAME    MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvda    202:0    0  16G  0 disk
##xvda1 202:1    0  16G  0 part /
xvdf    202:80   0  24G  0 disk
```

3. Amplíe el sistema de archivos.

   a. Obtenga el nombre, el tamaño, el tipo y el punto de montaje del sistema de archivos que necesita ampliar. Utilice el comando df -hT.

   Nitro instance example

   En el siguiente resultado de ejemplo se muestra que el sistema de archivos `/dev/nvme0n1p1` tiene un tamaño de 8 GB, su tipo es `xfs` y su punto de montaje es `/`.

   ```
   [ec2-user ~]$ df -hT
   Filesystem      Type  Size  Used Avail Use% Mounted on
   /dev/nvme0n1p1  xfs   8.0G  1.6G  6.5G  20% /
   /dev/nvme1n1    xfs   8.0G   33M  8.0G   1% /data
   ...
   ```

   Xen instance example

   En el siguiente resultado de ejemplo se muestra que el sistema de archivos `/dev/xvda1` tiene un tamaño de 8 GB, su tipo es `ext4` y su punto de montaje es `/`.

   ```
   [ec2-user ~]$ df -hT
   Filesystem      Type   Size    Used   Avail   Use%   Mounted on
   /dev/xvda1      ext4   8.0G    1.9G   6.2G    24%    /
   /dev/xvdf1      xfs    24.0G   45M    8.0G    1%     /data
   ...
   ```

   b. Los comandos para ampliar el sistema de archivos varían según el tipo de sistema de archivos. Elija el siguiente comando correcto según el tipo de sistema de archivos que anotó en el paso anterior.

- [Sistema de archivos XFS] Utilice el comando xfs_growfs y especifique el punto de montaje del sistema de archivos que anotó en el paso anterior.

  Nitro and Xen instance example

  Por ejemplo, para ampliar un sistema de archivos montado en `/`, utilice el siguiente comando.

  ```
  [ec2-user ~]$ sudo xfs_growfs -d /
  ```

  Consejos para la solución de problemas

  - `xfs_growfs: /data is not a mounted XFS filesystem`: indica que especificó el punto de montaje incorrecto o que el sistema de archivos no es XFS. Para verificar el punto de montaje y el tipo de sistema de archivos, utilice el comando df -hT.
  - `data size unchanged, skipping`: indica que el sistema de archivos ya amplía todo el volumen. Si el volumen no tiene particiones, confirme que la modificación del volumen se haya realizado correctamente. Si el volumen tiene particiones, asegúrese de que la partición se haya ampliado como se describe en el paso 2.

- [Sistema de archivos Ext4] Utilice el comando resize2fs y especifique el nombre del sistema de archivos que anotó en el paso anterior.

  Nitro instance example

  Por ejemplo, para ampliar un sistema de archivos montado denominado `/dev/nvme0n1p1`, utilice el siguiente comando.

  ```
  [ec2-user ~]$ sudo resize2fs /dev/nvme0n1p1
  ```

  Xen instance example

  Por ejemplo, para ampliar un sistema de archivos montado denominado `/dev/xvda1`, utilice el siguiente comando.

  ```
  [ec2-user ~]$ sudo resize2fs /dev/xvda1
  ```

> Consejos para la solución de problemas
>
> - `resize2fs: Bad magic number in super-block while trying to open /dev/xvda1`: indica que el sistema de archivos no es Ext4. Para verificar el tipo de sistema de archivos, utilice el comando df -hT.
> - `open: No such file or directory while opening /dev/xvdb1`: indica que especificó una partición incorrecta. Para verificar la partición, utilice el comando df -hT.
> - `The filesystem is already 3932160 blocks long. Nothing to do!`: indica que el sistema de archivos ya amplía todo el volumen. Si el volumen no tiene particiones, confirme que la modificación del volumen se haya realizado correctamente. Si el volumen tiene particiones, asegúrese de que la partición se haya extendido, como se describe en el paso 2.

- [Otro sistema de archivos] Consulte la documentación del sistema de archivos para obtener instrucciones.

c. Compruebe que el sistema de archivos se haya ampliado. Utilice el comando df -hT y confirme que el tamaño del sistema de archivos sea igual al tamaño del volumen.

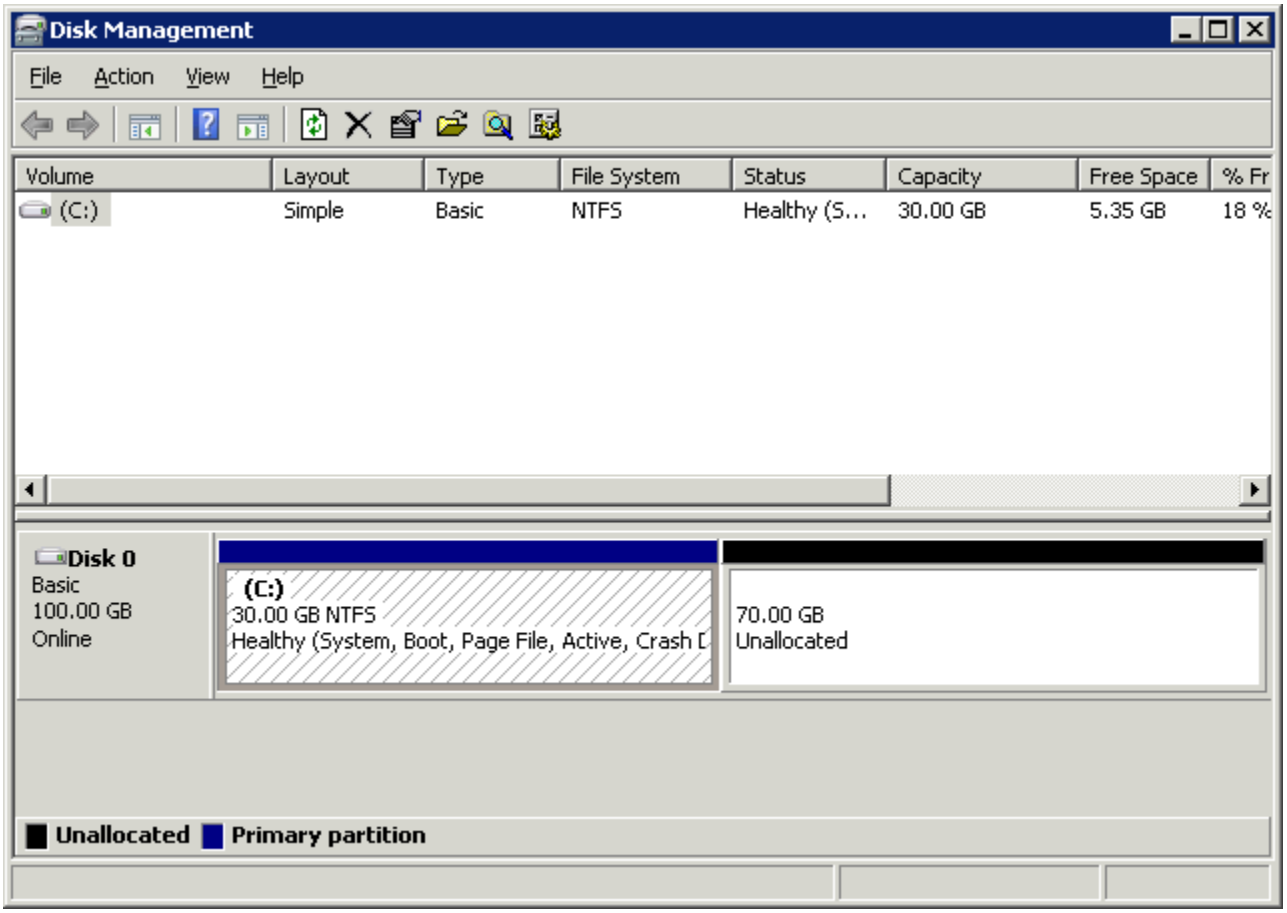
instancias de Windows

Utilice uno de los siguientes métodos para extender el sistema de archivos en una instancia de Windows.

Disk Management utility

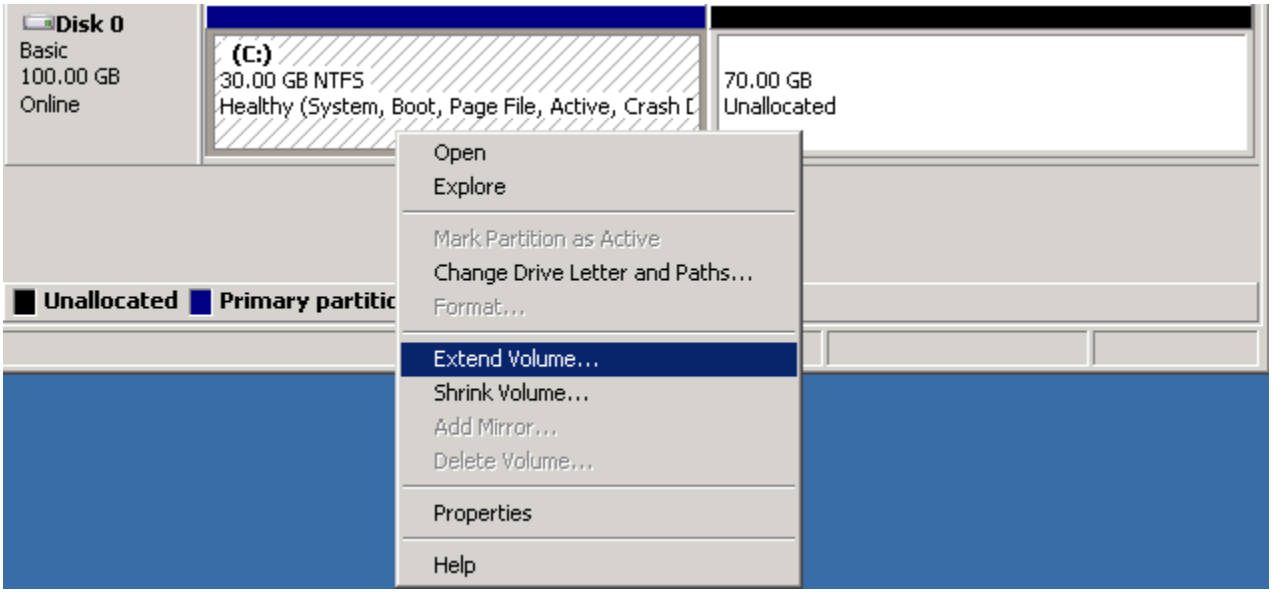
Para ampliar un sistema de archivos mediante Administración de discos

1. Antes de ampliar un sistema de archivos que contiene datos valiosos, una práctica recomendada consiste en crear una instantánea del volumen que lo contiene por si más adelante fuera necesario revertir los cambios. Para obtener más información, consulte Crear instantáneas de Amazon EBS.
2. Inicie sesión en la instancia de Windows mediante el Escritorio remoto.
3. En el cuadro de diálogo Run (Ejecutar), escriba diskmgmt.msc y pulse Enter (Intro). Se abre la utilidad Administración de discos.

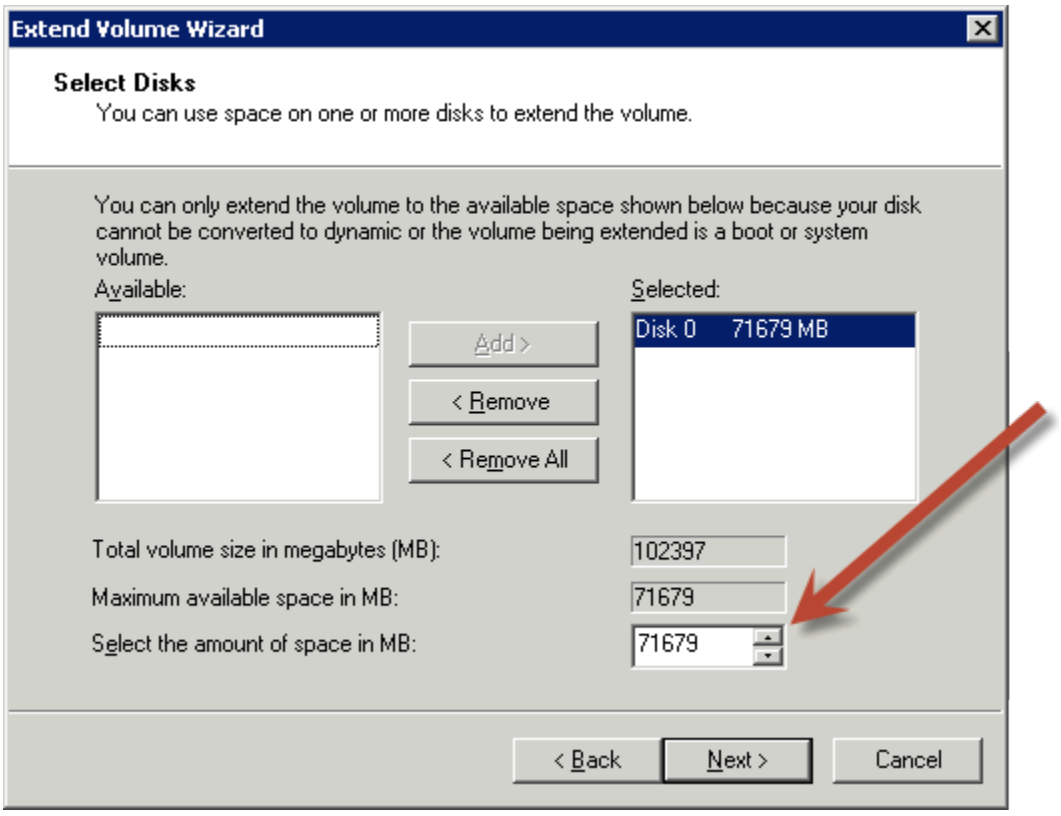


4. En el menú de Administración de discos, elija Acción, Volver a examinar los discos.
5. Abra el menú contextual de la unidad ampliada (haga clic con el botón derecho) y elija Extender volumen.

> **Note**
>
> Extender volumen podría estar deshabilitado (atenuado) si:
>
> - El espacio no asignado no está adyacente a la unidad. El espacio no asignado debe ser contiguo al lado correcto de la unidad que desea extender.
> - El volumen utiliza el estilo de partición Registro de arranque maestro (MBR) y ya tiene un tamaño de 2 TB. Los volúmenes que utilizan MBR no pueden superar los 2 TB de tamaño.



6. En el asistente Extend Volume (Ampliar volumen), elija Next (Siguiente). Para Seleccione la cantidad de espacio (MB), escriba el número de megabytes en que desea ampliar el volumen. Normalmente, se especifica el espacio máximo disponible. El texto resaltado en Seleccionado es la cantidad de espacio que se añade y no el tamaño final que tendrá el volumen. Complete el asistente.



7. Si aumenta el tamaño de un volumen NVMe en una instancia que no tiene el controlador NVMe de AWS , debe reiniciar la instancia para que Windows pueda ver el nuevo tamaño del volumen. Para obtener más información sobre la instalación del controlador AWS NVMe, consulte Controladores AWS NVMe para instancias de Windows.

PowerShell

Utilice el siguiente procedimiento para ampliar un sistema de archivos de Windows mediante. PowerShell

Para ampliar un sistema de archivos mediante PowerShell

1. Antes de ampliar un sistema de archivos que contiene datos valiosos, una práctica recomendada consiste en crear una instantánea del volumen que lo contiene por si más adelante fuera necesario revertir los cambios. Para obtener más información, consulte Crear instantáneas de Amazon EBS.
2. Inicie sesión en la instancia de Windows mediante el Escritorio remoto.
3. Ejecute PowerShell como administrador.
4. Ejecute el `Get-Partition` comando. PowerShell devuelve el número de partición correspondiente a cada partición, la letra de la unidad, el desplazamiento, el tamaño y el tipo. Anote la letra de unidad de la partición que va a ampliar.
5. Para volver a analizar el disco, ejecute el siguiente comando:

```
"rescan" | diskpart
```

6. Ejecute el siguiente comando, utilizando la letra de unidad que anotó en el paso 4 en lugar de**<drive-letter>**. PowerShell devuelve el tamaño mínimo y máximo de la partición permitido, en bytes.

```
Get-PartitionSupportedSize -DriveLetter <drive-letter>
```

7. Para ampliar la partición a una cantidad especificada, ejecute el siguiente comando, que especifica el nuevo tamaño del volumen en lugar de **<size>**. Puede especificar el tamaño en `KB`, `MB` y `GB` (por ejemplo, `50GB`).

```
Resize-Partition -DriveLetter <drive-letter> -Size <size>
```

Para ampliar la partición al tamaño máximo disponible, ejecute el siguiente comando.

```
Resize-Partition -DriveLetter <drive-letter> -Size $(Get-PartitionSupportedSize
 -DriveLetter <drive-letter>).SizeMax
```

Los siguientes PowerShell comandos muestran el flujo completo de comandos y respuestas para extender un sistema de archivos a un tamaño específico.

```
PS C:\> Get-Partition


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&26a12046&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                C           1048576                                     30 GB IFS


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&3476342 3&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                D           1048576                                     8 MB IFS


PS C:\> "rescan" | diskpart

Microsoft DiskPart version 10.0.17763.1911

Copyright (C) Microsoft Corporation.
On computer:

DISKPART>
Please wait while DiskPart scans your configuration...

DiskPart has finished scanning your configuration.

DISKPART>
PS C:\> Get-PartitionSupportedSize -DriveLetter D

SizeMin      SizeMax
-------      -------
8388608 107372085248


PS C:\> Resize-Partition -DriveLetter D -Size 50GB
PS C:\> Get-Partition


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&26a12046&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                C           1048576                                     30 GB IFS


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&3476342 3&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                D           1048576                                     50 GB IFS
```

Los siguientes PowerShell comandos muestran el flujo completo de comandos y respuestas para extender un sistema de archivos al tamaño máximo disponible.

```
PS C:\> Get-Partition


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&26a12046&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                C           1048576                                     30 GB IFS


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&3476423&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                D           1048576                                     50 GB IFS


PS C:\> "rescan" | diskpart

Microsoft DiskPart version 10.0.17763.1911

Copyright (C) Microsoft Corporation.
On computer:

DISKPART>
Please wait while DiskPart scans your configuration...

DiskPart has finished scanning your configuration.

DISKPART>
PS C:\> Get-PartitionSupportedSize -DriveLetter D

 SizeMin      SizeMax
 -------      -------
59047936 107372085248


PS C:\> Resize-Partition -DriveLetter D -Size $(Get-PartitionSupportedSize -DriveLetter D).SizeMax
PS C:\> Get-Partition


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&26a12046&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                C           1048576                                     30 GB IFS


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&3476423&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                D           1048576                                    100 GB IFS
```

Cómo separar un volumen de Amazon EBS de una instancia

Debe desconectar un volumen de Amazon Elastic Block Store (Amazon EBS) de una instancia antes de poder adjuntarlo a otra instancia o eliminarlo. La desasociación de un volumen no afecta a sus datos.

Temas

- Consideraciones
- Desmontar y desasociar un volumen

- Solución de problemas

Consideraciones

- Puede separar un volumen de Amazon EBS de una instancia explícitamente o terminando la instancia. No obstante, si la instancia se está ejecutando, primero debe desmontar el volumen de la instancia.
- Si un volumen de EBS es el dispositivo raíz de una instancia, debe detener la instancia antes de poder separar el volumen.
- Puede volver a asociar un volumen que ha desasociado (sin desmontarlo), pero puede que no llegue al mismo punto de montaje. Si existían escrituras en el volumen en curso cuando se desasoció, los datos del volumen pueden estar fuera de sincronización.
- Después de separar un volumen, se le seguirá cobrando por el almacenamiento por volumen siempre que la cantidad de almacenamiento supere el límite de la capa AWS gratuita. Para evitar incurrir en más cargos, debe eliminar el volumen. Para obtener más información, consulte Eliminar un volumen Amazon EBS.

Desmontar y desasociar un volumen

Utilice los siguientes procedimientos para desmontar y desconectar un volumen de una instancia. Esto puede ser útil cuando necesita adjuntar el volumen a una instancia diferente o cuando necesita eliminar el volumen.

Pasos

- Paso 1: Desmonte el volumen.
- Paso 2: Desconectar el volumen de la instancia
- Paso 3: (Solo instancias de Windows) desinstale las ubicaciones de dispositivos sin conexión

Paso 1: Desmonte el volumen.

instancias de Linux

Desde su instancia de Linux, utilice el siguiente comando para desmontar el dispositivo `/dev/sdh`.

```
[ec2-user ~]$ sudo umount -d /dev/sdh
```

instancias de Windows

En la instancia de Windows, desmonte el volumen como se indica a continuación.

1. Inicie la utilidad de Administración de discos.
   - (En Windows Server 2012 y versiones posteriores) En la barra de tareas, haga clic con el botón derecho en el logotipo de Windows y, a continuación, elija Administración de discos.
   - (En Windows Server 2008) Elija Inicio, Herramientas administrativas, Administración informática, Administración de disco.
2. Haga clic con el botón derecho (por ejemplo, haga clic con el botón derecho en Disk 1 [Disco 1]) y, a continuación, elija Offline (Sin conexión). Espere a que el estado del disco cambie a Offline (Sin conexión) antes de abrir la consola de Amazon EC2.

Paso 2: Desconectar el volumen de la instancia

Para desconectar el volumen de la instancia, utilice uno de los métodos siguientes:

Console

Para separar un volumen de EBS con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Volumes (Volúmenes).
3. Seleccione el volumen que desea desconectar y elija Actions (Acciones), Detach Volume (Desconectar volumen).
4. Cuando se le indique que confirme, elija Desasociar.

AWS CLI

Para separar un volumen de EBS de una instancia mediante el AWS CLI

Tras desmontar el volumen, utilice el comando detach-volume.

Tools for Windows PowerShell

Para separar un volumen de EBS de una instancia mediante las Herramientas de Windows PowerShell

Tras desmontar el volumen, utilice el comando. Dismount-EC2Volume

Paso 3: (Solo instancias de Windows) desinstale las ubicaciones de dispositivos sin conexión

Cuando desmonta y desconecta un volumen de una instancia, Windows marca la ubicación del dispositivo como sin conexión. La ubicación del dispositivo permanece sin conexión después de reiniciar y detener y reiniciar la instancia. Al reiniciar la instancia, Windows puede montar uno de los volúmenes restantes en la ubicación del dispositivo sin conexión. Esto hace que el volumen no esté disponible en Windows. Para evitar que esto ocurra y asegurarse de que todos los volúmenes estén conectados a ubicaciones de dispositivos en línea la próxima vez que se inicie Windows, realice los siguientes pasos:

1. En la instancia, abra el Administrador de dispositivos.
2. En el Administrador de dispositivos, seleccione Ver, Mostrar dispositivos ocultos.
3. En la lista de dispositivos, expanda el nodo Controladores de almacenamiento.

   Las ubicaciones de los dispositivos en las que se montaron los volúmenes desconectados se denominan `AWS NVMe Elastic Block Storage Adapter` y deben aparecer atenuadas.
4. Haga clic con el botón derecho en cada ubicación de dispositivo atenuada denominada `AWS NVMe Elastic Block Storage Adapter`, seleccione Uninstall device (Desinstalar dispositivo) y elija Uninstall (Desinstalar).

   > **Important**
   >
   > No active la casilla de verificación Eliminar el software del controlador para este dispositivo.

Solución de problemas

A continuación se muestran algunos problemas comunes a la hora de separar volúmenes y cómo resolverlos.

> **Note**
>
> Para protegerse frente a una posible pérdida de datos, tome una instantánea del volumen antes de intentar desmontarlo. La separación forzada de un volumen bloqueado puede provocar daños en el sistema de archivos o en los datos que contiene y puede impedir que

se adjunte un nuevo volumen utilizando el mismo nombre de dispositivo, a menos que se reinicie la instancia.

- Si tiene problemas al desasociar un volumen a través de la consola de Amazon EC2, podría resultarle útil utilizar el comando describe-volumes de la CLI para diagnosticar el problema. Para obtener más información, consulte describe-volumes.
- Si el volumen permanece en estado `detaching`, puede forzar su separación eligiendo Force Detach (Forzar desvinculación de volumen). Utilice esta opción solo como último recurso para separar un volumen de una instancia fallida o si desea separar un volumen con la intención de eliminarlo. La instancia no tiene la oportunidad de vaciar cachés ni metadatos de sistemas de archivos. Si utiliza esta opción, debe realizar los procedimientos de comprobación y reparación del sistema de archivos.
- Si ha intentado forzar la separación del volumen varias veces durante varios minutos y este permanece en estado `detaching`, puede enviar una solicitud de ayuda a AWS re:Post. Para ayudar a agilizar la solución, incluya el ID del volumen y describa los pasos que ha dado.
- Cuando intenta separar un volumen que aún está montado, este puede bloquearse y quedarse en estado `busy` mientras trata de separarse. El siguiente resultado del comando describe-volumes muestra un ejemplo de dicha condición:

```
"Volumes": [
    {
        "AvailabilityZone": "us-west-2b",
        "Attachments": [
            {
                "AttachTime": "2016-07-21T23:44:52.000Z",
                "InstanceId": "i-fedc9876",
                "VolumeId": "vol-1234abcd",
                "State": "busy",
                "DeleteOnTermination": false,
                "Device": "/dev/sdf"
            }
        ...
    }
]
```

Si se da este estado, la separación se puede demorar indefinidamente hasta que desmonte el volumen, fuerce la separación, reinicie la instancia o haga todo lo anterior.

Eliminar un volumen Amazon EBS

Cuando ya no necesite un volumen de Amazon EBS, puede eliminarlo. Al eliminar un volumen, sus datos se pierden y el volumen no se puede adjuntar a ninguna instancia. Antes de eliminarlo, puede almacenar una instantánea del volumen, que puede utilizar para recrear dicho volumen posteriormente.

> **Note**
>
> No se puede eliminar un volumen si está asociado a una instancia. Para eliminar un volumen, primero debe desconectarlo. Para obtener más información, consulte Cómo separar un volumen de Amazon EBS de una instancia.
> Puede comprobar si un volumen está asociado a una instancia. En la consola, en la página Volúmenes, puede ver el estado de los volúmenes.
>
> - Si un volumen está asociado a una instancia, está en el estado `in-use`.
> - Si un volumen está desconectado de una instancia, está en el estado `available`. Puede eliminar este volumen.

Puede eliminar un volumen de EBS utilizando alguno de los métodos siguientes.

Console

Para eliminar un volumen de EBS con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Volumes (Volúmenes).
3. Seleccione un volumen para eliminar y elija Actions (Acciones), Delete volume (Eliminar volumen).

   > **Note**
   >
   > Si Delete Volume (Eliminar volumen) se encuentra atenuado, el volumen está adjunto a una instancia. Debe desconectar el volumen de la instancia antes de poder eliminarlo.

4. En el cuadro de diálogo de confirmación, elija Eliminar.

AWS CLI

Para eliminar un volumen de EBS mediante el AWS CLI

Utilice el comando delete-volume.

Tools for Windows PowerShell

Para eliminar un volumen de EBS mediante las herramientas de Windows PowerShell

Utilice el comando Remove-EC2Volume.

Reemplazar un volumen Amazon EBS con una instantánea anterior

Las instantáneas de Amazon EBS son la herramienta de copia de seguridad preferida de Amazon EC2 por su velocidad, comodidad y precio. Cuando se crea un volumen a partir de una instantánea, se recrea el estado que tenía en un punto concreto del pasado con todos los datos guardados intactos hasta ese punto concreto. Si asocia un volumen creado a partir de una instantánea a una instancia, puede duplicar los datos entre las regiones, crear entornos de prueba, sustituir íntegramente un volumen de producción dañado o recuperar archivos y directorios específicos y transferirlos a otro volumen asociado. Para obtener más información, consulte Instantáneas de Amazon EBS.

Puede utilizar uno de los procedimientos siguientes para reemplazar un volumen de Amazon EBS por otro volumen creado a partir de una instantánea anterior de ese volumen.

Console

Reemplazo de un volumen mediante la consola

1. Cree un volumen a partir de la instantánea y anote el ID del nuevo volumen. Para obtener más información, consulte Creación de un volumen desde una instantánea.

   > **Note**
   >
   > Procure crear el volumen en la misma zona de disponibilidad que la instancia. Los volúmenes solo se pueden asociar a instancias que se encuentren en la misma zona de disponibilidad.

2. En la página de las instancias, seleccione la instancia en la que desea reemplazar el volumen y escriba el ID de instancia.

Con la instancia aún seleccionada, elija la pestaña Storage (Almacenamiento). En el sección Block devices (Dispositivos de bloques), busque el volumen que se va a reemplazar y escriba el nombre del dispositivo del volumen, por ejemplo `/dev/sda1`.

Elija el ID de volumen.

3. En la pantalla Volumes (Volúmenes), seleccione el volumen y elija Actions (Acciones), Detach volume (Desconectar volumen), Detach (Desconectar).
4. Seleccione el nuevo volumen que creó en el paso 1 y elija Actions (Acciones), Attach volume (Adjuntar volumen).

   En Instance (Instancia) y Device name (Nombre del dispositivo), ingrese el ID de instancia y el nombre del dispositivo que escribió en el paso 2 y, a continuación, elija Attach volume (Adjuntar volumen).
5. Conéctese a la instancia y monte el volumen. Para obtener más información, consulte Cómo hacer que un volumen de Amazon EBS esté disponible para su uso.

AWS CLI

Para reemplazar un volumen mediante el AWS CLI

1. Cree un nuevo volumen a partir de la instantánea. Utilice el comando create-volume. En `--snapshot-id`, especifique el ID de la instantánea que se va a usar. En `--availability-zone`, especifique la misma zona de disponibilidad que la de la instancia. Configure los demás parámetros según sea necesario.

   > **Note**
   >
   > Procure crear el volumen en la misma zona de disponibilidad que la instancia. Los volúmenes solo se pueden asociar a instancias que se encuentren en la misma zona de disponibilidad.

```
$ aws ec2 create-volume \
--volume-type volume_type \
--size volume_size \
--snapshot-id snapshot_id \
```

```
--availability-zone az_id
```

En la salida del comando, observe el ID del nuevo volumen.

2. Obtenga el nombre del dispositivo del volumen que se va a reemplazar. Utilice el comando describe-instances. En `--instance-ids`, especifique el ID de la instancia en la que desea reemplazar el volumen.

```
$ aws ec2 describe-instances --instance-ids instance_id
```

En `BlockDeviceMappings`, en la salida del comando, observe los valores de `DeviceName` y `VolumeId` del volumen que se va a reemplazar.

3. Desasocie el volumen que se va a reemplazar de la instancia. Utilice el comando detach-volume. En `--volume-id`, especifique el ID del volumen que se va a desasociar.

```
$ aws ec2 detach-volume --volume-id volume_id
```

4. Asocie el volumen de reemplazo a la instancia. Utilice el comando attach-volume. En `--volume-id`, especifique el ID del volumen de reemplazo. En `--instance-id`, especifique el ID de la instancia a la que se va a asociar el volumen. En `--device`, especifique el mismo nombre de dispositivo que anotó anteriormente.

```
$ aws ec2 attach-volume \
--volume-id volume_id \
--instance-id instance_id \
--device device_name
```

5. Conéctese a la instancia y monte el volumen. Para obtener más información, consulte Cómo hacer que un volumen de Amazon EBS esté disponible para su uso.

Monitoreo de los volúmenes de Amazon EBS

AWS proporciona automáticamente datos que se pueden utilizar para monitorear los volúmenes de Amazon EBS.

Contenido

- Utilizar un volumen dañado
- Utilizar el atributo de volumen de E/S habilitada automáticamente

Para obtener más información sobre monitorización, consulte CloudWatch Métricas de Amazon para Amazon EBS y Amazon EventBridge para Amazon EBS.

Comprobaciones de estado de volumen de EBS

Las comprobaciones del estado del volumen le permiten conocer, seguir y administrar mejor las posibles incoherencias en los datos de un volumen de Amazon EBS. Están diseñadas para ofrecerle la información que necesita para determinar si los volúmenes de Amazon EBS están dañados y para ayudarle a controlar la forma de gestionar un volumen potencialmente incoherente.

Las comprobaciones de estado del volumen son pruebas automáticas que se realizan cada 5 minutos y que devuelven el estado correcto o incorrecto. Si se pasan todas las comprobaciones, el estado del volumen es `ok`. Si una comprobación falla, el estado del volumen es `impaired`. Si el estado es `insufficient-data`, es posible que aún se estén realizando comprobaciones en el volumen. Puede ver los resultados de las comprobaciones de estado del volumen para identificar volúmenes dañados y tomar cualquier medida que sea necesaria.

Cuando Amazon EBS determina que los datos de un volumen son potencialmente incoherentes, deshabilita de manera predeterminada la E/S del volumen de cualquier instancia EC2 adjunta, lo que ayuda a evitar que se dañen los datos. Después de deshabilitar la E/S, la siguiente comprobación del estado del volumen falla y el estado del volumen es `impaired`. Asimismo, verá un evento que le permite saber si esa E/S está deshabilitada y que puede resolver el estado "impaired" del volumen habilitando la E/S en el volumen. Esperamos a que habilite la E/S para darle la oportunidad de decidir si desea continuar permitiendo que las instancias utilicen el volumen, o de realizar antes una comprobación de coherencia utilizando un comando, como fsck (instancias de Linux) o chkdsk (instancias de Windows).

> **Note**
>
> El estado del volumen se basa en las comprobaciones del estado del volumen y no refleja el estado del volumen. Por lo tanto, el estado del volumen no indica los volúmenes que se encuentran en el estado `error` (por ejemplo, cuando un volumen es incapaz de aceptar E/S). Para obtener información acerca de los estados de los volúmenes, consulte Estados del volumen.

Si la uniformidad de un volumen en particular no es un problema y prefiere que el volumen esté disponible de inmediato si se ha deteriorado, puede anular el comportamiento predeterminado configurando el volumen para que habilite automáticamente las E/S. Si habilita el atributo de volumen Auto-Enable IO (Activación automática de E/S) (en la API `autoEnableIO`), la comprobación de estado del volumen se seguirá aprobando. Asimismo, verá un evento que le permite saber que se ha determinado que el volumen es potencialmente incoherente, pero que su E/S se ha habilitado automáticamente. Esto le permite comprobar la coherencia del volumen o reemplazarlo posteriormente.

La comprobación del estado de rendimiento de E/S compara el rendimiento real del volumen con el rendimiento esperado de un volumen. Le avisa si el volumen está funcionando por debajo de las expectativas. Esta comprobación de estado solo está disponible para los volúmenes de SSD de IOPS provisionadas (`io1` y `io2`) y SSD de uso general (`gp3`) que están adjuntos a una instancia. La comprobación de estado no es válida para los volúmenes de SSD de uso general (`gp2`), de HDD con rendimiento optimizado (`st1`), de HDD en frío (`sc1`) o magnéticos (`standard`). La comprobación del estado del rendimiento de E/S se realiza una vez cada minuto y CloudWatch recopila estos datos cada 5 minutos. Puede tardar hasta 5 minutos desde el momento en que se adjunta un volumen `io1` o `io2` a una instancia para que la comprobación de estado informe sobre el estado del rendimiento de E/S.

> **Important**
>
> Cuando se inicializan volúmenes Provisioned IOPS SSD que se restauraron a partir de instantáneas, el rendimiento del volumen puede descender por debajo del 50 % del nivel esperado, lo que causa que el volumen muestre un estado `warning` en la comprobación de estado de I/O Performance (Rendimiento de E/S). Este comportamiento es el esperado y puede hacer caso omiso del estado `warning` en los volúmenes Provisioned IOPS SSD cuando se están inicializando. Para obtener más información, consulte Inicializar de volúmenes de Amazon EBS.

En la siguiente tabla, se muestran los estados de los volúmenes de Amazon EBS.

Estado del volumen	Estado de habilitación de E/S	Comprobación del estado de E/S (solo volúmenes **io1**, **io2** y **gp3**)
ok	Habilitado (E/S habilitada o E/S habilitada automáticamente)	Normal (rendimiento del volumen esperado)
warning	Habilitado (E/S habilitada o E/S habilitada automáticamente)	Degradado (rendimiento del volumen por debajo de las expectativas) Gravemente degradado (rendimiento del volumen muy por debajo de las expectativas)
impaired	Habilitado (E/S habilitada o E/S habilitada automáticamente) Deshabilitado (el volumen está fuera de línea y pendiente de recuperación o bien está esperando a que el usuario habilite la E/S)	Parado (rendimiento del volumen gravemente afectado) No disponible (no se puede determinar el rendimiento de E/S porque la E/S está deshabilitada)
insufficient-data	Habilitado (E/S habilitada o E/S habilitada automáticamente) Datos insuficientes	Datos insuficientes

Puede ver y trabajar con comprobaciones de estado utilizando los métodos siguientes.

Console

Para ver comprobaciones de estado

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Volumes (Volúmenes).

En la columna Volumen status (Estado del volumen), se muestra el estado operativo de cada volumen.

3. Para ver los detalles del estado de un volumen, seleccione el volumen en la cuadrícula y elija Status checks (Verificaciones de estado).
4. Si tiene un volumen con una verificación de estado no superada (el estado es `impaired`), consulte Utilizar un volumen dañado.

También puede utilizar Events (Eventos en el navegador o ver todos los eventos de sus instancias y volúmenes. Para obtener más información, consulte Eventos de volumen de EBS.

AWS CLI

Para ver la información de estado del volumen

Utilice el comando describe-volume-status.

Para obtener más información acerca de estas interfaces de la línea de comandos, consulte Acceso a Amazon EC2.

Tools for Windows PowerShell

Para ver la información de estado del volumen

Utilice el comando Get-EC2VolumeStatus.

Para obtener más información acerca de estas interfaces de la línea de comandos, consulte Acceso a Amazon EC2.

Eventos de volumen de EBS

Cuando Amazon EBS determina que los datos de un volumen son potencialmente incoherentes, deshabilita la E/S del volumen de todas las instancias EC2 adjuntadas de manera predeterminada. Esto hace que la comprobación del estado del volumen genere un error y crea un evento de estado del volumen que indica la causa del error.

Para habilitar automáticamente la E/S en un volumen con potenciales incoherencias de datos, cambie el ajuste del atributo de volumen Auto-Enabled IO (E/S habilitada automáticamente) (`autoEnableIO` en la API). Para obtener más información acerca del cambio de este atributo, consulte Utilizar un volumen dañado.

Cada evento incluye una hora de inicio que indica la hora a la que se ha producido el evento y una duración que indica cuánto tiempo estuvo deshabilitada la E/S del volumen. La hora de finalización se añade al evento cuando se habilita la E/S del volumen.

Los eventos de estado del volumen incluyen una de las siguientes descripciones:

`Awaiting Action: Enable IO`

Los datos del volumen son potencialmente incoherentes. La E/S se deshabilita para el volumen hasta que se habilite explícitamente. La descripción del evento cambia a IO Enabled después de habilitar explícitamente la E/S.

`IO Enabled`

Las operaciones de E/S se han habilitado explícitamente para este volumen.

`IO Auto-Enabled`

Las operaciones de E/S se han habilitado automáticamente en este volumen después de que se haya producido un evento. Le recomendamos que compruebe las incoherencias de los datos antes de continuar usándolos.

`Normal`

Solo para volúmenes `io1`, `io2` y `gp3`. El rendimiento del volumen es el esperado.

`Degraded`

Solo para volúmenes `io1`, `io2` y `gp3`. El rendimiento del volumen está por debajo de las expectativas.

`Severely Degraded`

Solo para volúmenes `io1`, `io2` y `gp3`. El rendimiento del volumen está muy por debajo de las expectativas.

`Stalled`

Solo para volúmenes `io1`, `io2` y `gp3`. El rendimiento del volumen está gravemente afectado.

Puede ver los eventos de los volúmenes utilizando los métodos siguientes.

Console

Para ver eventos de sus volúmenes

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Events. Se enumeran todas las instancias y volúmenes que tienen eventos.
3. Puede filtrar por volumen para ver únicamente los estados de los volúmenes. También puede filtrar por tipos de estados específicos.
4. Seleccione un volumen para ver su evento específico.

AWS CLI

Para ver eventos de sus volúmenes

Utilice el comando describe-volume-status.

Para obtener más información acerca de estas interfaces de la línea de comandos, consulte Acceso a Amazon EC2.

Tools for Windows PowerShell

Para ver eventos de sus volúmenes

Utilice el comando Get-EC2VolumeStatus.

Para obtener más información acerca de estas interfaces de línea de comandos, consulte Acceso a Amazon EC2.

Si tiene un volumen en el que la E/S está deshabilitada, consulte Utilizar un volumen dañado. Si tiene un volumen en el que el rendimiento de E/S está por debajo de lo normal, podría tratarse de un problema temporal debido a una acción que ha realizado (como crear una instantánea de un volumen durante un pico de uso, ejecutar el volumen en una instancia que no permite el ancho de banda de E/S que es necesario, obtener acceso a los datos del volumen por primera vez, etc.).

Utilizar un volumen dañado

Utilice las siguientes opciones de las que dispone si un volumen está dañado a causa de que los datos de dicho volumen son potencialmente incoherentes.

Opciones

- Opción 1: Realizar una comprobación de coherencia en el volumen asociado a su instancia
- Opción 2: Realizar una comprobación de coherencia en el volumen utilizando otra instancia
- Opción 3: Eliminar el volumen si ya no lo necesita

Opción 1: Realizar una comprobación de coherencia en el volumen asociado a su instancia

La opción más sencilla es habilitar la E/S y luego realizar una comprobación de coherencia de los datos en el volumen mientras que este sigue adjuntado a la instancia Amazon EC2.

Para realizar una comprobación de coherencia en el volumen adjuntado

1. Haga que las aplicaciones que estén usando el volumen dejen de hacerlo.
2. Habilite la E/S en el volumen. Utilice alguno de los métodos siguientes.

   Console

   1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
   2. En el panel de navegación, seleccione Events (Eventos).
   3. Seleccione el volumen en el que va a habilitar las operaciones de E/S.
   4. Elija Actions (Acciones), Enable I/O (Habilitar E/S).

   AWS CLI

   Habilitación de la E/S de un volumen con la AWS CLI

   Utilice el comando enable-volume-io.

   Tools for Windows PowerShell

   Habilitación de la E/S de un volumen mediante Herramientas para Windows PowerShell

   Utilice el comando Enable-EC2VolumeIO.
3. Compruebe los datos del volumen.

   a. Ejecute el comando fsck (instancias de Linux) o chkdsk (instancias de Windows).

b. (Opcional) Revise cualquier aplicación o registros del sistema disponibles para comprobar los mensajes de error relevantes.

c. Si el volumen lleva dañado más de 20 minutos, puede ponerse en contacto con el Centro de soporte de AWS. Elija Troubleshoot (Solucionar problemas) y, a continuación, en el cuadro de diálogo Troubleshoot Status Checks (Solucionar problemas con las comprobaciones de estado), elija Contact Support (Contactar con el soporte) para enviar un caso de soporte.

Opción 2: Realizar una comprobación de coherencia en el volumen utilizando otra instancia

Utilice el procedimiento siguiente para comprobar el volumen fuera del entorno de producción.

> **Important**
>
> Este procedimiento puede producir la pérdida de E/S de escritura que estaba suspendida cuando se deshabilitó el volumen.

Para realizar una comprobación de coherencia en un volumen aislado

1. Haga que las aplicaciones que estén usando el volumen dejen de hacerlo.
2. Separe el volumen de la instancia. Para obtener más información, consulte Cómo separar un volumen de Amazon EBS de una instancia.
3. Habilite la E/S en el volumen. Utilice alguno de los métodos siguientes.

   Console

   1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
   2. En el panel de navegación, seleccione Events (Eventos).
   3. Seleccione el volumen que ha separado en el paso anterior.
   4. Elija Actions (Acciones), Enable I/O (Habilitar E/S).

   AWS CLI

   Habilitación de la E/S de un volumen con la AWS CLI

   Utilice el comando enable-volume-io.

Tools for Windows PowerShell

Habilitación de la E/S de un volumen mediante Herramientas para Windows PowerShell

Utilice el comando Enable-EC2VolumeIO.

4. Adjunte el volumen a otra instancia. Para obtener más información, consulte Lanzamiento de la instancia en Adjunte un volumen de Amazon EBS a una instancia..
5. Compruebe los datos del volumen.
   a. Ejecute el comando fsck (instancias de Linux) o chkdsk (instancias de Windows).
   b. (Opcional) Revise cualquier aplicación o registros del sistema disponibles para comprobar los mensajes de error relevantes.
   c. Si el volumen lleva dañado más de 20 minutos, puede ponerse en contacto con el Centro de soporte de AWS. Elija Troubleshoot (Solucionar problemas) y, a continuación, en el cuadro de diálogo de solución de problemas, elija Contact Support (Contactar con el soporte) para enviar un caso de soporte.

Opción 3: Eliminar el volumen si ya no lo necesita

Si desea quitar el volumen de su entorno, simplemente elimínelo. Para obtener información acerca de cómo eliminar un volumen, consulte Eliminar un volumen Amazon EBS.

Si dispone de una instantánea reciente que es una copia de seguridad de los datos del volumen, puede crear un volumen nuevo a partir de la instantánea. Para obtener más información, consulte Creación de un volumen desde una instantánea.

Utilizar el atributo de volumen de E/S habilitada automáticamente

Cuando Amazon EBS determina que los datos de un volumen son potencialmente incoherentes, deshabilita la E/S del volumen de todas las instancias EC2 adjuntadas de manera predeterminada. Esto hace que la comprobación del estado del volumen genere un error y crea un evento de estado del volumen que indica la causa del error. Si la consistencia de un volumen en particular no es un problema y prefiere que el volumen esté disponible de inmediato si se ha deteriorado, puede anular el comportamiento predeterminado configurando el volumen para que habilite automáticamente las E/S. Si habilita el atributo de volumen Auto-Enabled IO (Activación automática de E/S) (en la API `autoEnableIO`), las E/S entre el volumen y la instancia se volverán a habilitar de forma automática y la comprobación de estado del volumen se aprobará. Asimismo, verá un evento que le permite

saber que se ha determinado que el volumen estaba en un estado potencialmente incoherente, pero que su E/S se ha habilitado automáticamente. Cuando se produzca este evento, debería comprobar la coherencia del volumen y reemplazarlo si es necesario. Para obtener más información, consulte Eventos de volumen de EBS.

Puede ver y modificar el atributo Auto-Enabled IO (E/S habilitadas automáticamente) de un volumen mediante los métodos siguientes.

Amazon EC2 console

Para ver el atributo E/S habilitada automáticamente de un volumen

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Volumes (Volúmenes).
3. Seleccione el volumen y elija Status Checks (Verificaciones de estado).

   El campo Auto-enabled I/O (E/S habilitadas automáticamente) muestra la configuración actual (Enabled [Habilitada] o Disabled [Desactivada]) para el volumen seleccionado.

Para modificar el atributo E/S habilitada automáticamente de un volumen

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Volumes (Volúmenes).
3. Seleccione el volumen y elija Actions (Acciones), Manage auto-enabled I/O (Administrar E/S habilitadas automáticamente).
4. Seleccione la casilla de verificación Auto-Enable Volumen IO for impaired volumes (Habilitar de automáticamente la E/S del volumen deteriorado) para habilitar de forma automática la E/S de un volumen deteriorado. Para deshabilitar la característica, desactive la casilla de verificación.
5. Seleccione Actualizar.

AWS CLI

Para ver el atributo AutoEnableIO de un volumen

Utilice el comando describe-volume-attribute.

Modificación del atributo autoEnableIO de un volumen

Utilice el comando modify-volume-attribute.

Para obtener más información acerca de estas interfaces de la línea de comandos, consulte Acceso a Amazon EC2

Tools for Windows PowerShell

Para ver el atributo AutoEnableIO de un volumen

Utilice el comando Get-EC2VolumeAttribute.

Modificación del atributo autoEnableIO de un volumen

Utilice el comando Edit-EC2VolumeAttribute.

Para obtener más información acerca de estas interfaces de la línea de comandos, consulte Acceso a Amazon EC2

Pruebas de fallos en Amazon EBS

Utilice AWS Fault Injection Service y la acción Pausar la E/S para detener temporalmente la E/S entre un volumen de Amazon EBS y las instancias a las que está conectado para comprobar cómo sus cargas de trabajo gestionan las interrupciones de E/S. Con AWS FIS, puede usar experimentos controlados para probar su arquitectura y monitoreo, como las CloudWatch alarmas de Amazon y las configuraciones de tiempo de espera del sistema operativo, y mejorar la resiliencia ante los fallos de almacenamiento.

Para obtener más información al respecto AWS FIS, consulte la Guía del AWS Fault Injection Service usuario.

Consideraciones

Tenga en cuenta las siguientes consideraciones para pausar la E/S del volumen:

- Puede pausar la E/S de todos los tipos de volumen de Amazon EBS que estén asociados a instancias creadas en Nitro System.
- Puede pausar la E/S del volumen raíz.
- Puede pausar la E/S de volúmenes habilitados para Multi-Attach. Si pausa la E/S de un volumen habilitado para Multi-Attach, la E/S se pausará entre el volumen y todas las instancias a las que esté asociado.

- Para probar la configuración de tiempo de espera del sistema operativo, establezca que la duración del experimento sea igual al valor especificado para `nvme_core.io_timeout`, o superior. Para obtener más información, consulte Tiempo de espera de las operaciones de E/S.
- Si realiza la E/S en un volumen que tiene la E/S en pausa, sucede lo siguiente:
  - El estado del volumen pasa a `impaired` en un plazo de 120 segundos. Para obtener más información, consulte Monitoreo de los volúmenes de Amazon EBS.
  - Las CloudWatch métricas de longitud de cola (`VolumeQueueLength`) no serán cero. Cualquier alarma o supervisión debe monitorearse para detectar una profundidad de cola distinta de cero. Para más información, consulte Métricas para los volúmenes de Amazon EBS.
  - Las CloudWatch métricas correspondientes `VolumeReadOps` o lo `VolumeWriteOps` serán`0`, lo que indica que el volumen ya no procesa E/S.

Limitaciones

Tenga en cuenta las siguientes limitaciones para pausar la E/S del volumen:

- No se admiten volúmenes del almacén de instancias.
- No se admiten tipos de instancia basados en Xen.
- No puede pausar la E/S de los volúmenes creados en un puesto avanzado de AWS Outposts, en una AWS Wavelength zona o en una zona local.

Puede realizar un experimento básico desde la consola Amazon EC2 o puede realizar experimentos más avanzados con la AWS FIS consola. Para obtener más información sobre cómo realizar experimentos avanzados con la AWS FIS consola, consulte los tutoriales de AWS FIS la Guía del AWS Fault Injection Service usuario.

Para realizar un experimento básico con la consola de Amazon EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Volumes (Volúmenes).
3. Seleccione el volumen para el que quiera pausar la E/S y elija Acciones, Inyección de errores y Pausar operaciones de E/S de volumen.
4. En Duración, ingrese la duración de la pausa de E/S entre el volumen y las instancias. El campo situado junto a la lista desplegable Duración muestra la duración en formato ISO 8601.

5. En la sección Acceso al servicio, seleccione la función de servicio de IAM AWS FIS que debe asumir para realizar el experimento. Puede utilizar el rol predeterminado o un rol existente que haya creado. Para obtener más información, consulte Creación de un rol de IAM para experimentos de AWS FIS.
6. Elija Pausar operaciones de E/S de volumen. Cuando se le solicite, ingrese `start` en el campo de confirmación y elija Iniciar experimento.
7. Supervise el progreso y el impacto de su experimento. Para obtener más información, consulte Supervisión de AWS FIS en la Guía del usuario de AWS FIS .

Instantáneas de Amazon EBS

Puede hacer copias de seguridad de los datos de sus volúmenes de Amazon EBS mediante point-in-time copias, conocidas como instantáneas de Amazon EBS. Una instantánea es una copia de seguridad incremental, lo que significa que solo se guardan los bloques del dispositivo que han cambiado desde la instantánea más reciente. Esto disminuye el tiempo necesario para crearlo y ahorra costos de almacenamiento, ya que no se duplican los datos.

> **Important**
>
> AWS no hace copias de seguridad automáticas de los datos almacenados en sus volúmenes de EBS. Para garantizar la resiliencia de los datos y la recuperación de desastres, es su responsabilidad crear copias instantáneas de EBS de forma regular o configurar la creación automática de instantáneas mediante Administrador de vida útil de datos de Amazon o AWS Backup.

Las instantáneas de EBS se almacenan en Amazon S3, en buckets de S3 a los que no puede acceder directamente. Puede crear y administrar las instantáneas con la consola de Amazon EC2 o la API de Amazon EC2. No puede acceder a las instantáneas mediante la consola de Amazon S3 o la API de Amazon S3.

Cada instantánea contiene toda la información necesaria para restaurar los datos (del momento en que se tomó) en un volumen de EBS nuevo. Cuando se crea un volumen de EBS basado en una instantánea, el nuevo volumen comienza como una réplica exacta del volumen utilizado para crear la instantánea. El volumen replicado carga los datos en segundo plano para que pueda comenzar a utilizarlo inmediatamente. Si tiene acceso a datos que aún no se han cargado, el volumen descarga inmediatamente los datos solicitados de Amazon S3 y después continúa cargando el resto de los datos del volumen en segundo plano. Para obtener más información, consulte Crear instantáneas de Amazon EBS. Cuando se elimina una instantánea, solo se borran los datos que son únicos de dicha instantánea. Para obtener más información, consulte Eliminar una instantánea de Amazon EBS.

Para obtener más información, consulte la página del producto Instantáneas de Amazon EBS.

Eventos de instantáneas

Puede realizar un seguimiento del estado de sus instantáneas de EBS a través de Eventos. CloudWatch Para obtener más información, consulte Eventos de instantánea de EBS.

Instantáneas coherentes con las aplicaciones (solo instancias de Windows)

Puede utilizar Systems Manager Run Command para tomar instantáneas coherentes con la aplicación de todos los volúmenes de EBS asociados a sus instancias de Amazon EC2 de Windows. El proceso de instantáneas usa el servicio Volume Shadow Copy Service (VSS) de Windows para crear copias de seguridad de nivel de imagen de aplicaciones con reconocimiento de VSS, incluidos datos de transacciones pendientes entre dichas aplicaciones y el disco. No es necesario que apague sus instancias o las desconecte cuando respalde todos los volúmenes adjuntos. Para obtener más información, consulte Creación de una instantánea coherente con la aplicación de VSS.

Instantáneas de varios volúmenes

Las instantáneas se pueden utilizar para crear una copia de seguridad de las cargas de trabajo críticas, como una base de datos grande o un sistema de archivos que abarca varios volúmenes de EBS. Las instantáneas de varios volúmenes le permiten realizar instantáneas exactas point-in-time, coordinadas con los datos y coherentes con los fallos de varios volúmenes de EBS conectados a una instancia de EC2. Como las instantáneas se generan automáticamente en varios volúmenes de EBS, ya no es necesario detener la instancia ni coordinar entre volúmenes para garantizar la coherencia frente a bloqueos. Para obtener más información, consulte los pasos para crear una instantánea de EBS de varios volúmenes e Crear instantáneas de Amazon EBS .

Precios de las instantáneas

Los cargos por las instantáneas se basan en la cantidad de datos almacenados. Dado que las instantáneas son incrementales, es posible que la eliminación de una instantánea no reduzca los costos de almacenamiento de datos. Los datos a los que hace referencia exclusivamente una instantánea se eliminan cuando se elimina esa instantánea, pero se conservan los datos a los que hacen referencia otras instantáneas. Para obtener más información, consulte Volúmenes e instantáneas de Amazon Elastic Block Store en la Guía del usuario de AWS Billing .

Contenido

- Papelera de reciclaje para instantáneas
- Amazon EBS local snapshots on Outposts

Cómo funcionan las instantáneas

La primera instantánea que crea a partir de un volumen es siempre una instantánea completa. Incluye todos los bloques de datos escritos en el volumen en el momento en que se creó la instantánea. Las instantáneas posteriores del mismo volumen son instantáneas progresivas. Incluyen solo los bloques de datos nuevos y modificados escritos en el volumen desde que se creó la última instantánea

El tamaño de una instantánea completa viene determinado por el tamaño de los datos de los que se hace una copia de seguridad, no del tamaño del volumen de origen. Del mismo modo, los costos de almacenamiento asociados a una instantánea completa vienen determinados por el tamaño de la instantánea, no por el tamaño del volumen de origen. Por ejemplo, tiene que crear la primera instantánea de un volumen de Amazon EBS de `200 GiB` que solo contiene `50 GiB` de datos. Esto da como resultado una instantánea completa con un tamaño de `50 GiB` y se le facturará por el almacenamiento de instantáneas de `50 GiB`.

Del mismo modo, el tamaño y los costos de almacenamiento de una instantánea progresiva vienen determinados por el tamaño de los datos que se hayan escrito en el volumen desde que se creó la instantánea anterior. Siguiendo con este ejemplo, si crea una segunda instantánea del volumen de `200 GiB` después de modificar `20 GiB` de datos y agregar `10 GiB` de datos, la instantánea progresiva tendrá un tamaño de `30 GiB`. Por lo tanto, se le facturará por ese almacenamiento de instantáneas de `30 GiB` adicionales.

Para obtener más información sobre los precios de las instantáneas, consulte Precios de Amazon EBS.

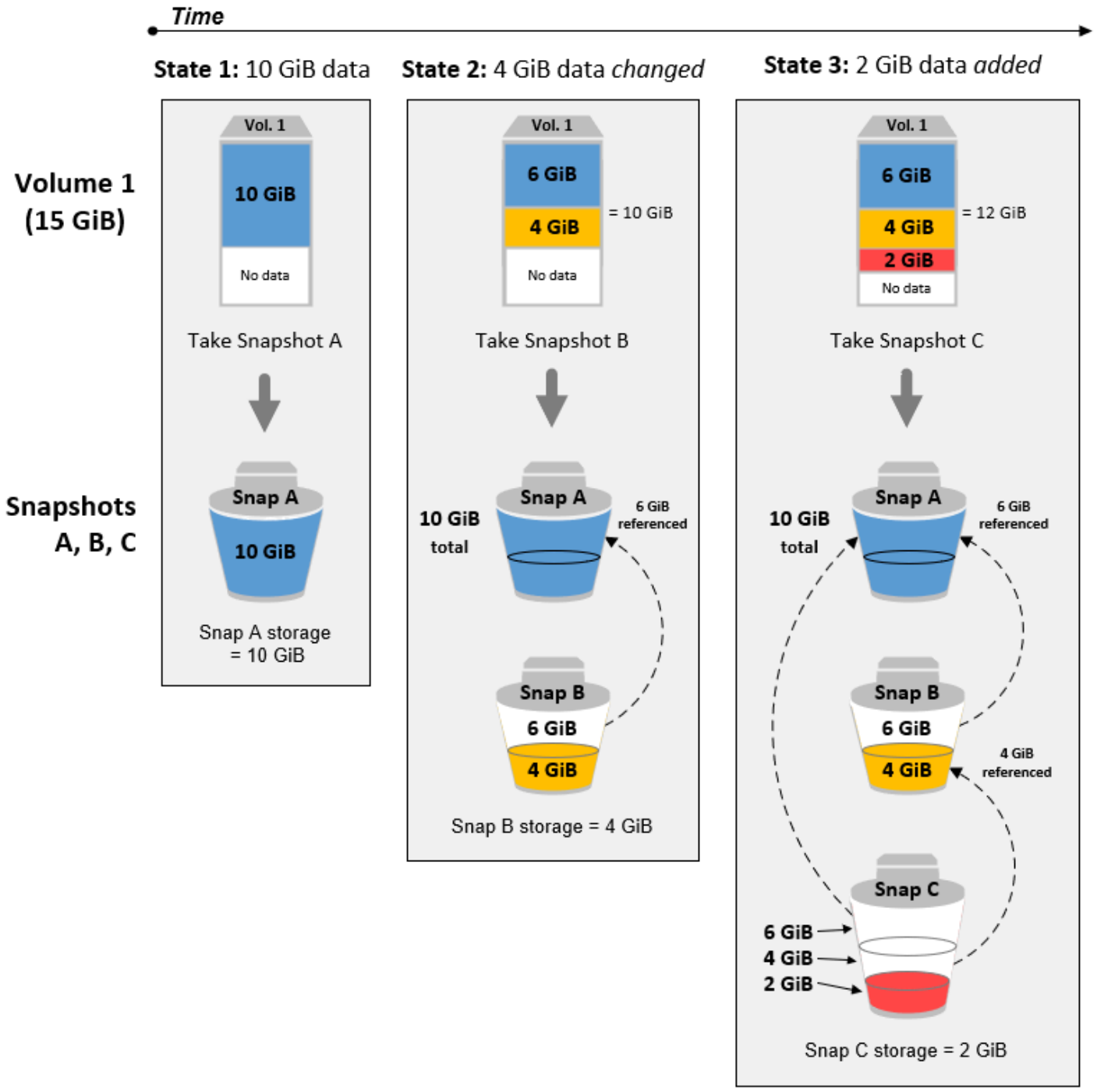
> **Important**
>
> Cuando archiva una instantánea progresiva, se convierte en una instantánea completa que incluye todos los bloques escritos en el volumen en el momento en que se creó la instantánea. A continuación, se lleva al nivel de archivo de instantáneas de Amazon EBS. Las instantáneas de archivos se facturan según una tarifa diferente a la de las instantáneas del nivel estándar. Para obtener más información, consulte Precios y facturación.

En las siguientes secciones, se muestra cómo una instantánea de EBS registra el estado de un volumen en un momento determinado y cómo las instantáneas sucesivas de un volumen que cambia crean un historial de dichos cambios.

Varias instantáneas del mismo volumen

En el diagrama de esta sección se muestra el volumen 1, que tiene un tamaño de 15 GiB, en tres momentos distintos. Se toma una instantánea de cada uno de los tres estados del volumen. En el diagrama se muestra específicamente lo siguiente:

- En el estado 1, el volumen tiene 10 GiB de datos. La instantánea A es la primera instantánea tomada del volumen. La instantánea A es una instantánea completa y se realiza una copia de seguridad de todos los 10 GiB de datos.
- En el estado 2, el volumen sigue conteniendo 10 GiB de datos, pero solo 4 GiB se han modificado después de tomar la instantánea A. La instantánea B es una instantánea progresiva. Solo tiene que hacer una copia de seguridad de los 4 GiB que se han modificado. La instantánea B hace referencia a los otros 6 GiB de datos que no se han modificado, que ya están copiados en la instantánea A, en lugar de volverlos a copiar. Esto se indica con la flecha discontinua.
- En el estado 3, se han agregado 2 GiB de datos al volumen, lo que da un total de 12 GiB, después de tomarse la instantánea B. La instantánea C es una instantánea progresiva. Solo tiene que hacer una copia de seguridad de los 2 GiB que se agregaron después de tomarse la instantánea B. Como muestran las flechas discontinuas, la instantánea C también hace referencia a los 4 GiB de datos almacenados en la instantánea B y a los 6 GiB de datos almacenados en la instantánea A.
- El espacio de almacenamiento total que requieren las tres instantáneas es de 16 GiB. Esto supone 10 GiB para la instantánea A, 4 GiB para la instantánea B y 2 GiB para la instantánea C.



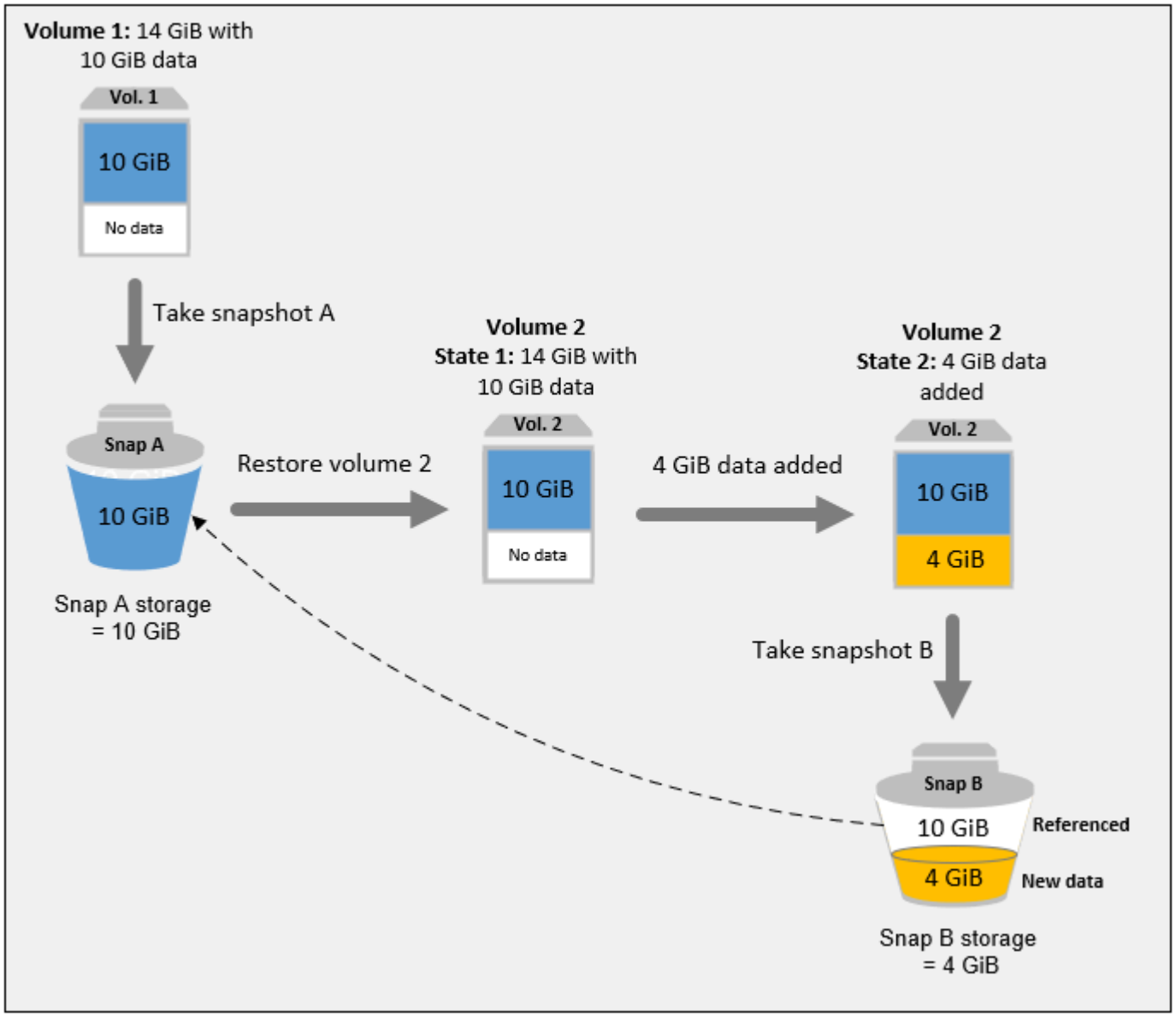
Instantáneas progresivas de diferentes volúmenes

En el diagrama de esta sección, se muestra cómo se pueden tomar instantáneas progresivas de volúmenes diferentes.

1. El volumen 1, con un tamaño de 14 GiB, tiene 10 GiB de datos. Como la instantánea A es la primera instantánea que se toma del volumen, es una instantánea completa y se deben copiar todos los 10 GiB de datos.
2. Vol 2 (Volumen 2) se crea a partir de Snap A (Instantánea A), por lo que es una réplica exacta de Vol 1 (Volumen 1) en el momento en que se realizó la instantánea.
3. Con el tiempo, se agregan 4 GiB de datos al volumen 2 y el tamaño total de sus datos es de 14 GiB.
4. Snap B (Instantánea B) se toma de Vol Volumen 2. En cuanto a la instantánea B, solo se hace una copia de seguridad de los 4 GiB de datos que se agregaron después de crearse el volumen a partir de la instantánea A. La instantánea B hace referencia a los otros 10 GiB de datos no modificados, que ya están almacenados en la instantánea A, en lugar de hacerse de nuevo una copia de seguridad de los mismos.

   Snap B (Instantánea B) es una instantánea progresiva de Snap A (Instantánea A), aunque se creó a partir de un volumen diferente.

> **Important**
>
> El diagrama supone que posee el volumen 1 y la instantánea A, y que el volumen 2 está cifrado con la misma clave de KMS que el volumen 1. Si el volumen 1 pertenecía a otra AWS cuenta y esa cuenta utilizaba Snap A y lo compartía contigo, Snap B sería una instantánea completa. O bien, si el volumen 2 se cifrara con una clave de KMS diferente a la del volumen 1, la instantánea B sería una instantánea completa.



Para obtener más información acerca del modo en que se administran los datos cuando se elimina una instantánea, consulte Eliminar una instantánea de Amazon EBS.

Copiar y compartir instantáneas

Puedes compartir una instantánea entre AWS cuentas modificando sus permisos de acceso. Puede hacer copias de sus instantáneas, así como de las instantáneas que se han compartido con usted. Para obtener más información, consulte Compartir una instantánea de Amazon EBS.

Una instantánea está restringida a la AWS región en la que se creó. Después de crear una instantánea de un volumen de EBS puede usarla para crear nuevos volúmenes en la misma región.

Para obtener más información, consulte Creación de un volumen desde una instantánea. También puede copiar instantáneas de unas regiones en otras, lo que posibilita el uso de varias regiones para la expansión geográfica, la migración de centros de datos y la recuperación de desastres. Puede copiar cualquier instantánea accesible que tenga el estado `completed`. Para obtener más información, consulte Copia de una instantánea de Amazon EBS.

Compatibilidad de cifrado para instantáneas

Las instantáneas de EBS son totalmente compatibles con el cifrado EBS.

- Las instantáneas de volúmenes cifrados se cifran automáticamente.
- Los volúmenes creados a partir de instantáneas cifradas se cifran automáticamente.
- Los volúmenes que cree a partir de una instantánea no cifrada que sea de su propiedad o a la que tenga acceso se pueden cifrar. on-the-fly
- Cuando se copia una instantánea no cifrado de su propiedad, puede cifrarla durante el proceso de copia.
- Cuando copie una instantánea cifrada que es de su propiedad o a la que tiene acceso, puede volver a cifrarla con una clave distinta durante el proceso de copia.
- La primera instantánea que tome de un volumen encriptado que se haya creado a partir de una instantánea cifrada es siempre una instantánea completa.
- La primera instantánea que tome de un volumen recifrado, la cual tiene una CMK diferente en comparación con la instantánea de origen, es siempre una instantánea completa.

Complete la documentación de las posibles situaciones de cifrado de instantáneas que se proporciona en Crear instantáneas de Amazon EBS y en Copia de una instantánea de Amazon EBS.

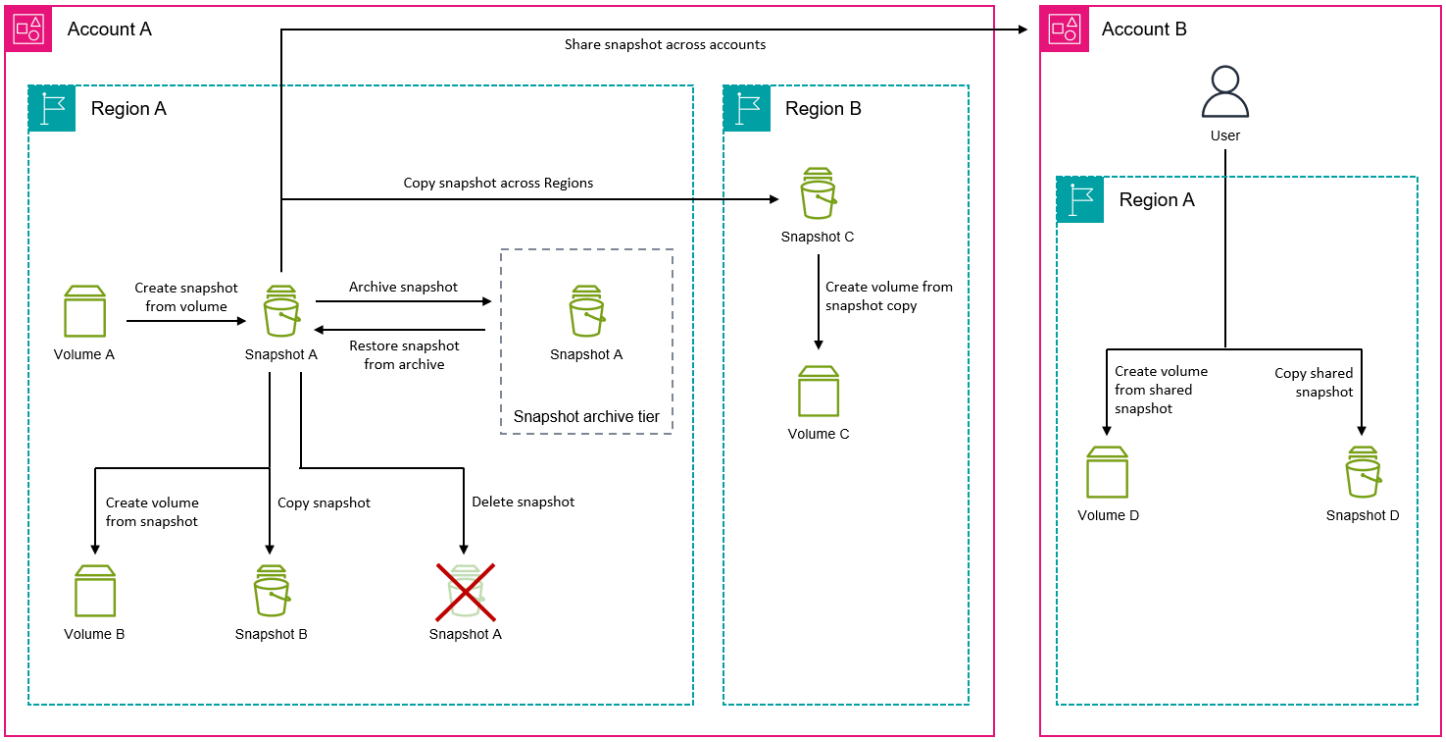
Para obtener más información, consulte Cifrado de Amazon EBS.

Ciclo de vida de las instantáneas de Amazon EBS

El ciclo de vida de una instantánea de Amazon EBS comienza con el proceso de creación. Las instantáneas se crean a partir de volúmenes de Amazon EBS. Puede usar instantáneas para restaurar nuevos volúmenes de Amazon EBS. Puede crear copias de instantáneas en la misma región o en regiones diferentes. Puede compartir las instantáneas con otras personas Cuentas de AWS, de forma pública o privada. Esas cuentas pueden restaurar volúmenes a partir de las

instantáneas compartidas o pueden crear copias de las instantáneas compartidas en su propia cuenta. Si no necesita acceso inmediato a una instantánea, puede archivarla para ahorrar costes de almacenamiento.

La siguiente imagen muestra las acciones que puede realizar en las instantáneas como parte de su ciclo de vida.



Tareas

- Crear instantáneas de Amazon EBS
- Ver información de instantáneas de Amazon EBS
- Copia de una instantánea de Amazon EBS
- Compartir una instantánea de Amazon EBS
- Archivar instantáneas de Amazon EBS
- Eliminar una instantánea de Amazon EBS
- Automatizar el ciclo de vida de instantáneas

Crear instantáneas de Amazon EBS

Para crear instantáneas coherentes con las aplicaciones en una instancia de Windows, consulte Creación de una instantánea coherente con las aplicaciones de VSS.

Puede crear una point-in-time instantánea de un volumen de EBS y utilizarla como referencia para nuevos volúmenes o para realizar copias de seguridad de datos. Si realiza instantáneas periódicas de un volumen, las instantáneas son incrementales—la nueva instantánea guarda únicamente los bloques que han cambiado desde su última instantánea.

Las instantáneas se producen de forma asíncrona; la point-in-time instantánea se crea inmediatamente, pero el estado de la instantánea es `pending` hasta que se complete (cuando todos los bloques modificados se hayan transferido a Amazon S3), lo que puede tardar varias horas en el caso de las instantáneas iniciales grandes o en las instantáneas posteriores en las que se hayan modificado muchos bloques. Mientras se completa, no le afectan las lecturas y escrituras continuas en el volumen.

Puede tomar una instantánea de un volumen adjunto que esté en uso. Sin embargo, las instantáneas solo capturan los datos que se han escrito en el volumen de Amazon EBS en el momento que se lanza el comando snapshot. Esto puede excluir los datos que las aplicaciones o el sistema operativo hayan guardado en la memoria caché. Si puede poner en pausa la escritura de archivos en el volumen el tiempo suficiente para tomar una instantánea, esta instantánea debería ser completa. Sin embargo, si no puede detener la escritura en los archivos del volumen, debe desmontarlo de la instancia, emitir el comando snapshot y después volver a montar el volumen para asegurarse de que la instantánea esté completa y sea coherente. Puede volver a montar y usar el volumen siempre que el estado de la instantánea sea `pending`.

Para facilitar la administración de las instantáneas, puede etiquetarlas durante la creación o añadirles etiquetas más tarde. Por ejemplo, puede aplicar etiquetas que describan el volumen original a partir del que se creó la instantánea o el nombre del dispositivo utilizado para adjuntar el volumen original a una instancia.

Cifrado de instantáneas

Las instantáneas que se crean a partir de volúmenes cifrados se cifran automáticamente. Los volúmenes que se crean a partir de instantáneas cifradas también se cifran automáticamente. Los datos de los volúmenes cifrados y cualquier instantánea asociada se protegen tanto en movimiento como parados. Para obtener más información, consulte Cifrado de Amazon EBS.

De manera predeterminada, solo puede crear volúmenes de instantáneas que sean de su propiedad. Sin embargo, puede compartir sus instantáneas no cifradas con AWS cuentas específicas o puede compartirlas con toda la comunidad haciéndolas públicas. AWS Para obtener más información, consulte Compartir una instantánea de Amazon EBS.

Puedes compartir una instantánea cifrada solo con cuentas específicas AWS . Para que otras personas usen la instantánea cifrada que ha compartido, debe también compartir la clave CMK empleada para cifrarla. Los usuarios con acceso a la instantánea cifrada deben crear una copia personal de la misma y usarla. La copia de una instantánea cifrada y compartida también se puede cifrar de nuevo mediante una clave diferente. Para obtener más información, consulte Compartir una instantánea de Amazon EBS.

Instantáneas de varios volúmenes

Puede crear instantáneas de varios volúmenes, que son point-in-time instantáneas de todos los volúmenes adjuntos a una instancia o de algunos de ellos.

De forma predeterminada, cuando crea instantáneas de varios volúmenes a partir de una instancia, Amazon EBS crea instantáneas de todos los volúmenes (raíz y datos [no raíz]) que se adjuntan a la instancia. Sin embargo, puede optar por crear instantáneas de un subconjunto de los volúmenes que están asociados a la instancia.

Puede etiquetar las instantáneas de varios volúmenes como lo haría con una única instantánea de volumen. Le recomendamos que etiquete sus instantáneas de varios volúmenes para gestionarlas de manera conjunta durante el proceso de restauración, copia o retención. También puede elegir copiar automáticamente las etiquetas del volumen de origen en las instantáneas correspondientes. Esta opción sirve de ayuda para configurar los metadatos de la instantánea, como las políticas de acceso, la información adjunta y la asignación de costos, para que coincidan con el volumen de origen.

Después de crear las instantáneas, cada una de ellas se trata como una instantánea individual. Puede realizar todas las operaciones relacionadas con las instantáneas, como restaurar, eliminar y copiar entre cuentas o regiones, como lo haría con una única instantánea de volumen.

Las instantáneas coherentes frente a bloqueos de varios volúmenes se restauran habitualmente como un conjunto. Resulta útil identificar las instantáneas que se encuentran en un conjunto coherente frente a bloqueos etiquetando dicho conjunto con el ID de la instancia, el nombre u otros datos relevantes.

Tras crear las instantáneas, aparecen en la consola EC2 creada exactamente igual. point-in-time

Si alguna de las instantáneas del conjunto de instantáneas de varios volúmenes falla, todas las demás instantáneas muestran un estado de error y `failed` se envía a su `createSnapshots` CloudWatch cuenta un evento con el resultado de. AWS Para obtener más información, consulte Crear instantáneas (createSnapshots).

Administrador de vida útil de datos de Amazon

Puede crear políticas de ciclo de vida de las instantáneas para automatizar la creación y la retención de instantáneas de volúmenes individuales y de varios volúmenes de las instancias. Para obtener más información, consulte Administrador de vida útil de datos de Amazon.

Consideraciones

Las siguientes consideraciones se aplican a la creación de instantáneas:

- Al crear una instantánea para un volumen de EBS que actúa como dispositivo raíz, le recomendamos que detenga la instancia antes de tomar la instantánea.
- No puede crear instantáneas a partir de instancias para las que la hibernación esté habilitada ni a partir de instancias hibernadas. Si crea una instantánea o AMI desde una instancia que esté hibernada o tenga habilitada la hibernación, es posible que no pueda conectarse a una nueva instancia que se lance desde la AMI o desde una AMI que se haya creado desde la instantánea.
- Aunque puede tomar una instantánea de un volumen mientras una instantánea previa de dicho volumen se encuentra en estado `pending`, muchas instantáneas `pending` de un volumen pueden reducir el rendimiento del volumen hasta que terminan.
- Existe un límite de una instantánea `pending` para un único volumen `st1` o `sc1`, o cinco instantáneas `pending` para un único volumen de los otros tipos de volumen. Si recibe un error `ConcurrentSnapshotLimitExceeded` mientras intenta crear varias instantáneas a la vez del mismo volumen, espere hasta que una o varias de las instantáneas `pending` se hayan completado antes de crear otra instantánea del volumen.
- Cuando se crea una instantánea a partir de un volumen con un código de AWS Marketplace producto, el código de producto se propaga a la instantánea.
- Al crear conjuntos de instantáneas de múltiples volúmenes a partir de instancias, puede especificar hasta 127 volúmenes de datos (no raíz) para excluirlos. La cantidad máxima de volúmenes de Amazon EBS que puede adjuntar a una instancia depende del tipo y tamaño de la instancia. Para obtener más información, consulte Límites de volumen de instancia.

Crear un snapshot

Siga alguno de los métodos siguientes para crear una instantánea a partir del volumen especificado.

Console

Para crear una instantánea con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Snapshots (Instantáneas), Create snapshots (Crear instantáneas).
3. En Resource type (Tipo de recurso), elija Device (Dispositivo).
4. En Volume ID (ID del volumen), seleccione el volumen desde el que se creará la instantánea.

   El campo Encryption (Cifrado) indica el estado de cifrado del volumen seleccionado. Si el volumen seleccionado está cifrado, la instantánea se cifra automáticamente con la misma clave de KMS. Si el volumen seleccionado no está cifrado, la instantánea no se cifra.
5. (Opcional) En Description (Descripción), introduzca una breve descripción para la instantánea.
6. (Opcional) Para asignar etiquetas personalizadas a la instantánea, en la sección Tags (Etiquetas), elija Add tag (Agregar etiqueta) y, a continuación, ingrese el par de valor de clave. Puede añadir hasta 50 etiquetas.
7. Seleccione Create snapshot (Crear instantánea).

AWS CLI

Para crear una instantánea con AWS CLI

Utilice el comando create-snapshot.

Tools for Windows PowerShell

Para crear una instantánea con las herramientas de Windows PowerShell

Utilice el comando New-EC2Snapshot.

Crear una instantánea de varios volúmenes

Cuando crea un conjunto de instantáneas de varios volúmenes a partir de una instancia, puede elegir si desea copiar las etiquetas del volumen de origen en la instantánea correspondiente. Puede especificar si desea crear una instantánea del volumen raíz. También puede especificar si se crearán instantáneas de todos los volúmenes de datos (no raíz) que se adjuntan a la instancia o si se crearán instantáneas de un subconjunto de esos volúmenes.

Consideraciones

- Las instantáneas de múltiples volúmenes admiten hasta 128 volúmenes de Amazon EBS para cada instancia, lo que incluye el volumen raíz y hasta 127 volúmenes de datos (no raíz). La cantidad máxima de volúmenes de Amazon EBS que puede adjuntar a una instancia depende del tipo y tamaño de la instancia. Para obtener más información, consulte Límites de volumen de instancia.

Siga alguno de los métodos siguientes para crear una instantánea a partir de los volúmenes de una instancia.

Console

Para crear instantáneas de varios volúmenes con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Snapshots (Instantáneas), Create snapshots (Crear instantáneas).
3. En Tipo de recurso, elija Instancia.
4. En Description (Descripción), ingrese una breve descripción para las instantáneas. Esta descripción se aplica a todas las instantáneas.
5. (Opcional) De forma predeterminada, Amazon EBS crea una instantánea del volumen raíz de la instancia. Si no desea crear una instantánea del volumen raíz de la instancia, seleccione Exclude root volume (Excluir volumen raíz).
6. (Opcional) De forma predeterminada, Amazon EBS crea instantáneas de todos los volúmenes de datos (no raíz) adjuntos a la instancia. Si desea crear instantáneas de un subconjunto de los volúmenes de datos (no raíz) adjuntos a la instancia, seleccione Exclude specific data volumes (Excluir volúmenes de datos específicos). En la sección Attached data volumes (Volúmenes de datos adjuntos) se enumeran todos los volúmenes de datos adjuntos actualmente a la instancia seleccionada.

   En la sección Attached data volumes (Volúmenes de datos adjuntos), seleccione los volúmenes de datos para los que no desea crear instantáneas. Solo los volúmenes que no se seleccionen se incluirán en el conjunto de instantáneas de varios volúmenes. Puede excluir hasta 127 volúmenes.
7. (Opcional) Para copiar etiquetas automáticamente de los volúmenes de origen en las instantáneas correspondientes, en Copy tags from source volume (Copiar etiquetas del

volumen de origen), seleccione Copy tags (Copiar etiquetas). Esta opción configura los metadatos de la instantánea, como las políticas de acceso, la información adjunta y la asignación de costos, para que coincidan con el volumen de origen.

8. (Opcional) Para asignar etiquetas personalizadas adicionales a las instantáneas, en la sección Tags (Etiquetas), elija Add tag (Agregar etiqueta) y, a continuación, ingrese el par clave-valor. Puede añadir hasta 50 etiquetas.
9. Seleccione Create snapshot (Crear instantánea).

   Las instantáneas se administran de manera conjunta durante la creación de la instantánea. Si una de las instantáneas del conjunto de volúmenes da error, el resto de las instantáneas pasarán a presentar el estado de error en el conjunto de volúmenes. Puede supervisar el progreso de las instantáneas mediante CloudWatchEvents. Una vez finalizado el proceso de creación de la instantánea, CloudWatch genera un evento que contiene el estado y todos los detalles relevantes de la instantánea de la instancia afectada.

AWS CLI

Para crear instantáneas de varios volúmenes mediante el AWS CLI, utilice el comando create-snapshots.

Si no desea crear una instantánea del volumen raíz, para `--instance-specification ExcludeBootVolume`, especifique `true`. Si no desea crear instantáneas de todos los volúmenes de datos (no raíz) adjuntos a la instancia, para `--instance-specification ExcludeDataVolumes`, especifique los ID de los volúmenes de datos para los que no desea crear instantáneas. Puede especificar hasta 127 volúmenes (no raíz) para que sean excluidos.

Tools for Windows PowerShell;

Para crear instantáneas de varios volúmenes mediante las herramientas de Windows, utilice el comando. PowerShell New-EC2SnapshotBatch

Si no desea crear una instantánea del volumen raíz, para `-InstanceSpecification_ExcludeBootVolume`, especifique 1. Si no desea crear instantáneas de todos los volúmenes de datos (no raíz) adjuntos a la instancia, para `-InstanceSpecification_ExcludeDataVolumes`, especifique los ID de los volúmenes de datos para los que no desea crear instantáneas. Puede especificar hasta 127 volúmenes (no raíz) para que sean excluidos.

Si todas las instantáneas se completan correctamente, se envía a su cuenta un `createSnapshots` CloudWatch evento con un resultado de`succeeded`. AWS Si alguna de las instantáneas del conjunto de instantáneas de varios volúmenes falla, todas las demás instantáneas muestran un estado de error y `failed` se envía a su cuenta un `createSnapshots` CloudWatch evento con un resultado de. AWS Para obtener más información, consulte Crear instantáneas (createSnapshots).

Utilizar instantáneas de EBS

Puede copiar instantáneas, compartir instantáneas y crear volúmenes a partir de instantáneas. Para más información, consulte los siguientes temas:

- Copia de una instantánea de Amazon EBS
- Compartir una instantánea de Amazon EBS
- Creación de un volumen desde una instantánea

Ver información de instantáneas de Amazon EBS

Puede ver información detallada acerca de las instantáneas mediante alguno de los métodos siguientes.

Console

Para ver información sobre las instantáneas mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instantáneas.
3. Para ver solo las instantáneas que sean de su propiedad, en la esquina superior izquierda de la pantalla, elija Owned by me (De mi propiedad). También puede filtrar la lista de instantáneas mediante etiquetas y otros atributos de instantáneas. En el campo Filter (Filtro), seleccione el campo de atributo y, a continuación, elija o ingrese el valor del atributo. Por ejemplo, para ver solo las instantáneas cifradas, seleccione Encryption (Cifrado) y, a continuación, ingrese `true`.
4. Para obtener más información acerca de una instantánea específica, elija el ID en la lista.

AWS CLI

Para ver la información de las instantáneas mediante la AWS CLI

Utilice el comando describe-snapshots.

Example Ejemplo 1: filtro basado en las etiquetas

En el siguiente comando se describen las instantáneas con la etiqueta stack=production.

```
aws ec2 describe-snapshots --filters Name=tag:Stack,Values=production
```

Example Ejemplo 2: filtro basado en el volumen

El siguiente comando describe las instantáneas creadas a partir del volumen especificado.

```
aws ec2 describe-snapshots --filters Name=volume-id,Values=vol-049df61146c4d7901
```

Example Ejemplo 3: filtro basado en la antigüedad de la instantánea

Con el AWS CLI, puede utilizar JMEspath para filtrar los resultados mediante expresiones. Por ejemplo, el siguiente comando muestra los ID de todas las instantáneas creadas por su cuenta de AWS (representada por *123456789012*) antes de la fecha especificada (representada por *2020-03-31*). Si no especifica el propietario, los resultados incluyen todas las instantáneas públicas.

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query
 "Snapshots[?(StartTime<='2020-03-31')].[SnapshotId]" --output text
```

El siguiente comando muestra los ID de todas las instantáneas creadas en el intervalo de fechas especificado.

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query
 "Snapshots[?(StartTime>='2019-01-01') && (StartTime<='2019-12-31')].[SnapshotId]"
 --output text
```

Tools for Windows PowerShell

Para ver la información de las instantáneas mediante las herramientas de Windows PowerShell

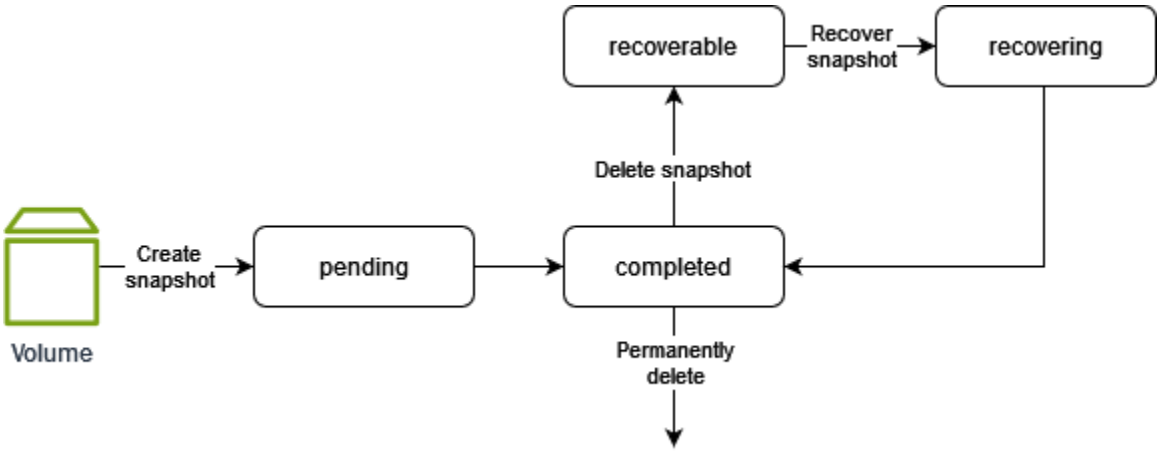
Utilice el comando Get-EC2Snapshot.

```
PS C:\> Get-EC2Snapshot -SnapshotId snapshot_id
```

Estados de las instantáneas

Una instantánea de Amazon EBS pasa por diferentes estados desde que se la crea hasta que se la elimina de forma permanente.

La siguiente ilustración muestra las transiciones entre los estados de una instantánea. Cuando crea una instantánea, esta pasa al estado `pending`. Una vez que la instantánea está lista para usarse, entra en el estado `completed`. Si decide que ya no necesita una instantánea, puede eliminarla. Si elimina una instantánea que coincide con una regla de retención de la papelera de reciclaje, se la retiene en la papelera de reciclaje y pasa al estado `recoverable`. Si recupera una instantánea de la papelera de reciclaje, pasará al estado `recovering` y, a continuación, al estado `completed`. De lo contrario, se la elimina de forma permanente.



En la siguiente tabla se indican los estados de las instantáneas.

Estado	Descripción
`pending`	El proceso de creación de instantáneas aún está en curso. No es posible utilizar una instantánea mientras se encuentre en el estado `pending`.
`completed`	El proceso de creación de la instantánea se ha completado y la instantánea está lista para utilizarse.
`recoverable`	La instantánea se encuentra actualmente en la papelera de reciclaje. Para utilizar la instantán

Estado	Descripción
	ea, primero debe recuperarla de la papelera de reciclaje.
`recovering`	Se está recuperando la instantánea de la papelera de reciclaje. Una vez recuperada la instantánea, pasa al estado `completed` y queda lista para utilizarse.
`error`	Se produjo un error en el proceso de creación de la instantánea. No es posible utilizar una instantánea mientras se encuentre en el estado `error`.

Copia de una instantánea de Amazon EBS

Con Amazon EBS, puede crear point-in-time instantáneas de volúmenes, que almacenamos para usted en Amazon S3. Una vez que haya creado una instantánea y haya terminado de copiarse en Amazon S3 (si el estado de la instantánea es`completed`), puede copiarla de una AWS región a otra o dentro de la misma región. El cifrado del lado del servidor de Amazon S3 (AES de 256 bits) protege los datos en tránsito de la instantánea durante una operación de copia. La copia de la instantánea recibe un ID que es diferente del ID de la instantánea original.

Para copiar instantáneas de varios volúmenes a otra AWS región, recupere las instantáneas con la etiqueta que aplicó al conjunto de instantáneas de varios volúmenes cuando lo creó. A continuación, copie una a una las instantáneas en otra región.

Si desea que otra cuenta pueda copiar su instantánea, debe modificar los permisos de la instantánea para permitir el acceso a esa cuenta o hacer que la instantánea sea pública para que todas AWS las cuentas puedan copiarla. Para obtener más información, consulte Compartir una instantánea de Amazon EBS.

Para obtener información sobre cómo copiar una instantánea de Amazon RDS, consulte Copia de una instantánea de base de datos en la Guía del usuario de Amazon RDS.

Casos de uso

- Expansión geográfica: lance sus aplicaciones en una nueva AWS región.

- Migración: mueva una aplicación a una región nueva para ofrecer más disponibilidad y minimizar costos.
- Recuperación de desastres: haga una copia de seguridad de los datos y los registros de distintas ubicaciones geográficas a intervalos regulares. En caso de desastre, puede restaurar sus aplicaciones mediante las point-in-time copias de seguridad almacenadas en la región secundaria. Esto reduce al mínimo la pérdida de datos y el tiempo de recuperación.
- Cifrado: cifre una instantánea que no está cifrada, cambie la clave con la que se cifra, cambiar la clave con la que se cifra la instantánea, o cree una copia de su propiedad para restaurar un volumen a partir de esta (para instantáneas cifradas que se han compartido con usted).
- Retención de datos y requisitos de auditoría: copie las instantáneas cifradas de EBS de una cuenta de AWS en otra para conservar los registros de datos u otros archivos para auditoría o retención de datos. El uso de una cuenta diferente ayuda a evitar la eliminación accidental de instantáneas y le protege en caso de que su AWS cuenta principal se vea comprometida.

Contenido

Requisitos previos

- Puede copiar cualquier instantánea accesible que tenga un estado `completed`, incluidas aquellas compartidas y las que haya creado.
- Puede copiar AWS Marketplace instantáneas de VM Import/Export y Storage Gateway, pero debe comprobar que la instantánea es compatible con la región de destino.
- Para copiar una instantánea cifrada, el usuario debe tener los siguientes permisos para utilizar el cifrado de Amazon EBS.
  - `kms:DescribeKey`
  - `kms:CreateGrant`
  - `kms:GenerateDataKey`

  - `kms:GenerateDataKeyWithoutPlaintext`
  - `kms:ReEncrypt`
  - `kms:Decrypt`
- Para copiar una instantánea cifrada compartida desde otra AWS cuenta, debe tener permisos para usar la clave administrada por el cliente que se utilizó para cifrar la instantánea. Para obtener más información, consulte Compartir una clave de KMS.

Consideraciones

- Hay un límite de `20` solicitudes de copia de instantáneas simultáneas por región de destino. Si supera esta cuota, recibe un error `ResourceLimitExceeded`. Si recibe este error, espere a que se completen una o varias solicitudes de copia antes de realizar una solicitud nueva de copia de instantánea.
- Las etiquetas definidas por el usuario no se copian desde la instantánea de origen a la instantánea nueva. Puede añadir etiquetas definidas por el usuario durante o después de la operación de copia.
- Las instantáneas creadas mediante la operación de copia de una instantánea tienen un ID de volumen arbitrario, como `vol-ffff` o `vol-ffffffff`. Estos ID de volumen arbitrarios no deben utilizarse para ningún fin.
- Los permisos de nivel de recursos especificados para la operación de copia instantánea solo se aplican a la nueva instantánea. No puede especificar permisos de nivel de recursos para la instantánea de origen. Para ver un ejemplo, consulte Ejemplo: copia de instantáneas.

Precios

- Para obtener información sobre los precios de la copia de instantáneas entre AWS regiones y cuentas, consulte los precios de Amazon EBS.
- Si copia una instantánea y la cifra con una clave de KMS nueva, se crea una copia completa (no progresiva). Esto da como resultado costos de almacenamiento adicionales.
- Si copia una instantánea a una nueva región, se crea una copia completa (no incremental). Esto da como resultado costos de almacenamiento adicionales. Las copias posteriores de la misma instantánea son incrementales.

- Si usa transferencias de datos externas o entre regiones, se aplicarán cargos adicionales por la transferencia de datos de EC2. Además, si elimina alguna instantánea después de iniciarla, se le seguirán cobrando los datos que ya se hayan transferido.

Copias de instantáneas incrementales

Si una copia de instantánea es incremental depende de la copia de la instantánea completada más recientemente. Al copiar una instantánea en las regiones o cuentas, la copia es incremental si se cumplen los siguientes criterios:

- La instantánea se ha copiado previamente a la región o cuenta de destino.
- La copia más reciente de la instantánea sigue presente en la región o cuenta de destino.
- La copia instantánea más reciente no se ha archivado.
- Todas las copias de la instantánea en la región o cuenta de destino o bien no están cifradas o bien se han cifrado con la misma clave KMS.

Si se ha borrado la copia más reciente de la instantánea, la siguiente copia será una copia completa, no una copia incremental. Si una copia sigue pendiente al iniciar otra copia, la segunda copia no se iniciará hasta que finalice la primera copia.

Las operaciones de copia de instantáneas dentro de la misma cuenta y región con la misma clave de KMS dan como resultado una copia incremental.

La copia de instantáneas progresivas reduce el tiempo necesario para copiar instantáneas y ahorra costos de almacenamiento y transferencia de datos, ya que no se duplican los datos.

Le recomendamos que marque las instantáneas con el ID de volumen y el tiempo de creación para poder realizar el seguimiento de la copia más reciente de la instantánea de un volumen en la región o cuenta de destino.

Para comprobar si las copias instantáneas son incrementales, compruebe el evento CopySnapshot CloudWatch .

Cifrado y copia de la instantánea

Cuando copia una instantánea, puede cifrarla o puede especificar una clave KMS diferente de la original y la instantánea copiada resultante usa la nueva clave KMS. Sin embargo, cambiar el estado de cifrado de una instantánea durante una operación de copia podría dar como resultado una copia

completa (no progresiva), lo que puede entrañar mayores cargos de almacenamiento y transferencia de datos. Para obtener más información, consulte Copias de instantáneas incrementales.

Para copiar una instantánea cifrada compartida desde otra AWS cuenta, debe tener permisos para utilizarla y la clave gestionada por el cliente (CMK) que se utilizó para cifrarla. Cuando use una instantánea cifrada que se haya compartido con usted, es recomendable que la vuelva a cifrar copiándola con una clave KMS de su propiedad. Esta es una manera de protegerse en caso de que la clave KMS original corra peligro o si el propietario la revoca, lo que haría que perdiera el acceso a los volúmenes cifrados creados con la instantánea. Para obtener más información, consulte Compartir una instantánea de Amazon EBS.

Para aplicar el cifrado a las copias de instantáneas de EBS, establezca el parámetro `Encrypted` en `true`. (El parámetro `Encrypted` es opcional si encryption by default está habilitado).

De forma opcional, puede utilizar `KmsKeyId` para especificar una clave personalizada que se utilizará para cifrar la copia de la instantánea. (El parámetro `Encrypted` también debe establecerse en `true`, incluso si se ha habilitado el cifrado predeterminado). Si no se especifica el `KmsKeyId`, la clave que se utiliza para el cifrado depende del estado de cifrado de la instantánea de origen y de su propiedad.

En la siguiente tabla, se describen los resultados de cifrado para cada combinación posible de configuraciones al momento de copiar las instantáneas que posee y las que se comparten con usted.

Cifrado de forma predeterminada	¿Se ha establecido el parámetro **`Encrypted`** ?	Estado de cifrado de la instantánea de origen	Predeterminado (no se ha especificado ninguna clave de KMS)	Personalizado (se ha especificado una clave de KMS)
Deshabilitado	No	Sin cifrar	Sin cifrar	N/A
		Encrypted	Cifrado por Clave administrada de AWS	
	Sí	Sin cifrar	Cifrado con la clave de KMS predeterminada	Cifrado con la clave de KMS especificada**

Cifrado de forma predeterminada	¿Se ha establecido el parámetro **`Encrypted`** ?	Estado de cifrado de la instantánea de origen	Predeterminado (no se ha especificado ninguna clave de KMS)	Personalizado (se ha especificado una clave de KMS)
		Encrypted	Cifrado con la clave de KMS predeterminada	
Habilitado	No	Sin cifrar	Cifrado con la clave de KMS predeterminada	N/A
		Encrypted	Cifrado con la clave de KMS predeterminada	
	Sí	Sin cifrar	Cifrado con la clave de KMS predeterminada	Cifrado con la clave de KMS especificada**
		Encrypted	Cifrado con la clave de KMS predeterminada	

** Esta es la clave de KMS especificada en la acción de copia de instantánea. Esta clave de KMS se utiliza en lugar de la clave de KMS predeterminada para la cuenta y la región.

Copia de una instantánea

Para copiar una instantánea, utilice alguno de los métodos siguientes.

Console

Para copiar una instantánea con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instantáneas.

3. Seleccione la instantánea que va a copiar y después elija Actions (Acciones), Copy snapshot (Copiar instantánea).
4. En Description (Descripción), ingrese una breve descripción para la copia de la instantánea.

   De forma predeterminada, la descripción incluye información acerca de la instantánea de origen para que pueda diferenciar la copia de la original. Puede cambiar esta descripción según sea necesario.
5. En Destination Region (Región de destino), seleccione la región en la que desea crear la copia de la instantánea.
6. Especifique el estado de cifrado de la copia de la instantánea.

   Si la instantánea de origen está cifrada o si la cuenta está habilitada para cifrado de forma predeterminada, la copia de la instantánea se cifra automáticamente y no se puede cambiar el estado de cifrado.

   Si la instantánea de origen no está cifrada y la cuenta no está habilitada para el cifrado de forma predeterminada, el cifrado es opcional. Para cifrar la copia de la instantánea, en Encryption (Cifrado), seleccione Encrypt this snapshot (Cifrar esta instantánea). Luego, en KMS key (Clave de KMS), seleccione la clave KMS que desea utilizar para cifrar la instantánea en la región de destino.
7. Elija Copy Snapshot (Copiar instantánea).

AWS CLI

Para copiar una instantánea mediante el AWS CLI

Utilice el comando copy-snapshot.

Tools for Windows PowerShell

Para copiar una instantánea mediante las herramientas de Windows PowerShell

Utilice el comando Copy-EC2Snapshot.

Para comprobar errores

Si intenta copiar una instantánea cifrada sin tener permiso para usar la clave de cifrado, la operación dará error silenciosamente. El estado del error no se muestra en la consola hasta que se actualiza la

página. También puede comprobar el estado de la instantánea desde la línea de comandos, como en el siguiente ejemplo.

```
aws ec2 describe-snapshots --snapshot-id snap-0123abcd
```

Si la copia ha fallado porque los permisos de clave son insuficientes, verá el siguiente mensaje: "StateMessage«: «El identificador de clave dado no es accesible».

Cuando copie una instantánea cifrada, debe tener permisos `DescribeKey` en la CMK predeterminada. La denegación explícita de estos permisos da como resultado un error de copiado. Para obtener más información sobre la administración de claves de CMK, consulte Autenticación y control de acceso de AWS KMS Secrets Manager.

Compartir una instantánea de Amazon EBS

Puede modificar los permisos de una instantánea si desea compartirla con otras cuentas de AWS . Puede compartir las instantáneas públicamente con todas las demás AWS cuentas o puede compartirlas de forma privada con AWS las cuentas individuales que especifique. Los usuarios que ha autorizado podrán usar las instantáneas que comparta para crear sus propios volúmenes de EBS, mientras que la instantánea original se mantendrá sin cambios.

> **Important**
>
> Cuando comparte una instantánea, concede a otras personas acceso a todos los datos de la instantánea. Comparta instantáneas solo con aquellas personas en las que confiaría todos los datos que contienen las instantáneas.

Para impedir que sus instantáneas se compartan públicamente, habilite el bloqueo del acceso público de las instantáneas. Para obtener más información, consulte Bloqueo del acceso público a las AMI.

Temas

- Antes de compartir una instantánea
- Compartir una instantánea
- Compartir una clave de KMS
- Ver las instantáneas compartidas con usted

- Usar las instantáneas compartidas con usted
- Determinar el uso de instantáneas que comparte

Antes de compartir una instantánea

Las siguientes consideraciones se aplican al uso compartido de instantáneas:

- Si la opción para bloquear el acceso público de las instantáneas está habilitada para la región, se bloquearán los intentos de compartir las instantáneas públicamente. Las instantáneas se pueden seguir compartiendo de forma privada.
- Las instantáneas están restringidas a la región en la que se han creado. Para compartir una instantánea con otra región, copie la instantánea en dicha región y, luego, comparta la copia. Para obtener más información, consulte Copia de una instantánea de Amazon EBS.
- No puede compartir instantáneas que estén cifradas con la Clave administrada de AWS predeterminada. Solo puede compartir instantáneas que estén cifradas con una clave administrada por el cliente. Para obtener más información, consulte Creación de claves en la Guía para desarrolladores de AWS Key Management Service .
- Solo puede compartir instantáneas sin cifrar de forma pública.
- Cuando comparta una instantánea cifrada, también deberá compartir la clave administrada por el cliente usada para cifrar la instantánea. Para obtener más información, consulte Compartir una clave de KMS.

Compartir una instantánea

Puede compartir una instantánea mediante alguno de los métodos descritos en la sección.

Console

Para compartir una instantánea

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instantáneas.
3. Seleccione la instantánea que desea compartir y después elija Actions (Acciones), Modify Permissions (Modificar permisos).
4. Especifique los permisos de la instantánea. Current setting (Configuración actual) indica los permisos de uso compartido actuales de la instantánea.

- Para compartir la instantánea públicamente con todas las AWS cuentas, selecciona Pública.
- Para compartir la instantánea de forma privada con AWS cuentas específicas, selecciona Privado. Luego, en la sección Sharing accounts (Cuentas para uso compartido), elija Add account (Agregar cuentas) e ingrese el ID de cuenta de 12 dígitos (sin guiones) de la cuenta con la que desea compartir.

5. Elija Guardar cambios.

AWS CLI

Los permisos para una instantánea se especifican mediante el atributo `createVolumePermission` de la instantánea. Para convertir una instantánea en pública, establezca el grupo en `all`. Para compartir una instantánea con una AWS cuenta específica, configura el ID de la AWS cuenta para el usuario.

Para compartir una instantánea de forma pública

Utilice el comando modify-snapshot-attribute.

En `--attribute`, especifique `createVolumePermission`. En `--operation-type`, especifique `add`. En `--group-names`, especifique `all`.

```
$  aws ec2 modify-snapshot-attribute --snapshot-id 1234567890abcdef0 --attribute
 createVolumePermission --operation-type add --group-names all
```

Para compartir una instantánea de forma privada

Utilice el comando modify-snapshot-attribute.

En `--attribute`, especifique `createVolumePermission`. En `--operation-type`, especifique `add`. Para `--user-ids` ello, especifique los ID de 12 dígitos de las AWS cuentas con las que desea compartir las instantáneas.

```
$  aws ec2 modify-snapshot-attribute --snapshot-id 1234567890abcdef0 --attribute
 createVolumePermission --operation-type add --user-ids 123456789012
```

Tools for Windows PowerShell

Los permisos para una instantánea se especifican mediante el atributo `createVolumePermission` de la instantánea. Para convertir una instantánea en pública,

establezca el grupo en `all`. Para compartir una instantánea con una AWS cuenta específica, configure el ID de la cuenta para el usuario. AWS

Para compartir una instantánea de forma pública

Utilice el comando Edit-EC2SnapshotAttribute.

En `-Attribute`, especifique `CreateVolumePermission`. En `-OperationType`, especifique `Add`. En `-GroupName`, especifique `all`.

```
PS C:\>  Edit-EC2SnapshotAttribute -SnapshotId 1234567890abcdef0 -Attribute
 CreateVolumePermission -OperationType Add -GroupName all
```

Para compartir una instantánea de forma privada

Utilice el comando Edit-EC2SnapshotAttribute.

En `-Attribute`, especifique `CreateVolumePermission`. En `-OperationType`, especifique `Add`. Para `UserId` ello, especifique los ID de 12 dígitos de las AWS cuentas con las que desea compartir las instantáneas.

```
PS C:\>  Edit-EC2SnapshotAttribute -SnapshotId 1234567890abcdef0 -Attribute
 CreateVolumePermission -OperationType Add -UserId 123456789012
```

Compartir una clave de KMS

Cuando comparta una instantánea cifrada, también deberá compartir la clave administrada por el cliente usada para cifrar la instantánea. Puede aplicar permisos entre cuentas a una clave administrada por el cliente en el momento de crearla o en un momento posterior.

Los usuarios de la clave administrada por el cliente compartida que tienen acceso a las instantáneas cifradas deben contar con los permisos para realizar las siguientes acciones sobre la clave:

- `kms:DescribeKey`
- `kms:CreateGrant`
- `kms:GenerateDataKey`
- `kms:GenerateDataKeyWithoutPlaintext`
- `kms:ReEncrypt`
- `kms:Decrypt`

> **Tip**
>
> Para seguir el principio de privilegios mínimos, no permita el acceso completo a `kms:CreateGrant`. En su lugar, utilice la clave de `kms:GrantIsForAWSResource` condición para permitir al usuario crear concesiones en la clave de KMS solo cuando un AWS servicio cree la concesión en nombre del usuario.

Para obtener más información acerca del control del acceso a una clave administrada por el cliente, consulte Uso de las políticas de claves en AWS KMS en la Guía para desarrolladores de AWS Key Management Service .

Para compartir la clave gestionada por el cliente mediante la AWS KMS consola

1. Abra la AWS KMS consola 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. Elija Customer managed keys (Claves administradas por el cliente) en el panel de navegación.
4. En la columna Alias elija el alias (enlace de texto) de la clave administrada por el cliente que utilizó para cifrar la instantánea. Los detalles de clave se abren en una nueva página.
5. En la sección Key policy (Política de claves), verá la vista de política o la vista predeterminada. La vista de política muestra el documento de políticas de claves. La vista predeterminada muestra secciones para Key administrators (Administradores de claves), Key deletion (Eliminación de claves), Key Use (Uso de claves) y Other AWS accounts (Otras cuentas de). La vista predeterminada se muestra si creó la política en la consola y no la ha personalizado. Si la vista predeterminada no está disponible, deberá editar manualmente la política en la vista de políticas. Para obtener más información, consulte Visualización de una política de claves (consola) en la Guía para desarrolladores de AWS Key Management Service .

   Utilice la vista de políticas o la vista predeterminada, según la vista a la que pueda acceder, para añadir uno o más identificadores de AWS cuenta a la política, de la siguiente manera:

   - (Vista de políticas) Elija Edit (Editar). Agrega uno o más identificadores de AWS cuenta a los siguientes estados de cuenta: `"Allow use of the key"` y `"Allow attachment of persistent resources"`. Elija Guardar cambios. En el siguiente ejemplo, el identificador de AWS cuenta `444455556666` se añade a la política.

     ```
     {
     ```

```
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": [
    "arn:aws:iam::111122223333:user/KeyUser",
    "arn:aws:iam::444455556666:root"
  ]},
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*"
},
{
  "Sid": "Allow attachment of persistent resources",
  "Effect": "Allow",
  "Principal": {"AWS": [
    "arn:aws:iam::111122223333:user/KeyUser",
    "arn:aws:iam::444455556666:root"
  ]},
  "Action": [
    "kms:CreateGrant",
    "kms:ListGrants",
    "kms:RevokeGrant"
  ],
  "Resource": "*",
  "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}
}
```

- (Vista predeterminada) Desplázate hacia abajo hasta Otras AWS cuentas. Selecciona Añadir otras AWS cuentas e introduce el ID de la AWS cuenta según se te solicite. Para añadir otra cuenta, selecciona Añadir otra AWS cuenta e introduce el ID de la AWS cuenta. Cuando haya añadido todas las cuentas de AWS , elija Save changes (Guardar cambios).

Ver las instantáneas compartidas con usted

Puede ver las instantáneas compartidas con usted mediante alguno de los métodos siguientes.

Console

Para ver las instantáneas compartidas mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. Filtre las instantáneas que aparecen en la lista. En la esquina superior izquierda de la pantalla, elija una de las siguientes opciones:
   - Private snapshots (Instantáneas privadas): para ver solo las instantáneas compartidas con usted de forma privada.
   - Public snapshots (Instantáneas públicas): para ver solo las instantáneas compartidas con usted de forma pública.

AWS CLI

Para ver los permisos de las instantáneas mediante la línea de comandos

Utilice el comando describe-snapshot-attribute.

Tools for Windows PowerShell

Para ver los permisos de las instantáneas mediante la línea de comandos

Utilice el comando Get-EC2SnapshotAttribute.

Usar las instantáneas compartidas con usted

Para usar una instantánea no cifrada compartida

Ubique la instantánea compartida por ID o descripción. Para obtener más información, consulte Ver las instantáneas compartidas con usted. Puede usar esta instantánea como lo haría con cualquier otra instantánea que posea en su cuenta. Por ejemplo, puede crear un volumen a partir de la instantánea o copiarla en una región diferente.

Para usar una instantánea no cifrada compartida

Ubique la instantánea compartida por ID o descripción. Para obtener más información, consulte Ver las instantáneas compartidas con usted. Cree una copia de la instantánea compartida en su cuenta y cifre la copia con una clave de KMS de su propiedad. A continuación, puede utilizar la copia para crear volúmenes o puede copiarla en regiones diferentes.

Determinar el uso de instantáneas que comparte

Puede utilizarla AWS CloudTrail para controlar si una instantánea que ha compartido con otras personas se copia o se utiliza para crear un volumen. Se registran los siguientes eventos CloudTrail:

- SharedSnapshotCopyInitiated— Se está copiando una instantánea compartida.
- SharedSnapshotVolumeCreated— Se está utilizando una instantánea compartida para crear un volumen.

Para obtener más información sobre el uso CloudTrail, consulte Registrar llamadas a las API de Amazon EC2 y Amazon EBS con. AWS CloudTrail

Archivar instantáneas de Amazon EBS

El archivo de instantáneas de Amazon EBS es un nuevo nivel de almacenamiento que puede utilizar como almacenamiento a bajo costo y largo plazo de las instantáneas de acceso poco frecuente y que no necesitan recuperación rápida o frecuente.

De forma predeterminada, al crear una instantánea, se almacena en el nivel estándar de instantáneas de Amazon EBS (nivel estándar). Las instantáneas almacenadas en el nivel estándar son progresivas. Eso significa que solo los bloques del volumen que han cambiado después de la última instantánea se guardan.

Al archivar una instantánea, la instantánea progresiva se convierte en una instantánea completa y se mueve del nivel estándar al nivel de archivo de instantáneas de Amazon EBS (nivel de archivo). Las instantáneas completas incluyen todos los bloques que se escribieron en el volumen en el momento en que se creó la instantánea.

Cuando necesite acceder a una instantánea archivada, puede restaurarla del nivel de archivo al nivel estándar y, a continuación, utilizarla de la misma manera que utiliza cualquier otra instantánea de su cuenta.

El archivo de instantáneas de Amazon EBS ofrece una reducción de hasta el 75 % menos de los costos de almacenamiento de instantáneas para las instantáneas que planea almacenar durante 90 días o más y a las que rara vez necesita acceder.

Algunos casos de uso típicos:

- Archivado de la única instantánea de un volumen, como instantáneas de fin de proyecto

- Archivado de instantáneas progresivas completas y puntuales por motivos de conformidad.
- Archivado de instantáneas progresivas mensuales, trimestrales o anuales.

Temas

Consideraciones y limitaciones

Consideraciones

- El periodo de archivo mínimo es de 90 días. Si elimina o restaura permanentemente una instantánea archivada antes del periodo de archivado mínimo de 90 días, se facturarán los días restantes en el nivel de archivo, redondeados a la hora más cercana. Para obtener más información, consulte Precios y facturación.
- Puede tardar hasta 72 horas en restaurar una instantánea archivada del nivel de archivo al nivel estándar, según el tamaño de la instantánea.
- Las instantáneas archivadas siempre son instantáneas completas. Una instantánea completa contiene todos los bloques escritos en el volumen en el momento en que se creó la instantánea. Es probable que la instantánea completa sea mayor que la instantánea progresiva a partir de la cual se creó. Sin embargo, si solo tiene una instantánea progresiva de un volumen en el nivel estándar, el tamaño de la instantánea completa del nivel de archivo será igual al de la instantánea en el nivel estándar. Esto se debe a que la primera instantánea tomada de un volumen es siempre una instantánea completa.
- Se recomienda archivar las instantáneas mensuales, trimestrales o anuales. Archivar instantáneas incrementales diarias de un solo volumen puede generar costos más altos en comparación con mantenerlas en el nivel estándar.
- Cuando se archiva una instantánea, los datos de la instantánea a la que hacen referencia otras instantáneas del linaje de instantáneas se retienen en el nivel estándar. Los costos de datos y

almacenamiento asociados a los datos referenciados que se retienen en el nivel estándar se asignan a la siguiente instantánea del linaje. Esto garantiza que las instantáneas posteriores del linaje no se vean afectadas por el archivado.

- Si elimina una instantánea archivada que coincide con una regla de retención de la papelera de reciclaje, la instantánea archivada se conserva en la papelera de reciclaje durante el periodo de retención definido en la regla de retención. Para utilizar la instantánea, primero debe recuperarla de la papelera de reciclaje y, a continuación, restaurarla desde el nivel de archivo. Para obtener más información, consulte Papelera de reciclaje y Precios y facturación.
- No puede utilizar una instantánea archivada en una asignación de dispositivos de bloques ni para crear un volumen de Amazon EBS.
- Puede archivar las instantáneas que cree AWS Backup mediante la Consola de AWS Backup, las API o las herramientas de línea de comandos. Para obtener más información, consulte Crear un plan de copia de seguridad en la Guía para desarrolladores de AWS Backup.

Limitaciones

- Puede archivar instantáneas que se encuentran solo en el estado `completed`.
- Solo puede archivar instantáneas que posea en su cuenta. Para archivar una instantánea que alguien le comparte, copie primero la instantánea a su cuenta y, a continuación, archive la copia de la instantánea.
- Antes de poder utilizar una instantánea archivada, primero debe restaurarla al nivel estándar. La restauración al nivel estándar es necesaria para crear un volumen a partir de la instantánea mediante las operaciones de la API `CreateVolume` y `RunInstances`, así como para compartir o copiar una instantánea. Para obtener más información, consulte Restaurar una instantánea archivada.
- Puede archivar una instantánea que esté asociada a una o varias AMI solo si todas las AMI asociadas están deshabilitadas. Para obtener más información, consulte Deshabilitar una AMI.
- No puede habilitar una AMI deshabilitada si las instantáneas asociadas se restauran temporalmente. Todas las instantáneas asociadas deben restaurarse permanentemente para poder habilitar la AMI.
- No puede cancelar el archivo de instantáneas o el proceso de restauración de instantáneas después de haberlo iniciado.
- No puede compartir instantáneas archivadas. Si archiva una instantánea que ha compartido con otras cuentas, las cuentas con las que se comparte la instantánea pierden el acceso después de archivar la instantánea.

- No puede copiar una instantánea archivada. Si necesita copiar una instantánea archivada, primero debe restaurarla.
- No se puede habilitar la restauración rápida de instantáneas para una instantánea archivada. La restauración rápida de instantáneas se desactiva automáticamente cuando se archiva una instantánea. Si necesita utilizar la restauración rápida de instantáneas, debe habilitarla de forma manual después de restaurar la instantánea.

Precios y facturación

Las instantáneas archivadas se facturan a una tarifa de 0,0125 USD por GB al mes. Por ejemplo, si archiva una instantánea de 100 GiB, se facturará 1,25 USD (100 GiB * 0,0125 USD) al mes.

Las restauraciones de instantáneas se facturan a una tarifa de 0,03 USD por GB de datos restaurados. Por ejemplo, si restaura una instantánea de 100 GiB desde el nivel de archivo, se facturará una vez por 3 USD (100 GiB * 0,03 USD).

Una vez restaurada la instantánea en el nivel estándar, la instantánea se facturará a la tarifa estándar para las instantáneas de 0,05 USD por GB al mes.

Para obtener más información, consulte Precios Amazon EBS.

Facturación durante el periodo de archivo mínimo

El periodo de archivo mínimo es de 90 días. Si elimina o restaura permanentemente una instantánea archivada antes del periodo de archivo mínimo de 90 días, se facturará un cargo prorrateado igual al cargo por almacenamiento del nivel de archivo durante los días restantes, redondeado a la hora más cercana. Por ejemplo, si elimina o restaura permanentemente una instantánea archivada transcurridos 40 días, se facturarán los 50 días restantes del periodo de archivo mínimo.

> **Note**
>
> La restauración temporal de una instantánea archivada antes del periodo de archivo mínimo de 90 días no supone este cargo.

Restauraciones temporales

Cuando restaura temporalmente una instantánea, la instantánea se restaura del nivel de archivo al nivel estándar y una copia de la instantánea permanece en el nivel de archivo. Se facturará tanto

la instantánea del nivel estándar como la copia de instantáneas en el nivel de archivo durante el periodo de restauración temporal. Cuando la instantánea restaurada temporalmente se elimina del nivel estándar, ya no se facturará y se facturará la instantánea únicamente en el nivel de archivo.

Restauraciones permanentes

Cuando restaura permanentemente una instantánea, la instantánea se restaura del nivel de archivo al nivel estándar y la instantánea se elimina del nivel de archivo. Solo se facturará la instantánea en el nivel estándar.

Eliminación de instantáneas

Si elimina una instantánea mientras se archiva, se facturarán los datos de instantáneas que ya se han movido al nivel de archivo. Estos datos están sujetos al periodo de archivo mínimo de 90 días y se facturan en consecuencia al eliminarlos. Por ejemplo, si archiva una instantánea de 100 GiB y la elimina después de que solo se hayan archivado 40 GiB, se le facturará 1,50 USD por el periodo mínimo de archivo de 90 días por los 40 GiB que ya se han archivado (0,0125 USD por GB por mes * 40 GB * (90 días * 24 horas) / (24 horas/día * mes de 30 días).

Si elimina una instantánea mientras se está restaurando desde el nivel de archivo, se facturará la restauración de instantáneas por el tamaño completo de la instantánea (tamaño de la instantánea * 0,03 USD). Por ejemplo, si restaura una instantánea de 100 GiB del nivel de archivo y la elimina en cualquier momento antes de que finalice la restauración de instantáneas, se facturarán 3 USD (tamaño de instantánea de 100 GiB * 0,03 USD).

Papelera de reciclaje

Las instantáneas archivadas se facturan al precio de las instantáneas archivadas mientras se encuentran en la papelera de reciclaje. Las instantáneas archivadas que se encuentran en la papelera de reciclaje están sujetas al periodo de archivado mínimo de 90 días y se facturan en consecuencia si la papelera de reciclaje las elimina antes del periodo de archivado mínimo. En otras palabras, si una regla de retención elimina una instantánea archivada de la papelera de reciclaje antes del periodo mínimo de 90 días, se facturarán los días restantes.

Si elimina una instantánea que coincide con una regla de retención mientras se archiva la instantánea, la instantánea archivada se conserva en la papelera de reciclaje durante el periodo de retención definido en la regla de retención. Se factura a la tarifa de las instantáneas archivadas.

Si elimina una instantánea que coincide con una regla de retención mientras se restaura la instantánea, la instantánea restaurada se conserva en la papelera de reciclaje durante el resto del

periodo de retención y se facturará al precio de instantáneas estándar. Para utilizar la instantánea restaurada, primero debe recuperarla de la papelera de reciclaje.

Para obtener más información, consulte Papelera de reciclaje.

Seguimiento de costos

Las instantáneas archivadas aparecen en el AWS Cost and Usage Report con el mismo ID de recurso y el mismo nombre de recurso de Amazon (ARN). Para obtener más información, consulte la Guía del usuario de AWS Cost and Usage Report.

Puede utilizar los siguientes tipos de uso para identificar los costos asociados:

- `SnapshotArchiveStorage`: tarifa por almacenamiento de datos mensual
- `SnapshotArchiveRetrieval`: tarifa de pago por única vez para restauraciones de instantáneas
- `SnapshotArchiveEarlyDelete`: tarifa por eliminar o restaurar permanentemente una instantánea antes del periodo mínimo de archivo (90 días)

Cuotas

En esta sección, se describen las cuotas predeterminadas para las instantáneas archivadas y en curso.

Cuota	Cuota predeterminada			
Instantáneas archivadas por volumen	25			
Archivos de instantáneas simultáneas en	25			

Cuota	Cuota predeterminada			
curso por cuenta				
Restauraciones de instantáneas simultáneas en curso por cuenta	5			

Si necesita incrementar los límites predeterminados, complete el formulario Create case (Crear caso) de AWS Support Center para solicitar el aumento del límite.

Directrices y prácticas recomendadas para archivar instantáneas

En esta sección, se proporcionan algunas directrices y prácticas recomendadas para archivar instantáneas.

Temas

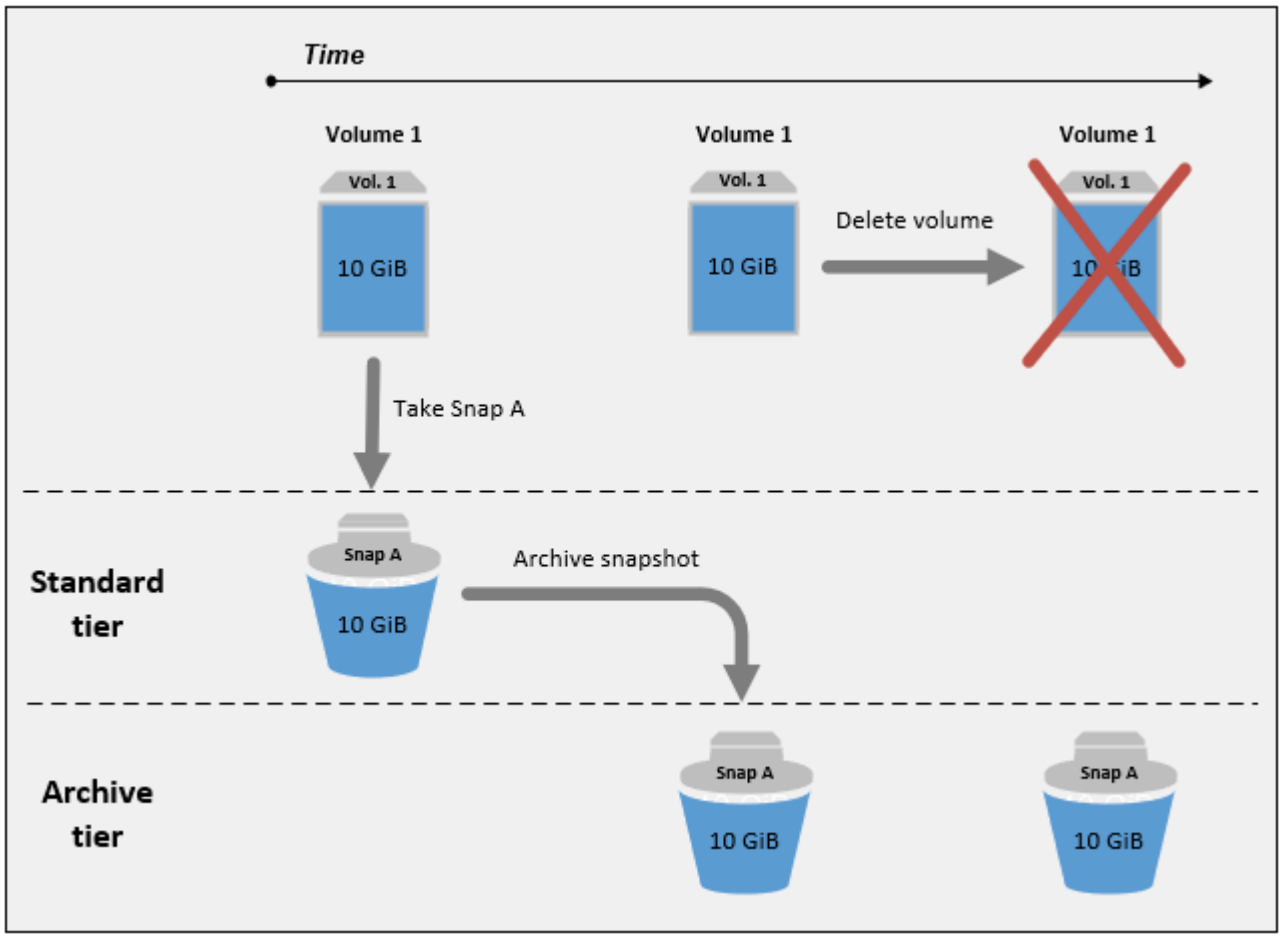
- Archivado de la única instantánea de un volumen
- Archivado de instantáneas progresivas de un solo volumen
- Archivado de instantáneas completas por motivos de conformidad
- Determinación de la reducción de los costos de almacenamiento del nivel estándar

Archivado de la única instantánea de un volumen

Cuando solo tiene una instantánea de un volumen, la instantánea siempre tiene el mismo tamaño que los bloques escritos en el volumen en el momento en que se creó la instantánea. Al archivar una

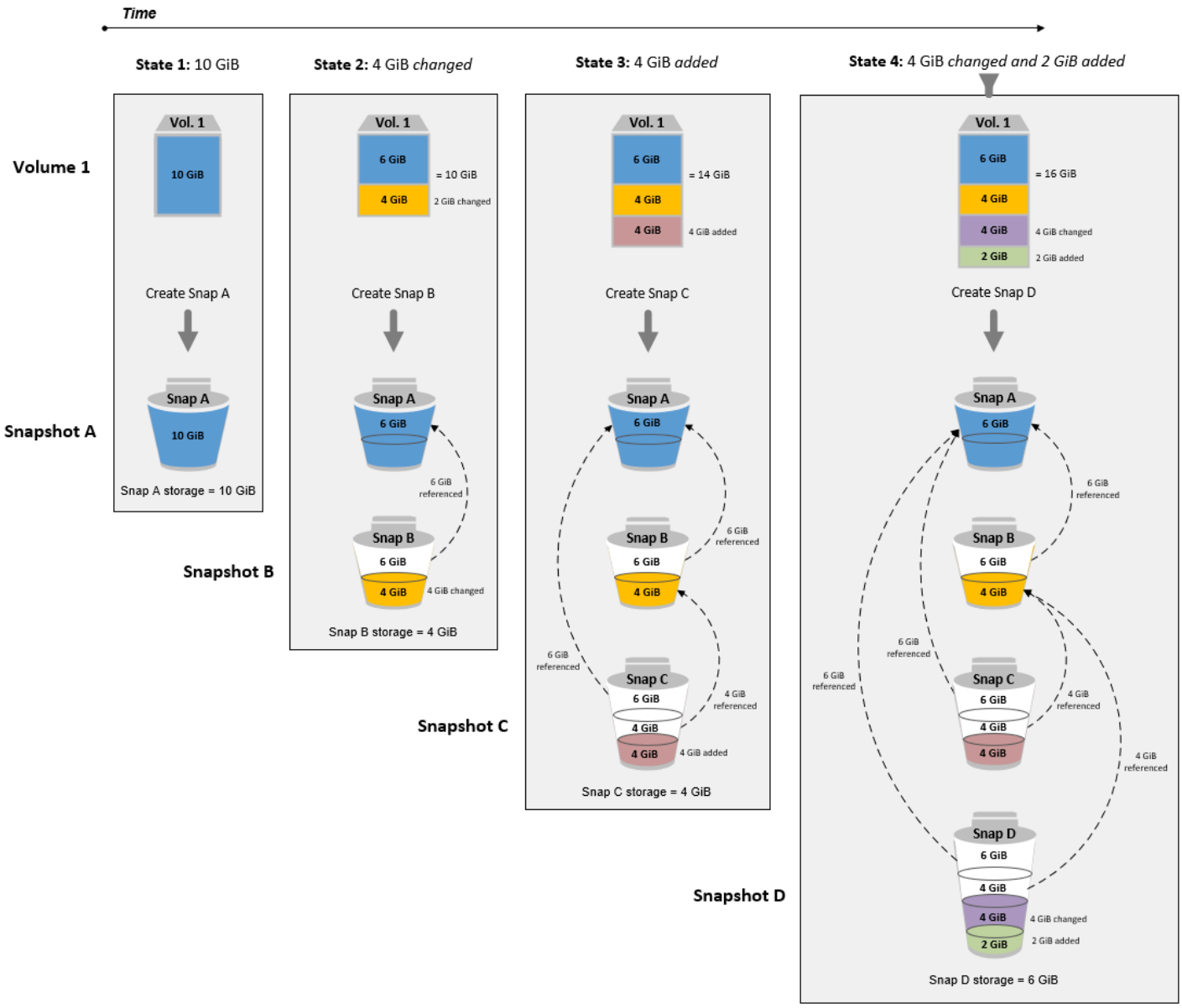
instantánea de este tipo, la instantánea del nivel estándar se convierte en una instantánea completa de tamaño equivalente y se mueve del nivel estándar al nivel de archivo.

El archivado de estas instantáneas puede ayudarlo a ahorrar con menores costos de almacenamiento. Si ya no necesita el volumen de origen, puede eliminarlo para obtener mayores ahorros en los costos de almacenamiento.



Archivado de instantáneas progresivas de un solo volumen

Cuando archiva una instantánea progresiva, la instantánea se convierte en una instantánea completa y se mueve al nivel de archivo. Por ejemplo, en la imagen siguiente, si archiva Snap B, la instantánea se convierte en una instantánea completa de 10 GiB de tamaño y se mueve al nivel de archivo. Del mismo modo, si archiva Snap C, el tamaño de la instantánea completa del nivel de archivo es de 14 GiB.



Si va a archivar instantáneas para reducir los costos de almacenamiento en el nivel estándar, no debe archivar la primera instantánea de un conjunto de instantáneas progresivas. A estas instantáneas se hace referencia mediante instantáneas posteriores en el linaje de instantáneas. En la mayoría de los casos, archivar estas instantáneas no reducirá los costos de almacenamiento.

> **Note**
>
> No debe archivar la última instantánea de un conjunto de instantáneas progresivas. La última instantánea es la más reciente tomada de un volumen. Necesitará esta instantánea en el

nivel estándar si desea crear volúmenes a partir de ella en caso de daños o pérdidas de volumen.

Si archiva una instantánea que contiene datos a los que hace referencia una instantánea posterior del linaje, los costos de almacenamiento y almacenamiento de datos asociados con los datos de referencia se asignan a la última instantánea del linaje. En este caso, archivar la instantánea no reducirá los costos de almacenamiento ni almacenamiento de datos. Por ejemplo, en la imagen anterior, si archiva Snap B, sus 4 GiB de datos se atribuyen a Snap C. En este caso, los costos generales de almacenamiento aumentarán porque incurre en costos de almacenamiento para la versión completa de Snap B en el nivel de archivo y los costos de almacenamiento de información del nivel estándar permanecen sin cambios.

Si archiva Snap C, el almacenamiento de nivel estándar disminuirá en 4 GiB porque ninguna otra instantánea hace referencia a los datos más adelante en el linaje. Además, el almacenamiento del nivel de archivo aumentará en 14 GiB porque la instantánea se convierte en una instantánea completa.

Archivado de instantáneas completas por motivos de conformidad

Es posible que tenga que crear copias de seguridad completas de volúmenes de forma mensual, trimestral o anual por motivos de conformidad. Para estas copias de seguridad, es posible que necesite instantáneas independientes sin referencias hacia atrás o hacia adelante a otras instantáneas del linaje de instantáneas. Las instantáneas archivadas con archivo de instantáneas de EBS son instantáneas completas y no tienen ninguna referencia a otras instantáneas del linaje. Además, es probable que deba retener estas instantáneas por motivos de conformidad durante varios años. El archivo de instantáneas de EBS hace que sea rentable archivar estas instantáneas completas para su retención a largo plazo.

Determinación de la reducción de los costos de almacenamiento del nivel estándar

Si desea archivar una instantánea progresiva para reducir los costos de almacenamiento, debe tener en cuenta el tamaño de la instantánea completa en el nivel de archivo y la reducción del almacenamiento en el nivel estándar. En esta sección, se explica cómo se realiza.

> **Important**
>
> Las respuestas de las API son datos precisos en el momento en que se llama a las API. Las respuestas de las API pueden variar a medida que los datos asociados a una instantánea cambian como resultado de los cambios en el linaje de instantáneas.

Para determinar la reducción de los costos de almacenamiento y el almacenamiento en el nivel estándar, siga los siguientes pasos.

1. Verifique el tamaño de la instantánea completa. Para determinar el tamaño completo de la instantánea, utilice el comando list-snapshot-blocks. Para `--snapshot-id`, especifique el ID de la instantánea que desea archivar.

   ```
   $  aws ebs list-snapshot-blocks --snapshot-id snapshot_id
   ```

   Devuelve información acerca de todos los bloques de la instantánea especificada. El `BlockIndex` del último bloque devuelto por el comando indica el número de bloques de la instantánea. El número de bloques multiplicados por 512 KiB, que es el tamaño del bloque de instantáneas, proporciona una aproximación cercana del tamaño de la instantánea completa en el nivel de archivo (bloques * 512 KiB = tamaño de instantánea completo).

   Por ejemplo, el siguiente comando enumera los bloques para la instantánea `snap-01234567890abcdef`.

   ```
   $  aws ebs list-snapshot-blocks --snapshot-id snap-01234567890abcdef
   ```

   A continuación se muestra el resultado del comando, con algunos bloques omitidos. El siguiente resultado indica que la instantánea incluye unos 16 383 bloques de datos. Esto se aproxima a un tamaño completo de instantánea de aproximadamente 8 GiB (16 383 * 512 KiB = 7,99 GiB).

   ```
    {
       "VolumeSize": 8,
       "Blocks": [
           {
               "BlockToken": "ABgBAeShfa5RwG+RiWUg2pwmnCU/
   YMnV7fGMxLbCWfEBEUmmuqac5RmoyVat",
               "BlockIndex": 0
           },
   ```

```
        {
            "BlockToken": "ABgBATdTONyThPUAbQhbUQXsn5TGoY/
J17GfE83j9WN7siupavOTw9E1KpFh",
            "BlockIndex": 1
        },
        {
            "BlockToken": "EBEUmmuqXsn5TGoY/QwmnCU/YMnV74eKE2TSsn5TGoY/
E83j9WQhbUQXsn5T",
            "BlockIndex": 4
        },
        .....
        {
            "BlockToken": "yThPUAbQhb5V8xpwmnCU/
YMnV74eKE2TSFY1sKP/4r05y47WETdTONyThPUA",
            "BlockIndex": 12890
        },
        {
            "BlockToken":
 "ABgBASHKD5V8xEbaRKdxdkZZS4eKE2TSFYlMG1sKP/4r05y47WEHqKaNPcLs",
            "BlockIndex": 12906
        },
        {
            "BlockToken": "ABgBARROGMUJo6P9X3CFHQGZNQ7av9B6vZtTTqV89QqC
+SkO0HWMlwkGXjnA",
            "BlockIndex": 16383
        }
    ],
    "VolumeSize": 8,
    "ExpiryTime": 1637677800.845,
    "BlockSize": 524288
}
```

2. Busque el volumen de origen a partir del cual se creó la instantánea que desea archivar. Utilice el comando describe-snapshots. Para `--snapshot-id`, especifique el ID de la instantánea que desea archivar. El parámetro de respuesta `VolumeId` indica el ID del volumen de origen.

```
$ aws ec2 describe-snapshots --snapshot-id snapshot_id
```

Por ejemplo, el siguiente comando devuelve información sobre la instantánea `snap-09c9114207084f0d9`.

```
$ aws ec2 describe-snapshots --snapshot-id snap-09c9114207084f0d9
```

A continuación, se muestra el resultado del comando, que indica que esa instantánea `snap-09c9114207084f0d9` se creó a partir del volumen `vol-0f3e2c292c52b85c3`.

```
{
    "Snapshots": [
        {
            "Description": "",
            "Tags": [],
            "Encrypted": false,
            VolumeId": "vol-0f3e2c292c52b85c3",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-11-16T08:29:49.840Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-09c9114207084f0d9"
        }
    ]
}
```

3. Busque todas las instantáneas creadas a partir del volumen de origen. Utilice el comando describe-snapshots. Especifique el filtro `volume-id` y, para el valor del filtro, especifique el ID de volumen del paso anterior.

```
$ aws ec2 describe-snapshots --filters "Name=volume-id, Values=volume_id"
```

Por ejemplo, el siguiente comando devuelve todas las instantáneas creadas a partir del volumen `vol-0f3e2c292c52b85c3`.

```
$ aws ec2 describe-snapshots --filters "Name=volume-id,
 Values=vol-0f3e2c292c52b85c3"
```

A continuación, se muestra el resultado del comando, que indica que se han creado tres instantáneas a partir del volumen `vol-0f3e2c292c52b85c3`.

```
{
    "Snapshots": [
        {
            "Description": "",
            "Tags": [],
```

```
            "Encrypted": false,
            "VolumeId": "vol-0f3e2c292c52b85c3",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-11-14T08:57:39.300Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-08ca60083f86816b0"
        },
        {
            "Description": "",
            "Tags": [],
            "Encrypted": false,
            "VolumeId": "vol-0f3e2c292c52b85c3",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-11-15T08:29:49.840Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-09c9114207084f0d9"
        },
        {
            "Description": "01",
            "Tags": [],
            "Encrypted": false,
            "VolumeId": "vol-0f3e2c292c52b85c3",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-11-16T07:50:08.042Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-024f49fe8dd853fa8"
        }
    ]
}
```

4. Con el resultado del comando anterior, ordene las instantáneas según sus tiempos de creación, de la más temprana a la más reciente. El parámetro de respuesta `StartTime` para cada instantánea indica su hora de creación, en formato de hora UTC.

   Por ejemplo, las instantáneas devueltas en el paso anterior organizadas por tiempo de creación, desde la más temprana hasta la más reciente, son las siguientes:

1. `snap-08ca60083f86816b0` (la más temprana: creada antes de la instantánea que desea archivar)
2. `snap-09c9114207084f0d9` (La instantánea que se va a archivar)
3. `snap-024f49fe8dd853fa8` (la más reciente: creada después de la instantánea que desea archivar)

5. Identifique las instantáneas que se crearon inmediatamente antes y después de la instantánea que desea archivar. En este caso, desea archivar la instantánea `snap-09c9114207084f0d9`, que fue la segunda instantánea progresiva creada en el conjunto de tres instantáneas. La instantánea `snap-08ca60083f86816b0` se creó inmediatamente antes y la instantánea `snap-024f49fe8dd853fa8` se creó inmediatamente después.
6. Busque los datos sin referencia en la instantánea que desea archivar. En primer lugar, busque los bloques diferentes entre la instantánea que se creó inmediatamente antes de la instantánea que desea archivar y la instantánea que desea archivar. Utilice el comando list-changed-blocks. Para `--first-snapshot-id`, especifique el ID de la instantánea creada inmediatamente antes de la instantánea que desea archivar. Para `--second-snapshot-id`, especifique el ID de la instantánea que desea archivar.

```
$ aws ebs list-changed-blocks --first-snapshot-id snapshot_created_before --second-
snapshot-id snapshot_to_archive
```

Por ejemplo, el siguiente comando muestra los índices de bloque de los bloques que son diferentes entre la instantánea `snap-08ca60083f86816b0` (la instantánea creada antes de la instantánea que desea archivar) y la instantánea `snap-09c9114207084f0d9` (la instantánea que desea archivar).

```
$ aws ebs list-changed-blocks --first-snapshot-id snap-08ca60083f86816b0 --second-
snapshot-id snap-09c9114207084f0d9
```

A continuación, se muestra el resultado del comando, con algunos bloques omitidos.

```
{
    "BlockSize": 524288,
    "ChangedBlocks": [
        {
            "FirstBlockToken": "ABgBAX6y
+WH6Rm9y5zq1VyeTCmEzGmTT0jNZG1cDirFq1rOVeFbWXsH3W4z/",
```

```
            "SecondBlockToken": "ABgBASyx0bHHBnTERu
+9USLxYK/81UT0dbHIUFqUjQUkwTwK5qkjP8NSGyNB",
            "BlockIndex": 4
        },
        {
            "FirstBlockToken": "ABgBAcfL
+EfmQmlNgstqrFnYgsAxR4SDSO4LkNLYOOChGBWcfJnpn90E9XX1",
            "SecondBlockToken": "ABgBAdX0mtX6aBAt3EBy
+8jFCESMpig7csKjbO2Ocd08m2iNJV2Ue+cRwUqF",
            "BlockIndex": 5
        },
        {
            "FirstBlockToken": "ABgBAVBaFJmbP/eRHGh7vnJlAwyiyNUi3MKZmEMxs2wC3AmM/
fc6yCOAMb65",
            "SecondBlockToken":
 "ABgBAdewWkHKTcrhZmsfM7GbaHyXD1Ctcn2nppz4wYItZRmAo1M72fpXU0Yv",
            "BlockIndex": 13
        },
        {
            "FirstBlockToken": "ABgBAQGxwuf6z095L6DpRoVRVnOqPxmx9r7Wf6O+i
+ltZ0dwPpGN39ijztLn",
            "SecondBlockToken": "ABgBAUdlitCVI7c6hGsT4ckkKCw6bMRclnV
+bKjViu/9UESTcW7CD9w4J2td",
            "BlockIndex": 14
        },
        {
            "FirstBlockToken":
 "ABgBAZBfEv4EHS1aSXTXxSE3mBZG6CNeIkwxpljzmgSHICGlFmZCyJXzE4r3",
            "SecondBlockToken":
 "ABgBAVWR7QuQQB0AP2TtmNkgS4Aec5KAQVCldnpc91zBiNmSfW9ouIlbeXWy",
            "BlockIndex": 15
        },
        .....
        {
            "SecondBlockToken": "ABgBAeHwXPL+z3DBLjDhwjdAM9+CPGV5VO5Q3rEEA
+ku50P498hjnTAgMhLG",
            "BlockIndex": 13171
        },
        {
            "SecondBlockToken":
 "ABgBAbZcPiVtLx6U3Fb4lAjRdrkJMwW5M2tiCgIp6ZZpcZ8AwXxkjVUUHADq",
            "BlockIndex": 13172
        },
        {
```

```
            "SecondBlockToken": "ABgBAVmEd/pQ9VW9hWiOujOAKcauOnUFCO
+eZ5ASVdWLXWWC04ijfoDTpTVZ",
            "BlockIndex": 13173
        },
        {
            "SecondBlockToken": "ABgBAT/jeN7w
+8ALuNdaiwXmsSfM6tOvMoLBLJ14LKvavw4IiB1d0iykWe6b",
            "BlockIndex": 13174
        },
        {
            "SecondBlockToken": "ABgBAXtGvUhTjjUqkwKXfXzyR2GpQei/
+pJSG/19ESwvt7Hd8GHaUqVs6Zf3",
            "BlockIndex": 13175
        }
    ],
    "ExpiryTime": 1637648751.813,
    "VolumeSize": 8
}
```

A continuación, utilice el mismo comando para buscar bloques que son diferentes entre la instantánea que desea archivar y la instantánea que se creó inmediatamente después de ella. Para `--first-snapshot-id`, especifique el ID de la instantánea que desea archivar. Para `--second-snapshot-id`, especifique el ID de la instantánea creada inmediatamente después de la instantánea que desea archivar.

```
$ aws ebs list-changed-blocks --first-snapshot-id snapshot_to_archive --second-
snapshot-id snapshot_created_after
```

Por ejemplo, el siguiente comando muestra los índices de bloque de los bloques que son diferentes entre la instantánea `snap-09c9114207084f0d9` (la instantánea que desea archivar) y la instantánea `snap-024f49fe8dd853fa8` (la instantánea creada después de la instantánea que desea archivar).

```
$ aws ebs list-changed-blocks --first-snapshot-id snap-09c9114207084f0d9 --second-
snapshot-id snap-024f49fe8dd853fa8
```

A continuación, se muestra el resultado del comando, con algunos bloques omitidos.

```
{
```

```
    "BlockSize": 524288,
    "ChangedBlocks": [
        {
            "FirstBlockToken": "ABgBAVax0bHHBnTERu
+9USLxYK/81UT0dbSnkDk0gqwRFSFGWA7HYbkkAy5Y",
            "SecondBlockToken":
 "ABgBASEvi9x8Om7Htp37cKG2NT9XUzEbLHpGcayelomSoHpGy8LGyvG0yYfK",
            "BlockIndex": 4
        },
        {
            "FirstBlockToken": "ABgBAeL0mtX6aBAt3EBy+8jFCESMpig7csfMrI4ufnQJT3XBm/
pwJZ1n2Uec",
            "SecondBlockToken": "ABgBAXmUTg6rAI
+v0LvekshbxCVpJjWILvxgC0AG0GQBEUNRVHkNABBwXLkO",
            "BlockIndex": 5
        },
        {
            "FirstBlockToken":
 "ABgBATKwWkHKTcrhZmsfM7GbaHyXD1CtcnjIZv9YzisYsQTMHfTfh4AhS0s2",
            "SecondBlockToken": "ABgBAcmiPFovWgXQio
+VBrxOqGy4PKZ9SAAHaZ2HQBM9fQQU0+EXxQjVGv37",
            "BlockIndex": 13
        },
        {
            "FirstBlockToken":
 "ABgBAbRlitCVI7c6hGsT4ckkKCw6bMRclnARrMt1hUbIhFnfz8kmUaZOP2ZE",
            "SecondBlockToken": "ABgBAXe935n544+rxhJ0INB8q7pAeoPZkkD27vkspE/
qKyvOwpozYII6UNCT",
            "BlockIndex": 14
        },
        {
            "FirstBlockToken": "ABgBAd+yxCO26I
+1Nm2KmuKfrhjCkuaP6LXuol3opCNk6+XRGcct4suBHje1",
            "SecondBlockToken": "ABgBAcPpnXz821NtTvWBPTz8uUFXnS8jXubvghEjZulIjHgc
+7saWys77shb",
            "BlockIndex": 18
        },
        .....
        {
            "SecondBlockToken": "ABgBATni4sDE5rS8/a9pqV03lU/lKCW
+CTxFl3cQ5p2f2h1njpuUiGbqKGUa",
            "BlockIndex": 13190
        },
        {
```

```
            "SecondBlockToken": "ABgBARbXo7zFhu7IEQ/9VMYFCTCtCuQ
+iSlWVpBIshmeyeS5FD/M0i64U+a9",
            "BlockIndex": 13191
        },
        {
            "SecondBlockToken": "ABgBAZ8DhMk+rROXa4dZlNK45rMYnVIGGSyTeiMli/sp/
JXUVZKJ9sMKIsGF",
            "BlockIndex": 13192
        },
        {
            "SecondBlockToken":
 "ABgBATh6MBVE904l6sqOC27s1nVntFUpDwiMcRWGyJHy8sIgGL5yuYXHAVty",
            "BlockIndex": 13193
        },
        {
            "SecondBlockToken":
 "ABgBARuZykaFBWpCWrJPXaPCneQMbyVgnITJqj4c1kJWPIj5Gn61OQyy+giN",
            "BlockIndex": 13194
        }
    ],
    "ExpiryTime": 1637692677.286,
    "VolumeSize": 8
}
```

7. Compare el resultado devuelto por ambos comandos en el paso anterior. Si aparece el mismo índice de bloques en los dos resultados de los comandos, significa que el bloque contiene datos sin referencia.

   Por ejemplo, el resultado del comando del paso anterior indica que los bloques 4, 5, 13 y 14 son exclusivos de la instantánea `snap-09c9114207084f0d9` y que ninguna otra instantánea del linaje de instantáneas hace referencia a ellos.

   Para determinar la reducción en el almacenamiento de niveles estándar, multiplique el número de bloques que aparecen en ambas salidas de comandos por 512 KiB, que es el tamaño del bloque de instantáneas.

   Por ejemplo, si aparecen 9950 índices de bloque en los dos resultados de comandos, indica que reducirá el almacenamiento de nivel estándar en unos 4,85 GiB (9950 bloques * 512 KiB = 4,85 GiB).

8. Determine los costos de almacenamiento para almacenar los bloques sin referencia en el nivel estándar durante 90 días. Compare este valor con el costo de almacenar la instantánea

completa, descrito en el paso 1, en el nivel de archivo. Puede determinar el ahorro de costos al comparar los valores y suponiendo que no restaurará la instantánea completa desde el nivel de archivo durante el periodo mínimo de 90 días. Para obtener más información, consulte Precios y facturación.

Permisos de IAM necesarios

De forma predeterminada, los usuarios no tienen permiso para utilizar el archivado de instantáneas. Para permitir a los usuarios de IAM utilizar el archivado de instantáneas, tiene que crear políticas que les concedan permisos para utilizar recursos y acciones de API específicos. Para obtener más información, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Para utilizar el archivado de instantáneas, los usuarios necesitan los siguientes permisos.

- `ec2:DescribeSnapshotTierStatus`
- `ec2:ModifySnapshotTier`
- `ec2:RestoreSnapshotTier`

Es posible que los usuarios de la consola necesiten permisos adicionales, por ejemplo `ec2:DescribeSnapshots`.

Para archivar y restaurar instantáneas cifradas, se requieren los siguientes permisos de AWS KMS adicionales.

- `kms:CreateGrant`
- `kms:Decrypt`
- `kms:DescribeKey`

A continuación, se muestra un ejemplo de política de IAM que concede a los usuarios de IAM permiso para archivar, restaurar y ver instantáneas cifradas y no cifradas. Incluye el permiso `ec2:DescribeSnapshots` para los usuarios de la consola. Si algunos permisos no se necesitan, puede eliminarlos de la política.

> **Tip**
>
> Para seguir el principio de privilegios mínimos, no permita el acceso completo a `kms:CreateGrant`. En su lugar, use la clave de condición

`kms:GrantIsForAWSResource` para permitir al usuario crear concesiones en la clave de KMS solo cuando un servicio de AWS haya creado la concesión en nombre del usuario, como se muestra en el siguiente ejemplo.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeSnapshotTierStatus",
            "ec2:ModifySnapshotTier",
            "ec2:RestoreSnapshotTier",
            "ec2:DescribeSnapshots",
            "kms:CreateGrant",
            "kms:Decrypt",
            "kms:DescribeKey"
        ],
        "Resource": "*",
        "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
    }]
}
```

Para dar acceso, añada permisos a los usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center.
- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones de Creación de un rol para un proveedor de identidades de terceros (federación) en la Guía del usuario de IAM.
- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.

- (No recomendado) Asocie una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Trabajo con el archivado de instantáneas

Temas

- Archivo de una instantánea
- Restaurar una instantánea archivada
- Modificar el periodo de restauración o el tipo de restauración de una instantánea restaurada temporalmente
- Ver instantáneas archivadas

Archivo de una instantánea

Puede archivar cualquier instantánea que se encuentre en el estado `completed` y que posea en su cuenta. No se pueden archivar instantáneas que se encuentran en el estado `pending` o `error`, o instantáneas que alguien le comparte. Para obtener más información, consulte Consideraciones y limitaciones.

Si la instantánea está asociada a una o varias AMI, primero debe deshabilitar esas AMI asociadas para poder archivar la instantánea. Para obtener más información, consulte Deshabilitar una AMI.

Las instantáneas archivadas retienen su ID de instantánea, el estado de cifrado, los permisos de AWS Identity and Access Management (IAM), información del propietario y etiquetas de recursos. Sin embargo, la restauración rápida de instantáneas y el uso compartido de instantáneas se desactivan automáticamente después de archivar la instantánea.

Puede seguir utilizando la instantánea mientras el archivo está en proceso. Tan pronto como el estado de agrupación por niveles de la instantánea llegue al estado `archival-complete`, ya no podrá utilizar la instantánea.

Puede archivar una instantánea mediante uno de los siguientes métodos.

Console

Para archivar una instantánea

Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.

1. En el panel de navegación, elija Instantáneas.
2. En la lista de instantáneas, seleccione la instantánea que desea archivar y elija Actions (Acciones), Archive snapshot (Archivar instantánea).
3. Para confirmar, elija Archive snapshot (Archivar instantánea).

AWS CLI

Para archivar una instantánea

Utilice el comando modify-snapshot-tier de la AWS CLI. Para `--snapshot-id`, especifique el ID de la instantánea a archivar. En `--storage-tier`, especifique `archive`.

```
$ aws ec2 modify-snapshot-tier \
--snapshot-id snapshot_id \
--storage-tier archive
```

Por ejemplo, el siguiente comando archiva la instantánea `snap-01234567890abcedf`.

```
$ aws ec2 modify-snapshot-tier \
--snapshot-id snap-01234567890abcedf \
--storage-tier archive
```

A continuación, se muestra el resultado de este comando. El parámetro de respuesta `TieringStartTime` indica la fecha y la hora en que se inició el proceso de archivo en formato de hora UTC (AAAA-MM-DDTHH:MM:SSZ).

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "TieringStartTime": "2021-09-15T16:44:37.574Z"
}
```

Restaurar una instantánea archivada

Antes de poder utilizar una instantánea archivada, primero debe restaurarla al nivel estándar. La instantánea restaurada tiene el mismo ID de instantánea, estado de cifrado, permisos de IAM, información del propietario y etiquetas de recursos que tenía antes de archivarse. Una vez restaurada, puede utilizarla de la misma forma que utiliza cualquier otra instantánea de la cuenta. La instantánea restaurada es siempre una instantánea completa.

Cuando restaura una instantánea, puede elegir restaurarla de manera permanente o temporal.

Si restaura una instantánea de forma permanente, la instantánea se mueve del nivel de archivo al nivel estándar permanentemente. La instantánea permanece restaurada y lista para utilizar hasta que la vuelva a archivar o la elimine manualmente. Cuando restaura permanentemente una instantánea, esta se elimina del nivel de archivo.

Si restaura una instantánea temporalmente, la instantánea se copia del nivel de archivo al nivel estándar durante un periodo de restauración especificado. La instantánea permanece restaurada y lista para utilizar únicamente durante el periodo de restauración. Durante el periodo de restauración, una copia de la instantánea permanece en el nivel de archivo. Una vez que se vence el periodo, la instantánea se elimina automáticamente del nivel estándar. Puede aumentar o disminuir el periodo de restauración o cambiar el tipo de restauración a permanente en cualquier momento durante el periodo de restauración. Para obtener más información, consulte Modificar el periodo de restauración o el tipo de restauración de una instantánea restaurada temporalmente.

Si va a restaurar instantáneas asociadas a una AMI deshabilitada y tiene intención de utilizar esa AMI, primero debe restaurar permanentemente todas las instantáneas asociadas y, a continuación, rehabilitar la AMI deshabilitada para poder utilizarla. No puede habilitar una AMI si las instantáneas asociadas se restauran temporalmente. Puede usar el siguiente comando para buscar todas las instantáneas asociadas a una AMI.

```
$ C:\> aws ec2 describe-images --image-id ami_id \
  --query Images[*].BlockDeviceMappings[*].Ebs[].SnapshotId[]
```

Puede restaurar una instantánea archivada mediante uno de los siguientes métodos.

Console

Para restaurar una instantánea del archivo

Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.

1. En el panel de navegación, elija Instantáneas.
2. En la lista de instantáneas, seleccione la instantánea archivada que desea restaurar y, a continuación, elija Actions (Acciones), Restore snapshot from archive (Restaurar instantánea desde el archivo).
3. Especifique el tipo de restauración que se va a realizar. En Restore type (Tipo de restauración), realice una de las siguientes operaciones:
   - Para restaurar la instantánea de forma permanente, seleccione Permanent (Permanente).
   - Para restaurar la instantánea temporalmente, seleccione Temporary (Temporal) y, a continuación, en Temporary restore period (Periodo de restauración temporal), ingrese el número de días durante los que desea restaurar la instantánea.
4. Para confirmar, elija Restore snapshot (Restaurar instantánea).

AWS CLI

Para restaurar permanentemente una instantánea archivada

Utilice el comando restore-snapshot-tier de la AWS CLI. Para `--snapshot-id`, especifique el ID de la instantánea que desea restaurar e incluya la opción `--permanent-restore`.

```
$ aws ec2 restore-snapshot-tier \
--snapshot-id snapshot_id \
--permanent-restore
```

Por ejemplo, el siguiente comando restaura la instantánea `snap-01234567890abcedf` de forma permanente.

```
$ aws ec2 restore-snapshot-tier \
--snapshot-id snap-01234567890abcedf \
--permanent-restore
```

A continuación, se muestra el resultado de este comando.

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "IsPermanentRestore": true
}
```

Para restaurar temporalmente una instantánea archivada

Utilice el comando restore-snapshot-tier de la AWS CLI. Omita la opción `--permanent-restore`. Para `--snapshot-id`, especifique el ID de la instantánea que desea restaurar y, en `--temporary-restore-days`, especifique el número de días durante los que desea restaurar la instantánea.

`--temporary-restore-days` debe especificarse en días. El rango permitido es de 1 a 180. Si no especifica ningún valor, el valor predeterminado es 1 día.

```
$ aws ec2 restore-snapshot-tier \
--snapshot-id snapshot_id \
--temporary-restore-days number_of_days
```

Por ejemplo, el siguiente comando restaura temporalmente la instantánea `snap-01234567890abcedf` durante un periodo de restauración de 5 días.

```
$ aws ec2 restore-snapshot-tier \
--snapshot-id snap-01234567890abcedf \
--temporary-restore-days 5
```

A continuación, se muestra el resultado de este comando.

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "RestoreDuration": 5,
    "IsPermanentRestore": false
}
```

Modificar el periodo de restauración o el tipo de restauración de una instantánea restaurada temporalmente

Al restaurar una instantánea temporalmente, debe especificar el número de días durante los que la instantánea permanecerá restaurada en su cuenta. Una vez que se vence el periodo de restauración, la instantánea se elimina automáticamente del nivel estándar.

Puede cambiar el periodo de restauración de una instantánea restaurada temporalmente en cualquier momento.

Puede elegir aumentar o disminuir el periodo de restauración o cambiar el tipo de restauración de temporal a permanente.

Si cambia el periodo de restauración, el nuevo periodo entrará en vigor a partir de la fecha actual. Por ejemplo, si especifica un nuevo periodo de restauración de 5días, la instantánea permanecerá restaurada durante cinco días a partir de la fecha actual.

> **Note**
>
> Puede finalizar una restauración temporal antes de tiempo si establece el periodo de restauración en 1 día.

Si cambia el tipo de restauración de temporal a permanente, la copia de instantáneas se elimina del nivel de archivo y la instantánea permanece disponible en la cuenta hasta que la vuelva a archivar manualmente o la elimine.

Puede modificar el periodo de restauración de una instantánea mediante uno de los siguientes métodos.

Console

Para modificar el periodo de restauración o el tipo de restauración

Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.

1. En el panel de navegación, elija Instantáneas.
2. En la lista de instantáneas, seleccione la instantánea que restauró temporalmente y, a continuación, elija Acciones, Restaurar instantánea desde el archivo.
3. En Tipo de restauración, realice una de las siguientes operaciones:
   - Para cambiar el tipo de restauración de temporal a permanente, seleccione Permanente.
   - Para aumentar o disminuir el periodo de restauración, mantenga Temporal y, a continuación, en Periodo de restauración temporal, ingrese el nuevo periodo de restauración en días.
4. Para confirmar, elija Restaurar instantánea.

AWS CLI

Para modificar el periodo de restauración o cambiar el tipo de restauración

Utilice el comando restore-snapshot-tier de la AWS CLI. En `--snapshot-id`, especifique el ID de la instantánea que restauró de manera temporal anteriormente. Para cambiar el tipo de restauración de temporal a permanente, especifique `--permanent-restore` y omita `--temporary-restore-days`. Para aumentar o disminuir el periodo de restauración, omita `--permanent-restore` y, en `--temporary-restore-days`, especifique el nuevo periodo de restauración en días.

Ejemplo: aumente o disminuya el periodo de restauración

El siguiente comando cambia el periodo de restauración de la instantánea `snap-01234567890abcedf` a `10` días.

```
$ aws ec2 restore-snapshot-tier \
--snapshot-id snap-01234567890abcedf
--temporary-restore-days 10
```

A continuación, se muestra el resultado de este comando.

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "RestoreDuration": 10,
    "IsPermanentRestore": false
}
```

Ejemplo: cambiar el tipo de restauración a permanente

El siguiente comando cambia el tipo de restauración de la instantánea `snap-01234567890abcedf` de temporal a permanente.

```
$ aws ec2 restore-snapshot-tier \
--snapshot-id snap-01234567890abcedf
--permanent-restore
```

A continuación, se muestra el resultado de este comando.

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "IsPermanentRestore": true
}
```

Ver instantáneas archivadas

Puede ver información del nivel de almacenamiento de las instantáneas mediante uno de los siguientes métodos.

Console

Para ver la información del nivel de almacenamiento de una instantánea

Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.

1. En el panel de navegación, elija Instantáneas.
2. En la lista de instantáneas, seleccione la instantánea y elija la pestaña de Nivel de almacenamiento.

   La pestaña proporciona la siguiente información:

   - Last tier change started on (El último cambio de nivel comenzó el): la fecha y la hora en que se inició el último archivo o restauración.
   - Tier change progress (Progreso de cambios de nivel): el porcentaje de progreso de la última acción de archivo o restauración.
   - Nivel de almacenamiento: el nivel de almacenamiento de la instantánea. Siempre `archive` para instantáneas archivadas y `standard` para instantáneas almacenadas en el nivel estándar, incluidas las instantáneas restauradas temporalmente.
   - Tiering status (Estado de la agrupación en niveles): el estado de la última acción de archivo o restauración.
   - Archive completed on (Archivo completado el): la fecha y la hora en que se completó el archivo.
   - Temporary restore expires on (La restauración temporal vence el): la fecha y la hora en que una instantánea restaurada temporalmente está configurada para vencerse.

AWS CLI

Para ver la información de archivo sobre una instantánea archivada

Utilice el comando describe-snapshot-tier-status de la AWS CLI. Especifique el filtro `snapshot-id` y, para el valor del filtro, especifique el ID de instantánea. Como alternativa, para ver todas las instantáneas archivadas, omita el filtro.

```
$ aws ec2 describe-snapshot-tier-status --filters "Name=snapshot-id,
 Values=snapshot_id"
```

El resultado incluye los siguientes parámetros de respuesta:

- `Status`: el estado de la instantánea. Siempre figura `completed` para instantáneas archivadas. Solo las instantáneas que se encuentran en el estado `completed` se pueden archivar.
- `LastTieringStartTime`: la fecha y la hora en que se inició el proceso de archivo en formato de hora UTC (AAAA-MM-DDTHH:MM:SSZ).
- `LastTieringOperationState`: el estado actual del proceso de archivado. Entre los estados posibles se incluyen: `archival-in-progress` | `archival-completed` | `archival-failed` | `permanent-restore-in-progress` | `permanent-restore-completed` | `permanent-restore-failed` | `temporary-restore-in-progress` | `temporary-restore-completed` | `temporary-restore-failed`
- `LastTieringProgress`: el porcentaje del progreso del proceso de archivado de instantáneas.
- `StorageTier`: el nivel de almacenamiento de la instantánea. Siempre `archive` para instantáneas archivadas y `standard` para instantáneas almacenadas en el nivel estándar, incluidas las instantáneas restauradas temporalmente.
- `ArchivalCompleteTime`: la fecha y la hora en que se completó el proceso de archivo en formato de hora UTC (AAAA-MM-DDTHH:MM:SSZ).

Ejemplo

El siguiente comando muestra información acerca de la instantánea `snap-01234567890abcedf`.

```
$ aws ec2 describe-snapshot-tier-status --filters "Name=snapshot-id,
 Values=snap-01234567890abcedf"
```

A continuación, se muestra el resultado de este comando.

```
{
    "SnapshotTierStatuses": [
        {
            "Status": "completed",
            "ArchivalCompleteTime": "2021-09-15T17:33:16.147Z",
```

```
            "LastTieringProgress": 100,
            "Tags": [],
            "VolumeId": "vol-01234567890abcedf",
            "LastTieringOperationState": "archival-completed",
            "StorageTier": "archive",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-01234567890abcedf",
            "LastTieringStartTime": "2021-09-15T16:44:37.574Z"
        }
    ]
}
```

Para ver instantáneas de nivel estándar y archivadas

Utilice el comando describe-snapshot de la AWS CLI. En `--snapshot-ids`, especifique el ID de la vista de instantánea.

```
$ aws ec2 describe-snapshots --snapshot-ids snapshot_id
```

Por ejemplo, el siguiente comando muestra información acerca de la instantánea `snap-01234567890abcedf`.

```
$ aws ec2 describe-snapshots --snapshot-ids snap-01234567890abcedf
```

A continuación, se muestra el resultado de este comando. El parámetro de respuesta `StorageTier` indica si la instantánea está archivada actualmente. `archive` indica que la instantánea está archivada y almacenada actualmente en el nivel de archivo y `standard` indica que la instantánea no está archivada por el momento y que se almacena en el nivel estándar.

En el siguiente ejemplo de salida, solo `Snap A` está archivada. `Snap B` y `Snap C` no están archivadas.

Además, el parámetro de respuesta `RestoreExpiryTime` se devuelve solo para las instantáneas que se restauran temporalmente desde el archivo. Indica cuándo se eliminarán automáticamente las instantáneas restauradas de forma temporal del nivel estándar. No es devuelto para instantáneas que se restauran de forma permanente.

En el siguiente ejemplo de salida, `Snap C` se restaura de manera temporal y se eliminará automáticamente del nivel estándar el 2021-09-19T21:00:00.000Z (19 de septiembre de 2021 a las 21.00 h UTC).

```
{
    "Snapshots": [
        {
            "Description": "Snap A",
            "Encrypted": false,
            "VolumeId": "vol-01234567890aaaaaa",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-09-07T21:00:00.000Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-01234567890aaaaaa",
            "StorageTier": "archive",
            "Tags": []
        },
        {
            "Description": "Snap B",
            "Encrypted": false,
            "VolumeId": "vol-09876543210bbbbbb",
            "State": "completed",
            "VolumeSize": 10,
            "StartTime": "2021-09-14T21:00:00.000Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-09876543210bbbbbb",
            "StorageTier": "standard",
            "RestoreExpiryTime": "2019-09-19T21:00:00.000Z",
            "Tags": []
        },
        {
            "Description": "Snap C",
            "Encrypted": false,
            "VolumeId": "vol-054321543210cccccc",
            "State": "completed",
            "VolumeSize": 12,
            "StartTime": "2021-08-01T21:00:00.000Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-054321543210cccccc",
            "StorageTier": "standard",
            "Tags": []
        }
    ]
```

```
}
```

Para ver solo las instantáneas que se almacenan en el nivel de archivo o en el nivel estándar

Utilice el comando describe-snapshot de la AWS CLI. Incluya la opción `--filter`; para el nombre del filtro, especifique `storage-tier` y, en el valor del filtro, especifique `archive` o `standard`.

```
$ aws ec2 describe-snapshots --filters "Name=storage-tier,Values=archive|standard"
```

Por ejemplo, el siguiente comando muestra solo instantáneas archivadas.

```
$ aws ec2 describe-snapshots --filters "Name=storage-tier,Values=archive"
```

Monitorear el archivo de instantáneas

Amazon EBS emite eventos relacionados con acciones de archivo de instantáneas. Puede utilizar AWS Lambda y Amazon CloudWatch Events para administrar las notificaciones de eventos mediante programación. Los eventos se emiten en la medida de lo posible. Para obtener más información, consulte la Guía del usuario de Amazon CloudWatch Events.

Están disponibles los siguientes eventos:

- `archiveSnapshot`: se emite cuando una acción de archivo de instantáneas se realiza correctamente o produce un error.

  A continuación, se muestra un ejemplo de un evento emitido cuando una acción de archivo de instantáneas se realiza correctamente.

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Snapshot Notification",
   "source": "aws.ec2",
   "account": "123456789012",
   "time": "2021-05-25T13:12:22Z",
   "region": "us-east-1",
   "resources": [
     "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
   ],
```

```
   "detail": {
     "event": "archiveSnapshot",
     "result": "succeeded",
     "cause": "",
     "request-id": "123456789",
     "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
     "startTime": "2021-05-25T13:12:22Z",
     "endTime": "2021-05-45T15:30:00Z",
     "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
```

A continuación, se muestra un ejemplo de un evento emitido cuando se produce un error en una acción de archivo de instantáneas.

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "archiveSnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

- `permanentRestoreSnapshot`: se emite cuando una acción de restauración permanente se realiza correctamente o falla.

  A continuación, se muestra un ejemplo de un evento emitido cuando una acción de restauración permanente se realiza correctamente.

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "permanentRestoreSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-10-45T15:30:00Z"
  }
}
```

A continuación, se muestra un ejemplo de un evento emitido cuando se produce un error en una acción de restauración permanente.

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "permanentRestoreSnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
```

```
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

- `temporaryRestoreSnapshot`: se emite cuando una acción de restauración temporal se realiza correctamente o falla.

  A continuación, se muestra un ejemplo de un evento emitido cuando una acción de restauración temporal se realiza correctamente.

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "temporaryRestoreSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "restoreExpiryTime": "2021-06-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

  A continuación, se muestra un ejemplo de un evento emitido cuando se produce un error en una acción de restauración temporal.

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
```

```
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "temporaryRestoreSnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```


- `restoreExpiry`: se emite cuando se vence el periodo de restauración de una instantánea restaurada temporalmente.

  A continuación, se muestra un ejemplo.


```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "restoryExpiry",
    "result": "succeeded",
    "cause": "",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
```

```
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

Eliminar una instantánea de Amazon EBS

Cuando ya no necesite una instantánea de Amazon EBS de un volumen, puede eliminarlo. La eliminación de una instantánea no tiene ningún efecto en el volumen. La eliminación de un volumen no tiene efecto en las instantáneas tomadas de él.

Eliminación de instantáneas incrementales

Si realiza instantáneas periódicas de un volumen, las instantáneas son incrementales. Esto significa que solo los bloques del dispositivo que han cambiado después de la instantánea más reciente se guardan en la nueva instantánea. Aunque las instantáneas se guarden de forma incremental, su proceso de eliminación está diseñado para que solo tenga que retener la instantánea más reciente para crear volúmenes.

Si los datos estuvieron presentes en un volumen llevado a cabo en una instantánea o en una serie de instantáneas anterior, que sea consecuentemente eliminada de dicho volumen de forma posterior, seguirán siendo considerados datos únicos de las instantáneas anteriores. Estos datos únicos solo se eliminan de la secuencia de instantáneas si se eliminan todas las instantáneas que hacen referencia a los datos únicos.

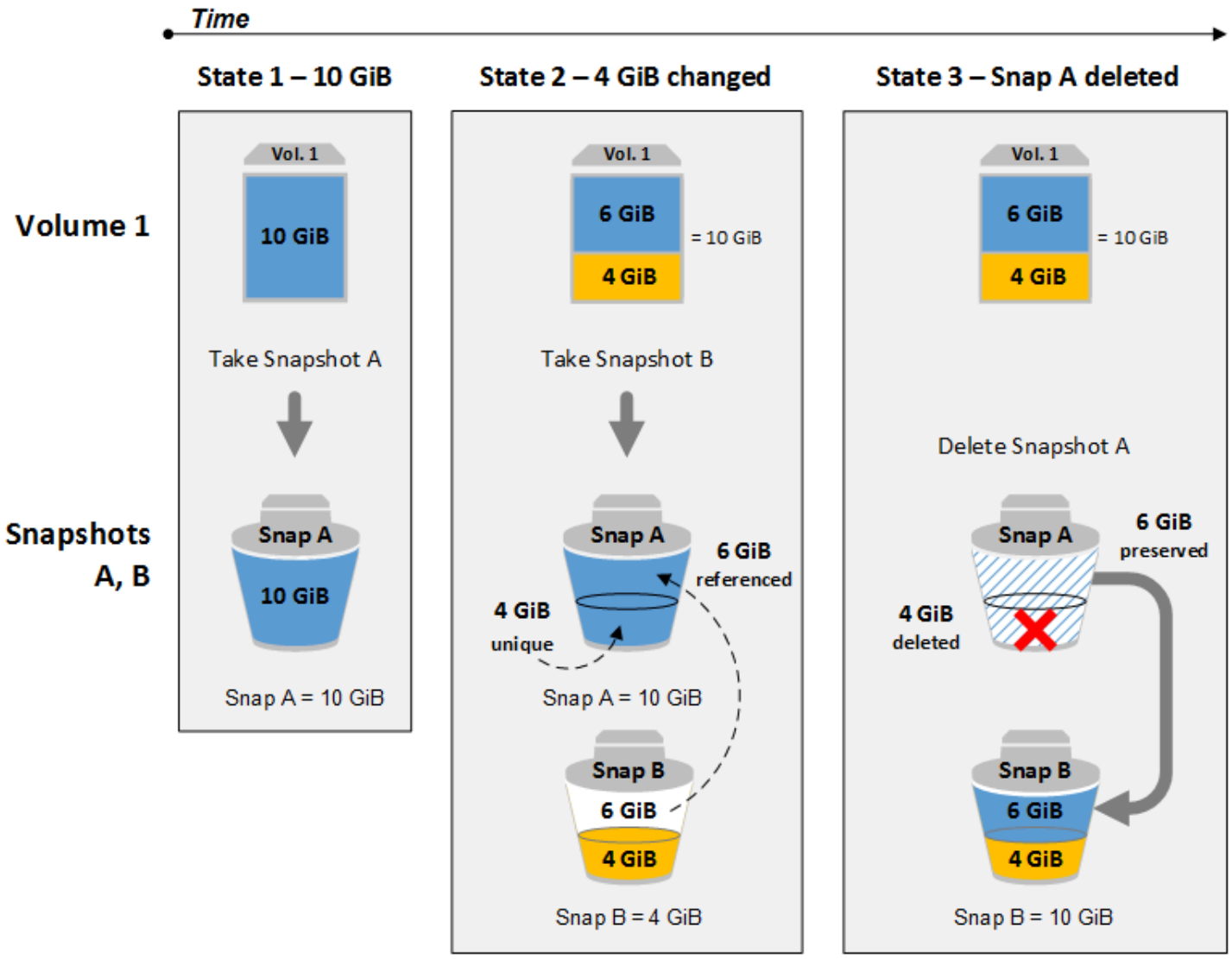
Cuando se elimina una instantánea, solo se borran los datos a los que se hace referencia en ella exclusivamente. Los datos únicos solo se eliminan si se eliminan todas las instantáneas que hacen referencia a ellos. Eliminar instantáneas previas de un volumen no afecta a la capacidad de crear volúmenes a partir de instantáneas posteriores de ese volumen.

Eliminar una instantánea no reduce necesariamente los costos de almacenamiento de datos de la organización. Es posible que otras instantáneas hagan referencia a los datos de esta, y los datos a los que se hace referencia se conservan siempre. Si elimina una instantánea que contiene los datos que después utiliza una instantánea posterior, los costos asociados con los datos de referencia se asignan a la última instantánea. Para obtener más información acerca de cómo se guardan los datos en las instantáneas, consulte Cómo funcionan las instantáneas y el ejemplo siguiente.

En el diagrama siguiente se muestra el volumen 1 en tres momentos distintos. Una instantánea ha capturado cada uno de los dos primeros estados y en el tercero se ha eliminado una instantánea.

- En el Estado 1, el volumen tiene 10 GiB de datos. Como Snap A es la primera instantánea que se toma del volumen, hay que copiar los 10 GiB de datos.
- En el Estado 2, el volumen sigue teniendo 10 GiB de datos pero 4 GiB han cambiado. La Snap B tiene que copiar y guardar solo los 4 GiB que cambiaron después de tomar la Snap A. La Snap B hace referencia a los restantes 6 GiB de datos sin cambios que ya están copiados y guardados en Snap A, en lugar de copiarlos de nuevo. Esto se indica con la flecha discontinua.
- En el estado 3, el volumen no ha cambiado desde el estado 2, pero la instantánea A ha sido eliminada. Los 6 GiB de datos guardados en la instantánea A y a los que se hace referencia en la instantánea B se han movido a la instantánea B, como muestra la flecha. Como resultado, se le cobrará por almacenar 10 GiB de datos, 6 GiB de datos no modificados que se conservan de la Snap A y 4 GiB de datos cambiados de Snap B.

Eliminación de una instantánea cuando otra instantánea hace referencia a algunos de sus datos



Consideraciones

Las siguientes consideraciones se aplican a la eliminación de instantáneas:

- No puede eliminar una instantánea del dispositivo raíz de un volumen de EBS usado en una AMI registrada. Esta consideración se aplica incluso si la AMI registrada está obsoleta o deshabilitada. Primero deber anular el registro de la AMI antes de eliminar la instantánea. Para obtener más información, consulte Anulación del registro de una AMI.
- No puede eliminar una instantánea gestionada por el AWS Backup servicio mediante Amazon EC2. En su lugar, utilice AWS Backup esta opción para eliminar los puntos de recuperación correspondientes del almacén de copias de seguridad. Para obtener más información, consulte Eliminación de copias de seguridad en la Guía para desarrolladores de AWS Backup .

- Puede crear, conservar y eliminar instantáneas manualmente, o puede utilizar Amazon Data Lifecycle Manager para administrar las instantáneas por usted. Para obtener más información, consulte Amazon Data Lifecycle Manager.
- Aunque puede eliminar una instantánea que aún está en progreso, debe completarse antes de que la eliminación surta efecto. Esto puede llevar mucho tiempo. Si también se encuentra en el límite de instantáneas simultáneas y si intenta tomar otra instantánea, es posible que se produzca un error `ConcurrentSnapshotLimitExceeded`. Para obtener más información, consulte Service Quotas para Amazon EBS en la Referencia general de Amazon Web Services.
- Si elimina una instantánea que cumple una regla de retención de la papelera de reciclaje, la instantánea se conserva en la papelera de reciclaje en lugar de eliminarse inmediatamente. Para obtener más información, consulte Papelera de reciclaje.
- No puede eliminar las instantáneas asociadas a las AMI deshabilitadas respaldadas por EBS. Para obtener más información, consulte Deshabilitar una AMI.
- No puede eliminar las instantáneas que se hayan compartido con usted.
- Si eliminas una instantánea compartida de tu propiedad, todas las cuentas con las que se comparte la instantánea perderán el acceso a ella.

Eliminar una instantánea

Para eliminar una instantánea, utilice alguno de los métodos siguientes.

Console

Para eliminar una instantánea con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instantáneas.
3. Seleccione la instantánea que desea eliminar y elija Actions (Acciones), Delete snapshot (Eliminar instantánea).
4. Elija Eliminar.

AWS CLI

Para eliminar una instantánea mediante el AWS CLI

Utilice el comando delete-snapshot.

Tools for Windows PowerShell

Para eliminar una instantánea mediante las herramientas de Windows PowerShell

Utilice el comando Remove-EC2Snapshot.

> **Consejo para la solución de problemas**
>
> Si recibe un error `Failed to delete snapshot` que indica que una AMI está utilizando la instantánea actualmente, tendrá que anular el registro de la AMI asociada antes de poder eliminar la instantánea. No puede eliminar las instantáneas asociadas a una AMI.
> Si utiliza la consola y la AMI asociada está deshabilitada, debe seleccionar el filtro Imágenes deshabilitadas en la pantalla de las AMI para ver las AMI deshabilitadas.

Eliminación de una instantánea de varios volúmenes

Para eliminar instantáneas de varios volúmenes, recupere todas las instantáneas de su conjunto de instantáneas de varios volúmenes con la etiqueta que haya aplicado al grupo al crear las instantáneas. A continuación, elimine las instantáneas una a una.

No se le impedirá eliminar una a una las instantáneas del conjunto de instantáneas de varios volúmenes. Si elimina una instantánea mientras está en `pending state`, solo se eliminará dicha instantánea. Las otras instantáneas del conjunto de instantáneas de varios volúmenes se completan correctamente.

Automatizar el ciclo de vida de instantáneas

Puede usar Amazon Data Lifecycle Manager para automatizar la creación, retención y eliminación de instantáneas usadas para las copias de seguridad de los volúmenes de Amazon EBS.

Para obtener más información, consulte Administrador de vida útil de datos de Amazon.

Restauración rápida de instantáneas de Amazon EBS

La restauración rápida de instantáneas (FSR) de Amazon EBS le permite crear un volumen a partir de una instantánea completamente inicializada durante la creación. Esto elimina la latencia de las operaciones de E/S en un bloque cuando se accede por primera vez. Los volúmenes creados utilizando la restauración rápida de instantáneas proporcionan todo el rendimiento aprovisionado.

Para comenzar, habilite la restauración rápida en instantáneas específicas de zonas de disponibilidad concretas. Cada par formado por una instantánea y una zona de disponibilidad hace referencia a una restauración rápida de instantáneas. Cuando cree un volumen a partir de una de estas instantáneas en una de las zonas de disponibilidad habilitadas, se utilizará la restauración rápida de instantáneas para restaurarlo.

La restauración rápida de instantáneas debe habilitarse de forma explícita para cada instantánea. Si crea una nueva instantánea de un volumen que se restauró a partir de una instantánea habilitada para la restauración rápida, la nueva instantánea no se habilita automáticamente para la restauración rápida de instantáneas. Esta se debe habilitar explícitamente para la nueva instantánea.

La cantidad de volúmenes que puede restablecer con el beneficio de un rendimiento completo de la restauración rápida de instantáneas se determina mediante los créditos de creación de volúmenes para la instantánea. Para obtener más información, consulte Créditos de creación de volúmenes.

Puede habilitar la restauración rápida de instantáneas para las instantáneas que posee y para las instantáneas públicas y privadas que se compartan con usted.

Contenido

Consideraciones

- La restauración rápida de instantáneas no es compatible con AWS Outposts las Local Zones y las zonas de Wavelength.
- La restauración rápida de instantáneas se puede habilitar en instantáneas con un tamaño de 16 TiB o menor.
- Los volúmenes aprovisionados con un desempeño de hasta 64 000 IOPS y un rendimiento de 1000 MiB/s reciben el beneficio de un desempeño completo de la restauración rápida de instantáneas. Para volúmenes aprovisionados con desempeño superior a 64 000 IOPS o

1000 MiB/s de rendimiento, le recomendamos que inicialice el volumen para recibir el desempeño completo.

Créditos de creación de volúmenes

El número de volúmenes que reciben el beneficio de un rendimiento completo de restauración de instantánea se determina mediante los créditos de creación de volúmenes para la instantánea. Hay un bucket de créditos por instantánea y zona de disponibilidad. Cada volumen que cree a partir de una instantánea con una restauración de instantánea rápida habilitada consume un crédito del bucket de créditos. Debe tener al menos un crédito en el bucket para crear un volumen inicializado a partir de la instantánea. Si crea un volumen pero hay menos de un crédito en el bucket, el volumen se crea sin beneficio de la restauración rápida de instantáneas.

Cuando habilita la restauración rápida de instantáneas para una instantánea que se comparte con usted, obtiene un bucket de créditos independiente para la instantánea compartida en su cuenta. Si crea volúmenes a partir de la instantánea compartida, los créditos se consumen del bucket de créditos; no se consumen del bucket de créditos del propietario de la instantánea.

El tamaño del bucket de créditos y la tarifa de carga dependen del tamaño de la instantánea, no del tamaño de los volúmenes creados a partir de la instantánea.

Cuando habilita la restauración rápida de instantáneas para una instantánea, el bucket de créditos comienza con cero créditos y se carga a una tarifa establecida hasta que alcanza su capacidad crediticia máxima. Además, a medida que consume créditos, el bucket de créditos se recarga con el tiempo hasta que alcanza su capacidad crediticia máxima.

La tarifa de carga para un bucket de créditos se calcula de la siguiente manera:

```
MIN (10, (1024 ÷ snapshot_size_gib))
```

Y el tamaño del bucket de créditos se calcula de la siguiente forma:

```
MAX (1, MIN (10, (1024 ÷ snapshot_size_gib)))
```

Por ejemplo, si habilita la restauración rápida de instantáneas para una instantánea con un tamaño de `128 GiB`, la tarifa de carga es de `0.1333` créditos por minuto.

```
MIN (10, (1024 ÷ 128))
```

```
 = MIN (10, 8)
 = 8 credits per hour
 = 0.1333 credits per minute
```

Y el tamaño máximo del bucket de créditos es de 8 créditos.

```
MAX (1, MIN (10, (1024 ÷ 128)))
 = MAX (1, MIN (10, 8))
 = MAX (1, 8)
 = 8 credits
```

En este ejemplo, cuando se habilita la restauración rápida de instantáneas, el bucket de créditos comienza con cero créditos. Después de 8 minutos, el bucket de créditos tiene créditos suficientes para crear un volumen inicializado (`0.1333 credits × 8 minutes = 1.066 credits`). Cuando el bucket de créditos está lleno, puede crear 8 volúmenes inicializados (8 créditos) de forma simultánea. Cuando el bucket está por debajo de su capacidad máxima, se recarga con `0.1333` créditos por minuto.

Puede usar las métricas de Cloudwatch para monitorear el tamaño de los buckets de créditos y el número de créditos disponibles en cada bucket. Para obtener más información, consulte Métricas para la restauración rápida de instantáneas.

Después de crear un volumen a partir de una instantánea rápida habilitada, puede describir el volumen mediante describe-volumes y marcar el campo `fastRestored` en la salida para determinar si el volumen se creó como un volumen inicializado con una restauración rápida de instantánea.

Administración de la restauración rápida de instantáneas

Temas

- Habilitación o desactivación de la restauración rápida de instantáneas
- Ver el estado de restauración rápida de instantáneas de una instantánea
- Consulta de volúmenes restaurados mediante la restauración rápida de instantáneas

Habilitación o desactivación de la restauración rápida de instantáneas

La restauración rápida de instantáneas está desactivada para una instantánea de forma predeterminada. Puede habilitar o desactivar la restauración rápida de instantáneas para las

instantáneas que posee y para las instantáneas que se comparten con usted. Cuando habilite o desactive la restauración rápida de instantáneas para una instantánea, los cambios se aplican únicamente a su cuenta.

> **Note**
>
> Cuando habilita la restauración rápida de instantáneas para una instantánea, se factura a su cuenta por cada minuto que la restauración rápida de instantáneas esté habilitada en una zona de disponibilidad determinada. Los cargos se prorratean y tienen un mínimo de una hora.

Cuando elimina una instantánea de su propiedad, la restauración rápida de instantáneas se desactiva automáticamente para esa instantánea en su cuenta. Si ha habilitado la restauración rápida de instantáneas para una instantánea que se comparte con usted y el propietario de la instantánea la elimina o deja de compartirla, la restauración rápida de instantáneas se desactiva automáticamente para la instantánea compartida en su cuenta.

Si ha habilitado la restauración rápida de instantáneas para una instantánea que le compartieron y se cifra mediante una CMK personalizada, la restauración rápida de instantáneas no se desactiva automáticamente para la instantánea cuando el propietario de la instantánea revoca el acceso a la CMK personalizada. Debe desactivar manualmente la restauración rápida de instantáneas para esa instantánea.

Utilice uno de los siguientes procedimientos a fin de habilitar o desactivar la restauración rápida de instantáneas para una instantánea de su propiedad o una instantánea que le compartieron.

Console

Para habilitar o deshabilitar la restauración rápida de instantáneas

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instantáneas.
3. Seleccione la instantánea y elija Acciones, Administrar la restauración rápida de instantáneas.
4. La sección Fast snapshot restore settings (Configuración de restauración rápida de instantáneas) enumera todas las zonas de disponibilidad, zonas locales y zonas Wavelength en las que puede habilitar la restauración rápida de instantáneas para la instantánea

seleccionada. El volumen Current status (Estado actual) indica si la restauración rápida de instantáneas está habilitada o desactivada actualmente para cada zona.

Para habilitar la restauración rápida de instantáneas en una zona en la que está desactivada actualmente, seleccione la zona y elija Enable (Habilitar) y, a continuación, para confirmar, elija Enable (Habilitar).

Para desactivar la restauración rápida de instantáneas en una zona en la que está habilitada actualmente, seleccione la zona y, a continuación, elija Disable (Desactivar).

5. Después de realizar los cambios necesarios, elija Cerrar.

AWS CLI

Para administrar la restauración rápida de instantáneas con la AWS CLI

- enable-fast-snapshot-restores
- disable-fast-snapshot-restores
- describe-fast-snapshot-restores

> **Note**
>
> Después de habilitar la restauración rápida de instantáneas para una instantánea, esta pasa al estado `optimizing`. Las instantáneas que se encuentran en el estado `optimizing` proporcionan algunas ventajas de rendimiento cuando se utilizan para restaurar volúmenes. Empiezan a proporcionar todos los beneficios de rendimiento de la restauración rápida de instantáneas solo después de pasar al estado `enabled`.

Ver el estado de restauración rápida de instantáneas de una instantánea

La restauración rápida de instantáneas para una instantánea puede estar en uno de los siguientes estados.

- `enabling` — se realizó una solicitud para habilitar la restauración rápida de instantáneas.
- `optimizing` — se está habilitando la restauración rápida de instantáneas. Optimizar una instantánea tarda 60 minutos por TiB. Las instantáneas en este estado ofrecen algunas ventajas de rendimiento al restaurar volúmenes.

- `enabled` — se ha habilitado la restauración rápida de instantáneas. Las instantáneas en este estado y que tienen suficientes créditos de creación de volúmenes ofrecen todas las ventajas de rendimiento al restaurar volúmenes.
- `disabling`: se realizó una solicitud para desactivar la restauración rápida de instantáneas o se ha producido un error en una solicitud para habilitar una restauración rápida de instantáneas.
- `disabled` — se ha deshabilitado la restauración rápida de instantáneas. Puede habilitar de nuevo la restauración rápida de instantáneas según sea necesario.

Utilice uno de los siguientes métodos para ver el estado de la restauración rápida de instantáneas de una instantánea de su propiedad o de una instantánea que le compartieron.

Console

Para ver el estado de la restauración rápida de instantáneas utilizando la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. Seleccione la instantánea.
4. En la pestaña Details (Detalles), Fast Snapshot Restore (Restauración rápida de instantáneas), figura el estado de la restauración rápida de instantáneas.

AWS CLI

Para ver las instantáneas que tienen la restauración rápida habilitada con la AWS CLI

Utilice el comando describe-fast-snapshot-restores para describir las instantáneas que tienen la restauración rápida habilitada.

```
aws ec2 describe-fast-snapshot-restores --filters Name=state,Values=enabled
```

A continuación, se muestra un ejemplo del resultado.

```
{
    "FastSnapshotRestores": [
        {
            "SnapshotId": "snap-0e946653493cb0447",
            "AvailabilityZone": "us-east-2a",
            "State": "enabled",
```

```
            "StateTransitionReason": "Client.UserInitiated - Lifecycle state
 transition",
            "OwnerId": "123456789012",
            "EnablingTime": "2020-01-25T23:57:49.596Z",
            "OptimizingTime": "2020-01-25T23:58:25.573Z",
            "EnabledTime": "2020-01-25T23:59:29.852Z"
        },
        {
            "SnapshotId": "snap-0e946653493cb0447",
            "AvailabilityZone": "us-east-2b",
            "State": "enabled",
            "StateTransitionReason": "Client.UserInitiated - Lifecycle state
 transition",
            "OwnerId": "123456789012",
            "EnablingTime": "2020-01-25T23:57:49.596Z",
            "OptimizingTime": "2020-01-25T23:58:25.573Z",
            "EnabledTime": "2020-01-25T23:59:29.852Z"
        }
    ]
}
```

Consulta de volúmenes restaurados mediante la restauración rápida de instantáneas

Cuando se crea un volumen a partir de una instantánea que tiene habilitada la restauración rápida en la zona de disponibilidad del volumen, se utiliza la restauración rápida de instantáneas para restaurarlo.

Utilice el comando describe-volumes para ver los volúmenes creados a partir de una instantánea con la restauración rápida habilitada.

```
aws ec2 describe-volumes --filters Name=fast-restored,Values=true
```

A continuación, se muestra un ejemplo del resultado.

```
{
    "Volumes": [
        {
            "Attachments": [],
            "AvailabilityZone": "us-east-2a",
            "CreateTime": "2020-01-26T00:34:11.093Z",
            "Encrypted": true,
```

```
            "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/8c5b2c63-b9bc-45a3-
a87a-5513e232e843",
            "Size": 20,
            "SnapshotId": "snap-0e946653493cb0447",
            "State": "available",
            "VolumeId": "vol-0d371921d4ca797b0",
            "Iops": 100,
            "VolumeType": "gp2",
            "FastRestored": true
        }
    ]
}
```

Monitorear la restauración rápida de instantáneas

Amazon EBS emite eventos Amazon CloudWatch cuando cambia el estado de restauración rápida de instantánea de una instantánea. Para obtener más información, consulte Eventos de restauración rápida de instantáneas de EBS.

Cuotas de restauración rápida de instantáneas

Puede habilitar hasta 5 instantáneas para una restauración rápida de instantáneas por región. La cuota se aplica a las instantáneas que posee y a las que se comparten con usted. Si habilita la restauración rápida de instantáneas para una instantánea que se comparte con usted, se tiene en cuenta para la cuota de restauración rápida de instantáneas. No se tiene en cuenta para la cuota de restauración rápida de instantáneas del propietario de la instantánea.

Precios y facturación

Se le facturará por cada minuto que se habilite la restauración rápida de instantáneas para una instantánea en una zona de disponibilidad determinada. Los cargos se prorratean con un mínimo de una hora.

Por ejemplo, si habilita la restauración rápida de instantáneas para una instantánea en `US-East-1a` durante un mes (30 días), se le facturarán 540 USD (1 instantánea x 1 zona de disponibilidad x `720` horas x `$0.75` por hora). Si habilita la restauración rápida de instantáneas para dos instantáneas en `us-east-1a`, `us-east-1b` y `us-east-1c` para el mismo periodo, se le facturarán 3240 USD (2 instantáneas x 3 zonas de disponibilidad x `720` horas x `$0.75` por hora).

Si habilita la restauración rápida de instantáneas para una instantánea pública o privada compartida con usted, se facturará su cuenta; no se facturará al propietario de la instantánea. Cuando el

propietario de la instantánea elimina o deja de compartir una instantánea compartida con usted, se desactiva la restauración rápida de la instantánea en su cuenta y se detiene la facturación.

Para obtener más información, consulte Precios Amazon EBS.

Bloqueo de instantáneas de Amazon EBS

Puede bloquear sus instantáneas de Amazon EBS para protegerlas contra eliminaciones accidentales o malintencionadas, o para almacenarlas en formato WORM (write-once-read-many) durante un período específico. Mientras una instantánea esté bloqueada, ningún usuario podrá eliminarla, independientemente de sus permisos de IAM. Puede seguir utilizando una instantánea bloqueada de la misma manera en que utiliza cualquier otra instantánea.

> **Note**
>
> Cohasset Associates ha evaluado el bloqueo de instantáneas para su uso en entornos sujetos a las normativas SEC 17a-4, CFTC y FINRA. Para obtener más información acerca de cómo el bloqueo de instantáneas está relacionado con estas normativas, consulte Cohasset Associates Compliance Assessment.

Puede bloquear las instantáneas en uno de estos dos modos: modo de conformidad o modo de gobernanza; además, se pueden bloquear durante un periodo específico o hasta una fecha concreta. Para obtener más información, consulte Modo de bloqueo y Duración del bloqueo.

Precios

Puede bloquear y desbloquear instantáneas sin costo adicional. Usted paga los costos estándar de almacenamiento de instantáneas de Amazon EBS para las instantáneas bloqueadas.

Temas

- Conceptos del bloqueo de instantáneas de Amazon EBS
- Consideraciones sobre el bloqueo de instantáneas de Amazon EBS
- Permisos necesarios para el bloqueo de instantáneas de Amazon EBS
- Uso del bloqueo de instantáneas de Amazon EBS
- Supervise los bloqueos de instantáneas de Amazon EBS mediante AWS CloudTrail
- Supervise los bloqueos de instantáneas de Amazon EBS mediante Amazon EventBridge

Conceptos del bloqueo de instantáneas de Amazon EBS

Los siguientes conceptos son importantes y debe comprenderlos al momento de utilizar el bloqueo de instantáneas.

Contenido

Modo de bloqueo

Puede bloquear una instantánea en uno de estos dos modos:

Modo Gobierno

Una vez bloqueada una instantánea, los usuarios con los permisos de IAM adecuados pueden desbloquearla y modificar el modo de bloqueo y la duración del bloqueo o la fecha de vencimiento en cualquier momento. Al bloquear una instantánea en el modo de gobernanza, la instantánea se bloquea inmediatamente; no hay ningún periodo de reflexión. Para eliminar una instantánea después de haberla bloqueado en el modo de gobernanza, primero debe desbloquearla o esperar a que caduque el bloqueo.

Puede usar el modo de gobernanza para cumplir con los requisitos de gobernanza de datos de su organización; para ello, asegúrese de que solo algunos usuarios tengan permiso para desbloquear las instantáneas y modificar las configuraciones del bloqueo de instantáneas. También puede utilizar el modo de gobernanza para probar la configuración del bloqueo antes de bloquear una instantánea en el modo de conformidad.

Modo Cumplimiento

Al bloquear una instantánea en el modo de conformidad, si lo desea, puede especificar un periodo de reflexión que comience inmediatamente después de bloquear la instantánea. Durante el periodo de reflexión, los usuarios con los permisos adecuados pueden desbloquear la instantánea, cambiar el modo de bloqueo, aumentar o disminuir el periodo de reflexión y aumentar o disminuir la duración o la fecha de caducidad del bloqueo. Una vez transcurrido el periodo de reflexión, no podrá desbloquear la instantánea, cambiar el modo de bloqueo ni reducir la duración o la fecha de

caducidad del bloqueo; solo podrá aumentar la duración o la fecha de caducidad del bloqueo. Para eliminar una instantánea después de que se haya bloqueado en el modo de conformidad y haya expirado el periodo de reflexión, debe esperar a que caduque el bloqueo.

> **Note**
>
> Para bloquear una instantánea en modo de conformidad sin un periodo de reflexión, omita el periodo de reflexión en la solicitud. Si hace esto, el bloqueo se hace efectivo inmediatamente y no podrá desbloquear la instantánea, cambiar el modo de bloqueo ni reducir la duración o la fecha de caducidad del bloqueo; solo podrá aumentar la duración o la fecha de caducidad del bloqueo.

Puede utilizar el modo de conformidad para proteger las instantáneas que no se deben eliminar durante un periodo específico por motivos de conformidad. El modo de conformidad ofrece los siguientes beneficios:

- Habilita la configuración WORM (escritura única, lectura múltiple) para sus instantáneas.
- Proporciona una capa de defensa adicional que protege las instantáneas de eliminaciones involuntarias o malintencionadas.
- Aplica periodos de retención, que evitan eliminaciones antes de tiempo por parte de usuarios privilegiados para así poder cumplir las políticas y los procedimientos de protección de datos de su organización.

> **Note**
>
> La única forma de eliminar una instantánea que esté bloqueada en modo de conformidad antes de que caduque su bloqueo es cerrar la cuenta asociada. AWS

Duración del bloqueo

La duración del bloqueo es el periodo de tiempo durante el que la instantánea debe permanecer bloqueada. Puede especificar la duración del bloqueo como una de las siguientes opciones, pero no ambas:

Número de días

La duración del bloqueo se especifica como el número de días durante los cuales la instantánea permanecerá bloqueada. Una vez transcurrido el número de días especificado, la instantánea se desbloquea automáticamente. La duración puede oscilar entre 1 día y 36 500 días (100 años).

Fecha de caducidad del bloqueo

La duración del bloqueo viene determinada por una fecha de vencimiento en el futuro. La instantánea permanece bloqueada hasta que se alcance la fecha de vencimiento del bloqueo. Cuando se alcanza la fecha de vencimiento del bloqueo, la instantánea se desbloquea automáticamente.

Periodo de reflexión

El periodo de reflexión es un periodo de tiempo opcional que puede especificar al bloquear una instantánea en modo de conformidad. Durante el periodo de reflexión, los usuarios con los permisos adecuados pueden desbloquear la instantánea, cambiar el modo de bloqueo, aumentar o disminuir el periodo de reflexión y aumentar o disminuir la duración del bloqueo. Una vez transcurrido el periodo de reflexión, los usuarios no pueden desbloquear la instantánea, cambiar el modo de bloqueo, restablecer el periodo de reflexión ni reducir la duración del bloqueo, independientemente de sus permisos.

No se puede eliminar una instantánea durante el periodo de reflexión.

Si se especifica, el periodo de reflexión comienza inmediatamente después de bloquear la instantánea. Si se omite, la instantánea se bloquea en modo de conformidad inmediatamente sin un periodo de reflexión.

El periodo de reflexión puede oscilar entre 1 y 72 horas. Para bloquear una instantánea en modo de conformidad sin un periodo de reflexión, no especifique ningún periodo de reflexión en la solicitud.

Estado de bloqueo

Un bloqueo de instantánea puede tener uno de los siguientes estados:

- `compliance-cooloff`: la instantánea se ha bloqueado en modo de conformidad, pero aún se encuentra dentro del periodo de reflexión. La instantánea no se puede eliminar, pero los usuarios con los permisos adecuados pueden desbloquearla y modificar la configuración del bloqueo.
- `governance`: la instantánea está bloqueada en modo de gobernanza. La instantánea no se puede eliminar, pero los usuarios con los permisos adecuados pueden desbloquearla y modificar la configuración del bloqueo.

- `compliance`: la instantánea está bloqueada en modo de conformidad sin un periodo de reflexión o el periodo de reflexión ha caducado. La instantánea no se puede desbloquear ni eliminar. Solo los usuarios con los permisos adecuados pueden aumentar la duración del bloqueo.
- `expired`: la instantánea se bloqueó en modo de conformidad o gobernanza, pero el bloqueo ha caducado. La instantánea no está bloqueada y se puede eliminar.

Consideraciones sobre el bloqueo de instantáneas de Amazon EBS

- Puede bloquear una instantánea solo si está en estado `pending` o `completed`.
  - Si bloquea una instantánea mientras está en estado `pending` y la bloquea durante un periodo específico, la duración del bloqueo solo comienza cuando la instantánea alcanza el estado `completed`. La instantánea no se puede eliminar mientras esté en estado `pending`.
  - Si bloquea una instantánea mientras está en estado `pending` y la creación de la instantánea falla por algún motivo, el bloqueo se cancela.
- Si prolonga la duración del bloqueo de una instantánea que está bloqueada en modo de conformidad una vez transcurrido el periodo de reflexión, no podrá especificar otro periodo de reflexión. Si especifica un periodo de reflexión, la solicitud producirá un error.
- Puede bloquear instantáneas archivadas. Además, puede archivar instantáneas bloqueadas.
- Puede bloquear instantáneas asociadas a una AMI.
- Puede anular el registro de una AMI que tenga asociadas instantáneas bloqueadas.
- Puede eliminar la clave de KMS utilizada para cifrar una instantánea bloqueada.
- Se recomienda no bloquear las instantáneas creadas por AWS Backup. AWS Backup ya se asegura de que sus instantáneas no se eliminen antes de que venza su período de retención. Para añadir un nivel de seguridad adicional a las instantáneas gestionadas por AWS Backup, le recomendamos que utilice AWS Backup Vault Lock. Para obtener más información, consulte Bloqueo de almacenes de AWS Backup.
- No puede bloquear las instantáneas durante la creación ni durante el registro de la AMI.
- No puede bloquear las instantáneas locales de Amazon EBS en AWS Outposts.
- La única forma de eliminar una instantánea que esté bloqueada en modo de conformidad antes de que caduque el bloqueo es cerrar la AWS cuenta asociada.

  Si cierra su AWS cuenta mientras tiene las instantáneas bloqueadas, la AWS suspende durante 90 días con las instantáneas intactas. Si no vuelve a abrir la cuenta en un plazo de 90 días, AWS eliminará las instantáneas, aunque estén bloqueadas.

Permisos necesarios para el bloqueo de instantáneas de Amazon EBS

De forma predeterminada, los usuarios no tienen permiso para trabajar con bloqueos de instantáneas. Para permitir a los usuarios utilizar bloqueos de instantáneas, tiene que crear políticas de IAM que les concedan permisos para utilizar recursos y acciones de API específicos. Para obtener más información, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Temas

Permisos necesarios

Para trabajar con bloqueos de instantáneas, los usuarios necesitan los siguientes permisos.

- `ec2:LockSnapshot`: para bloquear las instantáneas.
- `ec2:UnlockSnapshot`: para desbloquear las instantáneas.
- `ec2:DescribeLockedSnapshots`: para ver la configuración de bloqueo de instantáneas.

A continuación, se muestra un ejemplo de política de IAM que concede a los usuarios permiso para bloquear y desbloquear instantáneas y para ver la configuración de bloqueo de instantáneas. Incluye el permiso `ec2:DescribeSnapshots` para los usuarios de la consola. Si algunos permisos no se necesitan, puede eliminarlos de la política.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "ec2:LockSnapshot",
            "ec2:UnlockSnapshot",
            "ec2:DescribeLockedSnapshots",
            "ec2:DescribeSnapshots"
        ]
    }]
}
```

Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en: AWS IAM Identity Center

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center .
- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones descritas en Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.
- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Restricción del acceso con claves de condición

Puede utilizar claves de condición para restringir la forma en que los usuarios pueden bloquear las instantáneas.

Temas

- ec2: SnapshotLockDuration
- ec2: CoolOffPeriod

ec2: SnapshotLockDuration

Puede usar la clave de condición `ec2:SnapshotLockDuration` para restringir a los usuarios a periodos de bloqueo específicos al bloquear las instantáneas.

En el siguiente ejemplo de política se restringe a los usuarios a especificar una duración de bloqueo de entre `10` y `50` días.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:LockSnapshot",
```

```
      "Resource": "arn:aws:ec2:region::snapshot/*"
      "Condition": {
        "NumericGreaterThan" : {
          "ebs:SnapshotLockDuration" : 10
        }
        "NumericLessThan":{
          "ebs:SnapshotLockDuration": 50
        }
      }
    }
  ]
}
```

ec2: CoolOffPeriod

Puede utilizar la clave de condición `ec2:CoolOffPeriod` para evitar que los usuarios bloqueen las instantáneas en el modo de conformidad sin un periodo de reflexión.

En el siguiente ejemplo de política se restringe a los usuarios a especificar un periodo de reflexión superior a 48 horas al bloquear las instantáneas en el modo de conformidad.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:LockSnapshot",
      "Resource": "arn:aws:ec2:region::snapshot/*"
      "Condition": {
        "NumericGreaterThan": {
          "ec2:CoolOffPeriod": 48
        }
      }
    }
  ]
}
```

Uso del bloqueo de instantáneas de Amazon EBS

Utilice los siguientes procedimientos para trabajar con el bloqueo de instantáneas de Amazon EBS.

Tareas

- Bloqueo de una instantánea
- Desbloqueo de una instantánea
- Actualización de la configuración de bloqueo de instantáneas
- Visualización de la configuración de bloqueo de instantáneas

Bloqueo de una instantánea

Puede bloquear una instantánea que esté en estado `pending` o `completed`. Para obtener más información, consulte Consideraciones sobre el bloqueo de instantáneas de Amazon EBS.

Console

Bloqueo de una instantánea

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instantáneas.
3. Seleccione la instantánea que desee bloquear y elija Acciones, Configuración de instantánea, Administrar bloqueo de instantáneas.
4. Seleccione Bloquear instantánea.
5. En Modo de bloqueo, elija Modo de gobernanza o Modo de conformidad. Para obtener más información, consulte Modo de bloqueo.
6. En Duración del bloqueo, haga una de las siguientes acciones:

   - Para bloquear la instantánea durante un periodo específico, seleccione Bloquear instantánea durante y, a continuación, ingrese el periodo en días o años.
   - Para bloquear la instantánea hasta una fecha y hora específicas, seleccione Bloquear instantánea hasta y, a continuación, seleccione la fecha y hora de vencimiento.

   Para obtener más información, consulte Duración del bloqueo.
7. (Solo en el modo de conformidad) En Periodo de reflexión, especifique un periodo de reflexión durante el cual pueda desbloquear la instantánea y modificar la configuración de bloqueo. Para obtener más información, consulte Periodo de reflexión.
8. (Solo en el modo de conformidad) Para confirmar que desea bloquear la instantánea en el modo de conformidad y que no podrá desbloquearla una vez transcurrido el periodo de reflexión, seleccione Confirmar.

9. Elija Guardar configuración de bloqueo.

AWS CLI

Bloqueo de una instantánea en el modo de gobernanza

Utilice el comando de la AWS CLI lock-snapshot. En `--snapshot-id`, especifique el ID de la instantánea que se va a bloquear. En `--lock-mode`, especifique `governance`. Para bloquear la instantánea durante un periodo específico, en `--lock-duration`, especifique el periodo durante el que desea bloquear la instantánea. O bien, para bloquear la instantánea hasta una fecha específica, en `--expiration-date`, especifique la fecha y la hora en las que debe caducar el bloqueo, en la zona horaria UTC (`YYYY-MM-DDThh:mm:ss.sssZ`).

```
$ aws ec2 lock-snapshot --snapshot-id snapshot_id \
 --lock-mode governance \
 --lock-duration 1-36500_days | --expiration-date YYYY-MM-DDThh:mm:ss.sssZ
```

Bloqueo de una instantánea en modo de conformidad

Utilice el comando de la AWS CLI lock-snapshot. En `--snapshot-id`, especifique el ID de la instantánea que se va a bloquear. En `--lock-mode`, especifique `compliance`. En `--cool-off-period`, especifique un periodo de reflexión en horas de forma opcional. Para bloquear la instantánea durante un periodo específico, en `--lock-duration`, especifique el periodo durante el que desea bloquear la instantánea. O bien, para bloquear la instantánea hasta una fecha específica, en `--expiration-date`, especifique la fecha y la hora en las que debe caducar el bloqueo, en la zona horaria UTC (`YYYY-MM-DDThh:mm:ss.sssZ`).

```
$ aws ec2 lock-snapshot --snapshot-id snapshot_id \
 --lock-mode compliance \
 --cool-off-period 1-72_hours \
 --lock-duration 1-36500_days | --expiration-date YYYY-MM-DDThh:mm:ss.sssZ
```

Desbloqueo de una instantánea

Puede desbloquear una instantánea solo si está bloqueada en el modo de gobernanza o si está bloqueada en el modo de conformidad y aún se encuentra dentro del periodo de reflexión.

Console

Desbloqueo de una instantánea

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instantáneas.
3. Seleccione la instantánea que desee desbloquear y elija Acciones, Configuración de instantánea, Administrar bloqueo de instantáneas.
4. Seleccione Desbloquear instantánea y, a continuación, vuelva a seleccionar Desbloquear instantánea para confirmar.

AWS CLI

Desbloqueo de una instantánea

Utilice el comando de la AWS CLI unlock-snapshot. En `--snapshot-id`, especifique el ID de la instantánea que se va a desbloquear.

```
$ aws ec2 unlock-snapshot --snapshot-id snapshot_id
```

Actualización de la configuración de bloqueo de instantáneas

Las actualizaciones permitidas dependen del estado del bloqueo:

- `governance`: puede cambiar el modo de bloqueo y aumentar o disminuir la duración o la fecha de caducidad del bloqueo.
- `compliance-cooloff`: puede cambiar el modo de bloqueo, aumentar o disminuir el periodo de reflexión y aumentar o disminuir la duración o la fecha de caducidad del bloqueo.
- `compliance`: solo puede aumentar la duración o la fecha de caducidad del bloqueo.

Console

Actualización de la configuración de bloqueo de instantáneas

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instantáneas.

3. Seleccione la instantánea para la que quiere modificar la configuración de bloqueo y elija Acciones, Configuración de instantánea, Administrar bloqueo de instantáneas.
4. Actualice la configuración según sea necesario y, a continuación, seleccione Guardar configuración de bloqueo.

AWS CLI

Actualización de la configuración de bloqueo de instantáneas

Utilice el comando de la AWS CLI lock-snapshot. En `--snapshot-id`, especifique el ID de la instantánea para la que desea actualizar la configuración de bloqueo. A continuación, especifique solo las opciones que desee modificar.

Visualización de la configuración de bloqueo de instantáneas

Utilice uno de los métodos siguientes para ver la configuración de bloqueo de una instantánea.

Console

Visualización de la configuración de bloqueo de instantáneas

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instantáneas.
3. Seleccione la instantánea para la cual quiere ver la configuración de bloqueo y elija Acciones, Configuración de instantánea, Administrar bloqueo de instantáneas.

AWS CLI

Visualización de la configuración de bloqueo de instantáneas

Use el comando describe-locked-snapshots. AWS CLI En `--snapshot-ids`, especifique el ID de las instantáneas para las que desea ver la configuración de bloqueo.

```
$ aws ec2 describe-locked-snapshots --snapshot-ids snapshot_id
```

Supervise los bloqueos de instantáneas de Amazon EBS mediante AWS CloudTrail

Puede supervisar las llamadas a la API del bloqueo de instantáneas como eventos, incluidas las llamadas procedentes de la consola y las llamadas de código a las API. Con la información recopilada CloudTrail, puede determinar la solicitud que se realizó, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información, consulte Logging API calls using AWS CloudTrail.

Supervise los bloqueos de instantáneas de Amazon EBS mediante Amazon EventBridge

Amazon EBS emite eventos relacionados con acciones de bloqueo de instantáneas. Puedes usar AWS Lambda Amazon EventBridge para gestionar las notificaciones de eventos mediante programación. Los eventos se emiten en la medida de lo posible. Para obtener más información, consulta la Guía del EventBridge usuario de Amazon.

Se emiten los siguientes eventos:

- La instantánea se bloqueó correctamente en el modo de gobernanza o conformidad.

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "lockSnapshot",
    "result": "succeeded",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "source": 012345678901,
    "lockState": "compliance-cooloff",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockExpiresOn": "yyyy-mm-ddThh:mm:ssZ",
```

```
    "lockDuration": 123,
    "lockStartDurationTime": "yyyy-mm-ddThh:mm:ssZ",
    "cooOffPeriod": 24,
    "coolOffPeriodExpiresOn": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

- Evento de bloqueo fallido cuando una instantánea se bloquea mientras está en estado `pending` y no logra llegar al estado `completed`.

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "lockSnapshot",
    "result": "failed",
    "cause": "snapshot failed",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "lockState": "pending-compliance",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockDuration": 123,
    "lockStartDurationTime": "yyyy-mm-ddThh:mm:ssZ",
    "cooOffPeriod": 24,
    "coolOffPeriodExpiresOn": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

- Bloqueo vencido

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
```

```
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "lockDurationExpiry",
    "result": "succeeded",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "lockState": "expired",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockExpiresOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockDuration": 123
  }
}
```

- El periodo de reflexión expiró tras bloquearse en el modo de conformidad.

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "cooloffperiodExpiry",
    "result": "succeeded",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "lockState": "compliance",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockExpiresOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockDuration": 123,
    "lockStartDurationTime": "yyyy-mm-ddThh:mm:ssZ",
    "cooOffPeriod": 24,
    "coolOffPeriodExpiresOn": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

Bloqueo del acceso público de las instantáneas

Para impedir que sus instantáneas se compartan públicamente, puede habilitar el bloqueo del acceso público de las instantáneas. Tras habilitar el bloqueo del acceso público de las instantáneas de una región, se bloquea automáticamente cualquier intento de compartir públicamente las instantáneas en esa región. Esto puede ser de ayuda para mejorar la seguridad de sus instantáneas y para proteger sus datos contra el acceso no autorizado o no intencionado.

El bloqueo del acceso público de las instantáneas se puede habilitar de dos modos:

- Bloquear todo el uso compartido: bloquea todo el uso compartido público de sus instantáneas. Los usuarios de la cuenta no pueden solicitar un nuevo uso compartido público. Además, las instantáneas que ya se compartieron públicamente se consideran privadas y ya no están disponibles públicamente.
- Bloquear el nuevo uso compartido: bloquea solo el uso compartido público nuevo de sus instantáneas. Los usuarios de la cuenta no pueden solicitar un nuevo uso compartido público. Sin embargo, las instantáneas que ya se compartieron públicamente seguirán estando disponibles públicamente.

Precios

El bloqueo del acceso público de las instantáneas se puede habilitar sin costo adicional.

Contenido

Consideraciones

- Bloquear el acceso público de las instantáneas no impide que se compartan las instantáneas de forma privada.

- Si habilita la opción de bloquear el acceso público de las instantáneas en el modo Bloquear todo el uso compartido, no se cambiarán los permisos de las instantáneas que ya se hayan compartido públicamente. En su lugar, impide que estas instantáneas sean visibles y de acceso público. Por lo tanto, los atributos de estas instantáneas siguen indicando que se comparten públicamente, aunque no estén disponibles públicamente.
- Si la opción de bloquear el acceso público de las instantáneas está habilitada en el modo Bloquear todo el uso compartido y cambia al modo Bloquear el nuevo uso compartido o deshabilita el bloqueo del acceso público, todas las instantáneas que anteriormente se compartieron públicamente dejarán de considerarse privadas y volverán a ser de acceso público.
- El bloqueo del acceso público de las instantáneas es una configuración regional. Se aplica a todas las instantáneas de la región en la que está habilitado. Debe habilitar el bloqueo del acceso público de las instantáneas en cada región en la que quiera impedir que se compartan públicamente sus instantáneas.
- El bloqueo del acceso público es una configuración de nivel de cuenta. Se aplica a todos los usuarios de la cuenta, incluidos los administradores. No puede habilitar el bloqueo del acceso público de las instantáneas en el nivel de organización.
- El bloqueo del acceso público de las instantáneas no impide que se compartan públicamente las AMI respaldadas por EBS. Si habilita el bloqueo del acceso público de las instantáneas, los usuarios podrán seguir compartiendo públicamente las AMI respaldadas por EBS. Si una AMI respaldada por EBS se comparte públicamente, los usuarios con acceso a esa AMI pueden crear volúmenes a partir de las instantáneas asociadas. Para impedir que las AMI se compartan públicamente, habilite el bloqueo del acceso público de las AMI.
- Bloquear el acceso público a las instantáneas no es compatible con las instantáneas locales activadas. AWS Outposts

Permisos de IAM

De forma predeterminada, los usuarios no tienen permiso para usar el bloqueo del acceso público de las instantáneas. Para permitir que los usuarios trabajen con el bloqueo del acceso público de las instantáneas, tiene que crear políticas de IAM que les concedan permisos para utilizar acciones de API específicas. Una vez creadas las políticas, tendrá que agregar permisos a los usuarios, grupos o roles.

Para usar el bloqueo del acceso público de las instantáneas, los usuarios necesitan los siguientes permisos.

- `ec2:EnableSnapshotBlockPublicAccess`: habilitar el bloqueo del acceso público de las instantáneas y modificar el modo.
- `ec2:DisableSnapshotBlockPublicAccess`: deshabilite el bloqueo del acceso público de las instantáneas.
- `ec2:GetSnapshotBlockPublicAccessState`: ver el bloqueo del acceso público de las instantáneas de una región.

A continuación, se muestra una política de IAM de ejemplo. Si algunos permisos no se necesitan, puede eliminarlos de la política.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "ec2:EnableSnapshotBlockPublicAccess",
            "ec2:DisableSnapshotBlockPublicAccess",
            "ec2:GetSnapshotBlockPublicAccessState"
        ],
        "Resource": "*"
    }]
}
```

Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en: AWS IAM Identity Center

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center .
- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones descritas en Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.
- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.

- (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Habilitación del bloqueo del acceso público de las instantáneas

Utilice los siguientes procedimientos para configurar y supervisar el bloqueo del acceso público de las instantáneas.

Tareas

- Configuración del bloqueo del acceso público de las instantáneas
- Visualización de la configuración de bloqueo del acceso público de las instantáneas
- Deshabilitar el bloqueo del acceso público de las instantáneas

Configuración del bloqueo del acceso público de las instantáneas

Habilite el bloqueo del acceso público de las instantáneas para evitar que sus instantáneas se compartan públicamente en la región. Una vez habilitada esta característica, se bloquean las solicitudes para compartir públicamente las instantáneas en la región.

> **Important**
>
> Si la opción de bloquear el acceso público de las instantáneas está habilitada en el modo Bloquear todo el uso compartido y cambia al modo Bloquear el nuevo uso compartido, todas las instantáneas que anteriormente se compartieron públicamente dejarán de considerarse privadas y volverán a ser de acceso público.

Console

Configuración del bloqueo del acceso público de las instantáneas

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Panel de EC2 y, a continuación, en Atributos de la cuenta (a la derecha), elija Protección y seguridad de datos.
3. En la sección Bloquear el acceso público de las instantáneas de EBS, seleccione Administrar.

4. Seleccione Bloquear acceso público y, a continuación, elija una de las siguientes opciones:
   - Bloquear todo el uso compartido: para bloquear todo el uso compartido público de sus instantáneas. Los usuarios de la cuenta no pueden solicitar un nuevo uso compartido público. Además, las instantáneas que ya se compartieron públicamente se consideran privadas y dejan de ser de acceso público.
   - Bloquear el nuevo uso compartido público: para bloquear solo el uso compartido público nuevo de sus instantáneas. Los usuarios de la cuenta no pueden solicitar un nuevo uso compartido público. Sin embargo, las instantáneas que ya se compartieron públicamente seguirán siendo de acceso público.
5. Elija Actualizar.

AWS CLI

Habilitación o modificación del bloqueo del acceso público de las instantáneas

Utilice el comando enable-snapshot-block-public-access. En `--state`, especifique uno de los siguientes valores:

- `block-all-sharing`: para bloquear todo el uso compartido público de sus instantáneas. Los usuarios de la cuenta no pueden solicitar un nuevo uso compartido público. Además, las instantáneas que ya se compartieron públicamente se consideran privadas y dejan de ser de acceso público.
- `block-new-sharing`: para bloquear solo el nuevo uso compartido público de sus instantáneas. Los usuarios de la cuenta no pueden solicitar un nuevo uso compartido público. Sin embargo, las instantáneas que ya se compartieron públicamente seguirán siendo de acceso público.

```
aws ec2 enable-snapshot-block-public-access --state block-all-sharing|block-new-sharing
```

Visualización de la configuración de bloqueo del acceso público de las instantáneas

El bloqueo del acceso público puede encontrarse en uno de los siguientes estados para cada región de su cuenta.

- Bloquear todo el uso compartido: se bloquea todo el uso compartido público de sus instantáneas. Los usuarios de la cuenta no pueden solicitar un nuevo uso compartido público. Además, las instantáneas que ya se compartieron públicamente se consideran privadas y no son de acceso público.
- Bloquear el nuevo uso compartido: solo se bloquea el nuevo uso compartido público de sus instantáneas. Los usuarios de la cuenta no pueden solicitar un nuevo uso compartido público. Sin embargo, las instantáneas que ya se compartieron públicamente seguirán siendo de acceso público.
- Desbloqueado: el uso compartido público no está bloqueado. Los usuarios pueden compartir las instantáneas públicamente.

Console

Visualización de la configuración del bloqueo del acceso público de las instantáneas

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Panel de EC2 y, a continuación, en Atributos de la cuenta (a la derecha), elija Protección y seguridad de datos.
3. En la sección Bloquear el acceso público a las instantáneas de EBS se muestra la configuración actual.

AWS CLI

Visualización de la configuración del bloqueo del acceso público de las instantáneas

Utilice el comando get-snapshot-block-public-access-state.

```
aws ec2 get-snapshot-block-public-access-state
```

Deshabilitar el bloqueo del acceso público de las instantáneas

Deshabilite el bloqueo del acceso público de las instantáneas para permitir que sus instantáneas se compartan públicamente en la región. Una vez deshabilitada esta característica, los usuarios pueden compartir las instantáneas de forma pública en la región.

> **Important**
>
> Si el bloqueo del acceso público de las instantáneas está habilitado en el modo para bloquear todo el uso compartido y deshabilita el bloqueo del acceso público, todas las instantáneas que anteriormente se compartieron públicamente dejarán de considerarse privadas y volverán a ser de acceso público.

Console

Deshabilitación del bloqueo del acceso público de las instantáneas

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Panel de EC2 y, a continuación, en Atributos de la cuenta (a la derecha), elija Protección y seguridad de datos.
3. En la sección Bloquear el acceso público de las instantáneas de EBS, seleccione Administrar.
4. Desmarque Bloquear acceso público y elija Actualizar.

AWS CLI

Deshabilitación del bloqueo del acceso público de las instantáneas

Utilice el comando -accessdisable-snapshot-block-public.

```
aws ec2 disable-snapshot-block-public-access
```

Supervise y bloquee el acceso público a las instantáneas mediante Amazon EventBridge

Amazon EBS emite eventos relacionados con el bloqueo del acceso público de las instantáneas. Puedes usar AWS Lambda Amazon EventBridge para gestionar las notificaciones de eventos mediante programación. Los eventos se emiten en la medida de lo posible. Para obtener más información, consulta la Guía del EventBridge usuario de Amazon.

Se emiten los siguientes eventos:

- Habilitación del bloqueo del acceso público de las instantáneas en el modo para bloquear todo el uso compartido

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Block Public Access Enabled",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2019-05-31T21:49:54Z",
  "region": "us-east-1",
  "detail": {
    "SnapshotBlockPublicAccessState": "block-all-sharing",
    "message": "Block Public Access was successfully enabled in 'block-all-sharing'
 mode"
  }
}
```

- Habilitación del bloqueo del acceso público de las instantáneas en el modo para bloquear el nuevo uso compartido

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Block Public Access Enabled",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2019-05-31T21:49:54Z",
  "region": "us-east-1",
  "detail": {
    "SnapshotBlockPublicAccessState": "block-new-sharing",
    "message": "Block Public Access was successfully enabled in 'block-new-sharing'
 mode"
  }
}
```

- Deshabilitar el bloqueo del acceso público de las instantáneas

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Block Public Access Disabled",
  "source": "aws.ec2",
```

```
  "account": "123456789012",
  "time": "2019-05-31T21:49:54Z",
  "region": "us-east-1",
  "detail": {
    "SnapshotBlockPublicAccessState": "unblocked",
    "message": "Block Public Access was successfully disabled"
  }
}
```

Papelera de reciclaje para instantáneas

La papelera de reciclaje es una característica de recuperación de datos que le permite restaurar instantáneas de Amazon EBS y AMI basadas en EBS que se han eliminado por accidente. Cuando se utiliza la papelera de reciclaje, si se eliminan recursos, estos se retienen en la papelera de reciclaje durante un periodo que usted especifique antes de eliminarse de forma permanente.

Puede restaurar un recurso desde la papelera de reciclaje en cualquier momento antes de que se venza su periodo de retención. Después de restaurar un recurso desde la papelera de reciclaje, este se quita de la papelera de reciclaje y puede utilizarse de la misma manera que utiliza cualquier otro recurso de ese tipo en su cuenta. Si el periodo de retención se vence y el recurso no se restaura, este se elimina de forma permanente de la papelera de reciclaje y ya no estará disponible para su recuperación.

Las instantáneas de la papelera de reciclaje se facturan con la misma tarifa que las instantáneas normales de la cuenta. El uso de la papelera de reciclaje y las reglas de retención no tienen costos adicionales. Para obtener más información, consulte Precios Amazon EBS.

Para obtener más información, consulte Papelera de reciclaje.

Temas

- Permisos para trabajar con instantáneas en la papelera de reciclaje
- Ver instantáneas en la papelera de reciclaje
- Restaurar instantáneas desde la papelera de reciclaje

Permisos para trabajar con instantáneas en la papelera de reciclaje

De forma predeterminada, los usuarios no tienen permiso para trabajar con las instantáneas que se encuentran en la papelera de reciclaje. Para permitir a los usuarios trabajar con estos recursos, debe

crear políticas de IAM que concedan permisos para utilizar recursos específicos y acciones de la API. Una vez creadas las políticas, tendrá que agregar permisos a los usuarios, grupos o roles.

Para ver y recuperar las instantáneas que se encuentran en la papelera de reciclaje, los usuarios deben tener los siguientes permisos:

- `ec2:ListSnapshotsInRecycleBin`
- `ec2:RestoreSnapshotFromRecycleBin`

Para administrar las etiquetas de las instantáneas que se encuentran en la papelera de reciclaje, los usuarios necesitan los siguientes permisos adicionales.

- `ec2:CreateTags`
- `ec2:DeleteTags`

Para utilizar la consola de la papelera de reciclaje, los usuarios necesitan el permiso `ec2:DescribeTags`.

A continuación, se muestra una política de IAM de ejemplo. Incluye el permiso `ec2:DescribeTags` para los usuarios de la consola y los permisos `ec2:CreateTags` y `ec2:DeleteTags` para administrar etiquetas. Si los permisos no se necesitan, puede eliminarlos de la política.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
            "ec2:ListSnapshotsInRecycleBin",
            "ec2:RestoreSnapshotFromRecycleBin"
        ],
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags",
            "ec2:DeleteTags",
            "ec2:DescribeTags"
        ],
```

```
        "Resource": "arn:aws:ec2:Region:account-id:snapshot/*"
      },

    ]
}
```

Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center .
- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones descritas en Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.
- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Para obtener más información sobre los permisos necesarios para utilizar la papelera de reciclaje, consulte Permisos necesarios de IAM.

Ver instantáneas en la papelera de reciclaje

Mientras haya una instantánea en la papelera de reciclaje, podrá ver información limitada al respecto, que incluye:

- El ID de la instantánea.
- La descripción de la instantánea.
- El ID del volumen desde el que se creó la instantánea.
- La fecha y la hora en que se eliminó la instantánea e ingresó en la papelera de reciclaje.
- La fecha y la hora en que se vence el periodo de retención. La instantánea se eliminará de forma permanente de la papelera de reciclaje en este momento.

Puede ver las instantáneas en la papelera de reciclaje mediante uno de los siguientes métodos.

Recycle Bin console

Para ver las instantáneas en la papelera de reciclaje mediante la consola

1. Abra la consola de la papelera de reciclaje en https://console.aws.amazon.com/rbin/home/
2. En el panel de navegación, elija Recycle Bin (Papelera de reciclaje).
3. La cuadrícula enumera todas las instantáneas que se encuentran actualmente en la papelera de reciclaje. Para ver los detalles de una instantánea específica, selecciónela en la cuadrícula y elija Actions (Acciones), View details (Ver detalles).

AWS CLI

Para ver las instantáneas de la papelera de reciclaje mediante el AWS CLI

Utilice el comando list-snapshots-in-recycle-bin AWS CLI . Incluya la opción `--snapshot-id` para ver una instantánea específica. U omita la opción `--snapshot-id` para ver todas las instantáneas en la papelera de reciclaje.

```
$ C:\> aws ec2 list-snapshots-in-recycle-bin --snapshot-id snapshot_id
```

Por ejemplo, el siguiente comando proporciona información acerca de la instantánea `snap-01234567890abcdef` en la papelera de reciclaje.

```
$ C:\> aws ec2 list-snapshots-in-recycle-bin --snapshot-id snap-01234567890abcdef
```

Ejemplo de salida:

```
{
    "SnapshotRecycleBinInfo": [
        {
            "Description": "Monthly data backup snapshot",
            "RecycleBinEnterTime": "2021-12-01T13:00:00.000Z",
            "RecycleBinExitTime": "2021-12-15T13:00:00.000Z",
            "VolumeId": "vol-abcdef09876543210",
            "SnapshotId": "snap-01234567890abcdef"
        }
    ]
}
```

Restaurar instantáneas desde la papelera de reciclaje

No puede utilizar una instantánea de ninguna manera mientras está en la papelera de reciclaje. Para utilizar la instantánea, primero debe restaurarla. Cuando restaura una instantánea desde la papelera de reciclaje, la instantánea está disponible inmediatamente para su uso y se quita de la papelera de reciclaje. Puede utilizar una instantánea restaurada de la misma manera en que utiliza cualquier otra instantánea de la cuenta.

Puede restaurar una instantánea desde la papelera de reciclaje mediante uno de los siguientes métodos.

Recycle Bin console

Para restaurar una instantánea desde la papelera de reciclaje mediante la consola

1. Abra la consola de la papelera de reciclaje en https://console.aws.amazon.com/rbin/home/
2. En el panel de navegación, elija Recycle Bin (Papelera de reciclaje).
3. La cuadrícula enumera todas las instantáneas que se encuentran actualmente en la papelera de reciclaje. Seleccione la instantánea que desea restaurar y elija Recover (Recuperar).
4. Cuando se le pregunte, elija Recover (Recuperar).

AWS CLI

Para restaurar una instantánea eliminada de la papelera de reciclaje mediante el AWS CLI

Utilice el AWS CLI comando restore-snapshot-from-recycle-bin. En `--snapshot-id`, especifique el ID de la instantánea que desea restaurar.

```
$ C:\> aws ec2 restore-snapshot-from-recycle-bin --snapshot-id snapshot_id
```

Por ejemplo, el siguiente comando restaura la instantánea `snap-01234567890abcdef` de la papelera de reciclaje.

```
$ C:\> aws ec2 restore-snapshot-from-recycle-bin --snapshot-id
 snap-01234567890abcdef
```

Ejemplo de salida:

```
{
```

```
    "SnapshotId": "snap-01234567890abcdef",
    "Description": "Monthly data backup snapshot",
    "Encrypted": false,
    "OwnerId": "111122223333",
    "Progress": "100%",
    "StartTime": "2021-12-01T13:00:00.000000+00:00",
    "State": "recovering",
    "VolumeId": "vol-ffffffff",
    "VolumeSize": 30
}
```

Amazon EBS local snapshots on Outposts

Las instantáneas Amazon EBS son una copia puntual de los volúmenes de EBS.

De forma predeterminada, las instantáneas de volúmenes de EBS en un Outpost se almacenan en Amazon S3 en la región del Outpost. También puede utilizar Instantáneas locales de Amazon EBS en Outposts para almacenar instantáneas de volúmenes de forma local en un Outpost en Amazon S3 del propio Outpost. Esto garantiza que los datos de instantáneas residen en el Outpost y en las instalaciones. Además, puede utilizar políticas y permisos de AWS Identity and Access Management (IAM) para configurar políticas de aplicación de residencia de datos para que los datos de las instantáneas no abandonen el Outpost. Esto es especialmente útil si reside en un país o región que aún no cuenta con una región AWS y que tiene requisitos de residencia de datos.

Este tema proporciona información sobre cómo trabajar con Instantáneas locales de Amazon EBS en Outposts. Para obtener más información sobre las instantáneas de Amazon EBS y de la forma de trabajar con ellas en una región de AWS, consulte Instantáneas de Amazon EBS.

Para obtener más información sobre AWS Outposts, consulte Características de AWS Outposts y la Guía del usuario de AWS Outposts. Para obtener información sobre los precios, consulte Precios de AWS Outposts.

Temas

- Preguntas frecuentes
- Requisitos previos
- Consideraciones
- Controlar el acceso con IAM
- Trabajar con instantáneas locales

Preguntas frecuentes

1. ¿Qué son las instantáneas locales?

   De forma predeterminada, las instantáneas Amazon EBS de volúmenes de Outpost se almacenan en Amazon S3 en la región de Outpost. Si el Outpost está aprovisionado con Amazon S3 en Outposts, puede elegir almacenar las instantáneas de forma local en el mismo Outpost. Las instantáneas locales son progresivas, lo que significa que solo se guardan los bloques del volumen que se han cambiado después de la instantánea más reciente. Puede utilizar estas instantáneas para restaurar un volumen en el mismo Outpost que la instantánea en cualquier momento. Para obtener más información acerca de las instantáneas Amazon EBS, consulte Instantáneas de Amazon EBS.

2. ¿Por qué debo utilizar instantáneas locales?

   Las instantáneas son una forma práctica de hacer copias de seguridad de sus datos. Con instantáneas locales, todos los datos de las instantáneas se almacenan de forma local en Outpost. Esto significa que no sale de las instalaciones. Esto es especialmente útil si reside en un país o región que aún no cuenta con una región de AWS y que tiene requisitos de residencia.

   Además, el uso de instantáneas locales puede ayudar a reducir el ancho de banda utilizado para la comunicación entre la región y el Outpost en entornos con restricciones de ancho de banda.

3. ¿Cómo aplicar la residencia de datos de instantáneas en Outposts?

   Puede utilizar políticas de AWS Identity and Access Management (IAM) para controlar los permisos que tienen las entidades principales (cuentas de AWS, usuarios de IAM y roles de IAM) cuando trabajan con las instantáneas locales y para aplicar la residencia de datos. Puede crear una política que impida que las entidades principales creen instantáneas a partir de volúmenes e instancias de Outpost y almacenen las instantáneas en una región AWS. Actualmente, la copia de instantáneas e imágenes de un Outpost a una región no es compatible. Para obtener más información, consulte Controlar el acceso con IAM.

4. ¿Son compatibles las instantáneas locales coherentes frente a bloqueos en varios volúmenes?

   Sí, puede crear instantáneas locales coherentes frente a bloqueos en varios volúmenes a partir de instancias en un Outpost.

5. ¿Cómo puedo crear instantáneas locales?

   Puede crear instantáneas de forma manual utilizando la AWS Command Line Interface (AWS CLI) o la consola de Amazon EC2. Para obtener más información, consulte Trabajar con

instantáneas locales. También puede automatizar el ciclo de vida de la instantáneas locales utilizando Amazon Data Lifecycle Manager. Para obtener más información, consulte Automatice instantáneas en un Outpost.

6. ¿Puedo crear, usar o eliminar instantáneas locales si el Outpost pierde la conectividad con la región?

   No. El Outpost debe tener conectividad con la región, ya que la región proporciona los servicios de acceso, autorización, registro y supervisión que son fundamentales para el estado de las instantáneas. Si no hay conectividad, no puede crear nuevas instantáneas locales, crear volúmenes o iniciar instancias desde las existentes instantáneas locales, ni eliminarlas instantáneas locales.

7. ¿Con qué rapidez se dispone de la capacidad de almacenamiento de Amazon S3 después de eliminar instantáneas locales?

   La capacidad de almacenamiento de Amazon S3 se encontrará disponible en las 72 horas siguientes a la eliminación de instantáneas locales y los volúmenes que hacen referencia a ellos.

8. ¿Cómo puedo asegurarme de no quedarme sin capacidad de Amazon S3 en el Outpost?

   Recomendamos utilizar alarmas Amazon CloudWatch para supervisar la capacidad de almacenamiento de Amazon S3 y eliminar instantáneas y volúmenes que ya no necesite y así evitar quedarse sin capacidad de almacenamiento. Si utiliza Amazon Data Lifecycle Manager para automatizar el ciclo de vida de instantáneas locales, asegúrese de que las políticas de retención de instantáneas no retengan instantáneas durante más tiempo del necesario.

9. ¿Qué ocurre si me quedo sin capacidad local de Amazon S3 en mis Outposts?

   Si se queda sin capacidad local de Amazon S3 en sus Outposts, Amazon Data Lifecycle Manager no podrá crear instantáneas locales de manera exitosa en los Outposts. Amazon Data Lifecycle Manager intentará crear las instantáneas locales en los Outposts, pero las instantáneas pasan inmediatamente al estado `error` y, con el tiempo, Amazon Data Lifecycle Manager las elimina. Le recomendamos que utilice la métrica `SnapshotsCreateFailed` de Amazon CloudWatch para monitorear las políticas del ciclo de vida de las instantáneas a fin de detectar errores en la creación de instantáneas Para obtener más información, consulte Supervisa tus políticas con Amazon CloudWatch.

10. ¿Puedo usar instantáneas locales y las AMI respaldadas por instantáneas locales con instancias de spot y flotas de spot?

    No, no puede usar instantáneas locales o las AMI respaldadas por instantáneas locales con instancias de spot y flotas de spot.

11. ¿Puedo usar instantáneas locales y las AMI respaldadas por instantáneas locales con Amazon EC2 Auto Scaling?

Sí, puede utilizar instantáneas locales y las AMI respaldadas por instantáneas locales para iniciar grupos de Auto Scaling en una subred que se encuentre en el mismo Outpost que las instantáneas. El rol vinculado al servicio de grupo de Amazon EC2 Auto Scaling debe tener permiso para usar la Clave de KMS utilizada para cifrar las instantáneas.

No se pueden utilizar instantáneas locales ni AMI respaldadas por instantáneas locales para lanzar grupos de Auto Scaling en una región de AWS.

Requisitos previos

Para almacenar instantáneas en un Outpost, debe tener un Outpost aprovisionado con Amazon S3 en Outposts. Para obtener más información acerca de Amazon S3 en los Outposts, consulte Uso de Amazon S3 en Outposts en la Guía del usuario de Amazon Simple Storage Service.

Consideraciones

Tenga en cuenta lo siguiente cuando trabaje con instantáneas locales.

- Outposts debe tener conectividad con la región de AWS para utilizar instantáneas locales.
- Los metadatos de instantáneas se almacenan en la región AWS asociada al Outpost. Esto no incluye los datos de las instantáneas.
- Las instantáneas almacenadas en Outposts se cifran de forma predeterminada. Las instantáneas sin cifrar no son compatibles. Las instantáneas que se crean y copian en un Outpost se cifran mediante la Clave de KMS predeterminada para la región o una Clave de KMS diferente que especifique en el momento de la solicitud.
- Cuando se crea un volumen en un Outpost desde una instantánea local, no se puede volver a cifrar el volumen mediante una Clave de KMS diferente. Los volúmenes creados a partir de instantáneas locales deben cifrarse con la misma Clave de KMS que la instantánea de origen.
- Después de eliminar instantáneas locales de un Outpost, la capacidad de almacenamiento de Amazon S3 utilizada por las instantáneas eliminadas se encontrará disponible en un plazo de 72 horas. Para obtener más información, consulte Elimine instantáneas locales.
- No se puede exportar instantáneas locales desde un Outpost.
- No se puede habilitar la restauración rápida de instantáneas para instantáneas locales.
- API directas de EBS no es compatible con instantáneas locales.

- No se pueden copiar las instantáneas locales ni las AMI de un Outpost a una región de AWS, de un Outpost a otro ni dentro de un mismo Outpost. Sin embargo, puede copiar instantáneas de una región AWS a un Outpost. Para obtener más información, consulte Copiar instantáneas de una región AWS a un Outpost.
- Al copiar una instantánea de una región de AWS a un Outpost, los datos se transfieren a través del enlace de servicio. Copiar varias instantáneas simultáneamente podría afectar a otros servicios que se ejecutan en el Outpost.
- No puede compartir instantáneas locales.
- Debe utilizar políticas IAM para garantizar el cumplimiento de los requisitos de residencia de datos. Para obtener más información, consulte Controlar el acceso con IAM.
- Las Instantáneas locales son copias de seguridad incrementales. Solo los bloques del volumen que han cambiado después de la última instantánea se guardan en la nueva. Cada instantánea local contiene toda la información necesaria para restaurar los datos (del momento en que se tomó) en un volumen de EBS nuevo. Para obtener más información, consulte Cómo funcionan las instantáneas.
- No puede usar políticas de IAM para aplicar la residencia de datos para las acciones CopySnapshot y CopyImage.

Controlar el acceso con IAM

Puede utilizar políticas de AWS Identity and Access Management (IAM) para controlar los permisos que tienen las entidades principales (cuentas de AWS, usuarios de IAM y roles de IAM) cuando trabajan con las instantáneas locales. Los siguientes son ejemplos de políticas que puede utilizar para conceder o denegar permiso para realizar acciones específicas con instantáneas locales.

> **Important**
>
> Actualmente no es posible copiar instantáneas e imágenes de un Outpost a una región. Como resultado, actualmente no puede usar políticas de IAM para aplicar la residencia de datos para las acciones CopySnapshot y CopyImage.

Temas

- Aplicar la residencia de datos para las instantáneas
- Impedir que las entidades principales eliminen instantáneas locales

Aplicar la residencia de datos para las instantáneas

La siguiente política de ejemplo impide que todos las entidades principales creen instantáneas de volúmenes e instancias en Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef` y almacenen los datos de la instantánea en una región AWS. Las entidades principales aún pueden crear instantáneas locales. Esta política garantiza que todas las instantáneas permanezcan en el Outpost.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots"
            ],
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:SourceOutpostArn": "arn:aws:outposts:us-
east-1:123456789012:outpost/op-1234567890abcdef0"
                },
                "Null": {
                    "ec2:OutpostArn": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots"
            ],
            "Resource": "*"
        }
    ]
}
```

Impedir que las entidades principales eliminen instantáneas locales

La siguiente política de ejemplo impide que todas las entidades principales eliminen las instantáneas locales que se almacenan en Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ec2:DeleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:OutpostArn": "arn:aws:outposts:us-east-1:123456789012:outpost/
op-1234567890abcdef0"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteSnapshot"
            ],
            "Resource": "*"
        }
    ]
}
```

Trabajar con instantáneas locales

En las secciones siguientes se explica cómo utilizar instantáneas locales.

Temas

- Reglas para almacenar instantáneas
- Cree instantáneas locales a partir de volúmenes en un Outpost
- Cree instantáneas locales de varios volúmenes a partir de instancias en un Outpost

- Cree AMI a partir de instantáneas locales
- Copiar instantáneas de una región AWS a un Outpost
- Copiar AMI de una región AWS a un Outpost
- Cree volúmenes a partir de instantáneas locales
- Inicie instancias desde AMI respaldadas por instantáneas locales
- Elimine instantáneas locales
- Automatice instantáneas en un Outpost

Reglas para almacenar instantáneas

Las siguientes reglas se aplican al almacenamiento de instantáneas:

- Si la instantánea más reciente de un volumen se almacena en un Outpost, todas las instantáneas sucesivas deben almacenarse en el mismo Outpost.
- Si la instantánea más reciente de un volumen se almacena en una región AWS, todas las instantáneas sucesivas deben almacenarse en la misma región. Para empezar a crear instantáneas locales a partir de ese volumen, haga lo siguiente:

  1. Cree una instantánea del volumen en la región AWS.
  2. Copie la instantánea en el Outpost desde la región AWS.
  3. Cree un nuevo volumen a partir de instantánea local.
  4. Asocie el volumen a una instancia del Outpost.

  Para el nuevo volumen del Outpost, la siguiente instantánea se puede almacenar en el Outpost o en la región AWS. Todas las instantáneas sucesivas deben almacenarse en esa misma ubicación.
- Las instantáneas locales, incluidas las instantáneas creadas en un Outpost y las instantáneas copiadas en un Outpost de una región de AWS, solo se pueden utilizar para crear volúmenes en el mismo Outpost.
- Si crea un volumen en un Outpost a partir de una instantánea de una región, todas las instantáneas sucesivas de ese nuevo volumen deben estar en la misma región.
- Si crea un volumen en un Outpost a partir de una instantánea local, todas las instantáneas sucesivas de ese nuevo volumen deben estar en el mismo Outpost.

Cree instantáneas locales a partir de volúmenes en un Outpost

Puede crear instantáneas locales a partir de volúmenes en el Outpost. Puede optar por almacenar las instantáneas en el mismo Outpost que el volumen de origen o en la región del Outpost.

Instantáneas locales se puede utilizar para crear volúmenes solo en el mismo Outpost.

Puede crear instantáneas locales a partir de volúmenes en un Outpost utilizando uno de los siguientes métodos.

Console

Para crear instantáneas locales partir de volúmenes en un Outpost

Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.

1. En el panel de navegación, elija Volumes (Volúmenes).
2. Seleccione el volumen en el Outpost y elija Actions (Acciones), Create Snapshot (Crear instantánea).
3. (Opcional) En Description (Descripción), introduzca una breve descripción para la instantánea.
4. En Snapshot destination (Destino de instantáneas), seleccione AWS Outpost. La instantánea se creará en el mismo Outpost que el volumen de origen. El campo Outpost ARN (ARN del Outpost) muestra el nombre de recurso de Amazon (ARN) del Outpost de destino.
5. (Opcional) Elija Add Tag (Añadir etiqueta) para añadir etiquetas a su instantánea. Para cada etiqueta, proporcione un valor y una clave de etiqueta.
6. Elija Create Snapshot (Crear instantánea).

Command line

Para crear instantáneas locales partir de volúmenes en un Outpost

Utilice el comando create-snapshot. Especifique el ID del volumen desde el que se va a crear la instantánea y el ARN del Outpost de destino en el que desea almacenar la instantánea. Si omite el ARN del Outpost, la instantánea se almacena en la región AWS del Outpost.

Por ejemplo, el siguiente comando crea una instantánea local de volumen `vol-1234567890abcdef0`y almacena la instantánea en el Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`.

```
$ aws ec2 create-snapshot --volume-id vol-1234567890abcdef0 --outpost-arn
 arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0 --description
 "single volume local snapshot"
```

Cree instantáneas locales de varios volúmenes a partir de instancias en un Outpost

Puede crear instantáneas locales coherentes frente a bloqueos en varios volúmenes a partir de instancias del Outpost. Puede optar por almacenar las instantáneas en el mismo Outpost que la instancia de origen o en la región del Outpost.

instantáneas locales de varios volúmenes solo se pueden utilizar para crear volúmenes en el mismo Outpost.

Puede crear instantáneas locales de varios volúmenes a partir de instancias en un Outpost utilizando uno de los siguientes métodos.

Console

Para crear instantáneas locales de varios volúmenes a partir de instancias en un Outpost

Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.

1. En el panel de navegación, elija Snapshots (Instantáneas).
2. Elija Create Snapshot (Crear instantánea).
3. En Select resource type (Seleccionar tipo de recurso), elija Instance (Instancia).
4. En Instance ID (Id. de instancia), seleccione la instancia del Outpost desde la que desea crear las instantáneas.
5. (Opcional) En Description (Descripción), introduzca una breve descripción para las instantáneas.
6. En Snapshot destination (Destino de instantáneas), seleccione AWS Outpost. Las instantáneas se crearán en el mismo Outpost que la instancia de origen. El Outpost ARN (ARN del Outpost) muestra el ARN del Outpost de destino.
7. Para excluir el volumen raíz de la instancia del conjunto de instantáneas de varios volúmenes, seleccione Exclude root volume (Excluir volumen raíz). Si lo hace, Amazon EBS no creará una instantánea del volumen raíz de la instancia.
8. Para excluir volúmenes de datos específicos del conjunto de instantáneas de varios volúmenes, seleccione Exclude specific data volumes (Excluir volúmenes de datos

específicos). En la sección Attached data volumes (Volúmenes de datos adjuntos) se enumeran todos los volúmenes de datos adjuntos actualmente a la instancia seleccionada.

En la sección Attached data volumes (Volúmenes de datos adjuntos), anule la selección de los volúmenes de datos que se excluirán del conjunto de instantáneas de varios volúmenes. Solo los volúmenes que continúen seleccionados se incluirán en el conjunto de instantáneas de varios volúmenes.

9. (Opcional) Para copiar etiquetas automáticamente de los volúmenes de origen en las instantáneas correspondientes, en Copy tags from source volume (Copiar etiquetas del volumen de origen), seleccione Copy tags (Copiar etiquetas). Esta opción configura los metadatos de la instantánea, como las políticas de acceso, la información adjunta y la asignación de costos, para que coincidan con el volumen de origen.
10. (Opcional) Para asignar etiquetas personalizadas adicionales a las instantáneas, en la sección Tags (Etiquetas), elija Add tag (Agregar etiqueta) y, a continuación, ingrese el par clave-valor. Puede añadir hasta 50 etiquetas.
11. Elija Create Snapshot (Crear instantánea).

    Las instantáneas se administran de manera conjunta durante la creación de la instantánea. Si una de las instantáneas del conjunto de volúmenes da error, el resto de las instantáneas del conjunto de volúmenes pasarán al estado de error.

Command line

Para crear instantáneas locales de varios volúmenes a partir de instancias en un Outpost

Utilice el comando create-snapshots. Especifique el ID de la instancia desde la que se van a crear las instantáneas y el ARN del Outpost de destino en el que desea almacenar las instantáneas. Si omite el ARN del Outpost, las instantáneas se almacenan en la región AWS del Outpost.

Por ejemplo, el siguiente comando crea instantáneas de los volúmenes asociados a la instancia `i-1234567890abcdef0` y almacena las instantáneas en Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`.

```
$ aws ec2 create-snapshots --instance-specification InstanceId=i-1234567890abcdef0
 --outpost-arn arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0
 --description "multi-volume local snapshots"
```

Cree AMI a partir de instantáneas locales

Puede crear Imágenes de Amazon Machine (AMI) utilizando una combinación de instantáneas locales e instantáneas y almacenadas en la Región de Outpost. Por ejemplo, si tiene un Outpost en `us-east-1`, puede crear una AMI con volúmenes de datos respaldados por instantáneas locales en ese Outpost y un volumen raíz respaldado por una instantánea en la región `us-east-1`.

> **Note**
>
> - No puede crear AMI que incluyan instantáneas de respaldo almacenadas en varios Outposts.
> - Actualmente, no puede crear AMI directamente a partir de instancias de un Outpost mediante la API CreateImage o la consola de Amazon EC2 para Outposts habilitados con Amazon S3 en Outposts.
> - Las AMI respaldadas por instantáneas locales solo se pueden utilizar para iniciar instancias en el mismo Outpost.

Para crear una AMI en un Outpost a partir de instantáneas de una región

1. Copie las instantáneas de la región al Outpost. Para obtener más información, consulte Copiar instantáneas de una región AWS a un Outpost.
2. Utilice la consola de Amazon EC2 o el comando register-image para crear la AMI utilizando las copias de la instantánea en el Outpost. Para obtener más información, consulte Creación de una AMI a partir de una instantánea.

Para crear una AMI en un Outpost a partir de una instancia de un Outpost

1. Cree instantáneas a partir de la instancia en el Outpost y almacene las instantáneas en el Outpost. Para obtener más información, consulte Cree instantáneas locales de varios volúmenes a partir de instancias en un Outpost.
2. Utilice la consola de Amazon EC2 o el comando register-image para crear la AMI utilizando instantáneas locales. Para obtener más información, consulte Creación de una AMI a partir de una instantánea.

Para crear una AMI en una región a partir de una instancia en un Outpost

1. Cree instantáneas a partir de la instancia en el Outpost y almacene las instantáneas en la región. Para obtener más información, consulte Cree instantáneas locales a partir de volúmenes en un Outpost o Cree instantáneas locales de varios volúmenes a partir de instancias en un Outpost.
2. Utilice la consola de Amazon EC2 o el comando register-image para crear la AMI utilizando las copia de la instantánea en la región. Para obtener más información, consulte Creación de una AMI a partir de una instantánea.

Copiar instantáneas de una región AWS a un Outpost

Puede copiar instantáneas de una región AWS a un Outpost. Sólo puede hacerlo si las instantáneas se encuentran en la región del Outpost. Si las instantáneas se encuentran en una región diferente, primero debe copiar la instantánea en la región del Outpost y, a continuación, copiarla desde esa región al Outpost.

> **Note**
>
> No puede copiar instantáneas locales desde un Outpost a una región, de un Outpost a otro ni dentro del mismo Outpost.

Puede copiar instantáneas de una región a un Outpost utilizando uno de los métodos siguientes.

Console

Para copiar una instantánea de una región AWS a un Outpost

Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.

1. En el panel de navegación, elija Snapshots (Instantáneas).
2. Seleccione la instantánea en la región y elija Actions (Acciones), Copy (Copiar).
3. En Destination Region (Región de destino), seleccione la región para el Outpost de destino.
4. En Snapshot Destination (Destino de instantáneas), seleccione AWS Outpost.

   El campo Snapshot Destination (Destino de instantánea) sólo aparece si tiene Outposts en la región de destino seleccionada. Si el campo no aparece, no tiene ningún Outposts en la región de destino seleccionada.

5. En Destination Outpost ARN (ARN del Outpost de destino), introduzca el ARN del Outpost en el que desea copiar la instantánea.
6. (Opcional) En Description (Descripción), introduzca una breve descripción de la instantánea copiada.
7. El cifrado está habilitado de forma predeterminada para la copia de la instantánea. El cifrado no se puede deshabilitar. En Clave de KMS, elija la Clave de KMS que desea usar.
8. Elija Copy.

Command line

Para copiar una instantánea de una región a un Outpost

Utilice el comando copy-snapshot. Especifique el ID de la instantánea que se va a copiar, la región desde la que se va a copiar la instantánea y el ARN del Outpost de destino.

Por ejemplo, el siguiente comando copia la instantánea `snap-1234567890abcdef0` de la región `us-east-1` al Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`.

```
$ aws ec2 copy-snapshot --source-region us-east-1 --source-snapshot-
id snap-1234567890abcdef0 --destination-outpost-arn arn:aws:outposts:us-
east-1:123456789012:outpost/op-1234567890abcdef0 --description "Local snapshot copy"
```

Copiar AMI de una región AWS a un Outpost

Puede copiar las AMI de una región AWS a un Outpost. Al copiar una AMI de una región a un Outpost, todas las instantáneas asociadas a la AMI se copian de la región al Outpost.

Puede copiar una AMI de una región a un Outpost sólo si las instantáneas asociadas a la AMI se encuentran en la región del Outpost. Si las instantáneas se encuentran en una región diferente, primero debe copiar la AMI en la región del Outpost y, a continuación, copiarla desde esa región al Outpost.

> **Note**
>
> No se puede copiar una AMI de un Outpost a una región, de un Outpost a otro o dentro de un Outpost.

Puede copiar las AMI de una región a un Outpost utilizando solo el AWS CLI.

Command line

Para copiar una AMI de una región a un Outpost

Utilice el comando copy-image. Especifique el ID de la AMI que se va a copiar, la región de origen y el ARN del Outpost de destino.

Por ejemplo, el siguiente comando copia la AMI `ami-1234567890abcdef0` de la región `us-east-1` al Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`.

```
$ aws ec2 copy-image --source-region us-east-1 --source-image-
id ami-1234567890abcdef0 --name "Local AMI copy"  --destination-outpost-arn
 arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0
```

Cree volúmenes a partir de instantáneas locales

Puede crear volúmenes en Outposts desde instantáneas locales. Los volúmenes se deben crear en el mismo Outpost que las instantáneas de origen. No se puede utilizar instantáneas locales para crear volúmenes en la región para el Outpost.

Al crear un volumen a partir de una instantánea local, no puede volver a cifrar el volumen mediante una Clave de KMS diferente. Los volúmenes creados a partir de instantáneas locales deben cifrarse con la misma Clave de KMS que la instantánea de origen.

Para obtener más información, consulte Creación de un volumen desde una instantánea.

Inicie instancias desde AMI respaldadas por instantáneas locales

Puede iniciar instancias desde AMI respaldadas por instantáneas locales. Debe iniciar instancias en el mismo Outpost que la AMI de origen. Para obtener más información, consulte Lanzar una instancia en Outpost en la Guía del usuario de AWS Outposts.

Elimine instantáneas locales

Puede eliminar instantáneas locales de un Outpost. Después de eliminar una instantánea de un Outpost, la capacidad de almacenamiento de Amazon S3 utilizada por la instantánea eliminada se

encontrará disponible dentro de las 72 horas siguientes a eliminar la instantánea y los volúmenes que hacen referencia a esa instantánea.

Dado que la capacidad de almacenamiento de Amazon S3 no está disponible inmediatamente, le recomendamos que utilice alarmas Amazon CloudWatch para supervisar la capacidad de almacenamiento de Amazon S3. Elimine las instantáneas y los volúmenes que ya no necesite para evitar quedarse sin capacidad de almacenamiento.

Para obtener más información acerca de la eliminación de instantáneas, consulte Eliminar una instantánea.

Automatice instantáneas en un Outpost

Puede crear políticas de ciclo de vida de instantáneas Amazon Data Lifecycle Manager que creen, copien, retengan y eliminen automáticamente instantáneas de volúmenes e instancias en un Outpost. Puede elegir si desea almacenar las instantáneas en una Región o de forma local en un Outpost. Además, puede copiar automáticamente instantáneas creadas y almacenadas en una región AWS a un Outpost.

En la siguiente tabla se muestra una descripción general de las características compatibles.

Ubicación de recursos	Destino de instantánea	Copia entre regiones		Restauración rápida de instantáneas	Uso compartido entre cuentas
		En la región	En Outpost		
Region	Region	✓	✓	✓	✓
Outpost	Region	✓	✓	✓	✓
Outpost	Outpost	✗	✗	✗	✗

Consideraciones

- Actualmente sólo se admiten políticas de ciclo de vida de instantáneas Amazon EBS. Las políticas de AMI respaldadas por EBS y las políticas de eventos de uso compartido entre cuentas no son compatibles.
- Si una política administra instantáneas para volúmenes o instancias de una región, las instantáneas se crean en la misma región que el recurso de origen.

- Si una política administra instantáneas de volúmenes o instancias en un Outpost, las instantáneas se pueden crear en el Outpost de origen o en la región de ese Outpost.
- Una sola política no puede administrar tanto las instantáneas de una región como las instantáneas de un Outpost. Si necesita automatizar instantáneas en una región y en un Outpost, debe crear políticas independientes.
- La restauración rápida de instantáneas no es compatible con las instantáneas creadas en un Outpost o para las instantáneas copiadas en un Outpost.
- El uso compartido entre cuentas no es compatible con las instantáneas creadas en un Outpost.

Para obtener más información acerca de cómo crear un ciclo de vida de instantáneas que administre instantáneas locales, vea Automatizar ciclos de vida de instantáneas.

Cifrado de Amazon EBS

Utilice Cifrado de Amazon EBS como una solución de cifrado directa para sus recursos de EBS asociados con sus instancias EC2. Con el cifrado de Amazon EBS, no tendrá que crear, mantener ni proteger su propia infraestructura de administración de claves. El cifrado de Amazon EBS utiliza AWS KMS keys cuando crea volúmenes e instantáneas cifrados.

Las operaciones de cifrado se llevan a cabo en los servidores que alojan las instancias de EC2, lo que garantiza la seguridad tanto data-at-rest de una instancia como data-in-transit entre ella y su almacenamiento EBS adjunto.

Puede asociar volúmenes cifrados y no cifrados con una instancia simultáneamente.

Contenido

Cómo funciona el cifrado de EBS

Puede cifrar los volúmenes de datos y de arranque de una instancia EC2.

Cuando se crea un volumen de EBS y se adjunta a un tipo de instancia compatible, se cifran los tipos de datos siguientes:

- Datos en reposo dentro del volumen
- Todos los datos que se mueven entre el volumen y la instancia
- Todas las instantáneas creadas a partir del volumen
- Todos los volúmenes creados a partir de esas instantáneas

Amazon EBS cifra el volumen con una clave de datos que utiliza el cifrado de datos estándar de la industria AES-256. La clave de datos se genera AWS KMS y, a continuación, se cifra AWS KMS con

su AWS KMS clave antes de almacenarla con la información de volumen. Todas las instantáneas y cualquier volumen posterior creado a partir de esas instantáneas con la misma AWS KMS clave comparten la misma clave de datos. Para obtener más información, consulte Claves de datos en la Guía para desarrolladores de AWS Key Management Service .

Amazon EC2 funciona AWS KMS para cifrar y descifrar los volúmenes de EBS de formas ligeramente diferentes en función de si la instantánea a partir de la cual se crea un volumen cifrado está cifrada o no cifrada.

Funcionamiento del cifrado de EBS cuando se cifra la instantánea

Cuando crea un volumen cifrado a partir de una instantánea cifrada de su propiedad, Amazon EC2 lo utiliza AWS KMS para cifrar y descifrar los volúmenes de EBS de la siguiente manera:

1. Amazon EC2 envía una GenerateDataKeyWithoutPlaintextsolicitud a AWS KMS la que especifica la clave de KMS que ha elegido para el cifrado de volúmenes.
2. Si el volumen se cifra con la misma clave de KMS que la instantánea, AWS KMS utiliza la misma clave de datos que la instantánea y la cifra con esa misma clave de KMS. Si el volumen se cifra con una clave de KMS diferente, AWS KMS genera una nueva clave de datos y la cifra con la clave de KMS que especificó. La clave de datos cifrada se envía a Amazon EBS para almacenarla con los metadatos del volumen.
3. Al adjuntar el volumen cifrado a una instancia, Amazon EC2 envía una CreateGrantsolicitud para que AWS KMS pueda descifrar la clave de datos.
4. AWS KMS descifra la clave de datos cifrada y envía la clave de datos descifrada a Amazon EC2.
5. Amazon EC2 utiliza la clave de datos de texto no cifrado en el hardware de Nitro para cifrar las operaciones de E/S de disco en el volumen. La clave de datos de texto no cifrado persiste en la memoria siempre que el volumen esté asociado a la instancia EC2.

Funcionamiento del cifrado de EBS cuando la instantánea no está cifrada

Cuando crea un volumen cifrado a partir de una instantánea no cifrada, Amazon EC2 trabaja con AWS KMS para cifrar y descifrar los volúmenes de EBS de la siguiente manera:

1. Amazon EC2 envía una CreateGrantsolicitud a AWS KMS, para que pueda cifrar el volumen que se crea a partir de la instantánea.
2. Amazon EC2 envía una GenerateDataKeyWithoutPlaintextsolicitud a AWS KMS la que especifica la clave de KMS que ha elegido para el cifrado de volúmenes.

3. AWS KMS genera una nueva clave de datos, la cifra con la clave de KMS que haya elegido para el cifrado de volumen y envía la clave de datos cifrada a Amazon EBS para que la almacene con los metadatos del volumen.
4. Amazon EC2 envía una solicitud de descifrado AWS KMS a para descifrar la clave de datos cifrados, que luego utiliza para cifrar los datos del volumen.
5. Al adjuntar el volumen cifrado a una instancia, Amazon EC2 envía una CreateGrantsolicitud a AWS KMS, para que pueda descifrar la clave de datos.
6. Al adjuntar el volumen cifrado a una instancia, Amazon EC2 envía una solicitud de descifrado a AWS KMS la que especifica la clave de datos cifrados.
7. AWS KMS descifra la clave de datos cifrada y envía la clave de datos descifrada a Amazon EC2.
8. Amazon EC2 utiliza la clave de datos de texto no cifrado en el hardware de Nitro para cifrar las operaciones de E/S de disco en el volumen. La clave de datos de texto no cifrado persiste en la memoria siempre que el volumen esté asociado a la instancia EC2.

Para obtener más información, consulte Cómo Amazon Elastic Block Store (Amazon EBS) usa AWS KMS y Amazon EC2 ejemplo dos en la Guía para desarrolladores de AWS Key Management Service .

Cómo afectan las claves de KMS obsoletas a las claves de datos

Cuando una clave de KMS queda obsoleta, el efecto es casi inmediato (sujeto a la posible coherencia). El estado de clave de la clave de KMS cambia para reflejar su nueva condición y todas las solicitudes para utilizar la clave de KMS en operaciones criptográficas fallan.

Cuando se realiza una acción que inutiliza la clave de KMS, no se produce ningún efecto inmediato en la instancia de EC2 ni en los volúmenes de EBS asociados. Amazon EC2 usa la clave de datos, no la clave de KMS, para cifrar todas las E/S de disco mientras el volumen esté asociado a la instancia.

Sin embargo, cuando el volumen de EBS cifrado se separa de la instancia de EC2, Amazon EBS elimina la clave de datos del hardware de Nitro. La próxima vez que el volumen EBS cifrado se asocia a una instancia EC2, el accesorio devuelve un error, dado que Amazon EBS no puede utilizar la clave KMS para descifrar la clave de datos cifrada del volumen. Para volver a usar el volumen de EBS, debe hacer que la clave de KMS se pueda utilizar de nuevo.

> **Tip**
>
> Si ya no desea acceder a los datos almacenados en un volumen de EBS cifrado con una clave de datos generada a partir de una clave de KMS que pretende inutilizar, le recomendamos que separe el volumen de EBS de la instancia de EC2 antes de inutilizar la clave de KMS.

Para obtener más información, consulte Cómo afectan las claves de KMS inutilizables a las claves de datos en la Guía para desarrolladores de AWS Key Management Service .

Requisitos para el cifrado de Amazon EBS

Antes de comenzar, compruebe que se cumplen los siguientes requisitos.

Requisitos

- Tipos de volumen admitidos
- Tipos de instancias admitidas
- Permisos para los usuarios
- Permisos para instancias

Tipos de volumen admitidos

El cifrado se admite en todos los tipos de volúmenes de EBS. Puede esperar el mismo rendimiento de IOPS en los volúmenes cifrados que en los no cifrados, con un efecto mínimo en la latencia. Puede obtener acceso a los volúmenes cifrados del mismo modo que tiene acceso a los no cifrados. El cifrado y el descifrado se administran de forma transparente y no requieren ninguna acción adicional por su parte ni por parte de las aplicaciones.

Tipos de instancias admitidas

El cifrado de Amazon EBS está disponible en todos los tipos de instancias de la generación actual y la generación anterior.

Permisos para los usuarios

Cuando utiliza una clave de KMS para el cifrado de EBS, la política de claves de KMS permite a cualquier usuario con acceso a las AWS KMS acciones necesarias utilizar esta clave de KMS para cifrar o descifrar los recursos de EBS. Debe conceder a los usuarios permiso para llamar a las siguientes acciones para utilizar el cifrado de EBS:

- `kms:CreateGrant`
- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKeyWithoutPlainText`
- `kms:ReEncrypt`

> **Tip**
>
> Para seguir el principio de privilegios mínimos, no permita el acceso completo a `kms:CreateGrant`. En su lugar, utilice la clave de `kms:GrantIsForAWSResource` condición para permitir al usuario crear concesiones en la clave de KMS solo cuando un AWS servicio cree la concesión en nombre del usuario, como se muestra en el siguiente ejemplo.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "kms:CreateGrant",
            "Resource": [
                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-a123-456d-a12b-
a123b4cd56ef"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
```

```
    ]
}
```

Para obtener más información, consulte Permitir el acceso a la AWS cuenta y habilitar las políticas de IAM en la sección Política clave predeterminada de la Guía para AWS Key Management Service desarrolladores.

Permisos para instancias

Cuando una instancia intenta interactuar con una AMI, un volumen o una instantánea cifrados, se concede una clave de KMS al rol de solo identidad de la instancia. El rol de solo identidad es un rol de IAM que la instancia utiliza para interactuar con AMI, volúmenes o instantáneas cifrados en su nombre.

Los roles de solo identidad no necesitan crearse ni eliminarse de forma manual, y no tienen políticas asociadas. Además, no puede acceder a las credenciales del rol de solo identidad.

> **Note**
>
> Las aplicaciones de la instancia no utilizan los roles exclusivos de identidad para acceder a otros recursos AWS KMS cifrados, como los objetos de Amazon S3 o las tablas de Dynamo DB. Estas operaciones se realizan con las credenciales de un rol de instancia de Amazon EC2 u otras AWS credenciales que haya configurado en la instancia.

Los roles de solo identidad están sujetos a las políticas de control de servicio (SCP) y a las políticas de claves de KMS. Si una clave de SCP o KMS deniega al rol de solo identidad el acceso a una clave de KMS, es posible que no pueda lanzar instancias de EC2 con volúmenes cifrados ni utilizar AMI o instantáneas cifradas.

Si va a crear un SCP o una política de claves que deniegue el acceso en función de la ubicación de la red mediante las claves de condición `aws:SourceIp` `aws:VpcSourceIpaws:SourceVpc`,, o `aws:SourceVpce` AWS globales, debe asegurarse de que estas declaraciones de política no se apliquen a las funciones exclusivas de la instancia. Para ver ejemplos de políticas, consulte Ejemplos de políticas de perímetros de datos.

Los ARN de roles de solo identidad utilizan el siguiente formato:

```
arn:aws-partition:iam::account_id:role/aws:ec2-infrastructure/instance_id
```

Cuando se emite una concesión de clave para una instancia, la concesión de clave se emite para la sesión específica del rol asumido de esa instancia. El ARN de la entidad principal del beneficiario utiliza el siguiente formato:

```
arn:aws-partition:sts::account_id:assumed-role/aws:ec2-infrastructure/instance_id
```

Trabajo con el cifrado de Amazon EBS

Use los siguientes procedimientos para trabajar con el cifrado de Amazon EBS.

Tareas

- Selección de una clave de KMS para el cifrado de EBS
- Habilitación del cifrado de manera predeterminada
- Configuración del cifrado de forma predeterminada con la API y la CLI

Selección de una clave de KMS para el cifrado de EBS

Amazon EBS crea automáticamente un recurso único Clave administrada de AWS en cada región en la que almacene AWS los recursos. Esta Clave de KMS tiene el alias `alias/aws/ebs`. De forma predeterminada, Amazon EBS utiliza esta Clave de KMS para el cifrado. También puede especificar una clave de cifrado administrada por el cliente simétrica que haya creado como la clave de KMS predeterminada para el cifrado de EBS. Usar su propia Clave de KMS le da más flexibilidad, incluida la capacidad de crear, rotar y desactivar Claves de KMS.

> **Important**
>
> Amazon EBS no es compatible con las claves de cifrado de KMS asimétricas. Para obtener más información, consulte Uso de claves de cifrado de KMS simétricas y asimétricas en la Guía para desarrolladores de AWS Key Management Service .

Amazon EC2 console

A fin de configurar la Clave de KMS predeterminada para el cifrado de EBS en una región

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación, seleccione la región.

3. En el panel de navegación, seleccione EC2 Dashboard (Panel de EC2).
4. En la esquina superior derecha de la página, elija Account attributes (Atributos de cuenta), Data protection and security (Protección de datos y seguridad).
5. Elija Administrar.
6. En Default encryption key) (Clave de cifrado predeterminada), elija una clave de cifrado administrada por el cliente simétrica.
7. Elija Update EBS encryption (Actualizar el cifrado de EBS).

Habilitación del cifrado de manera predeterminada

Puede configurar su AWS cuenta para aplicar el cifrado de los nuevos volúmenes y copias instantáneas de EBS que cree. Por ejemplo, Amazon EBS cifra los volúmenes de EBS creados al lanzar una instancia y las instantáneas que copia a partir de una instantánea sin cifrar. Para obtener ejemplos de la transición de recursos de EBS sin cifrar a recursos cifrados, consulte Cifrar recursos no cifrados.

El cifrado de forma predeterminada no afecta a los volúmenes o las instantáneas de EBS existentes.

Consideraciones

- El cifrado de manera predeterminada es una configuración específica de la región. Si lo habilita para una región, puede deshabilitarlo para volúmenes o instantáneas individuales en esa región.
- El cifrado de Amazon EBS es admitido por defecto en todos los tipos de instancias de la generación actual y la generación anterior.
- Si copia una instantánea y la cifra con una clave de KMS nueva, se crea una copia completa (no progresiva). Esto da como resultado costos de almacenamiento adicionales.
- Al migrar servidores mediante AWS Server Migration Service (SMS), no active el cifrado de forma predeterminada. Si el cifrado de manera predeterminada ya está activado y está experimentando errores de replicación delta, desactive el cifrado predeterminado. En cambio, habilite el cifrado AMI al crear el trabajo de replicación.

Amazon EC2 console

Para habilitar el cifrado de manera predeterminada en una región

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.

2. En la barra de navegación, seleccione la región.
3. En el panel de navegación, seleccione EC2 Dashboard (Panel de EC2).
4. En la esquina superior derecha de la página, elija Account attributes (Atributos de cuenta), Data protection and security (Protección de datos y seguridad).
5. Seleccione Manage (Administrar).
6. Seleccione Enable (Habilitar). La conservas Clave administrada de AWS con el alias `alias/aws/ebs` creado en tu nombre como clave de cifrado predeterminada o eliges una clave de cifrado simétrica gestionada por el cliente.
7. Elija Update EBS encryption (Actualizar el cifrado de EBS).

AWS CLI

Para ver la configuración predeterminada de cifrado

- Para una región específica

```
$ aws ec2 get-ebs-encryption-by-default --region region
```

- Para todas las regiones de su cuenta

```
$ for region in $(aws ec2 describe-regions --region us-east-1 --query "Regions[*].
[RegionName]" --output text); do   default=$(aws ec2 get-ebs-encryption-by-default
 --region $region --query "{Encryption_By_Default:EbsEncryptionByDefault}" --
output text); kms_key=$(aws ec2 get-ebs-default-kms-key-id --region $region | jq
 '.KmsKeyId'); echo "$region  --- $default  --- $kms_key"; done
```

Para habilitar el cifrado de manera predeterminada

- Para una región específica

```
$ aws ec2 enable-ebs-encryption-by-default --region region
```

- Para todas las regiones de su cuenta

```
$ for region in $(aws ec2 describe-regions --region us-east-1 --query "Regions[*].
[RegionName]" --output text); do   default=$(aws ec2 enable-ebs-encryption-by-
default --region $region --query "{Encryption_By_Default:EbsEncryptionByDefault}"
```

```
 --output text); kms_key=$(aws ec2 get-ebs-default-kms-key-id --region $region |
 jq '.KmsKeyId'); echo "$region  --- $default  --- $kms_key"; done
```

Para deshabilitar el cifrado de manera predeterminada

- Para una región específica

```
$ aws ec2 disable-ebs-encryption-by-default --region region
```

- Para todas las regiones de su cuenta

```
$ for region in $(aws ec2 describe-regions --region us-east-1 --query "Regions[*].
[RegionName]" --output text); do   default=$(aws ec2 disable-ebs-encryption-by-
default --region $region --query "{Encryption_By_Default:EbsEncryptionByDefault}"
 --output text); kms_key=$(aws ec2 get-ebs-default-kms-key-id --region $region |
 jq '.KmsKeyId'); echo "$region  --- $default  --- $kms_key"; done
```

PowerShell

Para ver la configuración predeterminada de cifrado

- Para una región específica

```
PS C:\> Get-EC2EbsEncryptionByDefault -Region region
```

- Para todas las regiones de su cuenta

```
PS C:\> (Get-EC2Region).RegionName | ForEach-Object { [PSCustomObject]@{ Region
 = $_; EC2EbsEncryptionByDefault = Get-EC2EbsEncryptionByDefault -Region $_;
 EC2EbsDefaultKmsKeyId = Get-EC2EbsDefaultKmsKeyId -Region $_ } } | Format-Table -
AutoSize
```

Para habilitar el cifrado de manera predeterminada

- Para una región específica

```
PS C:\> Enable-EC2EbsEncryptionByDefault -Region region
```

- Para todas las regiones de su cuenta

```
PS C:\> (Get-EC2Region).RegionName | ForEach-Object { [PSCustomObject]@{ Region
 = $_; EC2EbsEncryptionByDefault = Enable-EC2EbsEncryptionByDefault -Region $_;
 EC2EbsDefaultKmsKeyId = Get-EC2EbsDefaultKmsKeyId -Region $_ } } | Format-Table -
AutoSize
```

Para deshabilitar el cifrado de manera predeterminada

- Para una región específica

```
PS C:\> Disable-EC2EbsEncryptionByDefault -Region region
```

- Para todas las regiones de su cuenta

```
PS C:\> (Get-EC2Region).RegionName | ForEach-Object { [PSCustomObject]@{ Region
 = $_; EC2EbsEncryptionByDefault = Disable-EC2EbsEncryptionByDefault -Region $_;
 EC2EbsDefaultKmsKeyId = Get-EC2EbsDefaultKmsKeyId -Region $_ } } | Format-Table -
AutoSize
```

No puede cambiar la Clave de KMS que está asociada con una instantánea existente o un volumen cifrado. Sin embargo, puede asociar una Clave de KMS distinta durante la operación de copia de una instantánea, de modo que la instantánea copiada resultante se cifre mediante la nueva Clave de KMS.

Configuración del cifrado de forma predeterminada con la API y la CLI

Puede administrar el cifrado de forma predeterminada y la Clave de KMS predeterminada mediante las siguientes acciones de la API y comandos de la CLI.

Acción de la API	Command de la CLI	Descripción
DisableEbsEncryptionByDefault	disable-ebs-encryption-by-predeterminado	Deshabilita el cifrado de manera predeterminada.
EnableEbsEncryptionByDefault	enable-ebs-encryption-by-predeterminado	Habilita el cifrado de manera predeterminada.

Acción de la API	Command de la CLI	Descripción
GetEbsDefaultKmsKeyId	get-ebs-default-kms-key-id	Describe la Clave de KMS predeterminada.
GetEbsEncryptionByDefault	get-ebs-encryption-by-predeterminado	Indica si se ha habilitado un cifrado de manera predeterminada.
ModifyEbsDefaultKmsKeyId	modify-ebs-default-kms-key-id	Cambia la Clave de KMS predeterminada utilizada para cifrar volúmenes de EBS.
ResetEbsDefaultKmsKeyId	reset-ebs-default-kms-key-id	Restablece la Clave administrada de AWS clave KMS predeterminada utilizada para cifrar los volúmenes de EBS.

Cifrar recursos de EBS

Puede cifrar los volúmenes de EBS habilitando el cifrado, ya sea mediante el cifrado de forma predeterminada o habilitando el cifrado al crear un volumen que desea cifrar.

Cuando cifra un volumen, puede especificar la clave de cifrado de KMS simétrica que se utilizará para cifrar el volumen. Si no especifica una Clave de KMS, la Clave de KMS que se utiliza para el cifrado depende del estado de cifrado de la instantánea de origen y de su propiedad. Para obtener más información, consulte la tabla de resultados de cifrado.

> **Note**
>
> Si utiliza la API o AWS CLI para especificar una clave de KMS, tenga en cuenta que AWS autentica la clave de KMS de forma asíncrona. Si especifica un ID de Clave de KMS, un

alias o un ARN que no es válido, puede parecer que la acción se ha completado, pero eventualmente falla.

No puede cambiar la Clave de KMS que está asociada a una instantánea o volumen existente. Sin embargo, puede asociar una Clave de KMS distinta durante la operación de copia de una instantánea, de modo que la instantánea copiada resultante se cifre mediante la nueva Clave de KMS.

Cifrar un volumen vacío al crearlo

Al crear un nuevo volumen de EBS vacío, puede cifrarlo habilitando el cifrado para la operación de creación de volúmenes específica. Si ha habilitado el cifrado de EBS de forma predeterminada, el volumen se cifra automáticamente con la Clave de KMS predeterminada para el cifrado de EBS. Como alternativa, puede especificar una clave de cifrado de KMS simétrica diferente para la operación de creación de volumen específica. El volumen se cifra desde el primer momento en el que está disponible, de manera que sus datos siempre están protegidos. Para obtener procedimientos detallados, consulte Creación de un volumen de Amazon EBS..

De forma predeterminada, la Clave de KMS que seleccionó al crear un volumen cifra las instantáneas que realice a partir del volumen y los volúmenes que se restauran a partir de esas instantáneas cifradas. No puede eliminar el cifrado de un volumen o instantánea cifrada, lo que significa que un volumen restaurado de una instantánea cifrada o una copia de una instantánea cifrada siempre se cifra.

Aunque no se admiten las instantáneas públicas de los volúmenes cifrados, puede compartir una instantánea cifrada con determinadas cuentas. Para obtener indicaciones detalladas, consulte Compartir una instantánea de Amazon EBS.

Cifrar recursos no cifrados

No puede cifrar de forma directa los volúmenes o las instantáneas sin cifrar ya existentes. Sin embargo, puede crear volúmenes o instantáneas cifradas a partir de volúmenes o instantáneas sin cifrar. Si ha habilitado el cifrado de forma predeterminada, Amazon EBS cifra volúmenes o instantáneas nuevos mediante la clave de KMS predeterminada para el cifrado de EBS. En caso contrario, puede habilitar el cifrado cuando cree un volumen o una instantánea individuales, mediante la clave de KMS predeterminada para el cifrado de Amazon EBS o una clave de cifrado administrada por el cliente simétrica. Para obtener más información, consulte Creación de un volumen de Amazon EBS. y Copia de una instantánea de Amazon EBS.

Para cifrar la copia instantánea en una Clave administrada por el cliente, debe habilitar el cifrado y especificar la Clave de KMS, como se muestra en Copia de una instantánea sin cifrar (cifrado de forma predeterminada no habilitado).

> **Important**
>
> Amazon EBS no es compatible con las claves de cifrado de KMS asimétricas. Para obtener más información, consulte Uso de claves de cifrado de KMS simétricas y asimétricas en la Guía para desarrolladores de AWS Key Management Service .

También puede aplicar nuevos estados de cifrado cuando lanza una instancia desde una AMI con respaldo EBS. Esto se debe a que las AMI con respaldo EBS incluyen instantáneas de volúmenes de EBS que se pueden cifrar tal y como se describe. Para obtener más información, consulte Usar el cifrado con las AMI basadas en EBS.

Claves giratorias AWS KMS

Las prácticas criptográficas recomendadas desaconsejan la reutilización generalizada de claves de cifrado.

Para crear nuevo material criptográfico para usarlo con el cifrado de Amazon EBS, puede crear una nueva clave administrada por el cliente y, a continuación, cambiar las aplicaciones para que usen esa nueva clave de KMS. También puede habilitar la rotación automática de claves para una clave administrada por el cliente existente.

Cuando habilita la rotación automática de claves para una clave administrada por el cliente, AWS KMS genera nuevo material criptográfico para la clave KMS cada año. AWS KMS guarda todas las versiones anteriores del material criptográfico para que pueda seguir descifrando y utilizando volúmenes e instantáneas previamente cifrados con ese material de clave de KMS. AWS KMS no elimina ningún material de clave girada hasta que elimine la clave KMS.

Cuando utiliza una clave girada gestionada por el cliente para cifrar un volumen o una instantánea nuevos, AWS KMS utiliza el material de clave actual (nuevo). Cuando utiliza una clave girada gestionada por el cliente para descifrar un volumen o una instantánea, AWS KMS utiliza la versión del material criptográfico que se utilizó para cifrarlo. Si un volumen o una instantánea están cifrados con una versión anterior del material criptográfico, seguirán utilizando esa versión AWS KMS anterior para descifrarlos. AWS KMS no vuelve a cifrar los volúmenes o instantáneas previamente cifrados

para utilizar el nuevo material criptográfico tras una rotación de claves. Permanecen cifrados con el material criptográfico con el que se cifraron originalmente. Puede utilizar de forma segura una clave girada gestionada por el cliente en aplicaciones y AWS servicios sin necesidad de cambiar el código.

> **Note**
>
> - La rotación automática de claves solo se admite para claves simétricas administradas por el cliente con material clave que se AWS KMS crea.
> - AWS KMS rota automáticamente Claves administradas por AWS cada año. No puede habilitar ni desactivar la rotación de claves de Claves administradas por AWS.

Para obtener más información, consulte Rotación de clave de KMS en la Guía para desarrolladores de AWS Key Management Service .

Ejemplos de cifrado de Amazon EBS

Cuando se crea un recurso de EBS cifrado, se cifra por la Clave de KMS predeterminada de su cuenta para el cifrado de EBS, a menos que especifique una Clave administrada por el cliente diferente en los parámetros de creación de volúmenes o en la asignación de dispositivos de bloque para la AMI o la instancia. Para obtener más información, consulte Selección de una clave de KMS para el cifrado de EBS.

Los siguientes ejemplos ilustran cómo puede administrar el estado de cifrado de sus volúmenes e instantáneas. Para obtener una lista completa de casos de cifrado, consulte la tabla de resultados de cifrado.

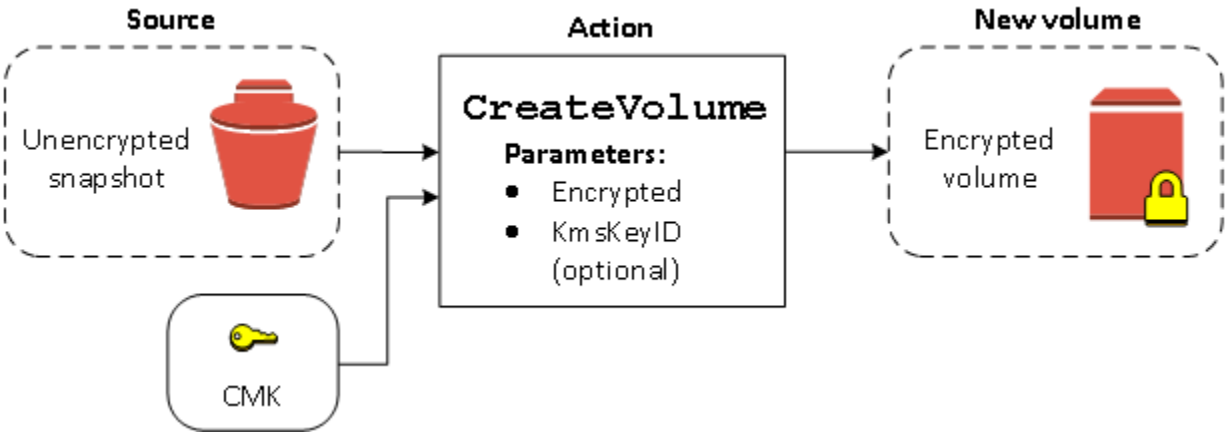
Ejemplos

- Restauración de un volumen sin cifrar (cifrado de forma predeterminada no habilitado)
- Restauración de un volumen sin cifrar (cifrado de forma predeterminada habilitado)
- Copia de una instantánea sin cifrar (cifrado de forma predeterminada no habilitado)
- Copia de una instantánea sin cifrar (cifrado de forma predeterminada habilitado)
- Nuevo cifrado de un volumen cifrado
- Nuevo cifrado de una instantánea cifrada
- Migrar datos entre volúmenes cifrados y no cifrados

- Resultados del cifrado

Restauración de un volumen sin cifrar (cifrado de forma predeterminada no habilitado)

Sin el cifrado de manera predeterminada habilitado, un volumen restaurado de una instantánea sin cifrar no se cifra de manera predeterminada. Sin embargo, puede cifrar el volumen resultante al configurar el parámetro `Encrypted` y, de manera opcional, el parámetro `KmsKeyId`. En el diagrama siguiente se ilustra el proceso.

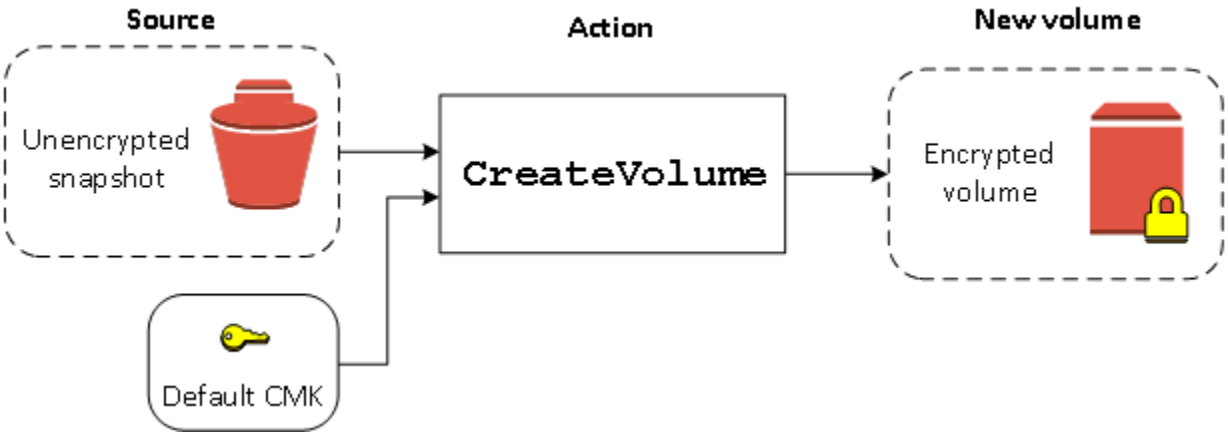


Si omite el parámetro `KmsKeyId`, el volumen resultante se cifra con la Clave de KMS predeterminada para el cifrado de EBS. Debe especificar un ID de Clave de KMS para cifrar el volumen en una Clave de KMS diferente.

Para obtener más información, consulte Creación de un volumen desde una instantánea.

Restauración de un volumen sin cifrar (cifrado de forma predeterminada habilitado)

Cuando ha habilitado el cifrado de forma predeterminada, este es obligatorio en los volúmenes restaurados a partir de instantáneas no cifradas y no se requieren parámetros de cifrado para que se utilice la Clave de KMS predeterminada. En el siguiente diagrama se muestra este caso predeterminado simple:

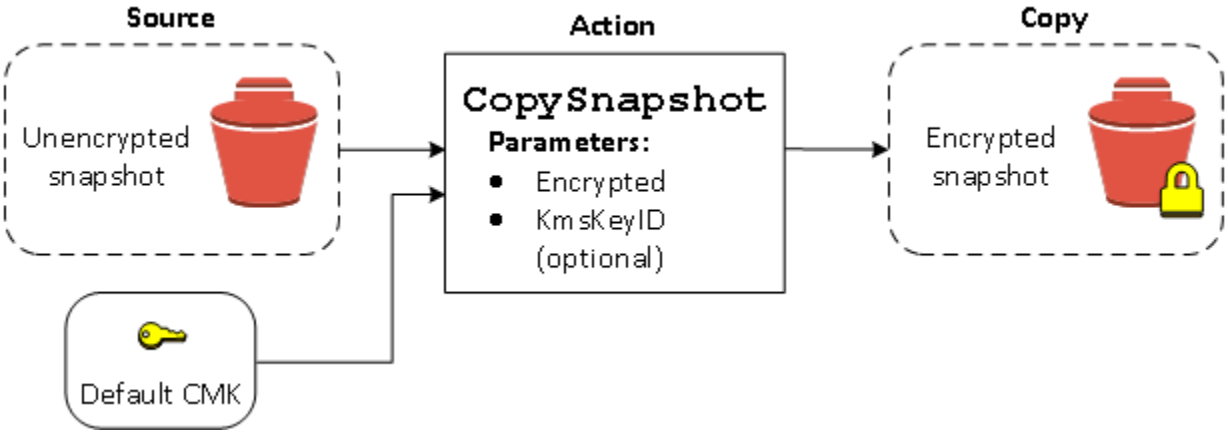


Si desea cifrar el volumen restaurado con una clave de cifrado administrada por el cliente simétrica, debe proporcionar los parámetros `KmsKeyId` y `Encrypted` tal y como se muestra en Restauración de un volumen sin cifrar (cifrado de forma predeterminada no habilitado).

Copia de una instantánea sin cifrar (cifrado de forma predeterminada no habilitado)

Sin el cifrado de manera predeterminada habilitado, una copia de una instantánea sin cifrar no se cifra de manera predeterminada. Sin embargo, puede cifrar la instantánea resultante al configurar el parámetro `Encrypted` y, de manera opcional, el parámetro `KmsKeyId`. Si omite `KmsKeyId`, la instantánea resultante se cifra mediante la Clave de KMS predeterminada. Debe especificar un ID de clave de KMS para cifrar el volumen en una clave de cifrado de KMS simétrica diferente.

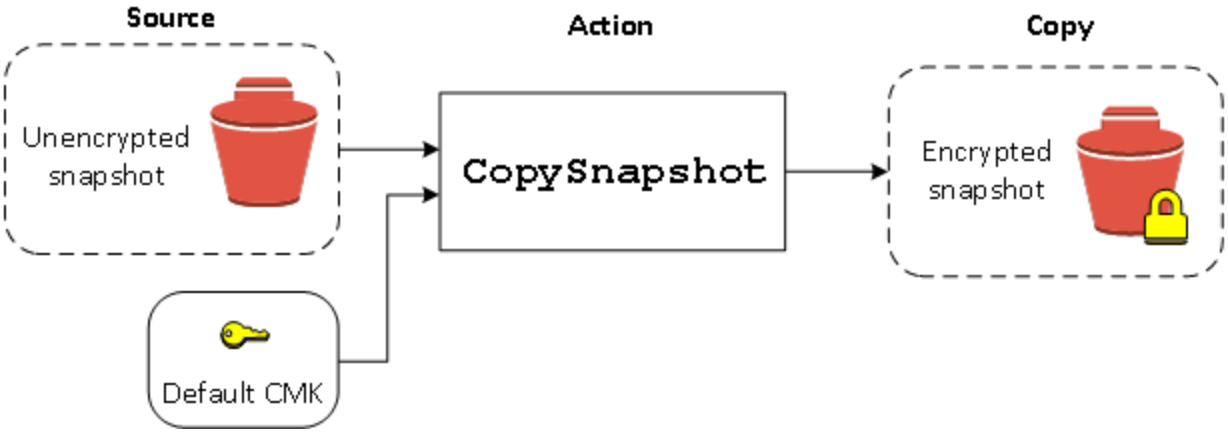
En el diagrama siguiente se ilustra el proceso.



Puede cifrar un volumen de EBS copiando una instantánea inesperada en una instantánea cifrada y luego creando un volumen a partir de la instantánea cifrada. Para obtener más información, consulte Copia de una instantánea de Amazon EBS.

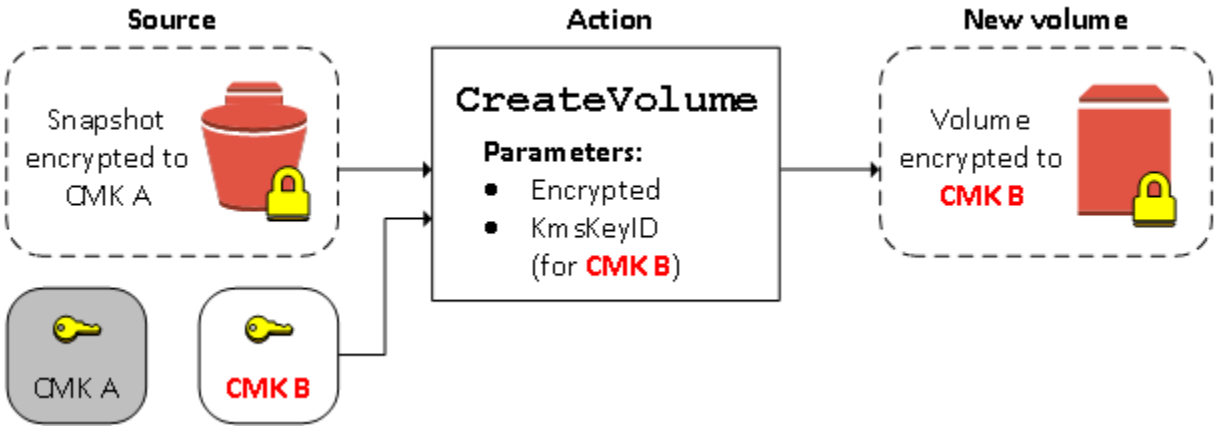
Copia de una instantánea sin cifrar (cifrado de forma predeterminada habilitado)

Cuando ha habilitado el cifrado de forma predeterminada, este es obligatorio para las copias de instantáneas no cifradas y no se requieren parámetros de cifrado si se utiliza la Clave de KMS predeterminada. En el siguiente diagrama se ilustra caso predeterminado:



Nuevo cifrado de un volumen cifrado

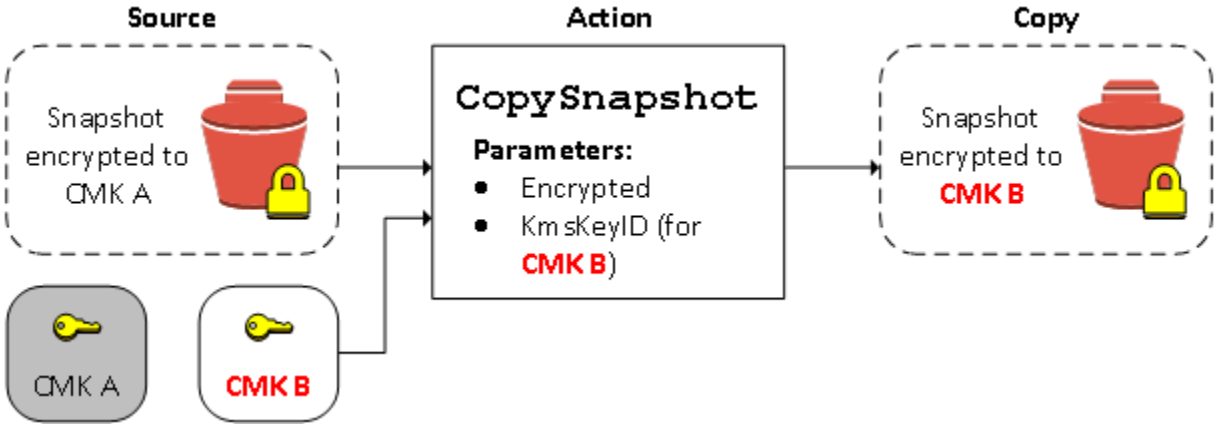
Cuando la acción `CreateVolume` funciona en una instantánea cifrada, tiene la opción de volver a cifrarla con otra Clave de KMS. En el diagrama siguiente se ilustra el proceso. En este ejemplo, posee dos Claves de KMS: Clave de KMS A y Clave de KMS B. La instantánea de origen se cifra mediante la Clave de KMS A. Durante la creación del volumen, con el ID de Clave de KMS de la Clave de KMS B especificado como parámetro, los datos de origen se descifran automáticamente y, a continuación, se vuelven a cifrar mediante la Clave de KMS B.



Para obtener más información, consulte Creación de un volumen desde una instantánea.

Nuevo cifrado de una instantánea cifrada

La capacidad de cifrar una instantánea durante la copia permite aplicar una nueva clave de cifrado de KMS simétrica a una instantánea ya cifrada de su propiedad. Solo se puede acceder a los volúmenes restaurados a partir de la copia resultante mediante la nueva Clave de KMS. En el diagrama siguiente se ilustra el proceso. En este ejemplo, posee dos Claves de KMS: Clave de KMS A y Clave de KMS B. La instantánea de origen se cifra mediante la Clave de KMS A. Durante la copia, con el ID de Clave de KMS de la Clave de KMS B especificado como parámetro, los datos de origen se vuelven a cifrar automáticamente mediante la Clave de KMS B.



En un escenario relacionado, puede optar por aplicar parámetros de cifrado nuevos a la copia de una instantánea que hayan compartido con usted. De forma predeterminada, la copia se cifra con una Clave de KMS compartida por el propietario de la instantánea. Sin embargo, se recomienda crear una copia de la instantánea compartida mediante el uso de una Clave de KMS diferente que usted controla. Esto protege el acceso al volumen si la Clave de KMS original está comprometida o si el propietario revoca la Clave de KMS por cualquier motivo. Para obtener más información, consulte Cifrado y copia de la instantánea.

Migrar datos entre volúmenes cifrados y no cifrados

Si tiene acceso a un volumen cifrado y a un volumen no cifrado, puede trasferir datos entre ambos libremente. EC2 lleva a cabo las operaciones de cifrado y descifrado con transparencia.

instancias de Linux

Por ejemplo, use el comando rsync para copiar los datos. En el siguiente comando, los datos de origen se encuentran en `/mnt/source` y el volumen de destino está montado en `/mnt/destination`.

```
[ec2-user ~]$ sudo rsync -avh --progress /mnt/source/ /mnt/destination/
```

instancias de Windows

Por ejemplo, use el comando robocopy para copiar los datos. En el siguiente comando, los datos de origen se encuentran en `D:\` y el volumen de destino está montado en `E:\`.

```
PS C:\> robocopy D:\sourcefolder E:\destinationfolder /e /copyall /eta
```

Recomendamos utilizar carpetas en lugar de copiar todo el volumen, con esto se evitan posibles problemas con carpetas ocultas.

Resultados del cifrado

En la siguiente tabla, se describe el resultado de cifrado para cada combinación posible de configuraciones.

¿El cifrado está habilitado?	¿El cifrado predeterminado está habilitado?	Fuente del volumen	Predeterminado (no se especificó ninguna clave administrada por el cliente)	Personalizado (se especificó una clave administrada por el cliente)
No	No	Nuevo volumen (vacío)	Sin cifrar	N/A
No	No	Instantánea no cifrada que posea	Sin cifrar	
No	No	Instantánea cifrada que posea	Cifrada con la misma clave	
No	No	Instantánea no cifrada compartida con usted	Sin cifrar	
No	No	Instantánea cifrada compartida con usted	Cifrado con clave administrada por el cliente predeterminada*	

¿El cifrado está habilitado?	¿El cifrado predeterminado está habilitado?	Fuente del volumen	Predeterminado (no se especificó ninguna clave administrada por el cliente)	Personalizado (se especificó una clave administrada por el cliente)
Sí	No	Nuevo volumen	Cifrado con clave administrada por el cliente predeterminada	Cifrado con una clave administrada por el cliente especificada**
Sí	No	Instantánea no cifrada que posea	Cifrado con clave administrada por el cliente predeterminada	
Sí	No	Instantánea cifrada que posea	Cifrada con la misma clave	
Sí	No	Instantánea no cifrada compartida con usted	Cifrado con clave administrada por el cliente predeterminada	
Sí	No	Instantánea cifrada compartida con usted	Cifrado con clave administrada por el cliente predeterminada	
No	Sí	Nuevo volumen (vacío)	Cifrado con clave administrada por el cliente predeterminada	N/A
No	Sí	Instantánea no cifrada que posea	Cifrado con clave administrada por el cliente predeterminada	

¿El cifrado está habilitado?	¿El cifrado predeterminado está habilitado?	Fuente del volumen	Predeterminado (no se especificó ninguna clave administrada por el cliente)	Personalizado (se especificó una clave administrada por el cliente)
No	Sí	Instantánea cifrada que posea	Cifrada con la misma clave	
No	Sí	Instantánea no cifrada compartida con usted	Cifrado con clave administrada por el cliente predeterminada	
No	Sí	Instantánea cifrada compartida con usted	Cifrado con clave administrada por el cliente predeterminada	
Sí	Sí	Nuevo volumen	Cifrado con clave administrada por el cliente predeterminada	Cifrado con una clave administrada por el cliente especificada
Sí	Sí	Instantánea no cifrada que posea	Cifrado con clave administrada por el cliente predeterminada	
Sí	Sí	Instantánea cifrada que posea	Cifrada con la misma clave	
Sí	Sí	Instantánea no cifrada compartida con usted	Cifrado con clave administrada por el cliente predeterminada	

¿El cifrado está habilitado?	¿El cifrado predeterminado está habilitado?	Fuente del volumen	Predeterminado (no se especificó ninguna clave administrada por el cliente)	Personalizado (se especificó una clave administrada por el cliente)
Sí	Sí	Instantánea cifrada compartida con usted	Cifrado con clave administrada por el cliente predeterminada	

* Esta es la clave predeterminada administrada por el cliente que se utiliza para el cifrado de EBS de la AWS cuenta y la región. De forma predeterminada, es única Clave administrada de AWS para EBS, o puede especificar una clave gestionada por el cliente. Para obtener más información, consulte Selección de una clave de KMS para el cifrado de EBS.

** Esta es una clave administrada por el cliente especificada para el volumen en el momento del lanzamiento. Se utiliza esta clave gestionada por el cliente en lugar de la clave gestionada por el cliente predeterminada para la AWS cuenta y la región.

Rendimiento del volumen de Amazon EBS

Existen varios factores que pueden afectar al rendimiento de Amazon EBS, como son la configuración de las instancias y los volúmenes, y las características de E/S. Si sigue las directrices incluidas en nuestras páginas de detalles sobre los productos de Amazon EBS y Amazon EC2, obtiene, en general, un buen rendimiento. No obstante, hay algunos casos en los que tal vez sea preciso realizar algunos ajustes para alcanzar el máximo rendimiento. Recomendamos que ajuste el rendimiento con información sobre la carga de trabajo, además de los análisis comparativos, para determinar la configuración óptima. Una vez que conoce los fundamentos del trabajo con los volúmenes de EBS, es buena idea examinar el rendimiento de E/S que precisa y las opciones a su alcance para aumentar el rendimiento de Amazon EBS para satisfacer esos requisitos.

AWS es posible que las actualizaciones del rendimiento de los tipos de volúmenes de EBS no se apliquen inmediatamente en los volúmenes existentes. Para ver el rendimiento total en un volumen antiguo, es necesario realizar en primer lugar una acción `ModifyVolume` en él. Para obtener más información, consulte Modificación de un volumen mediante Volúmenes elásticos de Amazon EBS.

Contenido

Consejos de rendimiento de Amazon EBS

Estas sugerencias constituyen las prácticas recomendadas para lograr el rendimiento óptimo de los volúmenes de EBS en diversos escenarios de uso.

Uso de instancias optimizadas para EBS

En las instancias que no admiten resultados optimizados para EBS, el tráfico de red puede competir con el tráfico entre la instancia y los volúmenes de EBS, mientras que en las instancias optimizadas para EBS, ambos tipos de tráfico se mantienen separados. Algunas configuraciones de instancias

optimizadas para EBS incurren en costos extra (como C3, R3 y M3), si bien otras están siempre optimizadas para EBS sin costo extra (como M4, C4, C5 y D2). Para obtener más información, consulte Optimización del rendimiento de Amazon EBS.

Entender cómo se calcula el rendimiento

Cuando mide el rendimiento de los volúmenes de EBS, es importante comprender las unidades de medida utilizadas y el modo en que se calcula el rendimiento. Para obtener más información, consulte Características de E/S de Amazon EBS y monitoreo.

Conocer la carga de trabajo

Hay una relación entre el rendimiento máximo de los volúmenes de EBS, el tamaño y el número de operaciones de E/S, y el tiempo que tarda cada acción en completarse. Cada uno de estos factores (rendimiento, E/S y latencia) afecta a los demás y algunas aplicaciones son más sensibles a uno u otro factor. Para obtener más información, consulte Análisis comparativo de volúmenes de EBS.

Conozca la penalización en el rendimiento cuando se inicializan volúmenes a partir de instantáneas

Cuando se tiene acceso por primera vez a cada bloque de datos de un volumen de EBS nuevo que se ha creado a partir de una instantánea, se produce un aumento significativo de la latencia. Puede evitar este efecto sobre el rendimiento si opta por una de las opciones siguientes:

- Acceder a cada bloque antes de poner el volumen a producir. Este proceso se llama inicialización (antes se conocía como precalentamiento). Para obtener más información, consulte Inicializar de volúmenes de Amazon EBS.
- Habilitar la restauración rápida de instantáneas en una instantánea para garantizar que los volúmenes de EBS creados desde la instantánea se inicialicen por completo durante la creación y proporcionen al instante todo su rendimiento aprovisionado. Para obtener más información, consulte Restauración rápida de instantáneas de Amazon EBS.

Factores que pueden degradar el rendimiento de las unidades de disco duro (HDD)

Cuando se crea una instantánea de un volumen de HDD con rendimiento optimizado (`st1`) o de un volumen de HDD en frío (`sc1`), el rendimiento puede caer hasta el valor de referencia del

volumen mientras la instantánea está en curso. Este comportamiento es específico de estos tipos de volúmenes. Otros factores que pueden limitar el rendimiento son impulsar el rendimiento por encima de lo que la instancia admite, la penalización en el rendimiento que se produce cuando se inicializan volúmenes creados a partir de una instantánea y la cantidad excesiva de operaciones de E/S aleatorias y pequeñas en el volumen. Para obtener más información acerca del cálculo del rendimiento de los volúmenes HDD, consulte Tipos de volúmenes de Amazon EBS.

El rendimiento también puede verse afectado si la aplicación no envía suficientes solicitudes de E/S. Esto se puede monitorizar comprobando la longitud de la cola del volumen y el tamaño de E/S. La longitud de la cola es el número de solicitudes de E/S pendientes de la aplicación al volumen. Para lograr la máxima uniformidad, los volúmenes con respaldo de HDD deben mantener una longitud de cola (redondeada al número entero más próximo) de 4 o más cuando efectúan E/S secuenciales de 1 MiB. Para obtener más información sobre cómo asegurar el rendimiento uniforme de sus volúmenes, consulte Características de E/S de Amazon EBS y monitoreo.

Aumento del valor de read-ahead para cargas de trabajo de lectura intensiva y de alto rendimiento en **st1** y **sc1** (solamente instancias de Linux)

Algunas cargas de trabajo son de lectura intensiva y tienen acceso al dispositivo de bloques a través de la caché de páginas del sistema operativo (por ejemplo, desde un sistema de archivos). En este caso, para alcanzar el rendimiento máximo, recomendamos configurar el valor read-ahead en 1 MiB. Esta es una per-block-device configuración que solo debe aplicarse a los volúmenes de su disco duro.

Para examinar el valor actual de read-ahead en los dispositivos de bloques, utilice el comando siguiente:

```
[ec2-user ~]$ sudo blockdev --report /dev/<device>
```

La información sobre el dispositivo de bloques se devuelve con el formato siguiente:

```
RO    RA   SSZ   BSZ   StartSec            Size   Device
rw   256   512  4096       4096      8587820544   /dev/<device>
```

El dispositivo mostrado registra un valor read-ahead de 256 (el predeterminado). Multiplique este número por el tamaño del sector (512 bytes) para obtener el tamaño del búfer read-ahead, que en este caso es de 128 KiB. Para establecer el valor del búfer en 1 MiB, use el comando siguiente:

```
[ec2-user ~]$ sudo blockdev --setra 2048 /dev/<device>
```

Compruebe que el valor de read-ahead muestra ahora 2048 ejecutando de nuevo el primer comando.

Utilice este valor solo cuando la carga de trabajo conste de E/S grandes y secuenciales. Si consiste, principalmente, en operaciones de E/S pequeñas y aleatorias, este valor degradará el rendimiento. En general, si la carga de trabajo consta principalmente de operaciones de E/S pequeñas o aleatorias, debería considerar el uso de un volumen de SSD de uso general (gp2 y gp3) en lugar de un volumen `st1` o `sc1`.

Uso de un kernel de Linux moderno (solo instancias de Linux)

Use un kernel de Linux moderno que admita descriptores indirectos. Cualquier kernel de Linux, versión 3.8 y posteriores, tiene esta compatibilidad, así como cualquier instancia EC2 de la generación actual. Si el tamaño de E/S está en 44 KiB o en un valor próximo, es posible que esté usando una instancia o un kernel que no admite descriptores indirectos. Para obtener información sobre cómo obtener el tamaño medio de E/S a partir de CloudWatch las métricas de Amazon, consulte. Características de E/S de Amazon EBS y monitoreo

Para alcanzar el rendimiento máximo en los volúmenes `st1` o `sc1`, recomendamos aplicar un valor de 256 al parámetro `xen_blkfront.max` (para las versiones del kernel de Linux inferiores a 4.6) o al parámetro `xen_blkfront.max_indirect_segments` (para las versiones del kernel de Linux 4.6 o superiores). El parámetro adecuado se puede establecer en la línea de comandos del sistema operativo.

Por ejemplo, en una AMI de Amazon Linux con un kernel anterior, puede añadirlo al final de la línea del kernel en la configuración de GRUB que se encuentra en `/boot/grub/menu.lst`:

```
kernel /boot/vmlinuz-4.4.5-15.26.amzn1.x86_64 root=LABEL=/ console=ttyS0
 xen_blkfront.max=256
```

Con un kernel posterior, el comando debería ser similar al siguiente:

```
kernel /boot/vmlinuz-4.9.20-11.31.amzn1.x86_64 root=LABEL=/ console=tty1 console=ttyS0
 xen_blkfront.max_indirect_segments=256
```

Arranque la instancia de nuevo para que este valor surta efecto.

Para obtener más información, consulte Configurar GRUB para las AMI paravirtuales. Otras distribuciones Linux, en especial las que no usan un cargador de arranque GRUB, pueden requerir un enfoque diferente para ajustar los parámetros del kernel.

Para obtener más información sobre las características de E/S de EBS, consulte la presentación de re:Invent Amazon EBS: Designing for Performance sobre este tema.

Utilizar RAID 0 para maximizar la utilización de los recursos de instancia

Algunos tipos de instancias pueden obtener más rendimiento de E/S de lo que es posible aprovisionar para un volumen de EBS único. Puede unir varios volúmenes en una configuración RAID 0 y utilizar el ancho de banda disponible para estas instancias. Para obtener más información, consulte Configuración de Amazon EBS y RAID.

Realiza un seguimiento del rendimiento con Amazon CloudWatch

Amazon Web Services proporciona métricas de rendimiento para Amazon EBS que puede analizar y ver con Amazon, CloudWatch y comprobaciones de estado que puede utilizar para supervisar el estado de sus volúmenes. Para obtener más información, consulte Monitoreo de los volúmenes de Amazon EBS.

Optimización del rendimiento de Amazon EBS

Una instancia optimizada para Amazon EBS utiliza una pila de configuración optimizada y proporciona capacidad adicional y dedicada para las E/S de Amazon EBS. Esta optimización proporciona el mejor rendimiento para sus volúmenes de EBS, ya que reduce al mínimo la contención entre las E/S de Amazon EBS y otro tráfico procedente de la instancia.

Las instancias optimizadas para EBS proporcionan ancho de banda dedicado para Amazon EBS. Cuando se adjuntan a una instancia optimizada para EBS, los volúmenes de SSD de uso general (`gp2` y `gp3`) están diseñados para ofrecer, al menos, el 90 % de su rendimiento de IOPS aprovisionadas el 99 % del tiempo en un año determinado, mientras que los volúmenes de SSD de IOPS aprovisionadas (`io1` y `io2`) están diseñados para ofrecer, al menos, el 90 % de su rendimiento de IOPS aprovisionadas el 99,9 % del tiempo de un año determinado. Tanto los volúmenes de HDD con rendimiento optimizado (`st1`) como los volúmenes HDD en frío (`sc1`) ofrecen un rendimiento del 90 % de su rendimiento esperado el 99 % del tiempo en un año determinado. Los periodos que no cumplen estas convenciones están distribuidos de manera prácticamente uniforme, alcanzándose

el 99 % del rendimiento total previsto cada hora. Para obtener más información, consulte Tipos de volúmenes de Amazon EBS.

Para obtener más información, consulte Instancias optimizadas para Amazon EBS en la Guía del usuario de Amazon EC2.

Características de E/S de Amazon EBS y monitoreo

En la configuración concreta de un volumen, algunas características de E/S controlan el rendimiento de los volúmenes de EBS. Los volúmenes con respaldo de SSD, es decir, los SSD de uso general (`gp2` y `gp3`) y los SSD de IOPS aprovisionadas (`io1` e `io2`), proporcionan un rendimiento uniforme, tanto si la operación de E/S es aleatoria como si es secuencial. Los volúmenes con respaldo de HDD, es decir, los HDD con rendimiento optimizado (`st1`) y los HDD en frío (`sc1`), proporcionan un rendimiento óptimo solo cuando las operaciones de E/S son grandes y secuenciales. Para comprender el modo en que los volúmenes SSD y HDD se comportarán en la aplicación, es importante conocer la relación entre la demanda que se hace al volumen, la cantidad de IOPS de que dispone el volumen, el tiempo que tarda una operación de E/S en completarse y los límites de rendimiento del volumen.

Temas

IOPS

IOPS es una unidad de medida que representa las operaciones de entrada y salida que se producen por segundo. Las operaciones se miden en KiB y la tecnología de disco subyacente determina la cantidad máxima de datos que un tipo de volumen considera como una operación única de E/S. El tamaño de la E/S se limita a 256 KiB para los volúmenes de SSD y a 1024 KiB para los volúmenes de HDD debido a que los volúmenes de SSD controlan las E/S pequeñas o aleatorias de una manera mucho más eficiente que los volúmenes de HDD.

Cuando las operaciones de E/S pequeñas son secuenciales físicamente, Amazon EBS intenta combinarlas en una única operación de E/S hasta el tamaño máximo. De igual modo, cuando

las operaciones de E/S superan el tamaño máximo de E/S, Amazon EBS intenta dividirlas en operaciones de E/S más pequeñas. En la siguiente tabla, se muestran algunos ejemplos.

Tipo de volumen	Tamaño máximo de las E/S	Operaciones de E/S de su aplicación	Cantidad de IOPS	Notas
SSD	256 KiB	1 operación de E/S de 1024 KiB	4 (1024 ÷ 256 = 4)	Amazon EBS divide la operación de E/S de 1024 KiB en cuatro operaciones más pequeñas de 256 KiB.
		8 operaciones secuenciales de E/S de 32 KiB	1 (8 x 32 = 256)	Amazon EBS fusiona las ocho operaciones secuenciales de E/S de 32 KiB en una única operación de 256 KiB.
		8 operaciones aleatorias de E/S de 32 KiB	8	Amazon EBS considera las operaciones aleatorias de E/S por separado.
HDD	1024 KiB	1 operación de E/S de 1024 KiB	1	La operación de E/S ya es igual al tamaño máximo de E/S. No se fusiona ni se divide.
		8 operaciones secuenciales de E/S de 128 KiB	1 (8 x 128 = 1024)	Amazon EBS fusiona las ocho operaciones secuenciales de

Tipo de volumen	Tamaño máximo de las E/S	Operaciones de E/S de su aplicación	Cantidad de IOPS	Notas
				E/S de 128 KiB en una única operación de E/S de 1024 KiB.
		8 operaciones aleatorias de E/S de 32 KiB	8	Amazon EBS considera las operaciones aleatorias de E/S por separado.

En consecuencia, cuando se crea un volumen respaldado por SSD que admite 3000 IOPS (tanto al aprovisionar un volumen Provisioned IOPS SSD de 3000 IOPS con al establecer el tamaño de un volumen SSD de uso general en 1,000 GiB) y se vincula a una instancia optimizada para EBS que ofrece suficiente ancho de banda, es posible transferir hasta 3000 operaciones de E/S de datos por segundo, con un rendimiento que viene determinado por el tamaño de E/S.

Longitud de cola del volumen y latencia

La longitud de la cola del volumen es el número de solicitudes de E/S pendientes de un dispositivo. La latencia es el tiempo real del end-to-end cliente durante una operación de E/S, es decir, el tiempo transcurrido entre el envío de una E/S a EBS y la recepción de un acuse de recibo por parte de EBS de que se ha completado la lectura o escritura de la E/S. La longitud de la cola debe calibrarse correctamente con el tamaño de E/S y la latencia para evitar crear cuellos de botella en el sistema operativo invitado o en el enlace de red con EBS.

La longitud de cola óptima varía con cada carga de trabajo, dependiendo de la sensibilidad específica de la aplicación a las operaciones de IOPS y la latencia. Si la carga de trabajo no proporciona suficientes solicitudes de E/S para hacer el uso completo del rendimiento disponible para el volumen de EBS, es posible que el volumen no proporcione la IOPS o el rendimiento que ha aprovisionado.

Las aplicaciones con alta intensidad de transacciones son sensibles al aumento de la latencia de E/S y resultan muy adecuadas para los volúmenes respaldados por SSD. Puede mantener una IOPS elevada y una latencia baja manteniendo la longitud de cola corta y un número elevado de IOPS

disponible para el volumen. Dirigir constantemente a un volumen más operaciones de IOPS de las que tiene disponibles puede provocar un aumento de la latencia de E/S.

Las aplicaciones con un rendimiento de alta intensidad son menos sensibles al aumento de la latencia de E/S y resultan muy adecuadas para los volúmenes respaldados por HDD. Puede mantener un rendimiento alto a los volúmenes con respaldo en HDD conservando una longitud de cola elevada cuando se realizan operaciones de E/S grandes y secuenciales.

Límites de rendimiento de los volúmenes y tamaño de E/S

Para los volúmenes con respaldo en SSD, si el tamaño de E/S es muy grande, puede experimentar un número menor de IOPS que lo que ha aprovisionado porque alcanza el límite de rendimiento del volumen. Por ejemplo, un volumen gp2 de menos de 1000 GiB con créditos de ráfaga disponibles tiene un límite de 3000 IOPS y un límite de rendimiento del volumen de 250 MiB/s. Si utiliza un tamaño de E/S de 256 KiB, el volumen alcanza el límite de rendimiento en 1000 IOPS (1000 x 256 KiB = 250 MiB). Para tamaños de E/S más pequeños (como 16 KiB), este mismo volumen puede soportar 3000 IOPS porque el rendimiento se encuentra muy por debajo de 250 MiB/s. (En estos ejemplos, se supone que la E/S del volumen no alcanza los límites de rendimiento de la instancia.) Para obtener más información acerca de los límites de rendimiento de cada tipo de volumen de EBS, consulte Tipos de volúmenes de Amazon EBS.

Para operaciones de E/S más pequeñas, es posible que vea un higher-than-provisioned valor de IOPS medido desde el interior de la instancia. Esto sucede cuando el sistema operativo de la instancia combina pequeñas operaciones de E/S con una operación mayor antes de pasarlas a Amazon EBS.

Si la carga de trabajo utiliza E/S secuencial en volúmenes `st1` y `sc1` respaldados por HDD, es posible que experimente un número de IOPS mayor del esperado si lo mide desde el interior de la instancia. Esto sucede cuando el sistema operativo de la instancia combina E/S secuenciales y las cuenta como unidades de 1024 KiB de tamaño. Si la carga de trabajo usa E/S pequeñas o aleatorias, puede experimentar un rendimiento menor del esperado. Esto es debido a que cada E/S aleatoria, no secuencial se cuenta en el cómputo total de IOPS, lo que puede hacer que se alcance el límite de IOPS del volumen antes de lo esperado.

Con independencia del tipo de volumen de EBS, si no logra el rendimiento o IOPS que espera en la configuración, asegúrese de que no sea el ancho de banda de la instancia EC2 el factor causante. Conviene usar siempre una instancia optimizada para EBS de la generación actual (o una que incluya una conexión de red de 10 Gb-s) para lograr el rendimiento óptimo. Otra causa posible de no

experimentar la IOPS esperada es que no dirija suficientes operaciones de E/S a los volúmenes de EBS.

Supervise las características de E/S mediante CloudWatch

Puede supervisar estas características de E/S con las métricas de volumen de cada CloudWatch volumen. Entre las métricas importantes que debe considerar se incluyen las siguientes:

- `VolumeStalledIOCheck`
- `BurstBalance`
- `VolumeReadBytes` | `VolumeWriteBytes`
- `VolumeReadOps` | `VolumeWriteOps`
- `VolumeQueueLength`

`VolumeStalledIOCheck` supervisa el estado de sus volúmenes de EBS para determinar cuándo están agotados. La métrica es un valor binario que devolverá un estado `0` (superado) o `1` (no superado) en función de si el volumen de EBS puede o no completar las operaciones de E/S. Esta comprobación detecta los problemas subyacentes de la infraestructura de Amazon EBS, como los siguientes:

- Problemas de hardware o software en los subsistemas de almacenamiento subyacentes a los volúmenes de EBS
- Problemas de hardware en el host físico que afectan a la accesibilidad de los volúmenes de EBS desde la instancia de EC2
- Problemas de conectividad entre la instancia y los volúmenes de EBS

Si la `VolumeStalledIOCheck` métrica falla, puede esperar AWS a que se resuelva el problema o tomar medidas, como reemplazar el volumen afectado o detener y reiniciar la instancia a la que está conectado el volumen. En la mayoría de los casos, cuando se produce un error en esta métrica, EBS diagnosticará y recuperará automáticamente el volumen en cuestión de minutos. Puede utilizar la acción Pausar la E/S para realizar experimentos controlados AWS Fault Injection Service a fin de probar la arquitectura y la supervisión en función de esta métrica para mejorar la resiliencia ante los fallos de almacenamiento.

Puede medir la latencia de E/S del almacenamiento de Amazon EBS mediante `VolumeReadOps`, `VolumeWriteOps`, `VolumeTotalReadTime` y `VolumeTotalWriteTime`. Puede usar la siguiente fórmula para supervisar la latencia promedio de E/S de su volumen:

```
Average I/O latency in ms/op = (VolumeTotalReadTime + VolumeTotalWriteTime) /
 (VolumeReadOps + VolumeWriteOps)
```

Si la latencia de E/S es superior a la que requiere, compruebe las IOPS dirigidas y asegúrese de que la aplicación no trata de dirigir más IOPS de las que ha aprovisionado. Puede usar la siguiente fórmula para supervisar las IOPS promedio dirigidas en su volumen:

```
Estimated average IOPS in ops/s = (Sum(VolumeReadOps) + Sum(VolumeWriteOps)) / (Period
 - Sum(VolumeIdleTime))
```

Si la aplicación necesita un número de IOPS mayor que el que puede proporcionar el volumen, debería plantearse el uso de uno de los siguientes:

- Un volumen `gp3`, `io2` o `io1` aprovisionado con suficientes IOPS para lograr la latencia requerida
- Un volumen `gp2` mayor que proporcione suficiente rendimiento de IOPS de base de referencia

Los volúmenes `st1` y `sc1` respaldados por HDD están diseñados para dar mejor resultado con cargas de trabajo que aprovechan el tamaño máximo de 1024 KiB para E/S. Para determinar el tamaño de E/S medio del volumen, divida `VolumeWriteBytes` entre `VolumeWriteOps`. El mismo cálculo se aplica a las operaciones de lectura. Si el tamaño de E/S promedio es inferior a 64 KiB, aumentar el tamaño de las operaciones de E/S que se envían a un volumen `st1` o `sc1` debería servir para mejorar el rendimiento.

> **Note**
>
> Si el tamaño de E/S está en 44 KiB o en un valor próximo, es posible que esté utilizando una instancia o kernel que no admite descriptores indirectos. Cualquier kernel de Linux, versión 3.8 y posteriores, tiene esta compatibilidad, así como todas las instancias de la generación actual.

`BurstBalance` muestra el balance del bucket de ráfagas para los volúmenes `gp2`, `st1` y `sc1` como un porcentaje del saldo total. Cuando el bucket por ráfaga se agota, el E/S del volumen (para los volúmenes `gp2`) o el rendimiento del volumen (para los volúmenes `st1` y `sc1`) se reducen a la base

de referencia. Compruebe el valor `BurstBalance` para determinar si el volumen se está reduciendo por esta razón. Para ver una lista completa de las métricas de Amazon EBS disponibles, consulte CloudWatch Métricas de Amazon para Amazon EBS y Métricas de Amazon EBS para instancias basadas en Nitro.

Recursos relacionados

Para obtener más información sobre las características de E/S de Amazon EBS, consulte la siguiente presentación de re:Invent Amazon EBS: Designing for Performance.

Inicializar de volúmenes de Amazon EBS

Los volúmenes de EBS vacíos disponen de su máximo rendimiento en cuanto se crean y no es necesario inicializarlos (proceso que antes se denominaba precalentamiento).

Para los volúmenes de cualquier tipo creados a partir de instantáneas, los bloques de almacenamiento deben extraerse de Amazon S3 y grabarse en el volumen antes de poder acceder a ellos. Esta acción preliminar lleva tiempo y puede provocar un aumento considerable de la latencia de las operaciones de E/S la primera vez que se accede a cada bloque. El rendimiento del volumen se alcanza después de descargar todos los bloques y de escribirlos en el volumen.

> **Important**
>
> Cuando se inicializan volúmenes Provisioned IOPS SSD que se crearon a partir de instantáneas, el rendimiento del volumen puede descender por debajo del 50 % del nivel esperado, lo que causa que el volumen muestre un estado de `warning` en la comprobación de estado de I/O Performance (Rendimiento de E/S). Este comportamiento es el esperado y puede hacer caso omiso del estado `warning` en los volúmenes Provisioned IOPS SSD cuando se están inicializando. Para obtener más información, consulte Comprobaciones de estado de volumen de EBS.

Para la mayoría de las aplicaciones, la amortización del costo de inicialización a lo largo de la vida útil del volumen es aceptable. Para evitar este efecto inicial sobre el rendimiento en un entorno productivo, puede usar una de las opciones siguientes:

- Forzar la incialización inmediata de todo el volumen. Para obtener más información, consulte instancias de Linux (instancias de Linux) o instancias de Windows (instancias de Windows).

- Habilitar la restauración rápida de instantáneas en una instantánea para garantizar que los volúmenes de EBS creados desde la instantánea se inicialicen por completo durante la creación y proporcionen al instante todo su rendimiento aprovisionado. Para obtener más información, consulte Restauración rápida de instantáneas de Amazon EBS.

instancias de Linux

Para inicializar un volumen creado a partir de una instantánea en Linux

1. Adjunte el volumen recién restaurado a la instancia de Linux.
2. Utilice el comando lsblk para enumerar los dispositivos de bloques de la instancia.

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvdf  202:80   0  30G  0 disk
xvda1 202:1    0   8G  0 disk /
```

   Aquí puede ver que el nuevo volumen, `/dev/xvdf`, se ha adjuntado pero no se ha montado porque no hay ninguna ruta en la columna `MOUNTPOINT`.
3. Emplee las utilidades dd o fio para leer todos los bloques del dispositivo. El comando dd se instala de manera predeterminada en los sistemas Linux, pero fio es considerablemente más rápido, ya que permite lecturas con varios subprocesos.

   > **Note**
   >
   > Este paso puede demorar entre varios minutos y varias horas según el ancho de banda de la instancia EC2, las IOPS aprovisionadas y el tamaño del volumen.

   [dd] El parámetro `if` (archivo de entrada) debe establecerse en la unidad que desea inicializar. El parámetro `of` (archivo de salida) debe establecerse en el dispositivo virtual nulo de Linux, `/dev/null`. El parámetro `bs` establece el tamaño de los bloques de la operación de lectura; para un rendimiento óptimo, este valor se debe establecer en 1 MB.

> **Important**
>
> El uso incorrecto de dd puede destruir fácilmente los datos de un volumen. Asegúrese de seguir con precisión el comando de ejemplo siguiente: Solo el parámetro `if=/dev/xvdf` variará en función del nombre del dispositivo que lea.

```
[ec2-user ~]$ sudo dd if=/dev/xvdf of=/dev/null bs=1M
```

[fio] Si ha instalado fio en el sistema, utilice el comando siguiente para inicializar el volumen. El parámetro `--filename` (archivo de entrada) debe establecerse en la unidad que desea inicializar.

```
[ec2-user ~]$ sudo fio --filename=/dev/xvdf --rw=read --bs=1M --iodepth=32 --
ioengine=libaio --direct=1 --name=volume-initialize
```

Utilice el siguiente comando para instalar fio en Amazon Linux:

```
sudo yum install -y fio
```

Para instalar fio en Ubuntu, utilice el siguiente comando:

```
sudo apt-get install -y fio
```

Cuando la operación finalice, verá un informe de la operación de lectura. El volumen está ahora listo para utilizarse. Para obtener más información, consulte Cómo hacer que un volumen de Amazon EBS esté disponible para su uso.

instancias de Windows

Antes de usar una de estas herramientas, recopile información sobre los discos del sistema del modo siguiente:

Recopilar información sobre los discos del sistema

1. Utilice el comando wmic para enumerar los discos disponibles en el sistema.

```
wmic diskdrive get size,deviceid
```

A continuación, se muestra un ejemplo del resultado:

```
DeviceID            Size
\\.\PHYSICALDRIVE2  80517265920
\\.\PHYSICALDRIVE1  80517265920
\\.\PHYSICALDRIVE0  128849011200
\\.\PHYSICALDRIVE3  107372805120
```

2. Identifique el disco de inicialización con dd o fio. La unidad `C:` se encuentra en `\\.\PHYSICALDRIVE0`. Puede usar la utilidad `diskmgmt.msc` para comparar las letras de la unidad con los números de unidad de disco si no tiene seguridad sobre qué número de unidad usar.

Use the dd utility

Complete los procedimientos siguientes para instalar y utilizar dd para inicializar un volumen.

Consideraciones importantes

- Inicializar un volumen demora entre varios minutos y varias horas según el ancho de banda de la instancia EC2, las IOPS provisionadas y el tamaño del volumen.
- El uso incorrecto de dd puede destruir fácilmente los datos de un volumen. Asegúrese de seguir este procedimiento con precisión.

Instalar dd para Windows

El programa dd para Windows proporciona una experiencia similar al programa dd que suele estar disponible con los sistemas Linux y Unix y permite inicializar los volúmenes de Amazon EBS que se han creado a partir de instantáneas. Las versiones beta más recientes admiten el dispositivo virtual `/dev/null`. Si instala una versión anterior, puede utilizar el dispositivo virtual `nul` en su lugar. La documentación completa está disponible en http://www.chrysocome.net/dd.

1. Descargue la versión más reciente de los archivos binarios de dd para Windows de http://www.chrysocome.net/dd.

2. (Opcional) Cree una carpeta para las utilidades de la línea de comandos que sea fácil de encontrar y recordar, por ejemplo `C:\bin`. Si ya ha designado una carpeta para las utilidades de la línea de comandos, puede usarla en el paso siguiente.
3. Descomprima el paquete de los binarios y copie el archivo `dd.exe` en la carpeta de utilidades de la línea de comandos (por ejemplo, `C:\bin`).
4. Agregue la carpeta de utilidades de línea de comandos a la variable de entorno Path para que pueda ejecutar los programas de la carpeta desde cualquier ubicación.
   a. Elija Inicio, abra el menú contextual (haga clic con el botón derecho) de Equipo y elija Propiedades.
   b. Elija Configuración avanzada del sistema, Variables de entorno.
   c. En Variables del sistema, seleccione la variable Path y elija Editar.
   d. En Valor de variable, escriba un punto y coma y la ubicación de la carpeta de utilidades de la línea de comandos (**`;C:\bin\`**) al final del valor existente.
   e. Elija Aceptar para cerrar la ventana Editar la variable del sistema.
5. Abra una nueva ventana del símbolo del sistema. El paso anterior no actualiza las variables de entorno en las ventanas del símbolo del sistema actuales. Se actualizan las ventanas del símbolo del sistema que abra ahora que completó el paso anterior.

Inicializar un volumen con dd para Windows

Ejecute el siguiente comando para leer todos los bloques del dispositivo especificado (y enviar el resultado al dispositivo virtual `/dev/null`). Este comando inicializa con seguridad los datos existentes.

```
dd if=\\.\PHYSICALDRIVEn of=/dev/null bs=1M --progress --size
```

Es posible que aparezca un error si dd intenta leer más allá del final del volumen. Puede omitir este error de forma segura.

Si utilizó una versión anterior del comando dd, no es compatible con el dispositivo `/dev/null`. En su lugar, puede usar el dispositivo `nul` de la siguiente manera.

```
dd if=\\.\PHYSICALDRIVEn of=nul bs=1M --progress --size
```

Use the fio utility

Complete los procedimientos siguientes para instalar y utilizar fio para inicializar un volumen.

Para instalar fio para Windows

El programa fio para Windows proporciona una experiencia similar al programa fio que suele estar disponible con los sistemas Linux y Unix, y permite inicializar los volúmenes de Amazon EBS creados a partir de instantáneas. Para obtener más información, consulte https://github.com/axboe/fio.

1. Descargue el instalador de fioMSI expandiendo Assets para obtener la última versión y seleccionando el instalador de MSI.
2. Instale fio.

Para inicializar un volumen con fio para Windows

1. Ejecute un comando similar al siguiente para inicializar un volumen:

```
fio --filename=\\.\PHYSICALDRIVEn  --rw=read --bs=128k --iodepth=32 --direct=1
 --name=volume-initialize
```

2. Cuando la operación finalice, podrá utilizar el nuevo volumen. Para obtener más información, consulte Cómo hacer que un volumen de Amazon EBS esté disponible para su uso.

Configuración de Amazon EBS y RAID

Con Amazon EBS, puede utilizar cualquiera de las configuraciones RAID estándar que usaría con un servidor tradicional bare metal, siempre que dicha configuración sea compatible con el sistema operativo de la instancia. Esto se debe a que RAID al completo se lleva a cabo en el nivel del software.

Los datos de los volúmenes de Amazon EBS se replican en varios servidores de una zona de disponibilidad para evitar la pérdida de datos debido a un error de alguno de los componentes únicos. Esta replicación hace que los volúmenes de Amazon EBS sean diez veces más de confianza que las unidades de disco habituales. Para obtener más información, consulte Disponibilidad y durabilidad de Amazon EBS en las páginas de los detalles del producto de Amazon EBS.

Contenidos

Opciones de configuración RAID

Crear una matriz de RAID 0 le permite alcanzar un nivel de rendimiento mayor de un sistema de archivos que el que puede aprovisionar en un único volumen de Amazon EBS. Utilice RAID 0 cuando el rendimiento de E/S sea de suma importancia. Con RAID 0, las E/S se distribuyen entre los volúmenes de una franja. Si agrega un volumen, obtiene la adición directa de rendimiento e IOPS. Sin embargo, tenga en cuenta que el rendimiento de la franja se limita al volumen con el peor rendimiento del conjunto, y que la pérdida de un solo volumen del conjunto da como resultado una pérdida completa de datos para la matriz.

El tamaño resultante de una matriz de RAID 0 es la suma de los tamaños de los volúmenes que la componen y el ancho de banda es la suma de ancho de banda disponible de los volúmenes que contiene. Por ejemplo, dos volúmenes `io1` de 500 GiB con 4000 IOPS provisionadas cada uno crean una matriz de RAID 0 de 1000 GiB con ancho de banda disponible de 8000 IOPS y 1000 MiB/s de rendimiento.

> **Important**
>
> No se recomienda RAID 5 y RAID 6 para Amazon EBS porque las operaciones de escritura paritaria de estos modos RAID consumen parte de la IOPS de que disponen los volúmenes. Dependiendo de la configuración de la matriz de RAID, estos modos RAID proporcionan un 20-30% menos IOPS utilizables que una configuración RAID 0. También el aumento de los costos es un factor con estos modos RAID; cuando se usan velocidades y tamaños de volúmenes idénticos, una matriz de RAID 0 con 2 volúmenes puede superar el rendimiento de una matriz de RAID 6 con cuatro volúmenes que cuesta el doble.
>
> Tampoco se recomienda el uso de RAID 1 con Amazon EBS. RAID 1 requiere más ancho de banda de Amazon EC2 a Amazon EBS que las configuraciones que no son RAID porque los datos se escriben en varios volúmenes simultáneamente. Además, RAID 1 no proporciona ninguna mejora en el rendimiento de escritura.

Creación de una matriz de RAID 0

Utilice el siguiente procedimiento para crear una matriz de RAID 0.

Consideraciones

- Antes de llevar a cabo este procedimiento, debe decidir el tamaño de la matriz de RAID 0 y la cantidad de IOPS que desea aprovisionar.
- Cree volúmenes con el mismo tamaño y valores de rendimiento de IOPS. Asegúrese de que no crea una matriz que supere el ancho de banda disponible de la instancia EC2.
- Evite hacer el arranque desde un volumen de RAID. Si se produce un error en uno de los dispositivos, es posible que no pueda arrancar el sistema operativo.

instancias de Linux

Para crear una matriz de RAID 0 en Linux

1. Cree los volúmenes de Amazon EBS para la matriz. Para obtener más información, consulte Creación de un volumen de Amazon EBS..
2. Adjunte los volúmenes de Amazon EBS a la instancia en la que quiere alojar la matriz. Para obtener más información, consulte Adjunte un volumen de Amazon EBS a una instancia..
3. Utilice el comando mdadm para crear un dispositivo RAID lógico a partir de los volúmenes de Amazon EBS que acaba de adjuntar. Sustituya el número de volúmenes de la matriz por *`number_of_volumes`* y los nombres de dispositivo de cada volumen de la matriz (como `/dev/xvdf`) por *`device_name`*. También puede sustituir *`MY_RAID`* por un nombre único propio para la matriz.

   > **Note**
   >
   > Puede enumerar los dispositivos de la instancia con el comando lsblk para buscar los nombres de dispositivo.

   Para crear una matriz de RAID 0, ejecute el siguiente comando (observe la opción `--level=0` para seccionar la matriz):

```
[ec2-user ~]$ sudo mdadm --create --verbose /dev/md0 --level=0 --name=MY_RAID --raid-devices=number_of_volumes device_name1 device_name2
```

> **Tip**
>
> Si aparece el error `mdadm: command not found`, utilice el siguiente comando para instalar mdadm: `sudo yum install mdadm`.

4. Deje un tiempo para que la matriz de RAID se inicialice y sincronice. Puede hacer seguimiento del progreso de estas operaciones con el comando siguiente:

```
[ec2-user ~]$ sudo cat /proc/mdstat
```

A continuación, se muestra un ejemplo del resultado:

```
Personalities : [raid0]
md0 : active raid0 xvdc[1] xvdb[0]
      41910272 blocks super 1.2 512k chunks

unused devices: <none>
```

En general, puede mostrar información detallada sobre la matriz de RAID con el comando siguiente:

```
[ec2-user ~]$ sudo mdadm --detail /dev/md0
```

A continuación, se muestra un ejemplo del resultado:

```
/dev/md0:
           Version : 1.2
     Creation Time : Wed May 19 11:12:56 2021
        Raid Level : raid0
        Array Size : 41910272 (39.97 GiB 42.92 GB)
      Raid Devices : 2
     Total Devices : 2
       Persistence : Superblock is persistent

       Update Time : Wed May 19 11:12:56 2021
```

```
              State : clean
     Active Devices : 2
    Working Devices : 2
     Failed Devices : 0
      Spare Devices : 0

         Chunk Size : 512K

Consistency Policy : none

               Name : MY_RAID
               UUID : 646aa723:db31bbc7:13c43daf:d5c51e0c
             Events : 0

    Number   Major   Minor   RaidDevice State
       0     202       16        0      active sync   /dev/sdb
       1     202       32        1      active sync   /dev/sdc
```

5. Cree un sistema de archivos en la matriz de RAID y añádale una etiqueta para usarla cuando lo monte más adelante. Por ejemplo, para crear un sistema de archivos ext4 con la etiqueta *MY_RAID*, ejecute el siguiente comando:

```
[ec2-user ~]$ sudo mkfs.ext4 -L MY_RAID /dev/md0
```

   Dependiendo de los requisitos de la aplicación o de las restricciones del sistema operativo, puede usar un tipo de sistema de archivos distinto, como ext3 o XFS (consulte en la documentación del sistema de archivos el comando para crear el sistema de archivos correspondiente).

6. Para asegurarse de que la matriz de RAID se vuelve a ensamblar automáticamente durante el arranque, cree un archivo de configuración que contenga la información de RAID:

```
[ec2-user ~]$ sudo mdadm --detail --scan | sudo tee -a /etc/mdadm.conf
```

   > **Note**
   >
   > Si utiliza una distribución de Linux distinta de Amazon Linux, es posible que necesite modificar este comando. Por ejemplo, puede necesitar colocar el archivo en una ubicación diferente o agregar el parámetro `--examine`. Para obtener más información, ejecute man mdadm.conf en la instancia de Linux.

7. Cree una nueva imagen de disco RAM para precargar correctamente los módulos de dispositivo de bloqueo para la nueva configuración RAID:

```
[ec2-user ~]$ sudo dracut -H -f /boot/initramfs-$(uname -r).img $(uname -r)
```

8. Cree un punto de montaje para la matriz de RAID.

```
[ec2-user ~]$ sudo mkdir -p /mnt/raid
```

9. Por último, monte el dispositivo RAID en el punto de montaje que ha creado:

```
[ec2-user ~]$ sudo mount LABEL=MY_RAID /mnt/raid
```

   El dispositivo RAID está ahora listo para utilizarse.

10. (Opcional) Para montar este volumen de Amazon EBS en cada reinicio del sistema, añada una entrada para el dispositivo en el archivo `/etc/fstab`.

    a. Cree un backup del archivo `/etc/fstab` que pueda utilizar si destruye o elimina accidentalmente este archivo al editarlo.

    ```
    [ec2-user ~]$ sudo cp /etc/fstab /etc/fstab.orig
    ```

    b. Abra el archivo `/etc/fstab` en el editor de textos que prefiera (como nano o vim).

    c. Comente las líneas que comiencen por "`UUID=`" y al final del archivo agregue una línea nueva para el volumen de RAID utilizando el siguiente formato:

    ```
    device_label mount_point file_system_type fs_mntops fs_freq fs_passno
    ```

    Los tres últimos campos de esta línea corresponden a las opciones de montaje del sistema de archivos, la frecuencia de volcado del sistema de archivos y el orden de las comprobaciones del sistema de archivos llevadas a cabo en el momento del arranque. Si no sabe cuáles deben ser estos valores, utilice los que aparecen en el siguiente ejemplo (`defaults,nofail 0 2`). Para obtener más información acerca de las entradas de `/etc/fstab`, consulte la página de manual de fstab (ingresando man fstab en la línea de comandos). Por ejemplo, para montar el sistema de archivos ext4 en el dispositivo con la etiqueta MY_RAID en el punto de montaje `/mnt/raid`, agregue la entrada siguiente a `/etc/fstab`.

> **Note**
>
> Si en algún momento intenta arrancar la instancia sin este volumen adjunto (por ejemplo, para que dicho volumen pueda alternar entre distintas instancias), debe añadir la opción de montaje `nofail` que permite a la instancia arrancar incluso si hay errores cuando se monta el volumen. Los derivados de Debian, como Ubuntu, también deben añadir la opción de montaje `nobootwait`.

```
LABEL=MY_RAID       /mnt/raid   ext4    defaults,nofail        0       2
```

d. Una vez que haya añadido la nueva entrada en `/etc/fstab`, necesita comprobar que funciona. Ejecute el comando sudo mount -a para montar todos los sistemas de archivos en `/etc/fstab`.

```
[ec2-user ~]$ sudo mount -a
```

Si el comando anterior no da error, el archivo `/etc/fstab` es correcto y el sistema de archivos se montará automáticamente durante el siguiente arranque. Si el comando da algún error, examínelo y trate de corregir `/etc/fstab`.

> **Warning**
>
> Los errores del archivo `/etc/fstab` pueden impedir el arranque del sistema. No apague un sistema que presente errores en el archivo `/etc/fstab`.

e. (Opcional) Si no sabe con seguridad cómo corregir errores en `/etc/fstab`, siempre puede restaurar el archivo de backup `/etc/fstab` con el siguiente comando.

```
[ec2-user ~]$ sudo mv /etc/fstab.orig /etc/fstab
```

instancias de Windows

Para crear una matriz de RAID 0 en Windows

1. Cree los volúmenes de Amazon EBS para la matriz. Para obtener más información, consulte Creación de un volumen de Amazon EBS..
2. Adjunte los volúmenes de Amazon EBS a la instancia en la que quiere alojar la matriz. Para obtener más información, consulte Adjunte un volumen de Amazon EBS a una instancia..
3. Conéctese a la instancia de Windows. Para obtener más información, consulte Conexión con su instancia de Windows.
4. Abra un símbolo del sistema y escriba el comando diskpart:

```
diskpart

Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: WIN-BM6QPPL51CO
```

5. En el símbolo de DISKPART, enumere los discos disponibles con el comando siguiente.

```
DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online           30 GB      0 B
  Disk 1    Online            8 GB      0 B
  Disk 2    Online            8 GB      0 B
```

   Identifique los discos que desea usar en la matriz y anote sus números de disco.

6. Cada disco que desee usar en la matriz debe ser un disco dinámico online que no contenga ningún volumen. Siga los pasos siguientes para convertir discos básicos en dinámicos y eliminar cualquier volumen existente.

   a. Seleccione un disco que desee usar en la matriz con el comando siguiente, sustituyendo *n* por el número del disco.

```
DISKPART> select disk n

Disk n is now the selected disk.
```

b. Si el disco seleccionado aparece como `Offline`, póngalo online ejecutando el comando online disk.

c. Si el disco seleccionado no tiene un asterisco en la columna Dyn del resultado del comando list disk anterior, tiene que convertirlo en un disco dinámico.

```
DISKPART> convert dynamic
```

> **Note**
>
> Si recibe un error porque el disco está protegido contra escritura, quite la marca de solo lectura con el comando ATTRIBUTE DISK CLEAR READONLY y, a continuación, intente de nuevo la conversión en disco dinámico.

d. Utilice el comando detail disk para comprobar los volúmenes que contiene el disco seleccionado.

```
DISKPART> detail disk

XENSRC PVDISK SCSI Disk Device
Disk ID: 2D8BF659
Type   : SCSI
Status : Online
Path   : 0
Target : 1
LUN ID : 0
Location Path : PCIROOT(0)#PCI(0300)#SCSI(P00T01L00)
Current Read-only State : No
Read-only  : No
Boot Disk  : No
Pagefile Disk  : No
Hibernation File Disk  : No
Crashdump Disk  : No
Clustered Disk  : No

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 2     D   NEW VOLUME   FAT32  Simple      8189 MB  Healthy
```

Observe cualquier número de volumen que haya en el disco. En este ejemplo, el número de volumen es 2. Si no hay volúmenes, puede saltar este paso.

e. (Solo se requiere si los volúmenes se han identificado en el paso previo) Seleccione y elimine cualquier volumen que haya en el disco y que haya identificado en el paso previo.

> **Warning**
>
> Esto destruye todos los datos existentes en el volumen.

i. Seleccione el volumen, sustituyendo *n* por el número del volumen.

```
DISKPART> select volume n
Volume n is the selected volume.
```

ii. Elimine el volumen.

```
DISKPART> delete volume

DiskPart successfully deleted the volume.
```

iii. Repita estos pasos secundarios con cada volumen que tenga que eliminar del disco seleccionado.

f. Repita Step 6 con cada disco que desee usar en la matriz.

7. Verifique que los discos que desea usar ahora son dinámicos. En este caso, estamos usando los discos 1 y 2 para el volumen de RAID.

```
DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online           30 GB      0 B
  Disk 1    Online            8 GB      0 B   *
  Disk 2    Online            8 GB      0 B   *
```

8. Cree la matriz de RAID. En Windows, un volumen de RAID 0 se conoce como un volumen seccionado.

   Para crear una matriz de volumen seccionado en los discos 1 y 2, ejecute el comando siguiente (observe la opción `stripe` para seccionar la matriz):

```
DISKPART> create volume stripe disk=1,2
```

```
DiskPart successfully created the volume.
```

9. Verifique el nuevo volumen.

```
DISKPART> list volume

  DISKPART> list volume

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     C                NTFS   Partition     29 GB  Healthy    System
  Volume 1                      RAW    Stripe        15 GB  Healthy
```

Tenga en cuenta que la columna Type ahora indica que el volumen 1 es un volumen `stripe`.

10. Seleccione y dé formato al volumen para poder comenzar a utilizarlo.

a. Seleccione el volumen al que quiere dar formato y sustituya *n* por el número del volumen.

```
DISKPART> select volume n

Volume n is the selected volume.
```

b. Dé formato al volumen.

> **Note**
>
> Para llevar a cabo una operación de formato completa, omita la opción `quick`.

```
DISKPART> format quick recommended label="My new volume"

  100 percent completed

DiskPart successfully formatted the volume.
```

c. Asigne la letra de una unidad de disco disponible al volumen.

```
DISKPART> assign letter f

DiskPart successfully assigned the drive letter or mount point.
```

El nuevo volumen está ahora listo para utilizarse.

Crear instantáneas de volúmenes en una matriz de RAID

Si desea realizar un backup de los datos de los volúmenes de EBS en una matriz de RAID utilizando instantáneas, debe asegurarse de que estas son consistentes. Esto se debe a que las instantáneas de estos volúmenes se crean de manera independiente. Para restaurar volúmenes de EBS en una matriz de RAID desde instantáneas que no están sincronizadas dañaría la integridad de la matriz.

Para crear un conjunto consistente de instantáneas para su matriz RAID, utilice Instantáneas de varios volúmenes de EBS. Las instantáneas de varios volúmenes le permiten tomar point-in-time instantáneas coordinadas con los datos y consistentes con los bloqueos en varios volúmenes de EBS conectados a una instancia EC2. Como las instantáneas se generan automáticamente en varios volúmenes de EBS, no tiene que detener la instancia para coordinar entre volúmenes para garantizar la coherencia. Para obtener más información, consulte los pasos para crear instantáneas de varios volúmenes en Creación de instantáneas de Amazon EBS.

Análisis comparativo de volúmenes de EBS

Puede probar el rendimiento de los volúmenes de Amazon EBS simulando cargas de trabajo de E/S. El proceso es el siguiente:

1. Lance una instancia optimizada para EBS.
2. Cree volúmenes nuevos de EBS
3. Adjunte los volúmenes a la instancia optimizada para EBS.
4. Configure y monte el dispositivo de bloques.
5. Instale una herramienta para el análisis comparativo del rendimiento de E/S.
6. Haga el análisis del rendimiento de E/S de los volúmenes.
7. Elimine los volúmenes y termine la instancia para dejar de incurrir en gastos.

> **Important**
>
> Algunos de los procedimientos darán como resultado la destrucción de los datos contenidos en los volúmenes de EBS que analice. Los procedimientos de análisis comparativos son para utilizarse en volúmenes creados especialmente con fines de pruebas, no de producción.

Configurar la instancia

Para lograr el rendimiento óptimo con los volúmenes de EBS, recomendamos que use una instancia optimizada para EBS. Las instancias optimizadas para EBS proporcionan rendimiento dedicado entre Amazon EC2 y Amazon EBS con la instancia. Las instancias optimizadas para EBS ofrecen un ancho de banda dedicado entre Amazon EC2 y Amazon EBS, con especificaciones en función del tipo de instancia.

Para crear una instancia optimizada para EBS, elija Lanzar como instancia optimizada para EBS cuando lance la instancia con la consola de Amazon EC2 o especifique --ebs-optimized cuando utilice la línea de comandos. Asegúrese de que selecciona un tipo de instancia que admita esta opción.

Configurar volúmenes Provisioned IOPS SSD o SSD de uso general

Para crear volúmenes de SSD de IOPS provisionadas (`io1` e `io2`) o de SSD de uso general (`gp2` y `gp3`) con la consola de Amazon EC2, en Volume Type (Tipo de volumen), elija Provisioned IOPS SSD (io1) (SSD de IOPS provisionadas [io1]), Provisioned IOPS SSD (io2) (SSD de IOPS provisionadas [io2]), General Purpose SSD (gp2) (SSD de uso general [gp2]) o General Purpose SSD (gp3) (SSD de uso general [gp3]). En la línea de comandos, especifique `io1io2`, `gp2` o `gp3` para el parámetro --volume-type. Para los volúmenes `io1`, `io2` y `gp3`, especifique el número de operaciones de E/S por segundo (IOPS) para el parámetro --iops. Para obtener más información, consulte Tipos de volúmenes de Amazon EBS y Creación de un volumen de Amazon EBS..

(Solamente instancias de Linux) Para las pruebas de ejemplo, recomendamos que cree una matriz de RAID 0 con 6 volúmenes, que ofrece un elevado nivel de rendimiento. Como se le cobra por la cantidad de gigabytes provisionados (y el número de IOPS provisionadas para los volúmenes de io1, io2 y gp3), en lugar de por el número de volúmenes, no hay cargo adicional por crear varios volúmenes más pequeños y utilizarlos para crear un conjunto seccionado (stripe set). Si utiliza Oracle Orion para el análisis comparativo de los volúmenes, puede simular el seccionado (striping) del mismo modo que Oracle ASM, de manera que recomendamos que deje que lo haga Orion. Si usa

otra herramienta para el análisis comparativo, tendrá que encargarse de seccionar usted mismo los volúmenes.

Para obtener más información acerca de cómo crear una matriz de RAID 0, consulte Creación de una matriz de RAID 0.

Configure volúmenes de HDD con rendimiento optimizado (**st1**) o volúmenes de HDD en frío (**sc1**)

Para crear un volumen `st1`, elija Throughput Optimized HDD (HDD de rendimiento optimizado) cuando lo cree con la consola de Amazon EC2, o especifique --type **st1** si utiliza la línea de comandos. Para crear un volumen `sc1`, elija Cold HDD (HDD en frío) cuando lo cree con la consola de Amazon EC2, o especifique --type **sc1** si utiliza la línea de comandos. Para obtener más información acerca de la creación de volúmenes de EBS, consulte Creación de un volumen de Amazon EBS.. Para obtener información acerca de cómo adjuntar estos volúmenes a la instancia, consulte Adjunte un volumen de Amazon EBS a una instancia..

(Solo instancias de Linux) AWS proporciona una plantilla JSON para su uso AWS CloudFormation que simplifica este procedimiento de configuración. Acceda a la plantilla y guárdela como un archivo JSON. AWS CloudFormation le permite configurar sus propias claves SSH y ofrece una forma más sencilla de configurar un entorno de pruebas de rendimiento para evaluar los `st1` volúmenes. La plantilla crea una instancia de la generación actual y un volumen `st1` con 2 TiB, y adjunta el volumen a la instancia en `/dev/xvdf`.

(Solamente instancias de Linux) Creación de un volumen HDD con la plantilla

1. Abra la AWS CloudFormation consola en https://console.aws.amazon.com/cloudformation.
2. Elija Create Stack.
3. Elija Upload a Template to Amazon S3 (Cargar una plantilla en Amazon S3) y seleccione la plantilla JSON que ha obtenido previamente.
4. Llame a la pila con un nombre como “ebs-perf-testing” y seleccione un tipo de instancia (la predeterminada es r3.8xlarge) y la clave SSH.
5. Elija Next (Siguiente) dos veces y, después, elija Create Stack (Crear pila).
6. Cuando el estado de la nueva pila cambie de CREATE_IN_PROGRESS (CREACIÓN EN PROCESO) a COMPLETE (COMPLETA), elija Outputs (Resultados) para ver la entrada DNS de pública de la nueva instancia, que tendrá adjunto un volumen `st1` de 2 TiB.

7. Conéctese mediante SSH a la nueva pila como el usuario **`ec2-user`**, con el nombre de host que ha obtenido de la entrada DNS en el paso anterior.
8. Continúe en Instalar herramientas para el análisis comparativo.

Instalar herramientas para el análisis comparativo

En la siguiente tabla se enumeran las herramientas que puede usar para el análisis comparativo del rendimiento de los volúmenes de EBS.

instancias de Linux

Herramienta	Descripción

fio	Para el análisis comparativo del rendimiento de E/S. (Observe que fio tiene una dependencia de `libaio-devel` .)
	
	Para instalar fio en Amazon Linux, ejecute el siguiente comando:
	
	`[ec2-user ~]$ sudo yum install -y fio`
	
	Para instalar fio en Ubuntu, ejecute el siguiente comando:
	
	`sudo apt-get install -y fio`

Oracle Orion Calibration Tool	Para calibrar el rendimiento de E/S de los sistemas de almacenamiento que se usan con las bases de datos de Oracle.

instancias de Windows

Herramienta	Descripción
DiskSpd	DiskSpd es una herramienta de rendimiento de almacenamiento de los equipos de ingeniería de infraestructura de Windows, Windows Server y Cloud Server de Microsoft. Puede descargarla en https://github.com/Microsoft/diskspd/releases.

Herramienta	Descripción
	Después de descargar el archivo ejecutable `diskspd.exe` , abra un símbolo del sistema con derechos administrativos (seleccionando "Ejecutar como administrador") y, a continuación, vaya al directorio donde copió el archivo `diskspd.exe` . Copie el archivo ejecutable `diskspd.exe` que desee de la carpeta de ejecutables correspondiente (`amd64fre`, `armfre` o `x86fre`) a una ruta corta y sencilla como `C:\DiskSpd` . En la mayoría de los casos, querrá la versión de 64 bits DiskSpd de la `amd64fre` carpeta. El código fuente DiskSpd está alojado GitHub en: https://github.com/Microsoft/diskspd.
CrystalDiskMark	CrystalDiskMark es un sencillo software de referencia de discos. Puede descargarlo en https://crystalmark.info/en/software/crystaldiskmark/.

Estas herramientas admiten una amplia gama de parámetros de prueba. Es conveniente que use comandos que se aproximen a las cargas de trabajo que admitirán los volúmenes. Los comandos que se ofrecen a continuación tienen por finalidad servir de ejemplo para ayudarle a comenzar.

Elegir la longitud de cola del volumen

Elija la mejor longitud de cola en función de la carga de trabajo y el tipo de volumen.

Longitud de las colas en los volúmenes con respaldo de SSD

Para determinar la longitud óptima de cola para la carga de trabajo en volúmenes respaldados por SSD, recomendamos una longitud de cola de 1 por cada 1000 IOPS disponibles (base de referencia para los volúmenes SSD de uso general y la cantidad provisionada para los volúmenes Provisioned IOPS SSD). Después, puede monitorizar el rendimiento de la aplicación y ajustar ese valor según las necesidades de la aplicación.

Aumentar la longitud de cola tiene ventajas hasta que alcanza las IOPS aprovisionadas, el rendimiento o el valor de longitud de cola del sistema óptimo, que está establecido en 32. Por ejemplo, un volumen con 3,000 IOPS aprovisionadas debería tener una longitud de cola de 3. Experimente con diversos ajustes de estos valores, mayores o menores, para ver cuál responde mejor a la aplicación.

Longitud de las colas en los volúmenes con respaldo de HDD

Para determinar la longitud de cola óptima de la carga de trabajo en volúmenes con respaldo en HDD, recomendamos que sea al menos de 4 cuando trabaje con E/S secuenciales de 1 MiB. Después, puede monitorizar el rendimiento de la aplicación y ajustar ese valor según las necesidades de la aplicación. Por ejemplo, un volumen `st1` con 2 TiB con rendimiento en ráfagas de 500 MiB/s e IOPS de 500 debería tener una longitud de cola de 4, 8 o 16 trabajando con E/S secuenciales de 1024 KiB, 512 KiB o 256 KiB respectivamente. Experimente con varios ajustes de estos valores, mayores o menores, para ver cuál responde mejor a la aplicación.

Deshabilitar los estados C

Antes de ejecutar los análisis comparativos, debe deshabilitar los estados C del procesador. Los núcleos que estén temporalmente inactivos en una CPU compatible pueden entrar en un estado C para ahorrar energía. Cuando se le solicita al núcleo que reanude el procesamiento, transcurre un determinado periodo de tiempo hasta que vuelve a estar totalmente operativo. Esta latencia puede interferir con las rutinas de análisis comparativos del procesador. Para obtener más información sobre los estados C y los tipos de instancias EC2 que los admiten, consulte Control de los estados del procesador de la instancia EC2.

instancias de Linux

Puede deshabilitar los estados C en Amazon Linux, RHEL y CentOS de la manera siguiente:

1. Obtenga el número de estados C.

```
$ C:\> cpupower idle-info | grep "Number of idle states:"
```

2. Deshabilite los estados C desde c1 a cN. Lo ideal es que los núcleos se encuentren en el estado c0.

```
$ C:\> for i in `seq 1 $((N-1))`; do cpupower idle-set -d $i; done
```

instancias de Windows

Puede deshabilitar los estados C en Windows de la siguiente manera:

1. Entra PowerShell, obtén el esquema de potencia activa actual.

```
$current_scheme = powercfg /getactivescheme
```

2. Obtenga la GUID del esquema de alimentación.

```
(Get-WmiObject -class Win32_PowerPlan -Namespace "root\cimv2\power" -Filter
 "ElementName='High performance'").InstanceID
```

3. Obtenga la GUID de la configuración de alimentación.

```
(Get-WmiObject -class Win32_PowerSetting -Namespace "root\cimv2\power" -Filter
 "ElementName='Processor idle disable'").InstanceID
```

4. Obtenga la GUID del subgrupo de configuración de alimentación.

```
(Get-WmiObject -class Win32_PowerSettingSubgroup -Namespace "root\cimv2\power" -
Filter "ElementName='Processor power management'").InstanceID
```

5. Deshabilite los estados C estableciendo el valor del índice en 1. Un valor de 0 indica que los estados C están deshabilitados.

```
powercfg /
setacvalueindex <power_scheme_guid> <power_setting_subgroup_guid> <power_setting_guid>
 1
```

6. Establezca el esquema activo para asegurarse de que se han guardado los ajustes.

```
powercfg /setactive <power_scheme_guid>
```

Efectuar el punto de referencia

Los procedimientos siguientes describen los comandos de análisis comparativo para diversos tipos de volúmenes de EBS.

Ejecute los comandos siguientes en una instancia optimizada para EBS con volúmenes de EBS adjuntos. Si los volúmenes de EBS se crearon a partir de instantáneas, asegúrese de inicializarlos antes de marcar un punto de referencia. Para obtener más información, consulte Inicializar de volúmenes de Amazon EBS.

Cuando termine de probar los volúmenes, consulte los temas siguientes para llevar a cabo la limpieza: Eliminar un volumen Amazon EBS y Terminar la instancia.

Volúmenes de referencia Provisioned IOPS SSD y SSD de uso general

instancias de Linux

Ejecute fio en la matriz RAID 0 que creó.

El comando siguiente lleva a cabo operaciones de escritura aleatorias de 16 KB.

```
[ec2-user ~]$ sudo fio --directory=/mnt/p_iops_vol0 --ioengine=psync --
name fio_test_file --direct=1 --rw=randwrite --bs=16k --size=1G --numjobs=16 --
time_based --runtime=180 --group_reporting --norandommap
```

El comando siguiente lleva a cabo operaciones de lectura aleatorias de 16 KB.

```
[ec2-user ~]$ sudo fio --directory=/mnt/p_iops_vol0 --name fio_test_file --direct=1
 --rw=randread --bs=16k --size=1G --numjobs=16 --time_based --runtime=180 --
group_reporting --norandommap
```

Para obtener más información acerca de la interpretación de los resultados, consulte este tutorial: Inspecting disk IO performance with fio.

instancias de Windows

Ejecute DiskSpd en el volumen que creó.

El siguiente comando ejecutará una prueba de E/S aleatoria de 30 segundos utilizando un archivo de prueba de 20 GB guardado en la unidad `C:`, con una proporción de escritura del 25 % y de lectura del 75 %, y un tamaño de bloque de 8 K. Utilizará ocho subprocesos de trabajo, cada uno con cuatro operaciones de E/S importantes y un valor de entropía de escritura de 1 GB. Los resultados de la prueba se guardarán en un archivo de texto llamado `DiskSpeedResults.txt`. Estos parámetros simulan una carga de trabajo OLTP de SQL Server.

```
diskspd -b8K -d30 -o4 -t8 -h -r -w25 -L -Z1G -c20G C:\iotest.dat > DiskSpeedResults.txt
```

Para obtener más información acerca de la interpretación de los resultados, consulte este tutorial: Inspecting disk IO performance with DiskSPd.

Análisis comparativo de los volúmenes **st1** y **sc1** (instancias de Linux)

Ejecute fio en el volumen `st1` o `sc1`.

> **Note**
>
> Antes de ejecutar estas pruebas, establezca la E/S de búfer de la instancia como se describe en Aumento del valor de read-ahead para cargas de trabajo de lectura intensiva y de alto rendimiento en `st1` y `sc1` (solamente instancias de Linux).

El comando siguiente lleva a cabo operaciones de lectura secuenciales de 1 MiB en un dispositivo de bloques `st1` asociado (por ejemplo, `/dev/xvdf`):

```
[ec2-user ~]$ sudo fio --filename=/dev/<device> --direct=1 --rw=read --randrepeat=0
 --ioengine=libaio --bs=1024k --iodepth=8 --time_based=1 --runtime=180 --
name=fio_direct_read_test
```

El comando siguiente lleva a cabo operaciones de escritura secuenciales de 1 MiB en un dispositivo de bloques de `st1` adjunto:

```
[ec2-user ~]$ sudo fio --filename=/dev/<device> --direct=1 --rw=write --randrepeat=0
 --ioengine=libaio --bs=1024k --iodepth=8 --time_based=1 --runtime=180 --
name=fio_direct_write_test
```

Algunas cargas de trabajo hacen operaciones de lectura y operaciones de escritura secuenciales en diferentes partes del dispositivo de bloques. Para el análisis de tales cargas de trabajo, recomendamos utilizar trabajos fio separados y simultáneos para lectura y escritura, y usar la opción fio `offset_increment` para llegar a distintas ubicaciones del dispositivo de bloques para cada trabajo.

La ejecución de esta carga de trabajo es un poco más complicada que la de una carga de lectura secuencial o una carga de escritura secuencial. Utilice un editor de texto para crear un archivo de trabajo fio, llamado `fio_rw_mix.cfg` en este ejemplo, que contiene lo siguiente:

```
[global]
clocksource=clock_gettime
randrepeat=0
runtime=180
```

```
[sequential-write]
bs=1M
ioengine=libaio
direct=1
iodepth=8
filename=/dev/<device>
do_verify=0
rw=write
rwmixread=0
rwmixwrite=100

[sequential-read]
bs=1M
ioengine=libaio
direct=1
iodepth=8
filename=/dev/<device>
do_verify=0
rw=read
rwmixread=100
rwmixwrite=0
offset=100g
```

A continuación, ejecute el siguiente comando:

```
[ec2-user ~]$ sudo fio fio_rw_mix.cfg
```

Para obtener más información acerca de la interpretación de los resultados, consulte este tutorial: Inspecting disk I/O performance with fio.

Varios trabajos fio para E/S directa, incluso utilizando operaciones de lectura o escritura secuenciales, pueden dar como resultado un rendimiento menor del esperado con los volúmenes `st1` y `sc1`. Recomendamos que use un trabajo de E/S directo y el parámetro `iodepth` para controlar el número de operaciones de E/S simultáneas.

Administrador de vida útil de datos de Amazon

Puede utilizar Amazon Data Lifecycle Manager para automatizar la creación, retención y eliminación de instantáneas de EBS y las AMI respaldadas por EBS. Cuando automatiza la administración de instantáneas y la AMI, lo ayuda a:

- Proteger datos valiosos aplicando una programación periódica de copias de seguridad
- Cree las AMI estandarizadas que se puedan actualizar a intervalos regulares.
- Conservar las copias de seguridad de acuerdo con los requisitos de los auditores o las políticas internas de conformidad
- Reducir los costos de almacenamiento al eliminar las copias de seguridad obsoletas
- Cree políticas de copia de seguridad de recuperación de desastres que hagan copias de seguridad de los datos en cuentas o regiones aisladas.

Cuando se combina con las funciones de monitoreo de Amazon EventBridge y Amazon Data Lifecycle Manager AWS CloudTrail, proporciona una solución de respaldo completa para las instancias de Amazon EC2 y los volúmenes individuales de EBS sin costo adicional.

> **Important**
>
> - Amazon Data Lifecycle Manager no puede administrar las instantáneas ni las AMI que se crean por cualquier otro medio.
> - Amazon Data Lifecycle Manager no puede automatizar la creación, retención y eliminación de las AMI respaldadas por el almacén de instancias.

Contenido

- AWS Identity and Access Management
- Monitorizar el ciclo de vida de las instantáneas y las AMI
- Resolución de problemas

Cuotas

Su AWS cuenta tiene las siguientes cuotas relacionadas con Amazon Data Lifecycle Manager:

Descripción	Cuota
Políticas de ciclo de vida personalizadas por región	100
Políticas predeterminadas para las instantáneas de EBS por región	1
Políticas predeterminadas para las AMI respaldadas por EBS por región	1
Etiquetas por recurso	45

Funcionamiento de Amazon Data Lifecycle Manager

A continuación, se muestran los elementos clave de Amazon Data Lifecycle Manager.

Elementos

- Políticas
- Programaciones de políticas (solo políticas personalizadas)
- Etiquetas de recursos de destino (solo políticas personalizadas)
- Instantáneas
- AMI respaldadas por EBS
- Amazon Data Lifecycle Manager etiquetas

Políticas

Con Amazon Data Lifecycle Manager, puede crear políticas para definir sus requisitos de creación y retención de copias de seguridad. Estas políticas suelen especificar lo siguiente:

- Tipo de política: define el tipo de recursos de copia de seguridad que administra la política (instantáneas o AMI respaldadas por EBS).
- Recursos de destino: define el tipo de recursos a los que se dirige la política (instancias o volúmenes de EBS).
- Frecuencia de creación: define la frecuencia con la que se ejecuta la política y con la que esta crea instantáneas o AMI.
- Umbral de retención: define durante cuánto tiempo la política conserva las instantáneas o las AMI tras su creación.
- Acciones adicionales: define las acciones adicionales que debe realizar la política, como copiar, archivar o etiquetar recursos entre regiones.

Amazon Data Lifecycle Manager ofrece políticas predeterminadas y políticas personalizadas.

Políticas predeterminadas

Las políticas predeterminadas realizan copias de seguridad de todos los volúmenes e instancias de una región que no tienen copias de seguridad recientes. Si lo desea, puede especificar los parámetros de exclusión para excluir volúmenes e instancias.

Amazon Data Lifecycle Manager admite los siguientes tipos de políticas predeterminadas:

- Política predeterminada para instantáneas de EBS: se dirige a los volúmenes y automatiza la creación, retención y eliminación de instantáneas.
- Política predeterminada para las AMI respaldadas por EBS: engloba las instancias y automatiza la creación, retención y anulación del registro de las AMI respaldadas por EBS.

Solo puede tener una política predeterminada por tipo de recurso en cada cuenta y región de AWS .

Políticas personalizadas

Las políticas personalizadas se centran en recursos específicos en función de las etiquetas asignadas y admiten características avanzadas, como la restauración rápida de instantáneas, el archivado de instantáneas, la copia entre cuentas y los scripts previos y posteriores. Una política

personalizada puede incluir hasta 4 programaciones y cada una puede tener su propia frecuencia de creación, umbral de retención y configuración de características avanzadas.

Amazon Data Lifecycle Manager admite los siguientes tipos de políticas personalizadas:

- Política de instantáneas de EBS: se dirige a los volúmenes o instancias la creación, retención y eliminación de instantáneas de EBS.
- Política de AMI respaldadas por EBS: se dirige a las instancias y automatiza la creación, retención y cancelación del registro de AMI respaldadas por EBS.
- Política de eventos de copia entre cuentas: automatiza las acciones de copia entre regiones para las instantáneas que se comparten con usted.

Para obtener más información, consulte Diferencias entre políticas predeterminadas y políticas personalizadas.

Programaciones de políticas (solo políticas personalizadas)

Las programaciones de políticas definen cuándo la política crea instantáneas o las AMI. Las políticas pueden tener hasta cuatro programaciones—una obligatoria y hasta tres opcionales.

Agregar varias programaciones a una única política permite crear instantáneas o las AMI a diferentes frecuencias al utilizar igual política. Por ejemplo, puede crear una única política que cree instantáneas diarias, semanales, mensuales y anuales. Esto elimina la necesidad de administrar varias políticas.

Para cada programación, puede definir la frecuencia, la configuración de restauración rápida de instantáneas (sólo políticas del ciclo de vida de instantáneas), las reglas de copia entre regiones y las etiquetas. Las etiquetas destinadas a una programación se asignan automáticamente a las instantáneas o las AMI que se crean cuando se inicia la programación. Además, asigna Amazon Data Lifecycle Manager automáticamente una etiqueta generada por el sistema en función de la frecuencia de la programación a cada instantánea o AMI.

Cada programación se inicia de forma individual en función de su frecuencia. Si se inician varias programaciones al mismo tiempo, Amazon Data Lifecycle Manager crea solo una instantánea o una AMI y aplica la configuración de retención de la programación que tiene el periodo de retención más alto. Las etiquetas de todas las programaciones iniciadas se aplican a la instantánea o la AMI.

- (Sólo políticas del ciclo de vida de las instantáneas). Si se habilita más de una de las programaciones iniciadas para la restauración rápida de instantáneas, la instantánea se

habilita para dicha restauración en todas las zonas de disponibilidad especificadas en todas las programaciones iniciadas. La configuración de retención más alta de las programaciones iniciadas se utiliza para cada zona de disponibilidad.

- Si se habilita más de una de las programaciones iniciadas para la copia entre regiones, la instantánea o la AMI se copiará en todas las regiones especificadas en todas las programaciones iniciadas. Se aplica el periodo de retención más alto de las programaciones iniciadas.

Etiquetas de recursos de destino (solo políticas personalizadas)

Las políticas personalizadas de Amazon Data Lifecycle Manager utilizan etiquetas de recursos para identificar los recursos de los que se van a realizar copias de seguridad. Al crear una política de AMI basada en EBS, puede especificar varias etiquetas de recursos de destino. La política se destinará a todos los recursos del tipo especificado (instancia o volumen) que tengan al menos una de las etiquetas de recursos de destino especificadas. Por ejemplo, si crea una política de instantáneas dirigida a los volúmenes y especifica `purpose=prod`, `costcenter=prod` y `environment=live` como etiquetas de recursos de destino, la política se dirigirá a todos los volúmenes que tengan alguno de esos pares de valores de etiqueta y clave.

Si quiere ejecutar varias políticas en un recurso, puede asignar varias etiquetas al recurso de destino y, a continuación, crear políticas independientes, cada una dirigida a una etiqueta de recurso específica.

No puede utilizar los caracteres \ o = en una clave de etiqueta. Las etiquetas de recursos de destino distinguen entre mayúsculas y minúsculas Para obtener más información, consulte Etiquetado de los recursos.

Instantáneas

Las instantáneas son el mecanismo principal para realizar copias de seguridad de los datos de los volúmenes de EBS. Para ahorrar costos de almacenamiento, las instantáneas sucesivas son incrementales y solo contienen los datos del volumen modificados desde la instantánea anterior. Cuando se elimina una instantánea de una serie de instantáneas de un volumen, solo se eliminan los datos que son exclusivos de esa instantánea. El resto del historial capturado del volumen se conserva. Para obtener más información, consulte Instantáneas de Amazon EBS.

AMI respaldadas por EBS

Una Amazon Machine Image (AMI) proporciona la información necesaria para lanzar una instancia. Cuando necesite varias instancias con la misma configuración, puede lanzarlas desde una misma AMI. Amazon Data Lifecycle Manager solo admite AMI respaldadas por EBS. Las AMI respaldadas por EBS incluyen una instantánea para cada volumen de EBS que está asociada a la instancia de origen. Para obtener más información, consulte Imagen de máquina de Amazon (AMI).

Amazon Data Lifecycle Manager etiquetas

Amazon Data Lifecycle Manager aplica las siguientes etiquetas del sistema a todas las instantáneas y las AMI que cree la política para distinguirlas de las instantáneas y las AMI que se creen por cualquier otro medio:

- `aws:dlm:lifecycle-policy-id`
- `aws:dlm:lifecycle-schedule-name`
- `aws:dlm:expirationTime`: para instantáneas que se han creado mediante programación basada en la antigüedad. Indica cuándo se eliminará la instantánea del nivel estándar.
- `dlm:managed`
- `aws:dlm:archived`: para instantáneas que se archivaron según una programación.
- `aws:dlm:pre-script`: para instantáneas creadas con scripts previos.
- `aws:dlm:post-script`: para instantáneas creadas con scripts posteriores.

También puede especificar etiquetas personalizadas que se aplicarán a las instantáneas y a las AMI en el proceso de creación. No puede utilizar los caracteres \ o = en una clave de etiqueta.

Las etiquetas de destino que Amazon Data Lifecycle Manager utiliza para asociar volúmenes a una política de instantáneas se pueden aplicar opcionalmente a las instantáneas creadas por la política. Del mismo modo, las etiquetas de destino que se utilizan para asociar instancias a una política AMI se pueden aplicar opcionalmente a las AMI creadas por la política.

Diferencias entre políticas predeterminadas y políticas personalizadas

En esta sección se comparan las políticas predeterminadas y las políticas personalizadas y se destacan sus similitudes y diferencias.

Temas

Comparación de políticas de instantáneas de EBS

En la siguiente tabla se destacan las diferencias entre la política predeterminada para las instantáneas de EBS y las políticas de instantáneas de EBS personalizadas.

Característica	Política predeterminada para las instantáneas de EBS	Política personalizada de instantán eas de EBS
Recurso de copia de seguridad administrado	Instantánea de EBS	Instantánea de EBS
Tipos de recursos de destino	Volúmenes	Volúmenes o instancias
Segmentación de recursos	Engloba todos los volúmenes de la región que no tienen instantán eas recientes. Puede especificar los parámetros de exclusión para excluir volúmenes específicos.	Engloba solo los volúmenes o instancias que tienen etiquetas específicas.
Parámetros de exclusión	Sí, puede excluir volúmenes de arranque, tipos de volúmenes específicos y volúmenes con etiquetas específicas.	Sí, puede excluir volúmenes de arranque y volúmenes con etiquetas específicas cuando se dirige a las instancias.
Support AWS Outposts	No	Sí

Característica	Política predeterminada para las instantáneas de EBS	Política personalizada de instantán eas de EBS
Compatibilidad con varias programaciones	No	Sí, hasta 4 programaciones por política
Tipos de retención admitidos	Solo retención basada en la antigüedad	Retención según la antigüedad y el recuento
Frecuencia de creación de instantáneas	Cada 1-7 días.	Frecuencia diaria, semanal, mensual, anual o personalizada mediante una expresión cron.
Retención de instantáneas	De 2 a 14 días.	Hasta 1000 instantáneas (según el recuento) o hasta 100 años (según la antigüedad).
Compatibilidad con instantáneas coherentes con las aplicaciones	No	Sí, utilizando scripts previos y posteriores
Compatibilidad con el archivo de instantáneas	No	Sí
Compatibilidad con la restaurac ión rápida de instantáneas	No	Sí
Compatibilidad con la copia entre regiones	Sí, con la configuración predeterm inada [1]	Sí, con la configuración personali zada

Característica	Política predeterminada para las instantáneas de EBS	Política personalizada de instantán eas de EBS
Compatibilidad con el uso compartido entre cuentas	No	Sí
Compatibilidad con la eliminaci ón ampliada [2]	Sí	No

[1] En el caso de las políticas predeterminadas:

- No puede copiar etiquetas en copias entre regiones.
- Las copias utilizan el mismo periodo de retención que la instantánea de origen.
- Las copias obtienen el mismo estado de cifrado que la instantánea de origen. Si la región de destino está habilitada para el cifrado de forma predeterminada, las copias siempre se cifran, incluso si las instantáneas de origen no están cifradas. Las copias siempre se cifran con la clave de KMS predeterminada para la región de destino.

[2] En el caso de las políticas predeterminadas y personalizadas:

- Si se elimina una instancia o un volumen de destino, Amazon Data Lifecycle Manager seguirá eliminando las instantáneas hasta la última, pero sin incluirla, en función del periodo de retención. En el caso de las políticas predeterminadas, puede ampliar la eliminación para incluir la última instantánea.
- Si se elimina una política o esta pasa al estado Error o Deshabilitada, Amazon Data Lifecycle Manager dejará de eliminar las instantáneas. En el caso de las políticas predeterminadas, puede ampliar la eliminación para seguir eliminando las instantáneas, incluida la última.

Comparación de políticas de AMI respaldadas por EBS

En la siguiente tabla se destacan las diferencias entre la política predeterminada para las AMI respaldadas por EBS y las políticas personalizadas de AMI respaldadas por EBS.

Característica	Política predeterminada para las AMI respaldadas por EBS	Política de AMI respaldadas por EBS personalizada
Recurso de copia de seguridad administrado	AMI respaldadas por EBS	AMI respaldadas por EBS
Tipos de recursos de destino	instancias	instancias
Segmentación de recursos	Engloba todas las instancias de la región que no tienen AMI recientes . Puede especificar los parámetros de exclusión para excluir instancias específicas.	Engloba solo las instancias que tienen etiquetas específicas.
Reiniciar las instancias antes de la creación de la AMI	No	Sí
Parámetros de exclusión	Sí, puede excluir instancias con etiquetas específicas.	No
Compatibilidad con varias programaciones	No	Sí, hasta 4 programaciones por política.
Frecuencia de creación de AMI	Cada 1-7 días.	Frecuencia diaria, semanal, mensual, anual o personalizada mediante una expresión cron.
Tipos de retención admitidos	Solo retención basada en la antigüedad.	Retención según la antigüedad y el recuento.

Característica	Política predeterminada para las AMI respaldadas por EBS	Política de AMI respaldadas por EBS personalizada
Retención de AMI	De 2 a 14 días.	Hasta 1000 AMI (según el recuento) o hasta 100 años (según la antigüedad).
Compatibilidad con la obsolescencia de AMI	No	Sí
Compatibilidad con la copia entre regiones	Sí, con la configuración predeterminada [1]	Sí, con la configuración personalizada
Compatibilidad con la eliminación ampliada [2]	Sí	No

[1] En el caso de las políticas predeterminadas:

- No puede copiar etiquetas en copias entre regiones.
- Las copias utilizan el mismo periodo de retención que la AMI de origen.
- Las copias obtienen el mismo estado de cifrado que la AMI de origen. Si la región de destino está habilitada para el cifrado de forma predeterminada, las copias siempre se cifran, incluso si las AMI de origen no están cifradas. Las copias siempre se cifran con la clave de KMS predeterminada para la región de destino.

[2] En el caso de las políticas predeterminadas y personalizadas:

- Si se cierra una instancia de destino, Amazon Data Lifecycle Manager sigue anulando el registro de las AMI hasta la última, sin incluir esta última, en función del periodo de retención. En el caso de las políticas predeterminadas, puede ampliar la anulación del registro para incluir la última AMI.
- Si se elimina una política o pasa al estado error o disabled, Amazon Data Lifecycle Manager deja de anular el registro de las AMI. En el caso de las políticas predeterminadas, puede ampliar la eliminación para seguir anulando el registro de las AMI, incluida la última.

Políticas predeterminadas

Para crear AMI periódicas respaldadas por EBS a partir de instancias, utilice la política predeterminada para las AMI respaldadas por EBS. Para crear instantáneas de todos los volúmenes, independientemente del estado de sus elementos asociados, o si desea excluir volúmenes específicos, utilice la política predeterminada para las instantáneas de EBS.

En esta sección se explica cómo crear políticas predeterminadas.

Temas

Consideraciones

Tenga en cuenta lo siguiente cuando trabaje con políticas predeterminadas:

- Las políticas predeterminadas no hacen copias de seguridad de los recursos de destino (instancias o volúmenes) que tengan copias de seguridad recientes (instantáneas o AMI). La frecuencia de creación determina los recursos de los que se hace una copia de seguridad. Solo se hace una copia de seguridad de un volumen o instancia si su última instantánea o AMI es anterior a la frecuencia de creación de la política. Por ejemplo, si especifica una frecuencia de creación de 3 días, la política predeterminada para las instantáneas de EBS solo creará una instantánea de un volumen si la última instantánea tiene más de 3 días.
- De forma predeterminada, las políticas predeterminadas se dirigen a todas las instancias o volúmenes de la región, a menos que se especifiquen los parámetros de exclusión.
- Las políticas predeterminadas crearán un conjunto mínimo de instantáneas únicas. Por ejemplo, si habilita la política de AMI respaldadas por EBS y la política de instantáneas de EBS, la política de instantáneas no duplicará las instantáneas de los volúmenes de los que la política de AMI respaldadas por EBS ya había hecho una copia de seguridad.
- Las políticas predeterminadas solo comenzarán a englobar los recursos que tengan al menos 24 horas de antigüedad.
- Si elimina un volumen o termina una instancia a la que se dirige una política predeterminada, Amazon Data Lifecycle Manager seguirá eliminando las copias de seguridad creadas

anteriormente (instantáneas o AMI) según el periodo de retención hasta la última copia de seguridad, pero sin incluirla. Elimine manualmente esta copia de seguridad si no es necesaria.

Si desea que Amazon Data Lifecycle Manager elimine la última copia de seguridad, puede activar la eliminación prolongada.

- Si se elimina una política predeterminada o esta pasa al estado Error o Deshabilitada, Amazon Data Lifecycle Manager dejará de eliminar las copias de seguridad creadas anteriormente (instantáneas o AMI). Si desea que Amazon Data Lifecycle Manager siga eliminando las copias de seguridad, incluida la última, debe activar la eliminación prolongada antes de eliminar la política o antes de que el estado de la política cambie a deshabilitada o eliminada.
- Al crear y habilitar una política predeterminada, Amazon Data Lifecycle Manager asigna de forma aleatoria los recursos específicos a un intervalo de tiempo de cuatro horas. Se hace una copia de seguridad de los recursos específicos durante el periodo asignado con la frecuencia de creación especificada. Por ejemplo, si una política tiene una frecuencia de creación de 3 días y se asigna un recurso de destino al periodo de 12:00 a 16:00 horas, se realizará una copia de seguridad de ese recurso cada 3 días entre las 12:00 y las 16:00 horas.

Política predeterminada para las instantáneas de EBS

En el siguiente procedimiento se muestra cómo crear una política predeterminada para las instantáneas de EBS.

Console

Creación de una política predeterminada para las instantáneas de EBS

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Administrador de ciclo de vida y, a continuación, elija Crear política de ciclo de vida.
3. En Tipo de política, elija Política predeterminada y, a continuación, Política de instantáneas de EBS.
4. En Description (Descripción), escriba una breve descripción de la política.
5. En Rol de IAM, elija el rol de IAM que tenga permisos para administrar instantáneas.

   Recomendamos que elija Predeterminado para utilizar el rol de IAM proporcionado por Amazon Data Lifecycle Manager. Sin embargo, también puede usar un rol de IAM personalizado creado anteriormente.

6. En Frecuencia de creación, especifique la frecuencia con la que desea que se ejecute la política y cree instantáneas de los volúmenes.

   La frecuencia que especifique también determina de qué volúmenes se van a hacer copias de seguridad. La política solo realizará copias de seguridad de los volúmenes de los que no se haya realizado ninguna otra copia de seguridad dentro de la frecuencia especificada. Por ejemplo, si especifica una frecuencia de creación de 3 días, la política solo creará instantáneas de los volúmenes de los que no se haya realizado una copia de seguridad en los últimos 3 días.
7. En Periodo de retención, especifique durante cuánto tiempo desea que la política conserve las instantáneas que crea. Cuando una instantánea alcanza el umbral de retención, se elimina automáticamente. El periodo de retención debe ser mayor o igual que la frecuencia de creación.
8. (Opcional) Configure Parámetros de exclusión para excluir volúmenes específicos de las copias de seguridad programadas. No se realizará una copia de seguridad de los volúmenes excluidos cuando se ejecute la política.

   a. Para excluir los volúmenes de arranque, seleccione Excluir los volúmenes de arranque. Si excluye los volúmenes de arranque, la política solo realizará copias de seguridad de los volúmenes de datos (que no sean de arranque). En otras palabras, no creará instantáneas de los volúmenes que estén asociados a las instancias como volumen de arranque.
   b. Para excluir tipos de volumen específicos, elija Excluir tipos de volumen específicos y, a continuación, seleccione los tipos de volumen que desee excluir. La política solo hará una copia de seguridad de los volúmenes de los tipos restantes.
   c. Para excluir los volúmenes que tienen etiquetas específicas, elija Agregar etiqueta y, a continuación, especifique las claves y los valores de las etiquetas. La política no creará instantáneas de volúmenes que tengan alguna de las etiquetas especificadas.
9. (Opcional) En Configuración avanzada, especifique las acciones adicionales que debe realizar la política.

   a. Para copiar las etiquetas de los volúmenes de origen en las instantáneas, seleccione Copiar etiquetas de los volúmenes.
   b. Con Eliminación propagada desactivada:

      - Si se elimina un volumen de origen, Amazon Data Lifecycle Manager sigue eliminando las instantáneas creadas anteriormente hasta la última, pero sin incluirla, en función

del periodo de retención. Si desea que Amazon Data Lifecycle Manager elimine todas las instantáneas, incluida la última, seleccione Eliminación prolongada.

- Si se elimina una política o esta pasa al estado `error` o `disabled`, Amazon Data Lifecycle Manager dejará de eliminar las instantáneas. Si desea que Amazon Data Lifecycle Manager siga eliminando instantáneas, incluida la última, seleccione Eliminación prolongada.

> **Note**
>
> Si habilita esta opción, anulará los dos comportamientos descritos anteriormente de forma simultánea.

c. Para copiar las instantáneas creadas por la política a otras regiones, seleccione Crear copia entre regiones y, a continuación, seleccione hasta 3 regiones de destino.

- Si la instantánea de origen está cifrada o si el cifrado está habilitado de forma predeterminada para la región de destino, las instantáneas copiadas se cifrarán con la clave de KMS predeterminada para el cifrado de EBS en la región de destino.
- Si la instantánea de origen no está cifrada y el cifrado está deshabilitado de forma predeterminada para la región de destino, las instantáneas copiadas no se cifrarán.

10. (Opcional) Para agregar una etiqueta a la política, elija Agregar etiqueta y especifique el par de clave y valor de la etiqueta.
11. Elija Crear política predeterminada.

> **Note**
>
> Si detecta un error `Role with name AWSDataLifecycleManagerDefaultRole already exists`, consulte Resolución de problemas para obtener más información.

AWS CLI

Creación de una política predeterminada para las instantáneas de EBS

Utilice el comando create-lifecycle-policy. Puede especificar los parámetros de la solicitud mediante uno de estos dos métodos, según su caso de uso o sus preferencias:

- Método 1

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy VOLUME \
--create-interval creation_frequency_in_days (1-7) \
--retain-interval retention_period_in_days (2-14) \
--copy-tags | --no-copy-tags \
--extend-deletion | --no-extend-deletion \
--cross-region-copy-targets TargetRegion=destination_region_code \
--exclusions ExcludeBootVolumes=true | false,
 ExcludeTags=[{Key=tag_key,Value=tag_value}], ExcludeVolumeTypes="standard | gp2 |
 gp3 | io1 | io2 | st1 | sc1"
```

Por ejemplo, para crear una política predeterminada para las instantáneas de EBS que se dirija a todos los volúmenes de la región, utilice el rol de IAM predeterminado, se ejecute a diario (valor predeterminado) y conserve las instantáneas durante 7 días (valor predeterminado), debe especificar los siguientes parámetros:

```
$ aws dlm create-lifecycle-policy \
--state ENABLED \
--description "Daily default snapshot policy" \
--execution-role-arn arn:aws:iam::account_id:role/
AWSDataLifecycleManagerDefaultRole \
--default-policy VOLUME
```

- Método 2

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy VOLUME \
--policy-details file://policyDetails.json
```

Donde `policyDetails.json` incluye lo siguiente:

```
{
    "PolicyLanguage": "SIMPLIFIED",
```

```
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceType": "VOLUME",
    "CopyTags": true | false,
    "CreateInterval": creation_frequency_in_days (1-7),
    "RetainInterval": retention_period_in_days (2-14),
    "ExtendDeletion": true | false,
    "CrossRegionCopyTargets": [{"TargetRegion":"destination_region_code"}],
    "Exclusions": {
        "ExcludeBootVolume": true | false,
  "ExcludeVolumeTypes": ["standard | gp2 | gp3 | io1 | io2 | st1 | sc1"],
        "ExcludeTags": [{
            "Key": "exclusion_tag_key",
            "Value": "exclusion_tag_value"
        }]
    }
}
```

Política predeterminada para las AMI respaldadas por EBS

En el siguiente procedimiento se muestra cómo crear una política predeterminada para las AMI respaldadas por EBS.

Console

Creación de una política predeterminada para las AMI respaldadas por EBS

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Lifecycle Manager y, a continuación, elija Crear política de ciclo de vida.
3. En Tipo de política, elija Política predeterminada y, a continuación, Política de AMI respaldadas por EBS.
4. En Description (Descripción), escriba una breve descripción de la política.
5. En Rol de IAM, elija el rol de IAM que tenga permisos para administrar AMI.

   Recomendamos que elija Predeterminado para utilizar el rol de IAM proporcionado por Amazon Data Lifecycle Manager. Sin embargo, también puede utilizar un rol de IAM personalizado creado anteriormente.
6. En Frecuencia de creación, especifique la frecuencia con la que desea que la política se ejecute y cree AMI de los volúmenes.

La frecuencia que especifique también determina de qué instancias se van a hacer copias de seguridad. La política solo realizará copias de seguridad de las instancias de las que no se haya realizado ninguna otra copia de seguridad dentro de la frecuencia especificada. Por ejemplo, si especifica una frecuencia de creación de 3 días, la política solo creará AMI de las instancias de las que no se haya realizado una copia de seguridad en los últimos 3 días.

7. En Periodo de retención, especifique durante cuánto tiempo desea que la política conserve las AMI que crea. Cuando una AMI alcanza el umbral de retención, su registro se anula automáticamente y sus instantáneas asociadas se eliminan. El periodo de retención debe ser mayor o igual que la frecuencia de creación.
8. (Opcional) Configure los parámetros de exclusión para excluir instancias específicas de las copias de seguridad programadas. No se realizará una copia de seguridad de las instancias excluidas cuando se ejecute la política.

   - Para excluir las instancias que tienen etiquetas específicas, elija Agregar etiqueta y, a continuación, especifique las claves y los valores de las etiquetas. La política no creará AMI a partir de instancias que tengan alguna de las etiquetas especificadas.

9. (Opcional) En Configuración avanzada, especifique las acciones adicionales que debe realizar la política.

   a. Para copiar las etiquetas asignadas de las instancias de origen en sus AMI, seleccione Copiar etiquetas de las instancias.

   b. Con la opción Eliminación prolongada deshabilitada:

      - Si se termina una instancia de origen, Amazon Data Lifecycle Manager sigue anulando el registro de las AMI creadas anteriormente hasta la última, pero sin incluirla, en función del periodo de retención. Si desea que Amazon Data Lifecycle Manager anule el registro de todas las AMI, incluida la última, seleccione Eliminación prolongada.
      - Si se elimina una política o pasa al estado `error` o `disabled`, Amazon Data Lifecycle Manager deja de anular el registro de las AMI. Si desea que Amazon Data Lifecycle Manager siga anulando el registro de las AMI, incluida la última, seleccione Eliminación prolongada.

> **Note**
>
> Si habilita la eliminación ampliada, anulará los dos comportamientos descritos anteriormente de forma simultánea.

c. Para copiar las AMI creadas por la política en otras regiones, seleccione Crear copia entre regiones y, a continuación, seleccione hasta 3 regiones de destino.

- Si la AMI de origen está cifrada o si el cifrado está habilitado de forma predeterminada para la región de destino, las AMI copiadas se cifrarán utilizando la clave de KMS predeterminada para el cifrado de EBS en la región de destino.
- Si la AMI de origen no está cifrada y el cifrado está deshabilitado de forma predeterminada para la región de destino, las AMI copiadas no se cifrarán.

10. (Opcional) Para agregar una etiqueta a la política, elija Agregar etiqueta y especifique el par de clave y valor de la etiqueta.
11. Elija Crear política predeterminada.

> **Note**
>
> Si detecta un error `Role with name AWSDataLifecycleManagerDefaultRoleForAMIManagement already exists`, consulte Resolución de problemas para obtener más información.

AWS CLI

Creación de una política predeterminada para las AMI respaldadas por EBS

Utilice el comando create-lifecycle-policy. Puede especificar los parámetros de la solicitud mediante uno de estos dos métodos, según su caso de uso o sus preferencias:

- Método 1

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
```

```
--default-policy INSTANCE \
--create-interval creation_frequency_in_days (1-7) \
--retain-interval retention_period_in_days (2-14) \
--copy-tags | --no-copy-tags \
--extend-deletion | --no-extend-deletion \
--cross-region-copy-targets TargetRegion=destination_region_code \
--exclusions ExcludeTags=[{Key=tag_key,Value=tag_value}]
```

Por ejemplo, para crear una política predeterminada para las AMI respaldadas por EBS que se dirija a todas las instancias de la región, utilice el rol de IAM predeterminado, se ejecute a diario (valor predeterminado) y conserve las instantáneas durante 7 días (valor predeterminado), debe especificar los siguientes parámetros:

```
$ aws dlm create-lifecycle-policy \
--state ENABLED \
--description "Daily default AMI policy" \
--execution-role-arn arn:aws:iam::account_id:role/
AWSDataLifecycleManagerDefaultRoleForAMIManagement \
--default-policy INSTANCE
```

- Método 2

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy INSTANCE \
--policy-details file://policyDetails.json
```

Donde `policyDetails.json` incluye lo siguiente:

```
{
    "PolicyLanguage": "SIMPLIFIED",
    "PolicyType": "IMAGE_MANAGEMENT",
    "ResourceType": "INSTANCE",
    "CopyTags": true | false,
    "CreateInterval": creation_frequency_in_days (1-7),
    "RetainInterval": retention_period_in_days (2-14),
    "ExtendDeletion": true | false,
 "CrossRegionCopyTargets": [{"TargetRegion":"destination_region_code"}],
    "Exclusions": {
        "ExcludeTags": [{
```

```
            "Key": "exclusion_tag_key",
            "Value": "exclusion_tag_value"
        }]
    }
}
```

Habilite las políticas predeterminadas en todas las cuentas y regiones

Con AWS CloudFormation StackSets él, puede activar las políticas predeterminadas de Amazon Data Lifecycle Manager en varias cuentas y AWS regiones con una sola operación.

Puede usar conjuntos apilados para habilitar las políticas predeterminadas de una de las siguientes maneras:

- En toda AWS la organización: garantiza que las políticas predeterminadas estén habilitadas y configuradas de forma coherente en toda AWS la organización o en unidades organizativas específicas de una organización. Esto se hace mediante permisos gestionados por el servicio. AWS CloudFormation StackSets crea las funciones de IAM necesarias en su nombre.
- En AWS cuentas específicas: garantiza que las políticas predeterminadas estén habilitadas y configuradas de forma coherente en todas las cuentas de destino específicas. Esto requiere permisos autogestionados. Debe crear las funciones de IAM necesarias para establecer la relación de confianza entre la cuenta de administrador del conjunto apilado y las cuentas de destino.

Para obtener más información, consulte los modelos de permisos para conjuntos apilados en la Guía del AWS CloudFormation usuario.

Utilice los siguientes procedimientos para activar las políticas predeterminadas de Amazon Data Lifecycle Manager en toda AWS la organización, en unidades organizativas específicas o en cuentas de destino específicas.

Requisitos previos

Realice una de las siguientes acciones, en función de cómo esté habilitando las políticas predeterminadas:

- (En todas AWS las organizaciones) Debe habilitar todas las funciones de su organización y activar el acceso confiable con AWS Organizations. También debe usar la cuenta de administración de la organización o una cuenta de administrador delegado.

- (En cuentas de destino específicas) Debe conceder permisos autogestionados mediante la creación de las funciones necesarias para establecer una relación de confianza entre la cuenta de administrador del conjunto de pilas y las cuentas de destino.

Console

Para habilitar las políticas predeterminadas en una AWS organización o en cuentas de destino específicas

1. Abre la AWS CloudFormation consola en https://console.aws.amazon.com/cloudformation.
2. En el panel de navegación, elija y StackSets, a continuación, elija Crear StackSet.
3. En el caso de los permisos, realice una de las siguientes acciones, en función de cómo esté habilitando las políticas predeterminadas:
   - (En toda AWS la organización) Elija permisos administrados por el servicio.
   - (En cuentas de destino específicas) Elija permisos de autoservicio. A continuación, para el ARN del rol de administrador de IAM, seleccione el rol de servicio de IAM que creó para la cuenta de administrador y, para el nombre del rol de ejecución de IAM, introduzca el nombre del rol de servicio de IAM que creó en las cuentas de destino.
4. En Preparar plantilla, selecciona Usar una plantilla de ejemplo.
5. Para las plantillas de muestra, realice una de las siguientes acciones:
   - (Política predeterminada para las instantáneas de EBS) Seleccione Crear políticas predeterminadas de Amazon Data Lifecycle Manager para las instantáneas de EBS.
   - (Política predeterminada para las AMI respaldadas por EBS) Seleccione Crear políticas predeterminadas de Amazon Data Lifecycle Manager para las AMI respaldadas por EBS.
6. Elija Siguiente.
7. Para el StackSet nombre y la StackSet descripción, introduzca un nombre descriptivo y una breve descripción.
8. En la sección Parámetros, configure los ajustes de política predeterminados según sea necesario.

> **Note**
>
> Para cargas de trabajo críticas, recomendamos CreateInterval = 1 día y RetainInterval = 7 días.

9. Elija Siguiente.
10. (Opcional) En el caso de las etiquetas, especifique etiquetas que le ayuden a identificar los recursos StackSet y a apilarlos.
11. En Ejecución gestionada, elija Activa.
12. Elija Siguiente.
13. En Add stacks to stack set (Agregar pilas al conjunto de pilas), seleccione Deploy new stacks (Implementar pilas nuevas).
14. Realice una de las siguientes acciones, en función de cómo esté habilitando las políticas predeterminadas:

    - (En toda AWS la organización) Para los objetivos de implementación, elija una de las siguientes opciones:
      - Para realizar la implementación en toda AWS la organización, elija Implementar en la organización.
      - Para realizar la implementación en unidades organizativas (OU) específicas, elija Implementar en unidades organizativas y, a continuación, para el ID de la OU, introduzca la ID de la OU. Para agregar unidades organizativas adicionales, elija Agregar otra unidad organizativa.
    - (En cuentas de destino específicas) En el caso de las cuentas, realice una de las siguientes acciones:
      - Para realizar la implementación en cuentas de destino específicas, selecciona Implementar pilas en las cuentas y, a continuación, en Números de cuenta, introduce los ID de las cuentas de destino.
      - Para realizar la implementación en todas las cuentas de una unidad organizativa específica, seleccione Implementar pila en todas las cuentas de una unidad organizativa y, a continuación, en Números de organización, introduzca el ID de la unidad organizativa de destino.
15. Para el despliegue automático, elija Activado.
16. Para ver el comportamiento de eliminación de cuentas, selecciona Conservar pilas.

17. En Especificar regiones, selecciona regiones específicas en las que habilitar las políticas predeterminadas o selecciona Agregar todas las regiones para habilitar las políticas predeterminadas en todas las regiones.
18. Elija Siguiente.
19. Revisa la configuración del conjunto de pilas, selecciona Sé que AWS CloudFormation podría crear recursos de IAM y, a continuación, selecciona Enviar.

AWS CLI

Para habilitar las políticas predeterminadas en una organización AWS

1. Cree el conjunto de pilas. Utilice el comando create-stack-set.

   En `--permission-model`, especifique `SERVICE_MANAGED`.

   Para`--template-url`, especifique una de las siguientes direcciones URL de plantilla:

   - (Políticas predeterminadas para las AMI respaldadas por EBS) `https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerAMIDefaultPolicy.yaml`
   - (Políticas predeterminadas para las instantáneas de EBS) `https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerEBSSnapshotDefaultPolicy.yaml`

   Para`--parameters`, especifique la configuración de las políticas predeterminadas. Para ver los parámetros compatibles, las descripciones de los parámetros y los valores válidos, descargue la plantilla mediante la URL y, a continuación, visualice la plantilla con un editor de texto.

   En `--auto-deployment`, especifique `Enabled=true,RetainStacksOnAccountRemoval=true`.

```
$ aws cloudformation create-stack-set \
--stack-set-name stackset_name \
--permission-model SERVICE_MANAGED \
--template-url template_url \
--parameters "ParameterKey=param_name_1,ParameterValue=param_value_1"
 "ParameterKey=param_name_2,ParameterValue=param_value_2" \
```

```
--auto-deployment "Enabled=true, RetainStacksOnAccountRemoval=true"
```

2. Implemente el conjunto de pilas. Usa el comando create-stack-instances.

   Para `--stack-set-name`, especifique el nombre del conjunto de pilas que creó en el paso anterior.

   Para `--deployment-targets OrganizationalUnitIds` ello, especifique el ID de la OU raíz para implementarla en toda la organización o los ID de la OU para implementarla en unidades organizativas específicas de la organización.

   Para `--regions`, especifique las AWS regiones en las que desea habilitar las políticas predeterminadas.

```
$ aws cloudformation create-stack-instances \
--stack-set-name stackset_name \
--deployment-targets OrganizationalUnitIds='["root_ou_id"]' | '["ou_id_1",
 "ou_id_2]' \
--regions '["region_1", "region_2"]'
```

Para habilitar las políticas predeterminadas en cuentas de destino específicas

1. Cree el conjunto de pilas. Utilice el comando create-stack-set.

   Para `--template-url`, especifique una de las siguientes direcciones URL de plantilla:

   - (Políticas predeterminadas para las AMI respaldadas por EBS) `https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerAMIDefaultPolicy.yaml`
   - (Políticas predeterminadas para las instantáneas de EBS) `https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerEBSSnapshotDefaultPolicy.yaml`

   Para `--administration-role-arn`, especifique el ARN del rol de servicio de IAM que creó anteriormente para el administrador del conjunto de pilas.

   Para `--execution-role-name`, especifique el nombre del rol de servicio de IAM que creó en las cuentas de destino.

Para `--parameters`, especifique la configuración de las políticas predeterminadas. Para ver los parámetros compatibles, las descripciones de los parámetros y los valores válidos, descargue la plantilla mediante la URL y, a continuación, visualice la plantilla con un editor de texto.

En `--auto-deployment`, especifique `Enabled=true, RetainStacksOnAccountRemoval=true`.

```
$ aws cloudformation create-stack-set \
--stack-set-name stackset_name \
--template-url template_url \
--parameters "ParameterKey=param_name_1,ParameterValue=param_value_1"
 "ParameterKey=param_name_2,ParameterValue=param_value_2" \
--administration-role-arn administrator_role_arn \
--execution-role-name target_account_role \
--auto-deployment "Enabled=true, RetainStacksOnAccountRemoval=true"
```

2. Implemente el conjunto de pilas. Usa el comando create-stack-instances.

   Para `--stack-set-name`, especifique el nombre del conjunto de pilas que creó en el paso anterior.

   Para `--accounts`, especifique los ID de las AWS cuentas de destino.

   Para `--regions`, especifique las AWS regiones en las que desea habilitar las políticas predeterminadas.

```
$ aws cloudformation create-stack-instances \
--stack-set-name stackset_name \
--accounts '["account_ID_1","account_ID_2"]' \
--regions '["region_1", "region_2"]'
```

Políticas personalizadas

En esta sección se explica cómo crear instantáneas de EBS personalizadas, AMI respaldadas por EBS y políticas de eventos de copia entre cuentas.

Temas

- Automatización de los ciclos de vida de las instantáneas

- Automatización de los ciclos de vida de las AMI
- Automatizar copias instantáneas entre cuentas

Automatización de los ciclos de vida de las instantáneas

En el siguiente procedimiento, se muestra cómo utilizar Amazon Data Lifecycle Manager para automatizar los ciclos de vida de las instantáneas de Amazon EBS.

Temas

- Para crear una política de ciclo de vida de las instantáneas
- Consideraciones sobre las políticas de ciclo de vida de instantáneas
- Recursos adicionales de
- Requisitos para usar scripts previos y posteriores
- Automatización de instantáneas coherentes con las aplicaciones con scripts previos y posteriores
- Otros casos de uso de scripts previos y posteriores
- Cómo funcionan los scripts previos y posteriores
- Identificación de las instantáneas creadas con scripts previos y posteriores
- Supervisión de la ejecución del script previo y posterior

Para crear una política de ciclo de vida de las instantáneas

Utilice alguno de los procedimientos siguientes para crear una política de ciclo de vida de instantáneas.

Console

Para crear una política de instantáneas

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Elastic Block Store, Lifecycle Manager (Administrador de ciclo de vida) y, a continuación, Create lifecycle policy (Crear política de ciclo de vida).
3. En la pantalla Select policy type (Seleccionar el tipo de política), elija EBS snapshot policy (Política de instantáneas de EBS) y, luego, seleccione Next (Siguiente).
4. En la sección Target resources (Recursos de destino), haga lo siguiente:

a. En Target resource types (Tipos de recursos de destino), elija el tipo de recurso del que se realizará una copia de seguridad. Elija `Volume` para crear instantáneas de volúmenes individuales o `Instance` para crear instantáneas de varios volúmenes a partir de los volúmenes asociados a una instancia.

b. (Solo para clientes de AWS Outpost) Especifique dónde se encuentran los recursos de destino.

   En Ubicación de los recursos de destino, especifique dónde se encuentran los recursos de destino.

   - Si los recursos de destino se encuentran en una AWS región, elija AWS Región. Amazon Data Lifecycle Manager realiza una copia de seguridad de todos los recursos del tipo especificado que tengan etiquetas de destino coincidentes solo en la región actual. Si el recurso se encuentra en una región, las instantáneas creadas por la política se almacenarán en la misma región.
   - Si los recursos de destino se encuentran en un Outpost de la cuenta, seleccione AWS Outpost. Amazon Data Lifecycle Manager realiza una copia de seguridad de todos los recursos del tipo especificado que tengan etiquetas de destino coincidentes en todos los Outposts de su cuenta. Si el recurso se encuentra en un Outpost, las instantáneas creadas por la política se pueden almacenar en la misma región o en el mismo Outpost que el recurso.
   - Si no tienes ningún Outposts en tu cuenta, esta opción está oculta y la AWS región está seleccionada para ti.

c. En Target resource tags (Etiquetas de los recursos de destino), elija las etiquetas de recursos que identifican los volúmenes o las instancias de los que se va a realizar una copia de seguridad. La política realiza una copia de seguridad solo de los recursos que tienen los pares de clave de etiqueta y valores especificados.

5. En Description (Descripción), escriba una breve descripción de la política.
6. En IAM role (Rol de IAM), elija el rol de IAM que tenga permisos para administrar instantáneas y para describir volúmenes e instancias. Para utilizar el rol predeterminado proporcionado por Amazon Data Lifecycle Manager. elija Default role (Rol predeterminado). De forma alternativa, para usar un rol de IAM personalizado que haya creado anteriormente, elija Choose another role (Elegir otro rol) y, luego, seleccione el rol que va a utilizar.
7. En Policy tags (Etiquetas de políticas), agregue las etiquetas que se aplicarán a la política de ciclo de vida. Puede utilizar estas etiquetas para identificar y clasificar las políticas.

8. Para Policy status (Estado de la política), elija Enable (Habilitar) para iniciar las ejecuciones de la política a la siguiente hora programada o Disable policy (Deshabilitar política) para evitar que se ejecute la política. Si no habilita la política ahora, no se comenzarán a crear instantáneas hasta que la habilite de forma manual después de la creación.
9. (Políticas que se dirigen solo a instancias) Excluya volúmenes de conjuntos de instantáneas de varios volúmenes.

   De forma predeterminada, Amazon Data Lifecycle Manager creará instantáneas de todos los volúmenes asociados a las instancias de destino. Sin embargo, puede optar por crear instantáneas de un subconjunto de los volúmenes adjuntos. En la sección Parameters (Parámetros), realice lo siguiente:

   - Si no desea crear instantáneas de los volúmenes raíz que se adjuntan a las instancias de destino, seleccione Exclude root volume (Excluir volumen raíz). Si selecciona esta opción, solo los volúmenes de datos (no raíz) que se adjuntan a las instancias de destino se incluirán en los conjuntos de instantáneas de varios volúmenes.
   - Si desea crear instantáneas de un subconjunto de volúmenes de datos (no raíz) adjuntos a las instancias de destino, seleccione Exclude specific data volumes (Excluir volúmenes de datos específicos) y, a continuación, especifique las etiquetas que se utilizarán para identificar los volúmenes de datos que no se deben tomar instantáneas. Amazon Data Lifecycle Manager no creará instantáneas de volúmenes de datos que tengan alguna de las etiquetas especificadas. Amazon Data Lifecycle Manager creará instantáneas de volúmenes de datos que tengan alguna de las etiquetas especificadas.
10. Elija Next (Siguiente).
11. En la pantalla Configure schedule (Configurar la programación), configure las programaciones de las políticas. Una política puede tener hasta 4 programaciones. La programación 1 es obligatoria Las programaciones 2, 3 y 4 son opcionales. Para cada programación de política que agregue, realice lo siguiente:

    a. En la sección Schedule details (Detalles de la programación), realice lo siguiente:

       i. En Schedule name (Nombre de la programación), especifique un nombre descriptivo para la programación.

       ii. En Frequency (Frecuencia) y en los campos relacionados, configure el intervalo entre las ejecuciones de la política.

Puede configurar las ejecuciones de políticas en una programación diaria, semanal, mensual o anual. Alternativamente, elija Custom cron expression (Expresión cron personalizada) para especificar un intervalo de hasta un año. Para obtener más información, consulte Expresiones cron en la Guía del usuario de Amazon CloudWatch Events.

> **Note**
>
> Si necesita habilitar el archivado de instantáneas para la programación, debe seleccionar la frecuencia mensual o anual, o bien debe especificar una expresión cron con una frecuencia de creación de al menos 28 días.
> Si especifica una frecuencia mensual que cree instantáneas en un día específico de una semana específica (por ejemplo, el segundo jueves del mes), en el caso de una programación basada en recuentos, el recuento de retención del nivel de archivo debe ser de 4 o más.

iii. En Starting at (Comenzar a), especifique la hora en la que se ha programado que comiencen las ejecuciones de la política. La primera ejecución de la política comienza una hora después de la hora programada. La hora se debe especificar con el formato `hh:mm` UTC.

iv. En Retention type (Tipo de retención), especifique la política de retención de las instantáneas creadas por la programación.

Puede retener instantáneas en función de su recuento total o de su antigüedad.

- Retención según los recuentos
  - Con el archivado de instantáneas deshabilitado, el intervalo va de `1` a `1000`. Cuando se alcanza el umbral de retención, la instantánea más antigua se elimina de forma permanente.
  - Con el archivado de instantáneas habilitado, el intervalo va de `0` (archivar inmediatamente después de la creación) a `1000`. Cuando se alcanza el umbral de retención, la instantánea más antigua se convierte en una instantánea completa y se mueve al nivel de archivo.
- Retención según la edad

- Con el archivado de instantáneas deshabilitado, el intervalo va de 1 día a 100 años. Cuando se alcanza el umbral de retención, la instantánea más antigua se elimina de forma permanente.
- Con el archivado de instantáneas habilitado, el intervalo va de 0 días (archivar inmediatamente después de la creación) a 100 años. Cuando se alcanza el umbral de retención, la instantánea más antigua se convierte en una instantánea completa y se mueve al nivel de archivo.

> **Note**
>
> - Todas las programaciones deben tener el mismo tipo de retención (basada en la antigüedad o en recuentos). Puede especificar el tipo de retención solo para la programación 1. Las programaciones 2, 3 y 4 heredan el tipo de retención de la programación 1. Cada programación puede tener su propio recuento o periodo de retención.
> - Si habilita la restauración rápida de instantáneas, la copia entre regiones o el intercambio de instantáneas, debe especificar un recuento de retención de 1 o más, o bien un período de retención de 1 días o más.

v. (solo AWS Outposts para clientes) Especifique el destino de la instantánea.

En Destino de la instantánea, especifique el destino de las instantáneas creadas por la política.

- Si la política se dirige a los recursos de una región, las instantáneas se deben crear en la misma región. AWS se selecciona por usted.
- Si la política se dirige a los recursos de un Outpost, puede elegir crear instantáneas en el mismo Outpost que el recurso de origen o en la misma región asociada al Outpost.
- Si no tienes ningún Outposts en tu cuenta, esta opción está oculta y la AWS región está seleccionada para ti.

b. Configure el etiquetado de las instantáneas.

En la sección Tagging (Etiquetado), realice lo siguiente:

i. Para copiar todas las etiquetas definidas por el usuario del volumen de origen en las instantáneas creadas por la programación, seleccione Copy tags from source (Copiar etiquetas de la fuente).

ii. Para especificar etiquetas adicionales y asignarlas a las instantáneas creadas por esta programación, elija Add tags (Agregar etiquetas).

c. Configure los scripts previos y posteriores de las instantáneas coherentes con las aplicaciones.

Para obtener más información, consulte Automatización de instantáneas coherentes con las aplicaciones con scripts previos y posteriores.

d. (Políticas que solo engloban volúmenes) Configure el archivado de instantáneas.

En la sección Archivado de instantáneas, haga lo siguiente:

> **Note**
>
> Puede habilitar el archivado de instantáneas solo para una programación de una política.

i. Para habilitar el archivado de instantáneas para la programación, seleccione Archive snapshots created by this schedule (Archivar las instantáneas creadas con esta programación).

> **Note**
>
> Puede habilitar el archivado de instantáneas solo si la frecuencia de creación de instantáneas es mensual o anual, o bien si especifica una expresión cron con una frecuencia de creación de al menos 28 días.

ii. Especifique la regla de retención para las instantáneas en el nivel de archivado.

- En programaciones basadas en recuentos, especifique el número de instantáneas que se retendrán en el nivel de archivo. Cuando se alcanza el umbral de retención, la instantánea más antigua se elimina de forma permanente del nivel de archivo. Por ejemplo, si especifica 3, la programación retendrá un máximo de

3 instantáneas en el nivel de archivo. Cuando se archiva la cuarta instantánea, se elimina la más antigua de las tres instantáneas existentes en el nivel de archivo.

- En horarios basados en la antigüedad, especifique el periodo de tiempo durante el que se van a retener las instantáneas en el nivel de archivo. Cuando se alcanza el umbral de retención, la instantánea más antigua se elimina de forma permanente del nivel de archivo. Por ejemplo, si especifica 120 días, la programación eliminará automáticamente las instantáneas del nivel de archivo cuando alcancen esa antigüedad.

> **Important**
>
> El periodo de retención mínimo de las instantáneas archivadas es de 90 días. Debe especificar una regla de retención que conserve la instantánea durante al menos 90 días.

e. Habilite la restauración rápida de instantáneas.

Para habilitar la restauración rápida de instantáneas para las instantáneas creadas por la programación, en la sección Fast snapshot restore (Restauración rápida de instantáneas), seleccione Enable fast snapshot restore (Habilitar la restauración rápida de instantáneas). Si habilita la restauración rápida de instantáneas, debe elegir las zonas de disponibilidad en las que se va a habilitar. Si la programación utiliza la retención basada en la antigüedad, debe especificar el periodo durante el cual se habilitará la restauración rápida de instantáneas para cada una de ellas. Si la programación utiliza la retención basada en el recuento, debe especificar el número máximo de instantáneas que habilitará para la restauración rápida.

Si la programación crea instantáneas en un Outpost, no puede habilitar la restauración rápida de ellas. La restauración rápida de instantáneas no es compatible con las instantáneas locales almacenadas en un Outpost.

> **Note**
>
> Se le facturará por cada minuto que se habilite la restauración rápida de instantáneas para una instantánea en una zona de disponibilidad determinada. Los cargos se prorratean con un mínimo de una hora.

f. Configure la copia entre regiones.

Para copiar instantáneas creadas por la programación en un Outpost o en una región diferente, en la sección Cross-Region copy (Copia entre regiones), seleccione Enable cross-Region copy (Habilitar la copia entre regiones).

Si la programación crea instantáneas en una región, puede copiarlas en hasta tres regiones o Outposts adicionales de su cuenta. Debe especificar una regla de copia entre regiones distinta para cada Outpost o región de destino.

Para cada Outpost o región, puede elegir diferentes políticas de retención y si desea copiar todas las etiquetas o ninguna. Si la instantánea de origen está cifrada o si está habilitado el cifrado de forma predeterminada, las instantáneas copiadas se cifrarán. Si no está cifrada, puede activar el cifrado. Si no especifica una clave de KMS, las instantáneas se cifrarán con la clave de KMS predeterminada para el cifrado de EBS en cada región de destino. Si especifica una Clave de KMS para la región de destino, el rol de IAM seleccionado debe tener acceso a la Clave de KMS.

> **Note**
>
> Debe asegurarse de no superar el número de instantáneas simultáneas por región.

Si la directiva crea instantáneas en un Outpost, no podrá copiar las instantáneas en una región o en otro Outpost y la configuración de copia entre regiones no estará disponible.

g. Configure el uso compartido entre cuentas.

Al compartir entre cuentas, configura la política para compartir automáticamente las instantáneas creadas por la programación con otras cuentas. AWS Haga lo siguiente:

i. Para habilitar el uso compartido con otras AWS cuentas, selecciona Habilitar el uso compartido entre cuentas.

ii. Para agregar las cuentas con las que compartirá las instantáneas, elija Add account (Agregar cuenta), ingrese el ID de 12 dígitos de la cuenta de AWS y elija Add (Agregar).

iii. Para dejar de compartir de forma automática las instantáneas compartidas después de un periodo específico, seleccione Unshare automatically (Dejar de compartir

automáticamente). Si elige dejar de compartir de forma automática las instantáneas compartidas, el periodo después del cual automáticamente se dejará de compartir las instantáneas no puede ser superior al periodo durante el cual la política retiene sus instantáneas. Por ejemplo, si la configuración de retención de la política retiene las instantáneas durante un periodo de 5 días, puede configurar la política para que automáticamente deje de compartir las instantáneas compartidas después de periodos de hasta 4 días. Esto se aplica a las políticas con configuraciones de retención de instantáneas basadas en la edad y en el recuento.

Si no habilita la cancelación automática del uso compartido, la instantánea se compartirá hasta que se elimine.

> **Note**
>
> Solo puede compartir instantáneas sin cifrar o cifradas mediante una Clave administrada por el cliente. No puede compartir instantáneas cifradas con la Clave de KMS de cifrado de EBS predeterminada. Si comparte instantáneas cifradas, también debe compartir la Clave de KMS que se utilizó para cifrar el volumen de origen con las cuentas de destino. Para obtener más información, consulte Permitir que los usuarios de otras cuentas utilicen una clave de KMS en la Guía para desarrolladores de AWS Key Management Service .

h. Para agregar programaciones adicionales, elija Add another schedule (Agregar otra programación), que se encuentra en la parte superior de la pantalla. En cada programación adicional, complete los campos tal como se describe con anterioridad en este tema.

i. Después de agregar las programaciones necesarias, elija Review policy (Revisar la política).

12. Revise el resumen de la política y, a continuación, elija Create policy (Crear política).

> **Note**
>
> Si detecta el error `Role with name AWSDataLifecycleManagerDefaultRole already exists`, consulte Resolución de problemas para obtener más información.

Command line

Ejecute el comando create-lifecycle-policy para crear una política de ciclo de vida de instantáneas. En `PolicyType`, especifique `EBS_SNAPSHOT_MANAGEMENT`.

> **Note**
>
> Para simplificar la sintaxis, en los siguientes ejemplos se utiliza un archivo JSON, `policyDetails.json`, que incluye los detalles de la política.

Ejemplo 1: política de ciclo de vida de instantánea con dos programaciones

En este ejemplo se crea una política de ciclo de vida de instantáneas que crea instantáneas de todos los volúmenes que tienen una clave de etiqueta de `costcenter` con un valor de 115. La política incluye dos programaciones. La primera programación crea una instantánea todos los días a las 03:00 UTC. La segunda programación crea una instantánea semanal todos los viernes a las 17:00 UTC.

```
aws dlm create-lifecycle-policy \
    --description "My volume policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

A continuación se muestra un ejemplo del archivo `policyDetails.json`.

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "VOLUME"
    ],
    "TargetTags": [{
        "Key": "costcenter",
        "Value": "115"
    }],
    "Schedules": [{
        "Name": "DailySnapshots",
        "TagsToAdd": [{
            "Key": "type",
```

```
            "Value": "myDailySnapshot"
        }],
        "CreateRule": {
            "Interval": 24,
            "IntervalUnit": "HOURS",
            "Times": [
                "03:00"
            ]
        },
        "RetainRule": {
            "Count": 5
        },
        "CopyTags": false
    },
    {
        "Name": "WeeklySnapshots",
        "TagsToAdd": [{
            "Key": "type",
            "Value": "myWeeklySnapshot"
        }],
        "CreateRule": {
            "CronExpression": "cron(0 17 ? * FRI *)"
        },
        "RetainRule": {
            "Count": 5
        },
        "CopyTags": false
    }
]}
```

Si se ejecuta correctamente, el comando devuelve el ID de la política recién creada. A continuación, se muestra un ejemplo del resultado.

```
{
   "PolicyId": "policy-0123456789abcdef0"
}
```

Ejemplo 2: política de ciclo de vida de las instantáneas que apunta a instancias y crea instantáneas de un subconjunto de volúmenes de datos (no raíz)

En este ejemplo se crea una política de ciclo de vida de instantáneas que crea conjuntos de instantáneas de varios volúmenes desde instancias con `code=production`. La política incluye

una sola programación. La programación no crea instantáneas de los volúmenes de datos etiquetados con `code=temp`.

```
aws dlm create-lifecycle-policy \
    --description "My volume policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

A continuación se muestra un ejemplo del archivo `policyDetails.json`.

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "code",
        "Value": "production"
    }],
    "Parameters": {
        "ExcludeDataVolumeTags": [{
            "Key": "code",
            "Value": "temp"
        }]
    },
    "Schedules": [{
        "Name": "DailySnapshots",
        "TagsToAdd": [{
            "Key": "type",
            "Value": "myDailySnapshot"
        }],
        "CreateRule": {
            "Interval": 24,
            "IntervalUnit": "HOURS",
            "Times": [
                "03:00"
            ]
        },
        "RetainRule": {
            "Count": 5
        },
```

```
        "CopyTags": false
    }
]}
```

Si se ejecuta correctamente, el comando devuelve el ID de la política recién creada. A continuación, se muestra un ejemplo del resultado.

```
{
   "PolicyId": "policy-0123456789abcdef0"
}
```

Ejemplo 3: política de ciclo de vida de instantáneas que automatiza las instantáneas locales de los recursos de Outpost

En este ejemplo se crea una política de ciclo de vida de instantáneas que crea instantáneas de volúmenes etiquetados con `team=dev` en todos los Outposts. La política crea las instantáneas en los mismos Outposts que los volúmenes de origen. La política crea instantáneas cada 12 horas a partir de las `00:00` UTC.

```
aws dlm create-lifecycle-policy \
    --description "My local snapshot policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

A continuación se muestra un ejemplo del archivo `policyDetails.json`.

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": "VOLUME",
 "ResourceLocations": "OUTPOST",
    "TargetTags": [{
        "Key": "team",
        "Value": "dev"
    }],
    "Schedules": [{
        "Name": "on-site backup",
        "CreateRule": {
            "Interval": 12,
            "IntervalUnit": "HOURS",
```

```
            "Times": [
                "00:00"
            ],
 "Location": [
  "OUTPOST_LOCAL"
 ]
        },
        "RetainRule": {
            "Count": 1
        },
        "CopyTags": false
    }
]}
```

Ejemplo 4: política de ciclo de vida de instantáneas que crea instantáneas en una región y las copia en un Outpost

En la siguiente política de ejemplo se crean instantáneas de volúmenes etiquetados con `team=dev`. Las instantáneas se crean en la misma región que el volumen de origen. Las instantáneas se crean cada 12 horas a partir de las `00:00` UTC y retiene un máximo de 1 instantáneas. La política también copia las instantáneas en Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`, cifra las instantáneas copiadas mediante la Clave de KMS de cifrado predeterminada y conserva las copias durante 1 un mes.

```
aws dlm create-lifecycle-policy \
    --description "Copy snapshots to Outpost" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

A continuación se muestra un ejemplo del archivo `policyDetails.json`.

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": "VOLUME",
    "ResourceLocations": "CLOUD",
    "TargetTags": [{
        "Key": "team",
        "Value": "dev"
    }],
    "Schedules": [{
```

```
        "Name": "on-site backup",
        "CopyTags": false,
        "CreateRule": {
            "Interval": 12,
            "IntervalUnit": "HOURS",
            "Times": [
                "00:00"
            ],
            "Location": "CLOUD"
        },
        "RetainRule": {
            "Count": 1
        },
        "CrossRegionCopyRules" : [
        {
            "Target": "arn:aws:outposts:us-east-1:123456789012:outpost/
op-1234567890abcdef0",
            "Encrypted": true,
            "CopyTags": true,
            "RetainRule": {
                "Interval": 1,
                "IntervalUnit": "MONTHS"
            }
        }]
    }
]}
```

Ejemplo 5: política de ciclo de vida de instantánea con una programación basada en la antigüedad y habilitada para el archivado

En este ejemplo se crea una política de ciclo de vida de instantáneas dirigida a volúmenes que están etiquetados con `Name=Prod`. La política tiene una programación basada en la antigüedad que crea instantáneas el primer día de cada mes a las 09:00 h. La programación retiene cada instantánea en el nivel estándar durante un día y después las mueve al nivel de archivo. Las instantáneas se almacenan en el nivel de archivo durante 90 días antes de que se eliminen.

```
aws dlm create-lifecycle-policy \
    --description "Copy snapshots to Outpost" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

A continuación se muestra un ejemplo del archivo `policyDetails.json`.

```
{
    "ResourceTypes": [ "VOLUME"],
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "Schedules" : [
      {
        "Name": "sched1",
        "TagsToAdd": [
          {"Key":"createdby","Value":"dlm"}
        ],
        "CreateRule": {
          "CronExpression": "cron(0 9 1 * ? *)"
        },
        "CopyTags": true,
        "RetainRule":{
          "Interval": 1,
          "IntervalUnit": "DAYS"
        },
        "ArchiveRule": {
            "RetainRule":{
              "RetentionArchiveTier": {
                 "Interval": 90,
                 "IntervalUnit": "DAYS"
              }
            }
        }
      }
    ],
    "TargetTags": [
      {
        "Key": "Name",
        "Value": "Prod"
      }
    ]
}
```

Ejemplo 6: política de ciclo de vida de instantánea con una programación basada en recuentos y habilitada para el archivado

En este ejemplo se crea una política de ciclo de vida de instantáneas dirigida a volúmenes etiquetados con `Purpose=Test`. La política tiene una programación basada en recuentos que crea instantáneas el primer día de cada mes a las 09:00 h. La programación archiva las

instantáneas inmediatamente después de su creación y retiene un máximo de tres instantáneas en el nivel de archivo.

```
aws dlm create-lifecycle-policy \
    --description "Copy snapshots to Outpost" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

A continuación se muestra un ejemplo del archivo `policyDetails.json`.

```
{
    "ResourceTypes": [ "VOLUME"],
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "Schedules" : [
      {
        "Name": "sched1",
        "TagsToAdd": [
          {"Key":"createdby","Value":"dlm"}
        ],
        "CreateRule": {
          "CronExpression": "cron(0 9 1 * ? *)"
        },
        "CopyTags": true,
        "RetainRule":{
          "Count": 0
        },
        "ArchiveRule": {
            "RetainRule":{
              "RetentionArchiveTier": {
                 "Count": 3
              }
            }
        }
      }
    ],
    "TargetTags": [
      {
        "Key": "Purpose",
        "Value": "Test"
      }
    ]
```

```
}
```

Consideraciones sobre las políticas de ciclo de vida de instantáneas

Las siguientes consideraciones generales se aplican a las políticas de ciclo de vida de instantáneas:

- Las políticas de ciclo de vida de instantáneas van dirigidas únicamente a instancias o volúmenes que se encuentran en la misma región que la política.
- La primera operación de creación de instantáneas se inicia una hora después de la hora de inicio especificada. Las operaciones posteriores de creación de instantáneas se inician una hora de su hora programada.
- Se pueden crear varias políticas para realizar una copia de seguridad de un volumen o una instancia. Por ejemplo, si un volumen tiene dos etiquetas, de las cuales la etiqueta A es el destino de la política A para crear una instantánea cada 12 horas y la etiqueta B es el destino de la política B para crear una instantánea cada 24 horas, Amazon Data Lifecycle Manager crea las instantáneas de acuerdo con las programaciones de ambas políticas. Alternativamente, puede lograr igual resultado mediante la creación de una única política que tenga varias programaciones. Por ejemplo, se puede crear una única política dirigida solo a la etiqueta A y especificar dos programaciones, una para cada 12 horas y otra para cada 24 horas.
- Las etiquetas de recursos de destino distinguen entre mayúsculas y minúsculas
- Si elimina las etiquetas de destino de un recurso al que se dirige una política, Amazon Data Lifecycle Manager deja de administrar las instantáneas existentes en el nivel estándar y en el nivel de archivo; deberá eliminarlas manualmente si ya no son necesarias.
- Si se crea una política dirigida a instancias y se adjuntan nuevos volúmenes a una instancia de destino después de crear esa política, los volúmenes recién agregados se incluirán en la copia de seguridad en la siguiente ejecución de la política. Se incluyen todos los volúmenes asociados a la instancia en el momento de la ejecución de la política.
- Si se crea una política con una programación basada en cron personalizada que está configurada para crear solo una instantánea, la política no eliminará automáticamente esa instantánea cuando se alcance el umbral de retención. Debe eliminar la instantánea de forma manual si ya no se necesita.
- Si crea una política basada en la antigüedad en la que el periodo de retención sea inferior a la frecuencia de creación, Amazon Data Lifecycle Manager retendrá siempre la última instantánea hasta que se cree la siguiente. Por ejemplo, si una política basada en la antigüedad crea una

instantánea cada mes con un periodo de retención de siete días, Amazon Data Lifecycle Manager retendrá cada instantánea durante un mes, aunque el periodo de retención sea de siete días.

Las siguientes consideraciones se aplican al archivado de instantáneas:

- Solo puede habilitar el archivado de instantáneas para las políticas de instantáneas dirigidas a los volúmenes.
- Puede especificar una regla de archivado para una sola programación para cada política.
- Si utiliza la consola, puede habilitar el archivado de instantáneas solo si la programación tiene una frecuencia de creación mensual o anual, o bien si la programación tiene una expresión cron con una frecuencia de creación de al menos 28 días.

  Si utilizas la AWS API o el AWS CLI AWS SDK, solo puedes habilitar el archivado de instantáneas si la programación tiene una expresión cron con una frecuencia de creación de al menos 28 días.
- El periodo mínimo de retención en el nivel de archivo es de 90 días.
- Cuando se archiva una instantánea, se convierte en una instantánea completa cuando se mueve al nivel de archivo. Esto puede dar lugar a mayores costos de almacenamiento de instantáneas. Para obtener más información, consulte Precios y facturación.
- La restauración rápida y el uso compartido de instantáneas están desactivados para las instantáneas cuando estas se archivan.
- Si, en el caso de un año bisiesto, la regla de retención da lugar a un periodo de retención de archivos inferior a 90 días, Amazon Data Lifecycle Manager garantiza que las instantáneas se retengan durante un periodo mínimo de 90 días.
- Si archiva de forma manual una instantánea que crea Amazon Data Lifecycle Manager y dicha instantánea sigue archivada cuando se alcanza el umbral de retención de la programación, Amazon Data Lifecycle Manager ya no administrará dicha instantánea. Sin embargo, si restaura la instantánea al nivel estándar antes de que se alcance el umbral de retención de la programación, la programación seguirá administrando la instantánea según las reglas de retención.
- Si restaura de forma permanente o temporal una instantánea que archiva Amazon Data Lifecycle Manager en el nivel estándar y dicha instantánea sigue en el nivel estándar cuando se alcanza el umbral de retención de la programación, Amazon Data Lifecycle Manager ya no administrará dicha instantánea. Sin embargo, si vuelve a archivar la instantánea antes de que se alcance el umbral de retención de la programación, la programación eliminará la instantánea cuando se alcance el umbral de retención.

- Las instantáneas que archiva Amazon Data Lifecycle Manager cuentan para las cuotas `Archived snapshots per volume` y `In-progress snapshot archives per account`.
- Si una programación no puede archivar una instantánea después de volver a intentarlo durante 24 horas, la instantánea permanece en el nivel estándar y se programa su eliminación en función del momento en el que se haya eliminado del nivel de archivo. Por ejemplo, si la programación archiva las instantáneas durante 120 días, permanecen en el nivel estándar durante 120 días después del error de archivado antes de eliminarse de forma permanente. Para los programas basados en recuentos, la instantánea no cuenta para el recuento de retención del programa.
- Las instantáneas se deben archivar en la misma región en la que se han creado. Si ha habilitado el archivado de copias e instantáneas entre regiones, Amazon Data Lifecycle Manager no archivará la copia de la instantánea.
- Las instantáneas archivadas por Amazon Data Lifecycle Manager se etiquetan con la etiqueta del sistema `aws:dlm:archived=true`. Además, las instantáneas creadas mediante una programación basada en la antigüedad y habilitada para el archivado se etiquetan con la etiqueta del sistema `aws:dlm:expirationTime`, que indica la fecha y la hora en la que se ha programado el archivado de la instantánea.

Las siguientes consideraciones se aplican para excluir los volúmenes raíz y los volúmenes de datos (no raíz):

- Si decide excluir los volúmenes de arranque y especifica etiquetas que, en consecuencia, excluyen todos los volúmenes de datos adicionales adjuntos a una instancia, Amazon Data Lifecycle Manager no creará ninguna instantánea para la instancia afectada y emitirá una `SnapshotsCreateFailed` CloudWatch métrica. Para obtener más información, consulte Supervise sus políticas utilizando CloudWatch.

Las siguientes consideraciones se aplican a la eliminación de volúmenes o terminación de instancias destinatarias de políticas de ciclo de vida de instantáneas:

- Si elimina un volumen o termina una instancia a la que se dirige una política con una programación de retención basada en recuentos, Amazon Data Lifecycle Manager ya no administrará las instantáneas en el nivel estándar y el nivel de archivo que se crearon a partir del volumen o la instancia eliminados. Debe eliminar manualmente esas instantáneas anteriores si ya no se necesitan.
- Si elimina un volumen o termina una instancia a la que se dirige una política con una programación de retención basada en la antigüedad, la política continuará con la eliminación de instantáneas

del nivel estándar y del nivel de archivo que se crearon a partir del volumen o la instancia que se eliminaron en la programación definida, hasta la última instantánea, pero sin incluirla. Debe eliminar manualmente la última instantánea si ya no la necesita.

Las siguientes consideraciones se aplican a las políticas de ciclo de vida de instantáneas y a la restauración rápida de instantáneas:

- Amazon Data Lifecycle Manager puede habilitar la restauración rápida de instantáneas solo para instantáneas con un tamaño de 16 TiB o menor. Para obtener más información, consulte Restauración rápida de instantáneas de Amazon EBS.
- Una instantánea que esté habilitada para la restauración rápida de instantáneas permanece habilitada incluso si se elimina o desactiva la política, se desactiva la restauración rápida de instantáneas para la política o se desactiva la restauración rápida de instantáneas para la zona de disponibilidad. Debe desactivar la restauración rápida para estas instantáneas manualmente.
- Si se habilita la restauración rápida de instantáneas para una política y se supera el número máximo de instantáneas que pueden habilitarse para la restauración rápida de instantáneas, Amazon Data Lifecycle Manager crea instantáneas conforme a la programación, pero no las habilita para la restauración rápida de instantáneas. Tras borrar una instantánea activada para la restauración rápida de instantáneas, la siguiente instantánea que cree Amazon Data Lifecycle Manager se activará para la restauración rápida de instantáneas.
- Cuando se habilita la restauración rápida de instantáneas para una instantánea, se necesitan 60 minutos por TiB para optimizar la instantánea. Se recomienda configurar las programaciones de modo que cada instantánea esté totalmente optimizada antes de que Amazon Data Lifecycle Manager cree la siguiente instantánea.
- Si habilita la restauración rápida de instantáneas para una política dirigida a instancias, Amazon Data Lifecycle Manager permite la restauración rápida de instantáneas para cada instantánea en el conjunto de instantáneas de varios volúmenes de forma individual. Si Amazon Data Lifecycle Manager no puede habilitar la restauración rápida de instantáneas para una de las instantáneas del conjunto de instantáneas de varios volúmenes, intentará habilitar la restauración rápida de instantáneas para las instantáneas restantes del conjunto de instantáneas.
- Se le facturará por cada minuto que se habilite la restauración rápida de instantáneas para una instantánea en una zona de disponibilidad determinada. Los cargos se prorratean con un mínimo de una hora. Para obtener más información, consulte Precios y facturación.

> **Note**
>
> En función de la configuración de las políticas de ciclo de vida, se puede disponer de varias instantáneas habilitadas para la restauración rápida de instantáneas en varias zonas de disponibilidad de manera simultánea.

Las siguientes consideraciones se aplican a las políticas de ciclo de vida de instantáneas y a los volúmenes habilitados para Multi-Attach:

- Cuando se crea una política de ciclo de vida dirigida a instancias que tienen el mismo volumen habilitado para Multi-Attach, Amazon Data Lifecycle Manager inicia una instantánea del volumen para cada instancia asociada. Utilice la etiqueta timestamp para identificar el conjunto de instantáneas en función de la marca de tiempo creadas a partir de las instancias asociadas.

Las siguientes consideraciones se aplican al uso compartido de instantáneas entre cuentas:

- Solo puede compartir instantáneas sin cifrar o cifradas mediante una Clave administrada por el cliente.
- No puede compartir instantáneas cifradas con la Clave de KMS de cifrado de EBS predeterminada.
- Si comparte instantáneas cifradas, también debe compartir la clave de KMS que se haya utilizado para cifrar el volumen de origen con las cuentas de destino. Para obtener más información, consulte Permitir que los usuarios de otras cuentas utilicen una clave de KMS en la Guía para desarrolladores de AWS Key Management Service .

Las siguientes consideraciones se aplican a las políticas de instantáneas y al archivado de instantáneas:

- Si archiva de forma manual una instantánea creada por una política y esa instantánea se encuentra en el nivel de archivo cuando se alcanza el umbral de retención de la política, Amazon Data Lifecycle Manager no eliminará la instantánea. Amazon Data Lifecycle Manager no administra instantáneas mientras se almacenan en el nivel de archivo. Si ya no necesita las instantáneas que se almacenan en la capa de archivo, debe eliminarlas manualmente.

Las siguientes consideraciones se aplican a las políticas de instantáneas y a la Papelera de reciclaje:

- Si Amazon Data Lifecycle Manager elimina una instantánea y la envía a la papelera de reciclaje cuando se alcanza el umbral de retención de la política y restaura manualmente la instantánea desde la papelera de reciclaje, debe eliminarla de forma manual cuando ya no sea necesaria. Amazon Data Lifecycle Manager dejará de administrar la instantánea.
- Si elimina manualmente una instantánea creada por una política y esa instantánea se encuentra en la papelera de reciclaje cuando se alcanza el umbral de retención de la política, Amazon Data Lifecycle Manager no eliminará la instantánea. Amazon Data Lifecycle Manager no administra instantáneas mientras se almacenan en la papelera de reciclaje.

  Si la instantánea se restaura desde la papelera de reciclaje antes de alcanzar el umbral de retención de la política, Amazon Data Lifecycle Manager eliminará la instantánea cuando se alcance el umbral de retención de la política.

  Si la instantánea se restaura desde la papelera de reciclaje una vez alcanzado el umbral de retención de la política, Amazon Data Lifecycle Manager ya no eliminará la instantánea. Debe eliminar manualmente la última instantánea cuando ya no la necesite.

Las siguientes consideraciones aplican a las políticas de ciclo de vida de instantáneas en estado error:

- Para políticas con una programación de retención basada en la edad, las instantáneas que están configuradas para caducar mientras la política está en estado `error` se conservan indefinidamente. Debe eliminar estas instantáneas manualmente. Cuando vuelve a habilitar la política, Amazon Data Lifecycle Manager reanuda la eliminación de instantáneas o anula el registro de las AMI conforme terminen los periodos de retención.
- Para las políticas con programas de retención basados en el recuento, la política deja de crear y eliminar instantáneas mientras está en estado `error`. Cuando vuelve a habilitar la política, Amazon Data Lifecycle Manager reanuda la creación de instantáneas y AMI, y reanuda la eliminación de instantáneas o AMI a medida que se alcanza el límite de retención.

Las siguientes consideraciones se aplican a las políticas y el bloqueo de instantáneas:

- Si bloquea de forma manual una instantánea que crea Amazon Data Lifecycle Manager y dicha instantánea sigue bloqueada cuando se alcanza el umbral de retención, Amazon Data Lifecycle Manager ya no administrará dicha instantánea. Debe eliminar la instantánea de forma manual si ya no se necesita.

- Si bloquea de forma manual una instantánea creada y habilitada para la restauración rápida de instantáneas por Amazon Data Lifecycle Manager y dicha instantánea sigue bloqueada cuando se alcanza el umbral de retención de la programación, Amazon Data Lifecycle Manager no deshabilitará la restauración rápida de instantáneas ni eliminará la instantánea. Debe deshabilitar de forma manual la restauración rápida de instantáneas y eliminar la instantánea si ya no se necesita.
- Si registra de forma manual una instantánea que crea Amazon Data Lifecycle Manager con una AMI y, a continuación, bloquea dicha instantánea y esa instantánea sigue bloqueada y asociada a la AMI cuando se alcanza el umbral de retención, Amazon Data Lifecycle Manager seguirá intentando eliminar dicha instantánea. Cuando se anula el registro de la AMI y se desbloquea la instantánea, Amazon Data Lifecycle Manager eliminará automáticamente dicha instantánea.

Recursos adicionales de

Para obtener más información, consulte el blog Automating Amazon EBS snapshots and AMI management using Amazon Data Lifecycle Manager AWS Storage blog.

Requisitos para usar scripts previos y posteriores

En la siguiente tabla se describen los requisitos para usar scripts previos y posteriores con Amazon Data Lifecycle Manager.

	Instantáneas coherentes con la aplicación		
Requisito	Copias de seguridad de VSS	Documento de SSM personalizado	Otros casos de uso
El agente SSM está instalado y se ejecuta en las instancias de destino	✓	✓	✓
Se cumplieron los requisitos del sistema VSS en las instancias de destino	✓		

	Instantáneas coherentes con la aplicación		
Perfil de instancia habilitado para VSS asociado a las instancias de destino	✓		
Componentes de VSS instalados en las instancias de destino	✓		
Prepare el documento SSM con comandos previos y posteriores al script		✓	✓
Prepare el rol de Amazon Data Lifecycle Manager (IAM), ejecute los scripts previos y posteriores	✓	✓	✓
Cree una política de instantáneas dirigida a las instancias y configurada para los scripts previos y posteriores	✓	✓	✓

Automatización de instantáneas coherentes con las aplicaciones con scripts previos y posteriores

Puede automatizar las instantáneas coherentes con la aplicación con Amazon Data Lifecycle Manager habilitando scripts previos y posteriores en sus políticas de ciclo de vida de instantáneas que engloben las instancias.

Amazon Data Lifecycle Manager se integra con AWS Systems Manager (Systems Manager) para admitir instantáneas coherentes con las aplicaciones. Amazon Data Lifecycle Manager utiliza documentos de comandos de Systems Manager (SSM) que incluyen scripts previos y posteriores para automatizar las acciones necesarias para completar instantáneas coherentes con las aplicaciones. Antes de que Amazon Data Lifecycle Manager inicie la creación de instantáneas, ejecuta los comandos del script previo para congelar y vaciar las E/S. Una vez que Amazon Data Lifecycle Manager inicia la creación de instantáneas, ejecuta los comandos del script posterior para descongelar las E/S.

Con Amazon Data Lifecycle Manager puede automatizar las instantáneas coherentes con las aplicaciones de lo siguiente:

- Aplicaciones de Windows con el Servicio de instantáneas de volumen (VSS)
- SAP HANA utiliza un documento SSDM AWS gestionado. Para obtener más información, consulte Amazon EBS snapshots for SAP HANA.
- Bases de datos autogestionadas, como MySQL, PostgreSQL InterSystems o IRIS, mediante plantillas de documentos SSM

Temas

Introducción a las instantáneas coherentes con las aplicaciones

En esta sección se explican los pasos que debe seguir para automatizar las instantáneas coherentes con las aplicaciones mediante Amazon Data Lifecycle Manager.

Paso 1: Preparar las instancias de destino

Debe preparar las instancias de destino para las instantáneas coherentes con las aplicaciones mediante Amazon Data Lifecycle Manager. Realice una de las siguientes acciones en función de su caso de uso.

Prepare for VSS Backups

Preparación de las instancias de destino para las copias de seguridad de VSS

1. Instale SSM Agent en las instancias de destino, si aún no está instalado. Si SSM Agent ya está instalado en las instancias de destino, omita este paso.

   Para obtener más información, consulte Instalación manual de SSM Agent en instancias de Amazon EC2 para Windows.
2. Asegúrese de que el agente SSM esté en ejecución. Para obtener más información, consulte Verificación del estado de SSM Agent e inicio del agente.
3. Configure Systems Manager para instancias de Amazon EC2. Para obtener más información, consulte Configuración de Systems Manager para instancias de Amazon EC2 en la Guía del usuario de AWS Systems Manager .
4. Asegúrese de que se cumplen los requisitos del sistema para las copias de seguridad de VSS.
5. Adjunte un perfil de instancia compatible con VSS a las instancias de destino.
6. Instale los componentes de VSS.

Prepare for SAP HANA backups

Preparación de las instancias de destino para las copias de seguridad de SAP HANA

1. Prepare el entorno de SAP HANA en sus instancias de destino.

   a. Configure su instancia con SAP HANA. Si aún no tiene un entorno de SAP HANA existente, puede consultar SAP HANA Environment Setup on AWS.

   b. Inicie sesión en SystemDB como un usuario administrador adecuado.

   c. Cree un usuario de copia de seguridad de base de datos para usarlo con Amazon Data Lifecycle Manager.

   ```
   CREATE USER username PASSWORD password NO FORCE_FIRST_PASSWORD_CHANGE;
   ```

   Por ejemplo, el siguiente comando crea un usuario llamado `dlm_user` con la contraseña `password`.

```
CREATE USER dlm_user PASSWORD password NO FORCE_FIRST_PASSWORD_CHANGE;
```

d. Asigne el rol BACKUP OPERATOR al usuario de copias de seguridad de bases de datos que creó en el paso anterior.

```
GRANT BACKUP OPERATOR TO username
```

Por ejemplo, el comando siguiente asigna el rol a un usuario denominado `dlm_user`.

```
GRANT BACKUP OPERATOR TO dlm_user
```

e. Inicie sesión en el sistema operativo como administrador, por ejemplo, *sid*`adm`.

f. Cree una entrada `hdbuserstore` para almacenar la información de conexión, de modo que el documento de SSM de SAP HANA pueda conectarse a SAP HANA sin que los usuarios tengan que ingresar la información.

```
hdbuserstore set DLM_HANADB_SNAPSHOT_USER
 localhost:3hana_instance_number13 username password
```

Por ejemplo:

```
hdbuserstore set DLM_HANADB_SNAPSHOT_USER localhost:30013 dlm_user password
```

g. Pruebe la conexión.

```
hdbsql -U DLM_HANADB_SNAPSHOT_USER "select * from dummy"
```

2. Instale SSM Agent en las instancias de destino, si aún no está instalado. Si SSM Agent ya está instalado en las instancias de destino, omita este paso.

   Para obtener más información, consulte Instalación manual de SSM Agent en instancias de Amazon EC2 para Linux.

3. Asegúrese de que SSM Agent esté en ejecución. Para obtener más información, consulte Verificación del estado de SSM Agent e inicio del agente.

4. Configure Systems Manager para instancias de Amazon EC2. Para obtener más información, consulte Configuración de Systems Manager para instancias de Amazon EC2 en la Guía del usuario de AWS Systems Manager .

Prepare for custom SSM documents

Preparación de los documentos de SSM personalizados de las instancias de destino

1. Instale SSM Agent en las instancias de destino, si aún no está instalado. Si SSM Agent ya está instalado en las instancias de destino, omita este paso.
   - (Instancias de Linux) Instalación manual de SSM Agent en instancias de Amazon EC2 para Linux
   - (Instancias de Windows) Instalación manual de SSM Agent en instancias de Amazon EC2 para Windows
2. Asegúrese de que SSM Agent esté en ejecución. Para obtener más información, consulte Verificación del estado de SSM Agent e inicio del agente.
3. Configure Systems Manager para instancias de Amazon EC2. Para obtener más información, consulte Configuración de Systems Manager para instancias de Amazon EC2 en la Guía del usuario de AWS Systems Manager .

Paso 2: Preparar el documento de SSM

> **Note**
>
> Este paso solo es necesario para los documentos de SSM personalizados. No es necesario para las copias de seguridad de VSS ni SAP HANA. Para las copias de seguridad de VSS y SAP HANA, Amazon Data Lifecycle Manager utiliza el documento SSM AWS gestionado.

Si va a automatizar instantáneas coherentes con las aplicaciones para una base de datos autogestionada, como MySQL, PostgreSQL o InterSystems IRIS, debe crear un documento de comandos SSM que incluya un script previo para congelar y vaciar las E/S antes de que se inicie la creación de las instantáneas, y un posscript para descongelar las E/S una vez iniciada la creación de las instantáneas.

Si su base de datos MySQL, PostgreSQL InterSystems o IRIS utiliza configuraciones estándar, puede crear un documento de comandos SSM utilizando el ejemplo de contenido del documento SSM que aparece a continuación. Si su base de datos MySQL, PostgreSQL InterSystems o IRIS utiliza una configuración no estándar, puede utilizar el siguiente contenido de ejemplo como punto de partida para su documento de comandos de SSM y, a continuación, personalizarlo para que se ajuste a sus necesidades. Como alternativa, si desea crear un nuevo documento de SSM desde

cero, puede utilizar la plantilla de documento de SSM vacía que aparece a continuación y agregar los comandos previos y posteriores en las secciones del documento correspondientes.

⚠ Tenga en cuenta lo siguiente:

- Es su responsabilidad asegurarse de que el documento de SSM realice las acciones correctas y necesarias para la configuración de su base de datos.
- Se garantiza que las instantáneas son coherentes con las aplicaciones solo si los scripts previos y posteriores del documento de SSM pueden congelar, vaciar y descongelar las E/S correctamente.
- El documento de SSM debe incluir los campos obligatorios para `allowedValues`, incluidos `pre-script`, `post-script` y `dry-run`. Amazon Data Lifecycle Manager ejecutará comandos en la instancia en función del contenido de esas secciones. Si su documento de SSM no incluye esas secciones, Amazon Data Lifecycle Manager lo considerará una ejecución fallida.

MySQL sample document content

```
###############################################################################
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of
 this
# software and associated documentation files (the "Software"), to deal in the
 Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
 IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###############################################################################
schemaVersion: '2.2'
description: Amazon Data Lifecycle Manager Pre/Post script for MySQL databases
```

```
parameters:
  executionId:
    type: String
    default: None
    description: (Required) Specifies the unique identifier associated with a pre
 and/or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{4}-[a-fA-F0-9]{12})$
  command:
  # Data Lifecycle Manager will trigger the pre-script and post-script actions
 during policy execution.
  # 'dry-run' option is intended for validating the document execution without
 triggering any commands
  # on the instance. The following allowedValues will allow Data Lifecycle Manager
 to successfully
  # trigger pre and post script actions.
    type: String
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
 be executed.
    allowedValues:
    - pre-script
    - post-script
    - dry-run

mainSteps:
- action: aws:runShellScript
  description: Run MySQL Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
    runCommand:
    - |
      #!/bin/bash


 ###============================================================================###
      ### Error Codes

 ###============================================================================###
```

```
    # The following Error codes will inform Data Lifecycle Manager of the type of
error
    # and help guide handling of the error.
    # The Error code will also be emitted via AWS Eventbridge events in the
'cause' field.
    # 1 Pre-script failed during execution - 201
    # 2 Post-script failed during execution - 202
    # 3 Auto thaw occurred before post-script was initiated - 203
    # 4 Pre-script initiated while post-script was expected - 204
    # 5 Post-script initiated while pre-script was expected - 205
    # 6 Application not ready for pre or post-script initiation - 206

    ###========================================================================###
    ### Global variables
    ###========================================================================###
    START=$(date +%s)
    # For testing this script locally, replace the below with OPERATION=$1.
    OPERATION={{ command }}
    FS_ALREADY_FROZEN_ERROR='freeze failed: Device or resource busy'
    FS_ALREADY_THAWED_ERROR='unfreeze failed: Invalid argument'
    FS_BUSY_ERROR='mount point is busy'

    # Auto thaw is a fail safe mechanism to automatically unfreeze the application
after the
    # duration specified in the global variable below. Choose the duration based
on your
    # database application's tolerance to freeze.
    export AUTO_THAW_DURATION_SECS="60"

    # Add all pre-script actions to be performed within the function below
    execute_pre_script() {
        echo "INFO: Start execution of pre-script"
        # Check if filesystem is already frozen. No error code indicates that
filesystem
        # is not currently frozen and that the pre-script can proceed with
freezing the filesystem.
        check_fs_freeze
        # Execute the DB commands to flush the DB in preparation for snapshot
        snap_db
        # Freeze the filesystem. No error code indicates that filesystem was
succefully frozen
        freeze_fs
```

```
        echo "INFO: Schedule Auto Thaw to execute in ${AUTO_THAW_DURATION_SECS}
seconds."
        $(nohup bash -c execute_schedule_auto_thaw  >/dev/null 2>&1 &)
    }

    # Add all post-script actions to be performed within the function below
    execute_post_script() {
        echo "INFO: Start execution of post-script"
        # Unfreeze the filesystem. No error code indicates that filesystem was
successfully unfrozen.
        unfreeze_fs
        thaw_db
    }

    # Execute Auto Thaw to automatically unfreeze the application after the
duration configured
    # in the AUTO_THAW_DURATION_SECS global variable.
    execute_schedule_auto_thaw() {
        sleep ${AUTO_THAW_DURATION_SECS}
        execute_post_script
    }

    # Disable Auto Thaw if it is still enabled
    execute_disable_auto_thaw() {
        echo "INFO: Attempting to disable auto thaw if enabled"
        auto_thaw_pgid=$(pgrep -f execute_schedule_auto_thaw | xargs -i ps -hp {}
-o pgid)
        if [ -n "${auto_thaw_pgid}" ]; then
            echo "INFO: execute_schedule_auto_thaw process found with pgid
${auto_thaw_pgid}"
            sudo pkill -g ${auto_thaw_pgid}
            rc=$?
            if [ ${rc} != 0 ]; then
                echo "ERROR: Unable to kill execute_schedule_auto_thaw process.
retval=${rc}"
            else
                echo "INFO: Auto Thaw  has been disabled"
            fi
        fi
    }

    # Iterate over all the mountpoints and check if filesystem is already in
freeze state.
    # Return error code 204 if any of the mount points are already frozen.
```

```
    check_fs_freeze() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
            # Hence, we will skip the root and boot mountpoints while checking if
filesystem is in freeze state.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi

            error_message=$(sudo mount -o remount,noatime $target 2>&1)
            # Remount will be a no-op without a error message if the filesystem is
unfrozen.
            # However, if filesystem is already frozen, remount will fail with
busy error message.
            if [ $? -ne 0 ];then
                # If the filesystem is already in frozen, return error code 204
                if [[ "$error_message" == *"$FS_BUSY_ERROR"* ]];then
                    echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"
                    exit 204
                fi
                # If the check filesystem freeze failed due to any reason other
than the filesystem already frozen, return 201
                echo "ERROR: Failed to check_fs_freeze on mountpoint $target due
to error - $errormessage"
                exit 201
            fi
        done
    }

    # Iterate over all the mountpoints and freeze the filesystem.
    freeze_fs() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous. Hence, skip
filesystem freeze
            # operations for root and boot mountpoints.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi
            echo "INFO: Freezing $target"
            error_message=$(sudo fsfreeze -f $target 2>&1)
            if [ $? -ne 0 ];then
                # If the filesystem is already in frozen, return error code 204
```

```
                if [[ "$error_message" == *"$FS_ALREADY_FROZEN_ERROR"* ]]; then
                    echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"
                    sudo mysql -e 'UNLOCK TABLES;'
                    exit 204
                fi
                # If the filesystem freeze failed due to any reason other than the
filesystem already frozen, return 201
                echo "ERROR: Failed to freeze mountpoint $targetdue due to error -
$errormessage"
                thaw_db
                exit 201
            fi
            echo "INFO: Freezing complete on $target"
        done
    }

    # Iterate over all the mountpoints and unfreeze the filesystem.
    unfreeze_fs() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
            # Hence, will skip the root and boot mountpoints during unfreeze as
well.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi
            echo "INFO: Thawing $target"
            error_message=$(sudo fsfreeze -u $target 2>&1)
            # Check if filesystem is already unfrozen (thawed). Return error code
204 if filesystem is already unfrozen.
            if [ $? -ne 0 ]; then
                if [[ "$error_message" == *"$FS_ALREADY_THAWED_ERROR"* ]]; then
                    echo "ERROR: Filesystem ${target} is already in thaw state.
Return Error Code: 205"
                    exit 205
                fi
                # If the filesystem unfreeze failed due to any reason other than
the filesystem already unfrozen, return 202
                echo "ERROR: Failed to unfreeze mountpoint $targetdue due to error
- $errormessage"
                exit 202
            fi
            echo "INFO: Thaw complete on $target"
```

```
        done
    }

    snap_db() {
        # Run the flush command only when MySQL DB service is up and running
        sudo systemctl is-active --quiet mysqld.service
        if [ $? -eq 0 ]; then
            echo "INFO: Execute MySQL Flush and Lock command."
            sudo mysql -e 'FLUSH TABLES WITH READ LOCK;'
            # If the MySQL Flush and Lock command did not succeed, return error
code 201 to indicate pre-script failure
            if [ $? -ne 0 ]; then
                echo "ERROR: MySQL FLUSH TABLES WITH READ LOCK command failed."
                exit 201
            fi
            sync
        else
            echo "INFO: MySQL service is inactive. Skipping execution of MySQL
Flush and Lock command."
        fi
    }

    thaw_db() {
        # Run the unlock command only when MySQL DB service is up and running
        sudo systemctl is-active --quiet mysqld.service
        if [ $? -eq 0 ]; then
            echo "INFO: Execute MySQL Unlock"
            sudo mysql -e 'UNLOCK TABLES;'
        else
            echo "INFO: MySQL service is inactive. Skipping execution of MySQL
Unlock command."
        fi
    }

    export -f execute_schedule_auto_thaw
    export -f execute_post_script
    export -f unfreeze_fs
    export -f thaw_db

    # Debug logging for parameters passed to the SSM document
    echo "INFO: ${OPERATION} starting at $(date) with executionId:
${EXECUTION_ID}"

    # Based on the command parameter value execute the function that supports
```

```
      # pre-script/post-script operation
      case ${OPERATION} in
          pre-script)
              execute_pre_script
              ;;
          post-script)
              execute_post_script
              execute_disable_auto_thaw
              ;;
          dry-run)
              echo "INFO: dry-run option invoked - taking no action"
              ;;
          *)
              echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
              exit 1 # return failure
              ;;
      esac

      END=$(date +%s)
      # Debug Log for profiling the script time
      echo "INFO: ${OPERATION} completed at $(date). Total runtime: $((${END} -
 ${START})) seconds."
```

PostgreSQL sample document content

```
###############################################################################
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of
 this
# software and associated documentation files (the "Software"), to deal in the
 Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
 IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
```

```
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###============================================================================###
schemaVersion: '2.2'
description: Amazon Data Lifecycle Manager Pre/Post script for PostgreSQL databases
parameters:
  executionId:
    type: String
    default: None
    description: (Required) Specifies the unique identifier associated with a pre
 and/or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{4}-[a-fA-F0-9]{12})$
  command:
  # Data Lifecycle Manager will trigger the pre-script and post-script actions
 during policy execution.
  # 'dry-run' option is intended for validating the document execution without
 triggering any commands
  # on the instance. The following allowedValues will allow Data Lifecycle Manager
 to successfully
  # trigger pre and post script actions.
    type: String
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
 be executed.
    allowedValues:
    - pre-script
    - post-script
    - dry-run

mainSteps:
- action: aws:runShellScript
  description: Run PostgreSQL Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
    runCommand:
    - |
      #!/bin/bash


 ###============================================================================###
```

```
    ### Error Codes

###================================================================================###
    # The following Error codes will inform Data Lifecycle Manager of the type of
error
    # and help guide handling of the error.
    # The Error code will also be emitted via AWS Eventbridge events in the
'cause' field.
    # 1 Pre-script failed during execution - 201
    # 2 Post-script failed during execution - 202
    # 3 Auto thaw occurred before post-script was initiated - 203
    # 4 Pre-script initiated while post-script was expected - 204
    # 5 Post-script initiated while pre-script was expected - 205
    # 6 Application not ready for pre or post-script initiation - 206


###================================================================================###
    ### Global variables

###================================================================================###
    START=$(date +%s)
    OPERATION={{ command }}
    FS_ALREADY_FROZEN_ERROR='freeze failed: Device or resource busy'
    FS_ALREADY_THAWED_ERROR='unfreeze failed: Invalid argument'
    FS_BUSY_ERROR='mount point is busy'

    # Auto thaw is a fail safe mechanism to automatically unfreeze the application
after the
    # duration specified in the global variable below. Choose the duration based
on your
    # database application's tolerance to freeze.
    export AUTO_THAW_DURATION_SECS="60"

    # Add all pre-script actions to be performed within the function below
    execute_pre_script() {
        echo "INFO: Start execution of pre-script"
        # Check if filesystem is already frozen. No error code indicates that
filesystem
        # is not currently frozen and that the pre-script can proceed with
freezing the filesystem.
        check_fs_freeze
        # Execute the DB commands to flush the DB in preparation for snapshot
        snap_db
```

```
        # Freeze the filesystem. No error code indicates that filesystem was
succefully frozen
        freeze_fs

        echo "INFO: Schedule Auto Thaw to execute in ${AUTO_THAW_DURATION_SECS}
seconds."
        $(nohup bash -c execute_schedule_auto_thaw  >/dev/null 2>&1 &)
    }

    # Add all post-script actions to be performed within the function below
    execute_post_script() {
        echo "INFO: Start execution of post-script"
        # Unfreeze the filesystem. No error code indicates that filesystem was
successfully unfrozen
        unfreeze_fs
    }

    # Execute Auto Thaw to automatically unfreeze the application after the
duration configured
    # in the AUTO_THAW_DURATION_SECS global variable.
    execute_schedule_auto_thaw() {
        sleep ${AUTO_THAW_DURATION_SECS}
        execute_post_script
    }

    # Disable Auto Thaw if it is still enabled
    execute_disable_auto_thaw() {
        echo "INFO: Attempting to disable auto thaw if enabled"
        auto_thaw_pgid=$(pgrep -f execute_schedule_auto_thaw | xargs -i ps -hp {}
-o pgid)
        if [ -n "${auto_thaw_pgid}" ]; then
            echo "INFO: execute_schedule_auto_thaw process found with pgid
${auto_thaw_pgid}"
            sudo pkill -g ${auto_thaw_pgid}
            rc=$?
            if [ ${rc} != 0 ]; then
                echo "ERROR: Unable to kill execute_schedule_auto_thaw process.
retval=${rc}"
            else
                echo "INFO: Auto Thaw  has been disabled"
            fi
        fi
    }
```

```
    # Iterate over all the mountpoints and check if filesystem is already in
freeze state.
    # Return error code 204 if any of the mount points are already frozen.
    check_fs_freeze() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
            # Hence, we will skip the root and boot mountpoints while checking if
filesystem is in freeze state.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi

            error_message=$(sudo mount -o remount,noatime $target 2>&1)
            # Remount will be a no-op without a error message if the filesystem is
unfrozen.
            # However, if filesystem is already frozen, remount will fail with
busy error message.
            if [ $? -ne 0 ];then
                # If the filesystem is already in frozen, return error code 204
                if [[ "$error_message" == *"$FS_BUSY_ERROR"* ]];then
                    echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"
                    exit 204
                fi
                # If the check filesystem freeze failed due to any reason other
than the filesystem already frozen, return 201
                echo "ERROR: Failed to check_fs_freeze on mountpoint $target due
to error - $errormessage"
                exit 201
            fi
        done
    }

    # Iterate over all the mountpoints and freeze the filesystem.
    freeze_fs() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous. Hence, skip
filesystem freeze
            # operations for root and boot mountpoints.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi
            echo "INFO: Freezing $target"
```

```
            error_message=$(sudo fsfreeze -f $target 2>&1)
            if [ $? -ne 0 ];then
                # If the filesystem is already in frozen, return error code 204
                if [[ "$error_message" == *"$FS_ALREADY_FROZEN_ERROR"* ]]; then
                    echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"
                    exit 204
                fi
                # If the filesystem freeze failed due to any reason other than the
filesystem already frozen, return 201
                echo "ERROR: Failed to freeze mountpoint $targetdue due to error -
$errormessage"
                exit 201
            fi
            echo "INFO: Freezing complete on $target"
        done
    }

    # Iterate over all the mountpoints and unfreeze the filesystem.
    unfreeze_fs() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
            # Hence, will skip the root and boot mountpoints during unfreeze as
well.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi
            echo "INFO: Thawing $target"
            error_message=$(sudo fsfreeze -u $target 2>&1)
            # Check if filesystem is already unfrozen (thawed). Return error code
204 if filesystem is already unfrozen.
            if [ $? -ne 0 ]; then
                if [[ "$error_message" == *"$FS_ALREADY_THAWED_ERROR"* ]]; then
                    echo "ERROR: Filesystem ${target} is already in thaw state.
Return Error Code: 205"
                    exit 205
                fi
                # If the filesystem unfreeze failed due to any reason other than
the filesystem already unfrozen, return 202
                echo "ERROR: Failed to unfreeze mountpoint $targetdue due to error
- $errormessage"
                exit 202
            fi
```

```
            echo "INFO: Thaw complete on $target"
        done
    }

    snap_db() {
        # Run the flush command only when PostgreSQL DB service is up and running
        sudo systemctl is-active --quiet postgresql
        if [ $? -eq 0 ]; then
            echo "INFO: Execute Postgres CHECKPOINT"
            # PostgreSQL command to flush the transactions in memory to disk
            sudo -u postgres psql -c 'CHECKPOINT;'
            # If the PostgreSQL Command did not succeed, return error code 201 to
indicate pre-script failure
            if [ $? -ne 0 ]; then
                echo "ERROR: Postgres CHECKPOINT command failed."
                exit 201
            fi
            sync
        else
            echo "INFO: PostgreSQL service is inactive. Skipping execution of
CHECKPOINT command."
        fi
    }

    export -f execute_schedule_auto_thaw
    export -f execute_post_script
    export -f unfreeze_fs

    # Debug logging for parameters passed to the SSM document
    echo "INFO: ${OPERATION} starting at $(date) with executionId:
${EXECUTION_ID}"

    # Based on the command parameter value execute the function that supports
    # pre-script/post-script operation
    case ${OPERATION} in
        pre-script)
            execute_pre_script
            ;;
        post-script)
            execute_post_script
            execute_disable_auto_thaw
            ;;
        dry-run)
            echo "INFO: dry-run option invoked - taking no action"
```

```
            ;;
        *)
            echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
            exit 1 # return failure
            ;;
    esac

    END=$(date +%s)
    # Debug Log for profiling the script time
    echo "INFO: ${OPERATION} completed at $(date). Total runtime: $((${END} -
 ${START})) seconds."
```

InterSystems IRIS sample document content

```
###############################################################################
# MIT License
#
# Copyright (c) 2024 InterSystems
#
# Permission is hereby granted, free of charge, to any person obtaining a copy
# of this software and associated documentation files (the "Software"), to deal
# in the Software without restriction, including without limitation the rights
# to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
# copies of the Software, and to permit persons to whom the Software is
# furnished to do so, subject to the following conditions:
#
# The above copyright notice and this permission notice shall be included in all
# copies or substantial portions of the Software.
#
# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
# IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
# FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
# AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
# LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
# OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
# SOFTWARE.
###############################################################################
schemaVersion: '2.2'
description: SSM Document Template for Amazon Data Lifecycle Manager Pre/Post script
 feature for InterSystems IRIS.
parameters:
  executionId:
```

```
    type: String
    default: None
    description: Specifies the unique identifier associated with a pre and/or post
 execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{4}-[a-fA-F0-9]{12})$
  command:
    type: String
    # Data Lifecycle Manager will trigger the pre-script and post-script actions.
 You can also use this SSM document with 'dry-run' for manual testing purposes.
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
 be executed.
    #The following allowedValues will allow Data Lifecycle Manager to successfully
 trigger pre and post script actions.
    allowedValues:
    - pre-script
    - post-script
    - dry-run

mainSteps:
- action: aws:runShellScript
  description: Run InterSystems IRIS Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
    runCommand:
    - |
      #!/bin/bash

 ###============================================================================###
      ### Global variables

 ###============================================================================###
      DOCKER_NAME=iris
      LOGDIR=./
      EXIT_CODE=0
      OPERATION={{ command }}
      START=$(date +%s)

      # Check if Docker is installed
```

```
     # By default if Docker is present, script assumes that InterSystems IRIS is
 running in Docker
     # Leave only the else block DOCKER_EXEC line, if you run InterSystems IRIS
 non-containerised (and Docker is present).
     # Script assumes irissys user has OS auth enabled, change the OS user or
 supply login/password depending on your configuration.
     if command -v docker &> /dev/null
     then
       DOCKER_EXEC="docker exec $DOCKER_NAME"
     else
       DOCKER_EXEC="sudo -i -u irissys"
     fi


     # Add all pre-script actions to be performed within the function below
     execute_pre_script() {
       echo "INFO: Start execution of pre-script"

       # find all iris running instances
       iris_instances=$($DOCKER_EXEC iris qall 2>/dev/null | tail -n +3 | grep
 '^up' | cut -c5-  | awk '{print $1}')
       echo "`date`: Running iris instances $iris_instances"

       # Only for running instances
       for INST in $iris_instances; do

         echo "`date`: Attempting to freeze $INST"

         # Detailed instances specific log
         LOGFILE=$LOGDIR/$INST-pre_post.log

         #check Freeze status before starting
         $DOCKER_EXEC irissession $INST -U '%SYS'
 "##Class(Backup.General).IsWDSuspendedExt()"
         freeze_status=$?
         if [ $freeze_status -eq 5 ]; then
           echo "`date`:   ERROR: $INST IS already FROZEN"
           EXIT_CODE=204
         else
           echo "`date`:   $INST is not frozen"
           # Freeze
           # Docs: https://docs.intersystems.com/irislatest/csp/documatic/
%25CSP.Documatic.cls?LIBRARY=%25SYS&CLASSNAME=Backup.General#ExternalFreeze
```

```
            $DOCKER_EXEC irissession $INST -U '%SYS'
"##Class(Backup.General).ExternalFreeze(\"$LOGFILE\",,,,,,600,,,300)"
            status=$?

            case $status in
              5) echo "`date`:   $INST IS FROZEN"
                ;;
              3) echo "`date`:   $INST FREEZE FAILED"
                EXIT_CODE=201
                ;;
              *) echo "`date`:   ERROR: Unknown status code: $status"
                EXIT_CODE=201
                ;;
            esac
            echo "`date`:   Completed freeze of $INST"
          fi
        done
        echo "`date`: Pre freeze script finished"
      }

      # Add all post-script actions to be performed within the function below
      execute_post_script() {
        echo "INFO: Start execution of post-script"

        # find all iris running instances
        iris_instances=$($DOCKER_EXEC iris qall 2>/dev/null | tail -n +3 | grep
'^up' | cut -c5-  | awk '{print $1}')
        echo "`date`: Running iris instances $iris_instances"

        # Only for running instances
        for INST in $iris_instances; do

          echo "`date`: Attempting to thaw $INST"

          # Detailed instances specific log
          LOGFILE=$LOGDIR/$INST-pre_post.log

          #check Freeze status befor starting
          $DOCKER_EXEC irissession $INST -U '%SYS'
"##Class(Backup.General).IsWDSuspendedExt()"
          freeze_status=$?
          if [ $freeze_status -eq 5 ]; then
            echo "`date`:  $INST is in frozen state"
            # Thaw
```

```
            # Docs: https://docs.intersystems.com/irislatest/csp/documatic/
%25CSP.Documatic.cls?LIBRARY=%25SYS&CLASSNAME=Backup.General#ExternalFreeze
            $DOCKER_EXEC irissession $INST -U%SYS
 "##Class(Backup.General).ExternalThaw(\"$LOGFILE\")"
            status=$?

            case $status in
              5) echo "`date`:   $INST IS THAWED"
                  $DOCKER_EXEC irissession $INST -U%SYS
 "##Class(Backup.General).ExternalSetHistory(\"$LOGFILE\")"
                ;;
              3) echo "`date`:   $INST THAW FAILED"
                  EXIT_CODE=202
                ;;
              *) echo "`date`:   ERROR: Unknown status code: $status"
                  EXIT_CODE=202
                ;;
            esac
            echo "`date`:   Completed thaw of $INST"
          else
            echo "`date`:   ERROR: $INST IS already THAWED"
            EXIT_CODE=205
          fi
        done
        echo "`date`: Post thaw script finished"
      }

      # Debug logging for parameters passed to the SSM document
        echo "INFO: ${OPERATION} starting at $(date) with executionId:
 ${EXECUTION_ID}"

      # Based on the command parameter value execute the function that supports
      # pre-script/post-script operation
      case ${OPERATION} in
        pre-script)
          execute_pre_script
          ;;
        post-script)
          execute_post_script
            ;;
        dry-run)
          echo "INFO: dry-run option invoked - taking no action"
          ;;
        *)
```

```
          echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
          # return failure
          EXIT_CODE=1
          ;;
      esac

      END=$(date +%s)
      # Debug Log for profiling the script time
      echo "INFO: ${OPERATION} completed at $(date). Total runtime: $((${END} -
 ${START})) seconds."
      exit $EXIT_CODE
```

Para obtener más información, consulte el repositorio. GitHub

Empty document template

```
###======================================================================###
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of
 this
# software and associated documentation files (the "Software"), to deal in the
 Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
 IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###======================================================================###
schemaVersion: '2.2'
description: SSM Document Template for Amazon Data Lifecycle Manager Pre/Post script
 feature
parameters:
  executionId:
    type: String
    default: None
```

```
    description: (Required) Specifies the unique identifier associated with a pre
 and/or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{4}-[a-fA-F0-9]{12})$
  command:
  # Data Lifecycle Manager will trigger the pre-script and post-script actions
 during policy execution.
  # 'dry-run' option is intended for validating the document execution without
 triggering any commands
  # on the instance. The following allowedValues will allow Data Lifecycle Manager
 to successfully
  # trigger pre and post script actions.
    type: String
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
 be executed.
    allowedValues:
    - pre-script
    - post-script
    - dry-run

mainSteps:
- action: aws:runShellScript
  description: Run Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
    runCommand:
    - |
      #!/bin/bash


 ###============================================================================###
      ### Error Codes

 ###============================================================================###
      # The following Error codes will inform Data Lifecycle Manager of the type of
 error
      # and help guide handling of the error.
      # The Error code will also be emitted via AWS Eventbridge events in the
 'cause' field.
```

```
    # 1 Pre-script failed during execution - 201
    # 2 Post-script failed during execution - 202
    # 3 Auto thaw occurred before post-script was initiated - 203
    # 4 Pre-script initiated while post-script was expected - 204
    # 5 Post-script initiated while pre-script was expected - 205
    # 6 Application not ready for pre or post-script initiation - 206


###============================================================================###
    ### Global variables

###============================================================================###
    START=$(date +%s)
    # For testing this script locally, replace the below with OPERATION=$1.
    OPERATION={{ command }}

    # Add all pre-script actions to be performed within the function below
    execute_pre_script() {
        echo "INFO: Start execution of pre-script"
    }

    # Add all post-script actions to be performed within the function below
    execute_post_script() {
        echo "INFO: Start execution of post-script"
    }

    # Debug logging for parameters passed to the SSM document
    echo "INFO: ${OPERATION} starting at $(date) with executionId:
${EXECUTION_ID}"

    # Based on the command parameter value execute the function that supports
    # pre-script/post-script operation
    case ${OPERATION} in
        pre-script)
            execute_pre_script
            ;;
        post-script)
            execute_post_script
            ;;
        dry-run)
            echo "INFO: dry-run option invoked - taking no action"
            ;;
        *)
```

```
              echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
              exit 1 # return failure
              ;;
      esac

      END=$(date +%s)
      # Debug Log for profiling the script time
      echo "INFO: ${OPERATION} completed at $(date). Total runtime: $((${END} -
 ${START})) seconds."
```

Una vez que tenga el contenido del documento de SSM, utilice uno de los procedimientos siguientes para crear el documento de SSM personalizado.

Console

Creación del documento de comandos de SSM

1. Abra la AWS Systems Manager consola en https://console.aws.amazon.com//systems-manager/.
2. En el panel de navegación, seleccione Documentos y, a continuación, seleccione Crear documento, Comando o sesión.
3. En Name (Nombre), ingrese un nombre descriptivo para el documento.
4. En Tipo de destino, seleccione/AWS::EC2::Instance.
5. En Tipo de documento, seleccione Comando.
6. En el campo Contenido, seleccione YAML y, a continuación, pegue el contenido del documento.
7. En la sección Etiquetas de documento, agregue una etiqueta con una clave de etiqueta de `DLMScriptsAccess` y un valor de etiqueta de `true`.

> **Important**
>
> La `DLMScriptsAccess:true` etiqueta la exige la política AWSDataLifecycleManagerSSMFullAccess AWS gestionada utilizada en el paso 3: Preparar la función de IAM de Amazon Data Lifecycle Manager. La política usa la clave de condición `aws:ResourceTag` para restringir el acceso a los documentos de SSM que tienen esta etiqueta.

8. Elija Create document (Crear documento).

AWS CLI

Creación del documento de comandos de SSM

Utilice el comando create-document. En `--name`, especifique un nombre descriptivo del documento. En `--document-type`, especifique `Command`. En `--content`, especifique la ruta al archivo .yaml con el contenido del documento de SSM. En `--tags`, especifique `"Key=DLMScriptsAccess,Value=true"`.

```
$ aws ssm create-document \
--content file://path/to/file/documentContent.yaml \
--name "document_name" \
--document-type "Command" \
--document-format YAML \
--tags "Key=DLMScriptsAccess,Value=true"
```

Paso 3: preparar el rol de IAM de Amazon Data Lifecycle Manager

> **Note**
>
> Este paso es necesario si:
>
> - Debe crear o actualizar una política de instantáneas con scripts previos o posteriores que utilice un rol de IAM personalizado.
> - La línea de comandos se utiliza para crear o actualizar una política de instantáneas habilitada para scripts previos o posteriores que utilice el rol predeterminado.
>
> Si utiliza la consola para crear o actualizar una política de instantáneas previa o posterior a las secuencias de comandos que utilice la función predeterminada para gestionar las instantáneas () AWSDataLifecycleManagerDefaultRole, omita este paso. En este caso, asociamos automáticamente la política a ese rol. AWSDataLifecycleManagerSSMFullAccess

Debe asegurarse de que el rol de IAM que utilice para la política conceda permiso a Amazon Data Lifecycle Manager para realizar las acciones de SSM necesarias para ejecutar scripts previos y posteriores en las instancias incluidas en la política.

Amazon Data Lifecycle Manager proporciona una política gestionada (AWSDataLifecycleManagerSSMFullAccess) que incluye los permisos necesarios. Puede asociar esta política a su rol de IAM para administrar las instantáneas y asegurarse de que incluya los permisos.

> **Important**
>
> La política AWSDataLifecycleManagerSSMFullAccess gestionada utiliza la clave de `aws:ResourceTag` condición para restringir el acceso a documentos SSM específicos cuando se utilizan scripts previos y posteriores. Para permitir que Amazon Data Lifecycle Manager acceda a los documentos de SSM, debe asegurarse de que sus documentos de SSM estén etiquetados con `DLMScriptsAccess:true`.

Como alternativa, puede crear manualmente una política personalizada o asignar los permisos necesarios directamente al rol de IAM que utilice. Puede utilizar los mismos permisos que se definen en la política AWSDataLifecycleManagerSSMFullAccess gestionada; sin embargo, la clave de `aws:ResourceTag` condición es opcional. Si decide no incluir esa clave de condición, no necesitará etiquetar sus documentos de SSM con `DLMScriptsAccess:true`.

Utilice uno de los siguientes métodos para añadir la AWSDataLifecycleManagerSSMFullAccesspolítica a su función de IAM.

Console

Asociación de la política administrada a su rol personalizado

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, elija Roles.
3. Busque y seleccione el rol personalizado para administrar instantáneas.
4. En la pestaña Permisos, elija Agregar permisos, Asociar políticas.
5. Busque y seleccione la política AWSDataLifecycleManagerSSMFullAccessgestionada y, a continuación, elija Añadir permisos.

AWS CLI

Asociación de la política administrada a su rol personalizado

Utilice el comando attach-role-policy. En `---role-name`, especifique el nombre de su rol personalizado. En `--policy-arn`, especifique `arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess`.

```
$ aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess \
--role-name your_role_name
```

Paso 4: crear una política de ciclo de vida de las instantáneas

Para automatizar las instantáneas coherentes con la aplicación, debe crear una política de ciclo de vida de las instantáneas que englobe las instancias y configurar los scripts previos y posteriores para esa política.

Console

Creación de una política de ciclo de vida de las instantáneas

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Elastic Block Store, Lifecycle Manager (Administrador de ciclo de vida) y, a continuación, Create lifecycle policy (Crear política de ciclo de vida).
3. En la pantalla Select policy type (Seleccionar el tipo de política), elija EBS snapshot policy (Política de instantáneas de EBS) y, luego, seleccione Next (Siguiente).
4. En la sección Target resources (Recursos de destino), haga lo siguiente:
   a. En Tipos de recursos de destino, elija `Instance`.
   b. En Etiquetas de recursos de destino, especifique las etiquetas de recursos que identifican las instancias de las que se va a realizar una copia de seguridad. Solo se realizará una copia de seguridad de los recursos que tengan las etiquetas especificadas.
5. Para el rol de IAM, elija AWSDataLifecycleManagerDefaultRole(el rol predeterminado para administrar las instantáneas) o elija un rol personalizado que haya creado y preparado para los guiones previos y posteriores.
6. Configure las programaciones y las opciones adicionales según sea necesario. Le recomendamos que programe las horas de creación de las instantáneas para periodos de tiempo que coincidan con su carga de trabajo; por ejemplo, durante los periodos de mantenimiento.

En el caso de SAP HANA, le recomendamos que habilite la restauración rápida de instantáneas.

> **Note**
>
> Si habilita una programación para las copias de seguridad de VSS, no podrá habilitar la opción Excluir volúmenes de datos específicos ni Copiar etiquetas del origen.

7. En la sección Scripts previos y posteriores, seleccione Habilitar scripts previos y posteriores y, a continuación, haga lo siguiente, en función de su carga de trabajo:

   - Para crear instantáneas coherentes con las aplicaciones de Windows, seleccione Copias de seguridad de VSS.
   - Para crear instantáneas coherentes con las aplicaciones de sus cargas de trabajo de SAP HANA, seleccione SAP HANA.
   - Para crear instantáneas coherentes con las aplicaciones de todas las demás bases de datos y cargas de trabajo, incluidas las bases de datos MySQL, PostgreSQL o InterSystems IRIS autogestionadas, mediante un documento SSM personalizado, seleccione Documento SSM personalizado.

     1. En Automatizar opción, seleccione Scripts previos y posteriores.
     2. En Documento de SSM, seleccione el documento de SSM que ha preparado.

8. En función de la opción que haya seleccionado, configure las siguientes opciones adicionales:

   - Tiempo de espera del script: (solo documento de SSM personalizado) el periodo de espera tras el cual Amazon Data Lifecycle Manager no logra ejecutar el script si no se ha completado. Si un script no se completa dentro de su periodo de espera, Amazon Data Lifecycle Manager devuelve un error. El periodo de espera se aplica individualmente a los scripts previos y posteriores. El valor mínimo y predeterminado del periodo de espera es de 10 segundos. Y el periodo de espera máximo es de 120 segundos.
   - Reintentar los scripts fallidos: seleccione esta opción para volver a intentar ejecutar los scripts que no se completen dentro del periodo de espera. Si el script previo falla, Amazon Data Lifecycle Manager vuelve a intentar todo el proceso de creación de instantáneas, incluida la ejecución de los scripts previos y posteriores. Si se produce un error en el script posterior, Amazon Data Lifecycle Manager vuelve a intentarlo únicamente con el script

posterior; en este caso, el script previo se habrá completado y es posible que se haya creado la instantánea.

- Instantáneas coherentes ante bloqueos predeterminadas: seleccione esta opción para utilizar de forma predeterminada las instantáneas coherentes ante bloqueos si el script previo no se ejecuta. Este es el comportamiento de creación de instantáneas predeterminado para Amazon Data Lifecycle Manager si los scripts previos y posteriores no están habilitados. Si ha habilitado los reintentos, Amazon Data Lifecycle Manager utilizará de forma predeterminada las instantáneas coherentes ante bloqueos solo después de que se hayan agotado todos los reintentos. Si el script previo falla y no utiliza de forma predeterminada instantáneas coherentes ante bloqueos, Amazon Data Lifecycle Manager no creará instantáneas para la instancia durante esa ejecución programada.

> **Note**
>
> Si va a crear instantáneas para SAP HANA, puede que desee deshabilitar esta opción. Las instantáneas coherentes ante bloqueos de las cargas de trabajo de SAP HANA no se pueden restaurar de la misma manera.

9. Elija Crear política predeterminada.

> **Note**
>
> Si detecta un error `Role with name AWSDataLifecycleManagerDefaultRole already exists`, consulte Resolución de problemas para obtener más información.

AWS CLI

Creación de una política de ciclo de vida de las instantáneas

Utilice el comando create-lifecycle-policy e incluya los parámetros `Scripts` en `CreateRule`. Para obtener más información sobre los parámetros, consulte la Referencia de la API de Amazon Data Lifecycle Manager.

```
$ aws dlm create-lifecycle-policy \
--description "policy_description" \
--state ENABLED \
--execution-role-arn iam_role_arn \
```

```
--policy-details file://policyDetails.json
```

Donde `policyDetails.json` incluye una de las siguientes acciones, en función de su caso de uso:

- Copias de seguridad de VSS

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "tag_key",
        "Value": "tag_value"
    }],
    "Schedules": [{
        "Name": "schedule_name",
        "CreateRule": {
            "CronExpression": "cron_for_creation_frequency",
            "Scripts": [{
                "ExecutionHandler":"AWS_VSS_BACKUP",
                "ExecuteOperationOnScriptFailure":true|false,
                "MaximumRetryCount":retries (0-3)
            }]
        },
        "RetainRule": {
            "Count": retention_count
        }
    }]
}
```

- Copias de seguridad de SAP HANA

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "tag_key",
        "Value": "tag_value"
    }],
```

```
    "Schedules": [{
        "Name": "schedule_name",
        "CreateRule": {
            "CronExpression": "cron_for_creation_frequency",
            "Scripts": [{
                "Stages": ["PRE","POST"],
                "ExecutionHandlerService":"AWS_SYSTEMS_MANAGER",
                "ExecutionHandler":"AWSSystemsManagerSAP-
CreateDLMSnapshotForSAPHANA",
                "ExecuteOperationOnScriptFailure":true|false,
                "ExecutionTimeout":timeout_in_seconds (10-120),
                "MaximumRetryCount":retries (0-3)
            }]
        },
        "RetainRule": {
            "Count": retention_count
        }
    }]
}
```

- Documento de SSM personalizado

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "tag_key",
        "Value": "tag_value"
    }],
    "Schedules": [{
        "Name": "schedule_name",
        "CreateRule": {
            "CronExpression": "cron_for_creation_frequency",
            "Scripts": [{
                "Stages": ["PRE","POST"],
                "ExecutionHandlerService":"AWS_SYSTEMS_MANAGER",
                "ExecutionHandler":"ssm_document_name|arn",
                "ExecuteOperationOnScriptFailure":true|false,
                "ExecutionTimeout":timeout_in_seconds (10-120),
                "MaximumRetryCount":retries (0-3)
            }]
        },
```

```
        "RetainRule": {
            "Count": retention_count
        }
    }]
}
```

Consideraciones sobre las copias de seguridad de VSS con Amazon Data Lifecycle Manager

Con Amazon Data Lifecycle Manager, puede realizar copias de seguridad y restaurar aplicaciones de Windows habilitadas para VSS (Servicio de instantáneas de volumen) que se ejecuten en instancias de Amazon EC2. Si la aplicación tiene un escritor VSS registrado en Windows VSS, Amazon Data Lifecycle Manager crea una instantánea que sea coherente con esa aplicación.

> **Note**
>
> Amazon Data Lifecycle Manager actualmente solo admite copias de seguridad coherentes con las aplicaciones de recursos que se ejecutan en Amazon EC2, específicamente para situaciones de copias de seguridad en las que los datos de la aplicación se pueden restaurar al sustituir una instancia existente por una nueva creada a partir de la copia de seguridad. No todos los tipos de instancia o aplicaciones son compatibles con las copias de seguridad de VSS. Para obtener más información, consulte ¿Qué es VSS? AWS en la Guía del usuario de Amazon EC2.

Tipos de instancias no admitidos

No se admiten los siguientes tipos de instancias de Amazon EC2 para las copias de seguridad de VSS. Si su política se dirige a uno de estos tipos de instancias, Amazon Data Lifecycle Manager puede seguir creando copias de seguridad de VSS, pero es posible que las instantáneas no se etiqueten con las etiquetas de sistema requeridas. Sin estas etiquetas, Amazon Data Lifecycle Manager no administrará las instantáneas tras su creación. Puede ser que necesite eliminar estas instantáneas manualmente.

- T3: `t3.nano` | `t3.micro`
- T3a: `t3a.nano` | `t3a.micro`
- T2: `t2.nano` | `t2.micro`

Responsabilidad compartida de instantáneas coherentes con las aplicaciones

Debe asegurarse de que:

- El agente SSM está instalado y se está ejecutando en las instancias de destino up-to-date
- Systems Manager tenga permisos para realizar las acciones necesarias en las instancias de destino
- Amazon Data Lifecycle Manager tiene permisos para realizar las acciones de Systems Manager necesarias para ejecutar scripts previos y posteriores en las instancias de destino.
- Para las cargas de trabajo personalizadas, como las bases de datos MySQL, PostgreSQL o InterSystems IRIS autogestionadas, el documento SSM que utilice incluye las acciones correctas y necesarias para congelar, vaciar y descongelar las E/S de la configuración de la base de datos.
- Las horas de creación de instantáneas se ajustan a la programación de su carga de trabajo. Por ejemplo, intente programar la creación de instantáneas durante los periodos de mantenimiento programados.

Amazon Data Lifecycle Manager garantiza que:

- La creación de instantáneas se inicia dentro de los 60 minutos posteriores a la hora programada para crear instantáneas.
- Los scripts previos se ejecutan antes de que se inicie la creación de la instantánea.
- Los scripts posteriores se ejecutan una vez que el script previo se ejecuta correctamente y se ha iniciado la creación de la instantánea. Amazon Data Lifecycle Manager ejecuta el script posterior solo si el script previo se ejecuta correctamente. Si el script previo falla, Amazon Data Lifecycle Manager no ejecutará el script posterior.
- Las instantáneas se etiquetan con las etiquetas correspondientes en el momento de su creación.
- CloudWatch las métricas y los eventos se emiten cuando se inician los scripts y cuando fallan o se ejecutan correctamente.

Otros casos de uso de scripts previos y posteriores

Además de utilizar scripts previos y posteriores para automatizar las instantáneas coherentes con la aplicación, puede utilizarlos de forma conjunta o individual para automatizar otras tareas administrativas antes o después de la creación de las instantáneas. Por ejemplo:

- Puede usar un script previo para aplicar las revisiones antes de crear las instantáneas. Esto puede ser de utilidad para crear instantáneas después de aplicar las actualizaciones de software semanales o mensuales habituales.

> **Note**
>
> Si opta por ejecutar solo un script previo, la opción Instantáneas coherentes ante bloqueos predeterminadas está habilitada de forma predeterminada.

- Puede usar un script posterior para aplicar las revisiones después de crear las instantáneas. Esto puede ser de utilidad para crear instantáneas antes de aplicar las actualizaciones de software semanales o mensuales habituales.

Introducción para otros casos de uso

En esta sección se explican los pasos que hay que seguir cuando se utilizan scripts previos o posteriores para casos de uso distintos de las instantáneas coherentes con la aplicación.

Paso 1: preparar las instancias de destino

Preparación de las instancias de destino para los scripts previos o posteriores

1. Instale SSM Agent en las instancias de destino, si aún no está instalado. Si SSM Agent ya está instalado en las instancias de destino, omita este paso.
   - (Instancias de Linux) Instalación manual de SSM Agent en instancias de Amazon EC2 para Linux
   - (Instancias de Windows) Instalación manual de SSM Agent en instancias de Amazon EC2 para Windows
2. Asegúrese de que SSM Agent esté en ejecución. Para obtener más información, consulte Verificación del estado de SSM Agent e inicio del agente.
3. Configure Systems Manager para instancias de Amazon EC2. Para obtener más información, consulte Configuración de Systems Manager para instancias de Amazon EC2 en la Guía del usuario de AWS Systems Manager .

Paso 2: preparar el documento de SSM

Debe crear un documento de comandos de SSM que incluya los scripts previos o posteriores con los comandos que desee ejecutar.

Puede crear un documento de SSM utilizando la plantilla de documento de SSM vacía que aparece a continuación y agregar los comandos previos y posteriores al script en las secciones del documento correspondientes.

⚠ Tenga en cuenta lo siguiente:

- Es su responsabilidad asegurarse de que el documento de SSM realice las acciones correctas y necesarias para su carga de trabajo.
- El documento de SSM debe incluir los campos obligatorios para `allowedValues`, incluidos `pre-script`, `post-script` y `dry-run`. Amazon Data Lifecycle Manager ejecutará comandos en la instancia en función del contenido de esas secciones. Si su documento de SSM no incluye esas secciones, Amazon Data Lifecycle Manager lo considerará una ejecución fallida.

```
###======================================================================================###
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of this
# software and associated documentation files (the "Software"), to deal in the Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###======================================================================================###
schemaVersion: '2.2'
description: SSM Document Template for Amazon Data Lifecycle Manager Pre/Post script
 feature
parameters:
```

```
  executionId:
    type: String
    default: None
    description: (Required) Specifies the unique identifier associated with a pre and/
or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-
[a-fA-F0-9]{12})$
  command:
  # Data Lifecycle Manager will trigger the pre-script and post-script actions during
 policy execution.
  # 'dry-run' option is intended for validating the document execution without
 triggering any commands
  # on the instance. The following allowedValues will allow Data Lifecycle Manager to
 successfully
  # trigger pre and post script actions.
    type: String
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should be
 executed.
    allowedValues:
    - pre-script
    - post-script
    - dry-run

mainSteps:
- action: aws:runShellScript
  description: Run Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
    runCommand:
    - |
      #!/bin/bash


 ###============================================================================###
      ### Error Codes

 ###============================================================================###
      # The following Error codes will inform Data Lifecycle Manager of the type of
 error
```

```
    # and help guide handling of the error.
    # The Error code will also be emitted via AWS Eventbridge events in the 'cause'
field.
    # 1 Pre-script failed during execution - 201
    # 2 Post-script failed during execution - 202
    # 3 Auto thaw occurred before post-script was initiated - 203
    # 4 Pre-script initiated while post-script was expected - 204
    # 5 Post-script initiated while pre-script was expected - 205
    # 6 Application not ready for pre or post-script initiation - 206


###############################################################################
    ### Global variables

###############################################################################
    START=$(date +%s)
    # For testing this script locally, replace the below with OPERATION=$1.
    OPERATION={{ command }}

    # Add all pre-script actions to be performed within the function below
    execute_pre_script() {
        echo "INFO: Start execution of pre-script"
    }

    # Add all post-script actions to be performed within the function below
    execute_post_script() {
        echo "INFO: Start execution of post-script"
    }

    # Debug logging for parameters passed to the SSM document
    echo "INFO: ${OPERATION} starting at $(date) with executionId: ${EXECUTION_ID}"

    # Based on the command parameter value execute the function that supports
    # pre-script/post-script operation
    case ${OPERATION} in
        pre-script)
            execute_pre_script
            ;;
        post-script)
            execute_post_script
            ;;
        dry-run)
            echo "INFO: dry-run option invoked - taking no action"
            ;;
```

```
          *)
              echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
              exit 1 # return failure
              ;;
      esac

      END=$(date +%s)
      # Debug Log for profiling the script time
      echo "INFO: ${OPERATION} completed at $(date). Total runtime: $((${END} -
 ${START})) seconds."
```

Paso 3: preparar el rol de IAM de Amazon Data Lifecycle Manager

> **Note**
>
> Este paso es necesario si:
>
> - Debe crear o actualizar una política de instantáneas con scripts previos o posteriores que utilice un rol de IAM personalizado.
> - La línea de comandos se utiliza para crear o actualizar una política de instantáneas habilitada para scripts previos o posteriores que utilice el rol predeterminado.
>
> Si utiliza la consola para crear o actualizar una política de instantáneas habilitada antes o después de los scripts que utilice la función predeterminada para administrar las instantáneas (AWSDataLifecycleManagerDefaultRole), omita este paso. En este caso, asociamos automáticamente la política a ese rol. AWSDataLifecycleManagerSSMFullAccess

Debe asegurarse de que el rol de IAM que utilice para la política conceda permiso a Amazon Data Lifecycle Manager para realizar las acciones de SSM necesarias para ejecutar scripts previos y posteriores en las instancias incluidas en la política.

Amazon Data Lifecycle Manager proporciona una política gestionada (AWSDataLifecycleManagerSSMFullAccess) que incluye los permisos necesarios. Puede asociar esta política a su rol de IAM para administrar las instantáneas y asegurarse de que incluya los permisos.

> **Important**
>
> La política AWSDataLifecycleManagerSSMFullAccess gestionada utiliza la clave de `aws:ResourceTag` condición para restringir el acceso a documentos SSM específicos cuando se utilizan scripts previos y posteriores. Para permitir que Amazon Data Lifecycle Manager acceda a los documentos de SSM, debe asegurarse de que sus documentos de SSM estén etiquetados con `DLMScriptsAccess:true`.

Como alternativa, puede crear manualmente una política personalizada o asignar los permisos necesarios directamente al rol de IAM que utilice. Puede utilizar los mismos permisos que se definen en la política AWSDataLifecycleManagerSSMFullAccess gestionada; sin embargo, la clave de `aws:ResourceTag` condición es opcional. Si decide no utilizar esa clave de condición, no tendrá que etiquetar sus documentos de SSM con `DLMScriptsAccess:true`.

Utilice uno de los siguientes métodos para añadir la AWSDataLifecycleManagerSSMFullAccesspolítica a su función de IAM.

Console

Asociación de la política administrada a su rol personalizado

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, elija Roles.
3. Busque y seleccione el rol personalizado para administrar instantáneas.
4. En la pestaña Permisos, elija Agregar permisos, Asociar políticas.
5. Busque y seleccione la política AWSDataLifecycleManagerSSMFullAccessgestionada y, a continuación, elija Añadir permisos.

AWS CLI

Asociación de la política administrada a su rol personalizado

Utilice el comando attach-role-policy. En `---role-name`, especifique el nombre de su rol personalizado. En `--policy-arn`, especifique `arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess`.

```
$ aws iam attach-role-policy \
```

```
--policy-arn arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess \
--role-name your_role_name
```

Creación de una política de ciclo de vida de las instantáneas

Console

Creación de una política de ciclo de vida de las instantáneas

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Elastic Block Store, Lifecycle Manager (Administrador de ciclo de vida) y, a continuación, Create lifecycle policy (Crear política de ciclo de vida).
3. En la pantalla Select policy type (Seleccionar el tipo de política), elija EBS snapshot policy (Política de instantáneas de EBS) y, luego, seleccione Next (Siguiente).
4. En la sección Target resources (Recursos de destino), haga lo siguiente:
   a. En Tipos de recursos de destino, elija `Instance`.
   b. En Etiquetas de recursos de destino, especifique las etiquetas de recursos que identifican las instancias de las que se va a realizar una copia de seguridad. Solo se realizará una copia de seguridad de los recursos que tengan las etiquetas especificadas.
5. Para el rol de IAM, elija AWSDataLifecycleManagerDefaultRole(el rol predeterminado para administrar las instantáneas) o elija un rol personalizado que haya creado y preparado para los guiones previos y posteriores.
6. Configure las programaciones y las opciones adicionales según sea necesario. Le recomendamos que programe las horas de creación de las instantáneas para periodos de tiempo que coincidan con su carga de trabajo; por ejemplo, durante los periodos de mantenimiento.
7. En la sección Scripts previos y posteriores, seleccione Habilitar scripts previos y posteriores y, a continuación, haga lo siguiente:
   a. Seleccione Documento de SSM personalizado.
   b. En Automatizar opción, elija la opción que coincida con los scripts que desee ejecutar.
   c. En Documento de SSM, seleccione el documento de SSM que ha preparado.
8. Configure las siguientes opciones adicionales si es necesario:

- Tiempo de espera del script: es el periodo de espera tras el cual Amazon Data Lifecycle Manager no logra ejecutar el script si no se ha completado. Si un script no se completa dentro de su periodo de espera, Amazon Data Lifecycle Manager devuelve un error. El periodo de espera se aplica individualmente a los scripts previos y posteriores. El valor mínimo y predeterminado del periodo de espera es de 10 segundos. Y el periodo de espera máximo es de 120 segundos.
- Reintentar los scripts fallidos: seleccione esta opción para volver a intentar ejecutar los scripts que no se completen dentro del periodo de espera. Si el script previo falla, Amazon Data Lifecycle Manager vuelve a intentar todo el proceso de creación de instantáneas, incluida la ejecución de los scripts previos y posteriores. Si se produce un error en el script posterior, Amazon Data Lifecycle Manager vuelve a intentarlo únicamente con el script posterior; en este caso, el script previo se habrá completado y es posible que se haya creado la instantánea.
- Instantáneas coherentes ante bloqueos predeterminadas: seleccione esta opción para utilizar de forma predeterminada las instantáneas coherentes ante bloqueos si el script previo no se ejecuta. Este es el comportamiento de creación de instantáneas predeterminado para Amazon Data Lifecycle Manager si los scripts previos y posteriores no están habilitados. Si ha habilitado los reintentos, Amazon Data Lifecycle Manager utilizará de forma predeterminada las instantáneas coherentes ante bloqueos solo después de que se hayan agotado todos los reintentos. Si el script previo falla y no utiliza de forma predeterminada instantáneas coherentes ante bloqueos, Amazon Data Lifecycle Manager no creará instantáneas para la instancia durante esa ejecución programada.

9. Elija Crear política predeterminada.

> **Note**
>
> Si detecta un error `Role with name AWSDataLifecycleManagerDefaultRole already exists`, consulte Resolución de problemas para obtener más información.

AWS CLI

Creación de una política de ciclo de vida de las instantáneas

Utilice el comando create-lifecycle-policy e incluya los parámetros `Scripts` en `CreateRule`. Para obtener más información sobre los parámetros, consulte la Referencia de la API de Amazon Data Lifecycle Manager.

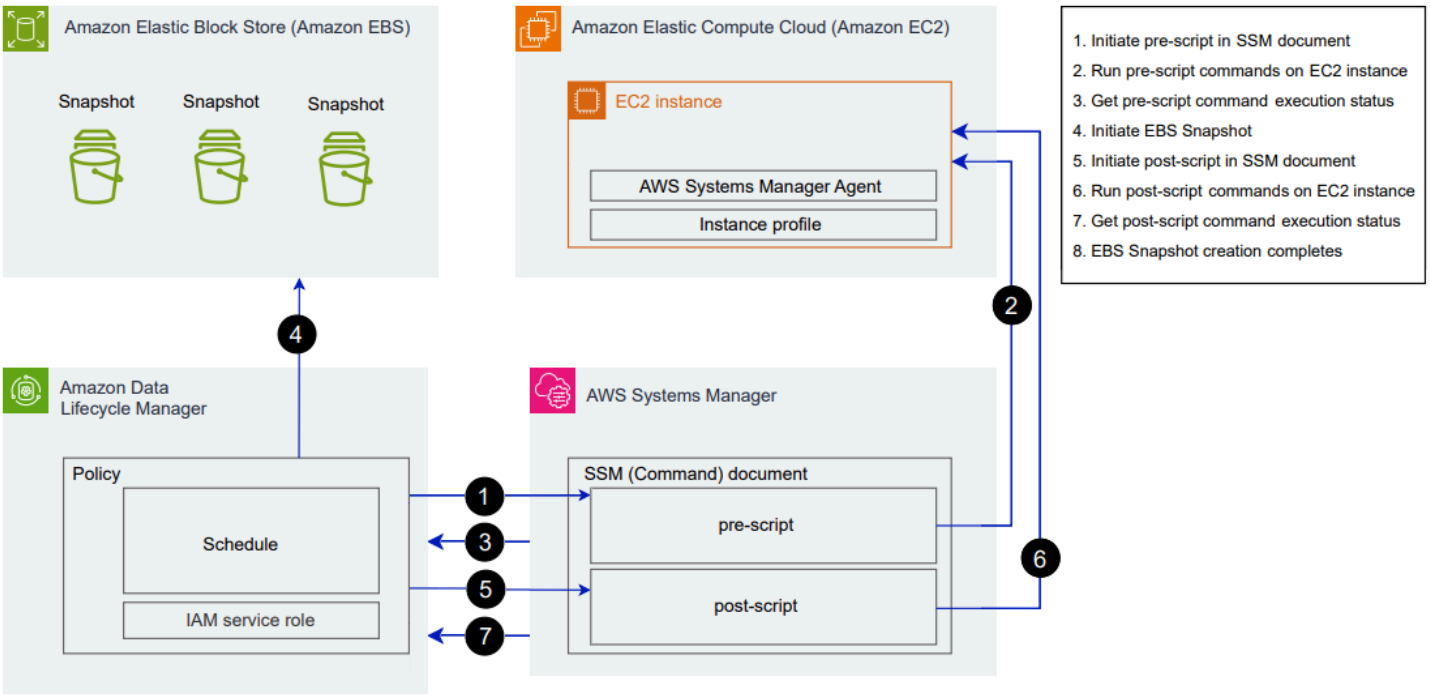
```
$ aws dlm create-lifecycle-policy \
--description "policy_description" \
--state ENABLED \
--execution-role-arn iam_role_arn \
--policy-details file://policyDetails.json
```

Donde `policyDetails.json` incluye lo siguiente.

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "tag_key",
        "Value": "tag_value"
    }],
    "Schedules": [{
        "Name": "schedule_name",
        "CreateRule": {
            "CronExpression": "cron_for_creation_frequency",
            "Scripts": [{
                "Stages": ["PRE" | "POST" | "PRE","POST"],
                "ExecutionHandlerService":"AWS_SYSTEMS_MANAGER",
                "ExecutionHandler":"ssm_document_name|arn",
                "ExecuteOperationOnScriptFailure":true|false,
                "ExecutionTimeout":timeout_in_seconds (10-120),
                "MaximumRetryCount":retries (0-3)
            }]
        },
        "RetainRule": {
            "Count": retention_count
        }
    }]
}
```

Cómo funcionan los scripts previos y posteriores

En la siguiente imagen se muestra el flujo del proceso de los scripts previos y posteriores al utilizar documentos de SSM personalizados. Esto no se aplica a las copias de seguridad de VSS.



A la hora programada de creación de la instantánea, se producen las siguientes acciones e interacciones entre servicios.

1. Amazon Data Lifecycle Manager inicia la acción del script previo; para ello, llama al documento de SSM y pasa el parámetro `pre-script`.

   > **Note**
   >
   > Los pasos del 1 al 3 solo se llevan a cabo si ejecuta scripts previos. Si solo ejecuta scripts posteriores, se omiten los pasos del 1 al 3.

2. Systems Manager envía comandos del script previo a la instancia de SSM Agent que se ejecuta en las instancias de destino. SSM Agent ejecuta los comandos en la instancia y envía la información de estado a Systems Manager.

   Por ejemplo, si el documento de SSM se utiliza para crear instantáneas coherentes con las aplicaciones, es posible que el script previo se bloquee y vacíe las E/S para garantizar que todos los datos almacenados en el búfer se escriban en el volumen antes de tomar la instantánea.

3. Systems Manager envía actualizaciones del estado de los comandos del script previo a Amazon Data Lifecycle Manager. Si se produce un error en el script previo, Amazon Data Lifecycle Manager lleva a cabo una de las siguientes acciones, según la configuración de las opciones del script previo y posterior:

Reintentos	Uso por defecto de instantáneas coherentes ante bloqueos	Acción
Se habilitan con los reintentos restantes	Habilitado	Se vuelve a intentar ejecutar el script hasta que el proceso se realice correctamente o hasta que se agoten los reintentos.
Agotado sin completarlo correctamente	Habilitado	Se crean instantáneas coherente ante bloqueos y no se ejecuta un script posterior.
Se habilitan con los reintentos restantes	Deshabilitad	Se vuelve a intentar ejecutar el script hasta que el proceso se realice correctamente o hasta que se agoten los reintentos.
Se agota sin completarse correctamente	Deshabilitad	Se omite la creación de instantán eas para la instancia de destino y no se ejecuta un script posterior.
Deshabilitad	Habilitado	Se crean instantáneas coherente ante bloqueos y no se ejecuta un script posterior.
Deshabilitad	Deshabilitad	Se omite la creación de instantán eas para la instancia de destino y no se ejecuta un script posterior.

4. Amazon Data Lifecycle Manager inicia la creación de instantáneas.
5. Amazon Data Lifecycle Manager inicia la acción del script posterior, para ello; llama al documento de SSM y pasa el parámetro `post-script`.

> **Note**
>
> Los pasos del 5 al 7 solo se llevan a cabo si ejecuta scripts previos. Si solo ejecuta scripts posteriores, se omiten los pasos del 1 al 3.

6. Systems Manager envía comandos del script posterior a la instancia de SSM Agent que se ejecuta en las instancias de destino. SSM Agent ejecuta los comandos en la instancia y envía la información de estado a Systems Manager.

   Por ejemplo, si el documento de SSM permite realizar instantáneas coherentes con las aplicaciones, este script posterior podría descongelar la E/S para garantizar que las bases de datos reanuden las operaciones de E/S normales una vez realizada la instantánea.

7. Si ejecuta un script posterior y Systems Manager indica que se ha completado correctamente, el proceso finaliza.

   Si se produce un error en el script posterior, Amazon Data Lifecycle Manager lleva a cabo una de las siguientes acciones, según la configuración de las opciones del script previo y posterior:

Reintentos	Acción
Se habilitan con los reintentos restantes	Se vuelve a intentar ejecutar el script posterior hasta que el proceso se realice correctamente o hasta que se agoten los reintentos.
Se agota sin éxito	Se omite el script posterior.
Deshabilitad	Se omite el script posterior.

   Tenga en cuenta que si el script posterior falla, el script previo (si está habilitado) se habrá completado correctamente y es posible que se hayan creado las instantáneas. Es posible que tenga que tomar más medidas en la instancia para asegurarse de que funciona según lo previsto. Por ejemplo, si el script previo hizo una pausa y vació las E/S, pero el script posterior no pudo descongelar las E/S, es posible que deba configurar la base de datos para que descongele automáticamente las E/S o que tenga que descongelar las E/S manualmente.

8. Es posible que el proceso de creación de la instantánea se complete una vez finalizado el script posterior. El tiempo que lleva completar la instantánea depende del tamaño de esta.

Identificación de las instantáneas creadas con scripts previos y posteriores

Amazon Data Lifecycle Manager asigna automáticamente las siguientes etiquetas de sistema a las instantáneas creadas con scripts previos y posteriores.

- Clave: `aws:dlm:pre-script`; valor: `SUCCESS|FAILED`

  Un valor de etiqueta de `SUCCESS` indica que el script previo se ejecutó correctamente. Un valor de etiqueta de `FAILED` indica que el script previo no se ejecutó correctamente.
- Clave: `aws:dlm:post-script`; valor: `SUCCESS|FAILED`

  Un valor de etiqueta de `SUCCESS` indica que el script posterior se ejecutó correctamente. Un valor de etiqueta de `FAILED` indica que el script posterior no se ejecutó correctamente.

En el caso de los documentos de SSM personalizados y las copias de seguridad de SAP HANA, puede inferir que la creación de instantáneas coherentes con las aplicaciones se ha realizado correctamente si la instantánea está etiquetada con `aws:dlm:pre-script:SUCCESS` y `aws:dlm:post-script:SUCCESS`.

Además, las instantáneas coherentes con las aplicaciones creadas mediante la copia de seguridad de VSS se etiquetan automáticamente con:

- Clave: `AppConsistent tag`; valor: `true|false`

  Un valor de etiqueta de `true` indica que la copia de seguridad de VSS se realizó correctamente y que las instantáneas son coherentes con las aplicaciones. Un valor de etiqueta de `false` indica que la copia de seguridad de VSS no se realizó correctamente y que las instantáneas son coherentes con las aplicaciones.

Supervisión de la ejecución del script previo y posterior

CloudWatch Métricas de Amazon

Amazon Data Lifecycle Manager publica las siguientes CloudWatch métricas cuando los scripts previos y posteriores fallan y son correctos y cuando los respaldos de VSS fallan y se realizan correctamente.

- `PreScriptStarted`
- `PreScriptCompleted`

- `PreScriptFailed`
- `PostScriptStarted`
- `PostScriptCompleted`
- `PostScriptFailed`
- `VSSBackupStarted`
- `VSSBackupCompleted`
- `VSSBackupFailed`

Para obtener más información, consulte Supervisa tus políticas con Amazon CloudWatch.

Amazon EventBridge

Amazon Data Lifecycle Manager emite el siguiente EventBridge evento de Amazon cuando un script previo o posterior se inicia, se ejecuta correctamente o no se produce

- `DLM Pre Post Script Notification`

Para obtener más información, consulte Supervise sus políticas mediante CloudWatch Events.

Automatización de los ciclos de vida de las AMI

En el siguiente procedimiento, se muestra cómo utilizar Amazon Data Lifecycle Manager para automatizar los ciclos de vida de las AMI con respaldo de EBS.

Temas

- Crear una política de ciclo de vida de AMI
- Consideraciones sobre las políticas de ciclo de vida de AMI
- Recursos adicionales de

Crear una política de ciclo de vida de AMI

Utilice uno de los siguientes procedimientos para crear una política de ciclo de vida de AMI.

Console

Para crear una política de AMI

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Elastic Block Store, Lifecycle Manager (Administrador de ciclo de vida) y, a continuación, Create lifecycle policy (Crear política de ciclo de vida).
3. En la pantalla Select policy type (Seleccionar el tipo de política), elija EBS-backed AMI policy (Política de AMI con respaldo EBS) y, luego, seleccione Next (Siguiente).
4. En la sección Target resources (Recursos de destino), en Target resource tags (Etiquetas de recursos de destino), elija las etiquetas de recursos que identifican los volúmenes o las instancias de los que se va a realizar una copia de seguridad. La política realiza una copia de seguridad solo de los recursos que tienen los pares de clave y valor de la etiqueta especificados.
5. En Description (Descripción), escriba una breve descripción de la política.
6. En IAM Rol (Rol de IAM), elija el rol de IAM que tenga permisos para administrar las AMI y las instantáneas y para describir las instancias. Para utilizar el rol predeterminado proporcionado por Amazon Data Lifecycle Manager, elija Default role (Rol predeterminado). De forma alternativa, para usar un rol de IAM personalizado que haya creado anteriormente, elija Choose another role (Elegir otro rol) y, luego, seleccione el rol que va a utilizar.
7. En Policy tags (Etiquetas de políticas), agregue las etiquetas que se aplicarán a la política de ciclo de vida. Puede utilizar estas etiquetas para identificar y clasificar las políticas.
8. En Policy status after creation (Estado de la política después de su creación), elija Enable policy (Habilitar política) para iniciar las ejecuciones de la política a la hora programada siguiente o Disable policy (Desactivar política) para evitar que se ejecute la política. Si no habilita la política ahora, no se comenzarán a crear AMI hasta que la habilite de forma manual después de la creación.
9. En la sección Instance reboot (Reinicio de instancias), indique si las instancias deben reiniciarse antes de la creación de la AMI. Para evitar que se reinicien las instancias de destino, elija No (No). Elegir No (No) podría provocar problemas de consistencia de datos. Para reiniciar las instancias antes de la creación de la AMI, elija Yes (Sí). La elección de esta opción garantiza la consistencia de los datos, pero podría dar lugar a que varias instancias de destino se reinicien simultáneamente.
10. Elija Next (Siguiente).

11. En la pantalla Configure schedule (Configurar la programación), configure las programaciones de las políticas. Una política puede tener hasta cuatro programaciones. La programación 1 es obligatoria Las programaciones 2, 3 y 4 son opcionales. Para cada programación de política que agregue, realice lo siguiente:

    a. En la sección Schedule details (Detalles de la programación), realice lo siguiente:

        i. En Schedule name (Nombre de la programación), especifique un nombre descriptivo para la programación.

        ii. En Frequency (Frecuencia) y en los campos relacionados, configure el intervalo entre las ejecuciones de la política.

            Puede configurar las ejecuciones de políticas en una programación diaria, semanal, mensual o anual. Alternativamente, elija Custom cron expression (Expresión cron personalizada) para especificar un intervalo de hasta un año. Para obtener más información, consulte Expresiones cron en la Guía del usuario de Amazon CloudWatch Events.

        iii. En Starting at (Comenzar a), especifique la hora en que comenzarán las ejecuciones de la política. La primera ejecución de la política comenzará dentro de una hora después de la hora que programe. Debe especificar la hora con el formato `hh:mm` UTC.

        iv. En Retention type (Tipo de retención), especifique la política de retención de las AMI creadas por la programación.

            Puede retener las AMI en función de su recuento total o de su antigüedad.

            Para la retención basada en el recuento, el rango es de `1` a `1000`. Una vez alcanzado el recuento máximo, la AMI más antigua se eliminará del registro cuando se cree una nueva.

            Para la retención basada en la antigüedad, el rango es de `1` día a `100` años. Luego de que el periodo de retención de cada AMI vence, esta última se elimina del registro.

            > **Note**
            >
            > Todas las programaciones deben tener el mismo tipo de retención. Puede especificar el tipo de retención solo para la programación 1. Las

programaciones 2, 3 y 4 heredan el tipo de retención de la programación 1. Cada programación puede tener su propio recuento o periodo de retención.

b. Configure el etiquetado de las AMI.

   En la sección Tagging (Etiquetado), realice lo siguiente:

   i. Para copiar todas las etiquetas definidas por el usuario de la instancia de origen a las AMI creadas por la programación, seleccione Copy tags from source (Copiar las etiquetas de la fuente).

   ii. De forma predeterminada, las AMI creadas por la programación se etiquetan automáticamente con el ID de la instancia de origen. Para evitar que se lleve a cabo este etiquetado automático, en Variable tags (Etiquetas de variables), elimine el icono `instance-id:$(instance-id)`.

   iii. Para especificar etiquetas adicionales y asignarlas a las AMI creadas por esta programación, elija Add tags (Agregar etiquetas).

c. Configure la obsolescencia de la AMI.

   A fin de dar de baja las AMI cuando ya no deberían utilizarse, en la sección AMI deprecation (Obsolescencia de AMI), seleccione Enable AMI deprecation for this schedule (Habilitar la obsolescencia de AMI para esta programación) y, a continuación, especifique la regla de obsolescencia de AMI. La regla de obsolescencia de AMI especifica cuándo deben darse de baja las AMI.

   Si la programación utiliza la retención de AMI basada en el recuento, debe especificar el número de AMI más antiguas que se darán de baja. El recuento de obsolescencia debe ser menor o igual que el recuento de retención de AMI de la programación y no puede ser mayor a 1000. Por ejemplo, si la programación está configurada a fin de retener un máximo de 5 AMI, puede configurar la programada para dar de baja hasta las 5 AMI más antiguas.

   Si la programación utiliza la retención de AMI basada en la antigüedad, debe especificar el periodo después del cual deben darse de baja las AMI. El recuento de obsolescencia debe ser menor o igual que el periodo de retención de AMI de la programación y no puede ser superior a 10 años (120 meses, 520 semanas o 3650 días). Por ejemplo, si la programación está configurada a fin de retener las AMI durante 10 días, puede configurar la programada para que dé de baja las AMI después de periodos de hasta 10 días luego de la creación.

d. Configure la copia entre regiones.

   Para copiar las AMI creadas por la programación en regiones diferentes, en la sección Cross-Region copy (Copia entre regiones), seleccione Enable cross-Region copy (Habilitar la copia entre regiones). Puede copiar las AMI en hasta tres regiones adicionales de su cuenta. Debe especificar una regla de copia entre regiones independiente para cada región de destino.

   Puede especificar lo siguiente para cada región de destino:

   - Una política de retención para la copia de la AMI. Cuando vence el periodo de retención, la copia en la región de destino se anula de forma automática.
   - Estado de cifrado para la copia de la AMI. Si la AMI fuente se encuentra cifrada o si el cifrado se encuentra habilitado de forma predeterminada, siempre se cifrarán las AMI copiadas. Si la AMI fuente no se encuentra cifrada y el cifrado se encuentra desactivado de forma predeterminada, puede habilitar el cifrado de forma opcional. Si no especifica una clave de KMS, las AMI se cifrarán con la clave de KMS predeterminada para el cifrado de EBS en cada región de destino. Si especifica una Clave de KMS para la región de destino, el rol de IAM seleccionado debe tener acceso a la Clave de KMS.
   - Una regla de obsolescencia para la copia de la AMI. Cuando vence el periodo de obsolescencia, la copia de la AMI queda obsoleta de forma automática. El periodo de obsolescencia debe ser inferior o igual al periodo de retención de copia y no puede ser superior a 10 años.
   - Si se deben copiar todas las etiquetas, o ninguna de ellas, de la AMI fuente.

   > **Note**
   >
   > No debe superar el número de copias de AMI simultáneas por región.

e. Para agregar programaciones adicionales, elija Add another schedule (Agregar otra programación), que se encuentra en la parte superior de la pantalla. En cada programación adicional, complete los campos tal como se describe con anterioridad en este tema.

f. Después de agregar las programaciones necesarias, elija Review policy (Revisar la política).

12. Revise el resumen de la política y, a continuación, elija Create policy (Crear política).

> **Note**
>
> Si detecta el error `Role with name AWSDataLifecycleManagerDefaultRoleForAMIManagement already exists`, consulte Resolución de problemas para obtener más información.

Command line

Ejecute el comando create-lifecycle-policy para crear una política de ciclo de vida de AMI. En `PolicyType`, especifique `IMAGE_MANAGEMENT`.

> **Note**
>
> Para simplificar la sintaxis, en los siguientes ejemplos se utiliza un archivo JSON, `policyDetails.json`, que incluye los detalles de la política.

Ejemplo 1: retención en función de la edad y la obsolescencia de la AMI

En este ejemplo se genera una política de ciclo de vida de la AMI que crea las AMI de todas las instancias que tienen una clave de etiqueta de `purpose` con un valor de `production` sin reiniciar las instancias de destino. La política incluye una programación que crea una AMI todos los días a las `01:00` UTC. La política retiene las AMI por 2 días y las da de baja después de 1 día. También copiará las etiquetas de la instancia de origen a las AMI que cree.

```
aws dlm create-lifecycle-policy \
    --description "My AMI policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRoleForAMIManagement \
    --policy-details file://policyDetails.json
```

A continuación se muestra un ejemplo del archivo `policyDetails.json`.

```
{
    "PolicyType": "IMAGE_MANAGEMENT",
```

```
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "purpose",
        "Value": "production"
    }],
    "Schedules": [{
            "Name": "DailyAMIs",
            "TagsToAdd": [{
                "Key": "type",
                "Value": "myDailyAMI"
            }],
            "CreateRule": {
                "Interval": 24,
                "IntervalUnit": "HOURS",
                "Times": [
                    "01:00"
                ]
            },
            RetainRule":{
                "Interval" : 2,
                "IntervalUnit" : "DAYS"
            },
            DeprecateRule": {
                "Interval" : 1,
                "IntervalUnit" : "DAYS"
            },
            "CopyTags": true
        }
    ],
    "Parameters" : {
        "NoReboot":true
    }
}
```

Si se ejecuta correctamente, el comando devuelve el ID de la política recién creada. A continuación, se muestra un ejemplo del resultado.

```
{
   "PolicyId": "policy-9876543210abcdef0"
}
```

Ejemplo 2: retención en función de los recuentos y la obsolescencia de la AMI con copia entre regiones

En este ejemplo, se genera una política de ciclo de vida de AMI que crea las AMI de todas las instancias que tienen una clave de etiqueta de `purpose` con un valor de `production` y reinicia las instancias de destino. La política incluye una programación que crea una AMI cada 6 horas desde las `17:30` UTC. La política retiene 3 AMI y da de baja de forma automática las 2 AMI más antiguas. También tiene una regla de copia entre regiones que copia AMI a `us-east-1`, retiene 2 copias de AMI y da de baja de forma automática la AMI más antigua.

```
aws dlm create-lifecycle-policy \
    --description "My AMI policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRoleForAMIManagement \
    --policy-details file://policyDetails.json
```

A continuación se muestra un ejemplo del archivo `policyDetails.json`.

```
{
    "PolicyType": "IMAGE_MANAGEMENT",
    "ResourceTypes" : [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key":"purpose",
        "Value":"production"
    }],
    "Parameters" : {
          "NoReboot": true
    },
    "Schedules" : [{
        "Name" : "Schedule1",
        "CopyTags": true,
        "CreateRule" : {
            "Interval": 6,
            "IntervalUnit": "HOURS",
            "Times" : ["17:30"]
        },
        "RetainRule":{
            "Count" : 3
        },
```

```
        "DeprecateRule":{
            "Count" : 2
        },
        "CrossRegionCopyRules": [{
            "TargetRegion": "us-east-1",
            "Encrypted": true,
            "RetainRule":{
                "IntervalUnit": "DAYS",
                "Interval": 2
            },
            "DeprecateRule":{
                "IntervalUnit": "DAYS",
                "Interval": 1
            },
            "CopyTags": true
        }]
    }]
}
```

Consideraciones sobre las políticas de ciclo de vida de AMI

Las siguientes consideraciones generales se aplican a la creación de políticas de ciclo de vida de AMI:

- Las políticas de ciclo de vida de AMI van dirigidas únicamente a instancias que se encuentran en la misma región que la política.
- La primera operación de creación de AMI se inicia una hora después de la hora de inicio especificada. Las operaciones posteriores de creación de AMI se inician una hora después de la hora que tengan programada.
- Cuando Amazon Data Lifecycle Manager anula el registro de una AMI, elimina automáticamente sus instantáneas de respaldo.
- Las etiquetas de recursos de destino distinguen entre mayúsculas y minúsculas
- Si elimina las etiquetas de destino de una instancia a la que se dirige una política, Amazon Data Lifecycle Manager deja de administrar las AMI existentes en el estándar; deberá eliminarlas manualmente si ya no las necesita.
- Se pueden crear varias políticas para realizar una copia de seguridad de una instancia. Por ejemplo, si una instancia tiene dos etiquetas, de las cuales la etiqueta A es el destino de la política A para crear una AMI cada 12 horas y la etiqueta B es el destino de la política B para

crear una AMI cada 24 horas, Amazon Data Lifecycle Manager crea las AMI de acuerdo con las programaciones de ambas políticas. Alternativamente, puede lograr igual resultado mediante la creación de una única política que tenga varias programaciones. Por ejemplo, se puede crear una única política dirigida solo a la etiqueta A y especificar dos programaciones, una para cada 12 horas y otra para cada 24 horas.

- Los nuevos volúmenes que se adjunten a una instancia de destino después de crear la política se incluirán automáticamente en la copia de seguridad en la siguiente ejecución de la política. Se incluyen todos los volúmenes asociados a la instancia en el momento de la ejecución de la política.
- Si se crea una política con una programación basada en cron personalizada que está configurada para crear solo una AMI, la política no anulará automáticamente el registro de esa AMI cuando se alcance el umbral de retención. Debe anular manualmente el registro de la AMI si ya no se necesita.
- Si crea una política basada en la antigüedad en la que el periodo de retención sea inferior a la frecuencia de creación, Amazon Data Lifecycle Manager retendrá siempre la última AMI hasta que se cree la siguiente. Por ejemplo, si una política basada en la antigüedad crea una AMI cada mes con un periodo de retención de siete días, Amazon Data Lifecycle Manager retendrá cada AMI durante un mes, aunque el periodo de retención sea de siete días.
- En el caso de las políticas basadas en el recuento, Amazon Data Lifecycle Manager siempre crea las AMI según la frecuencia de creación antes de intentar anular el registro de la AMI más antigua según la política de retención.
- Puede tardar varias horas anular correctamente el registro de una AMI y eliminar sus instantáneas de respaldo asociadas. Si Amazon Data Lifecycle Manager crea la siguiente AMI antes de que se anule correctamente el registro de la AMI creada con anterioridad, podría retener temporalmente una cantidad de AMI superior a su recuento de retención.

Las siguientes consideraciones se aplican a la terminación de instancias destinatarias de una política:

- Si termina una instancia que era destinataria de una política con una programación de retención basada en recuento, la política deja de administrar las AMI que haya creado anteriormente desde la instancia terminada. Debe anular manualmente el registro de esas AMI anteriores si ya no se necesitan.
- Si termina una instancia que era destinataria de una política con una programación de retención basada en antigüedad, la política seguirá anulando el registro de las AMI que se hayan creado anteriormente desde la instancia terminada conforme a la programación definida hasta la última

AMI, pero sin incluir esta. Debe anular manualmente el registro de la última AMI si ya no se necesita.

Las siguientes consideraciones se aplican a las políticas de AMI y a la obsolescencia de AMI:

- Si aumenta el recuento de obsolescencia de AMI para una programación con retención basada en recuento, el cambio se aplica a todas las AMI (existentes y nuevas) que crea el programa.
- Si aumenta el periodo de eliminación de obsolescencia de AMI para una programación con retención basada en la antigüedad, el cambio solo se aplica a las AMI nuevas. Las AMI existentes no se ven afectadas.
- Si quita la regla de obsolescencia de AMI de una programación, Amazon Data Lifecycle Manager no cancelará la obsolescencia de las AMI que anteriormente habían quedado obsoletas en esa programación.
- Si reduce el recuento o el periodo de obsolescencia de AMI para una programación, Amazon Data Lifecycle Manager no cancelará la obsolescencia de las AMI que anteriormente habían quedado obsoletas en esa programación.
- Si da de baja manualmente una AMI creada por una política de AMI, Amazon Data Lifecycle Manager no anulará la obsolescencia.
- Si cancela manualmente la obsolescencia de una AMI que anteriormente había quedado obsoleta por una política de AMI, Amazon Data Lifecycle Manager no anulará la cancelación.
- Si una AMI se crea mediante varias programaciones conflictivas y una o varias de esas programaciones no tienen una regla de obsolescencia de AMI, Amazon Data Lifecycle Manager no dará de baja esa AMI.
- Si varias programaciones conflictivas crean una AMI y todas ellas tienen una regla de obsolescencia de AMI, Amazon Data Lifecycle Manager utilizará la regla de obsolescencia cuyo resultado sea la fecha de obsolescencia más tardía.

Las siguientes consideraciones se aplican a las políticas de AMI y a la Papelera de reciclaje:

- Si Amazon Data Lifecycle Manager cancela el registro de una AMI y la envía a la papelera de reciclaje cuando se alcanza el umbral de retención de la política y restaura manualmente la AMI desde la papelera de reciclaje, debe cancelar el registro de la AMI de forma manual cuando ya no sea necesaria. Amazon Data Lifecycle Manager dejará de administrar la AMI.
- Si cancela manualmente el registro de una AMI creada por una política y esa AMI se encuentra en la papelera de reciclaje cuando se alcanza el umbral de retención de la política, Amazon

Data Lifecycle Manager no cancelará el registro de la AMI. Amazon Data Lifecycle Manager no administra AMI mientras están en la papelera de reciclaje.

Si la AMI se restaura desde la papelera de reciclaje antes de alcanzar el umbral de retención de la política, Amazon Data Lifecycle Manager cancelará el registro de la AMI cuando se alcance el umbral de retención de la política.

Si la AMI se restaura desde la papelera de reciclaje una vez alcanzado el umbral de retención de la política, Amazon Data Lifecycle Manager ya no cancelará el registro de la AMI. Debe eliminarla manualmente cuando ya no la necesite.

Las siguientes consideraciones aplican a las políticas de AMI en estado error:

- Para políticas con una programación de retención basada en la edad, las AMI que están configuradas para caducar mientras la política está en estado `error` se conservan indefinidamente. Debe anular el registro de las AMI manualmente. Cuando vuelve a habilitar la política, Amazon Data Lifecycle Manager reanuda la eliminación de instantáneas o anula el registro de las AMI conforme terminen los periodos de retención.
- Para las políticas con programas de retención basados en el recuento, la política deja de crear y anular el registro de AMI mientras está en estado `error`. Cuando vuelve a habilitar la política, Amazon Data Lifecycle Manager reanuda la creación de instantáneas y AMI, y reanuda la eliminación de instantáneas o AMI a medida que se alcanza el límite de retención.

Las siguientes consideraciones se aplican a las políticas de AMI y a la desactivación de las AMI:

- Si deshabilita una AMI creada por Amazon Data Lifecycle Manager y esa AMI se deshabilita cuando se alcanza su umbral de retención, Amazon Data Lifecycle Manager anulará el registro de la AMI y eliminará las instantáneas asociadas.
- Si desactiva una AMI creada por Amazon Data Lifecycle Manager y archiva manualmente las instantáneas asociadas, y esas instantáneas se archivan cuando se alcanza su umbral de retención, Amazon Data Lifecycle Manager no eliminará esas instantáneas y dejará de administrarlas.

La siguiente consideración se aplica a las políticas de la AMI y a la protección de la anulación del registro de la AMI:

- Si habilita manualmente la protección de anulación del registro para una AMI creada por Amazon Data Lifecycle Manager y sigue habilitada cuando se alcanza el umbral de retención de la AMI, Amazon Data Lifecycle Manager ya no administra esa AMI. Debe anular manualmente el registro de la AMI y eliminar sus instantáneas subyacentes si ya no es necesaria.

Recursos adicionales de

Para obtener más información, consulte el blog Automating Amazon EBS snapshots and AMI management using Amazon Data Lifecycle Manager AWS Storage blog.

Automatizar copias instantáneas entre cuentas

La automatización de copias instantáneas entre cuentas permite copiar las instantáneas de Amazon EBS en regiones específicas de una cuenta aislada y cifrarlas con una clave de cifrado. Esto permite que pueda protegerse contra la pérdida de datos en caso de que su cuenta se vea comprometida.

La automatización de copias instantáneas entre cuentas implica dos cuentas:

- Cuenta de origen—La cuenta de origen es la cuenta que crea y comparte las instantáneas con la cuenta de destino. En esta cuenta, debe crear una política de instantáneas de EBS que cree instantáneas a intervalos establecidos y, a continuación, las comparta con otras cuentas. AWS
- Cuenta de destino—La cuenta de destino es la cuenta con la cuenta de destino con la que se comparten las instantáneas y es la que crea copias de las instantáneas compartidas. En esta cuenta, debe crear una política de eventos de copia entre cuentas que copia automáticamente instantáneas compartidas con ella por una o varias cuentas de origen especificadas.

Temas

Crear políticas de copia de instantáneas entre cuentas

A fin de preparar las cuentas de origen y destino para la copia instantánea entre cuentas, debe realizar los siguientes pasos:

Paso 1: crear la política de instantáneas de EBS (Cuenta de origen)

En la cuenta de origen, genere una política de instantáneas de EBS que creará las instantáneas y compártalas con las cuentas de destino necesarias.

Al crear la política, asegúrese de habilitar el uso compartido entre cuentas y de especificar AWS las cuentas de destino con las que compartir las instantáneas. Estas son las cuentas con las que se van a compartir las instantáneas. Si comparte instantáneas cifradas, debe conceder permiso a las cuentas de destino seleccionadas para utilizar la Clave de KMS usada con el fin de cifrar el volumen de origen. Para obtener más información, consulte Paso 2: compartir la Clave administrada por el cliente (cuenta de origen).

> **Note**
>
> Solo puede compartir instantáneas sin cifrar o cifradas mediante una Clave administrada por el cliente. No puede compartir instantáneas cifradas con la Clave de KMS de cifrado de EBS predeterminada. Si comparte instantáneas cifradas, también debe compartir la Clave de KMS que se utilizó para cifrar el volumen de origen con las cuentas de destino. Para obtener más información, consulte Permitir que los usuarios de otras cuentas utilicen una clave de KMS en la Guía para desarrolladores de AWS Key Management Service .

Para obtener más información acerca de la creación de una política de instantáneas de EBS, consulte Automatización de los ciclos de vida de las instantáneas.

Utilice uno de los métodos siguientes para crear la política de instantáneas de EBS.

Paso 2: compartir la Clave administrada por el cliente (cuenta de origen)

Si comparte instantáneas cifradas, debe otorgar al rol de IAM y a las cuentas de AWS de destino (que seleccionó en el paso anterior) los permisos necesarios para usar la clave administrada por el cliente que se utilizó para cifrar el volumen de origen.

> **Note**
>
> Realice este paso solo si va a compartir instantáneas cifradas. Si comparte instantáneas sin cifrar, omita este paso.

Console

1. Abra la AWS KMS consola en https://console.aws.amazon.com/kms.
2. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
3. En el panel de navegación, elija Customer managed key (Clave administradas por el cliente) y, a continuación, seleccione la clave de KMS que debe compartir con las cuentas de destino.

   Tome nota del ARN de la Clave de KMS, lo necesitará más tarde.
4. En la pestaña Política de claves, desplácese hacia abajo hasta la sección Usuarios de claves. Elija Add (Agregar), escriba el nombre del rol de IAM seleccionado en el paso anterior y, a continuación, elija Add (Agregar).
5. En la pestaña Políticas de claves, desplácese hacia abajo hasta la sección Otras cuentas de AWS . Selecciona Añadir otras AWS cuentas y, a continuación, añade todas las AWS cuentas de destino con las que decidiste compartir las instantáneas en el paso anterior.
6. Elija Save changes.

Command line

Utilice el comando get-key-policy para recuperar la política de clave que está actualmente asociada a la Clave de KMS.

Por ejemplo, el comando siguiente recupera la política de clave de una Clave de KMS con un ID de `9d5e2b3d-e410-4a27-a958-19e220d83a1e` y la escribe en un archivo denominado `snapshotKey.json`.

```
$ aws kms get-key-policy \
    --policy-name default \
    --key-id 9d5e2b3d-e410-4a27-a958-19e220d83a1e \
    --query Policy \
    --output text > snapshotKey.json
```

Abra la política de claves con el editor de texto preferido. Agregue el ARN del rol de IAM que especificó al crear la política de instantáneas y los ARN de las cuentas de destino con las que compartir la Clave de KMS.

Por ejemplo, en la siguiente política, agregamos el ARN del rol de IAM predeterminado y el ARN de la cuenta raíz para la cuenta de destino `222222222222`.

> **Tip**
>
> Para seguir el principio de privilegios mínimos, no permita el acceso completo a `kms:CreateGrant`. En su lugar, utilice la clave de `kms:GrantIsForAWSResource` condición para permitir al usuario crear concesiones en la clave de KMS solo cuando un AWS servicio cree la concesión en nombre del usuario, como se muestra en el siguiente ejemplo.

```
{
    "Sid" : "Allow use of the key",
    "Effect" : "Allow",
    "Principal" : {
        "AWS" : [
            "arn:aws:iam::111111111111:role/service-role/
AWSDataLifecycleManagerDefaultRole",
            "arn:aws:iam::222222222222:root"
        ]
    },
    "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource" : "*"
},
{
    "Sid" : "Allow attachment of persistent resources",
    "Effect" : "Allow",
    "Principal" : {
        "AWS" : [
            "arn:aws:iam::111111111111:role/service-role/
AWSDataLifecycleManagerDefaultRole",
            "arn:aws:iam::222222222222:root"
        ]
    },
    "Action" : [
```

```
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
    ],
    "Resource" : "*",
    "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
    }
}
```

Guarde y cierre el archivo. A continuación, utilice el comando put-key-policy para asociar la política de clave actualizada a la Clave de KMS.

```
$ aws kms put-key-policy \
    --policy-name default \
    --key-id 9d5e2b3d-e410-4a27-a958-19e220d83a1e \
    --policy file://snapshotKey.json
```

Paso 3: crear política de eventos de copia entre cuentas (Cuenta de destino)

En la cuenta de destino, debe crear una política de eventos de copia entre cuentas que copiará automáticamente instantáneas compartidas por las cuentas de origen necesarias.

Esta política solo se ejecuta en la cuenta de destino cuando una de las cuentas de origen especificadas comparte instantáneas con la cuenta.

Utilice uno de los métodos siguientes para crear la política de eventos de copia entre cuentas.

Console

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Elastic Block Store, Lifecycle Manager (Administrador de ciclo de vida) y, a continuación, Create lifecycle policy (Crear política de ciclo de vida).
3. En la pantalla Select policy type (Seleccionar tipo de política), elija Cross-account copy event policy (Política de eventos de copias entre cuentas) y, luego, seleccione Next (Siguiente).
4. En Policy description (Descripción de la política), escriba una breve descripción de la política.

5. En Policy tags (Etiquetas de políticas), agregue las etiquetas que se aplicarán a la política de ciclo de vida. Puede utilizar estas etiquetas para identificar y clasificar las políticas.
6. En la sección Event settings (Configuración de eventos), defina el evento de uso compartido de instantáneas que provocará la ejecución de la política. Haga lo siguiente:

   a. En el caso de las cuentas compartidas, especifique AWS las cuentas de origen desde las que desea copiar las instantáneas compartidas. Seleccione Añadir cuenta, introduzca el ID de AWS cuenta de 12 dígitos y, a continuación, seleccione Añadir.

   b. En Filter by description (Filtrar por descripción), ingrese la descripción requerida de la instantánea con una expresión regular. La política copia solo las instantáneas compartidas por las cuentas de origen especificadas y que tienen descripciones que coinciden con el filtro especificado. Para obtener más información, consulte Especificar filtros de descripción de instantáneas.
7. En IAM rol (Rol de IAM), elija el rol de IAM que tenga permisos para realizar acciones de copia de instantáneas. Para utilizar el rol predeterminado proporcionado por Amazon Data Lifecycle Manager, elija Default role (Rol predeterminado). De forma alternativa, para usar un rol de IAM personalizado que haya creado anteriormente, elija Choose another role (Elegir otro rol) y, luego, seleccione el rol que va a utilizar.

   Si copia instantáneas cifradas, debe conceder permisos al rol de IAM seleccionado para utilizar la Clave de KMS de cifrado usada con el fin de cifrar el volumen de origen. Del mismo modo, si cifra la instantánea en la región de destino mediante otra Clave de KMS, debe conceder permiso al rol de IAM para usar la Clave de KMS de destino. Para obtener más información, consulte Paso 4: permitir que el rol de IAM use la Claves de KMS requerida (cuenta de destino).
8. En la sección Copy action (Copiar acción), defina las acciones de copia de instantáneas que la política debe realizar cuando está activada. La política puede copiar instantáneas en hasta tres regiones. Debe especificar una regla de copia independiente para cada región de destino. Realice lo siguiente para cada regla que agregue:

   a. En Name (Nombre), escriba un nombre descriptivo para la acción de copia.

   b. En Target Region (Región de destino), seleccione la región en la que desea copiar las instantáneas.

   c. En Expire (Vencimiento), especifique cuánto tiempo se retendrán las copias de instantáneas en la región de destino después de su creación.

d. Para cifrar la copia de la instantánea, en Encryption (Cifrado), seleccione Enable encryption (Habilitar cifrado). Si la instantánea fuente se encuentra cifrada o si el cifrado de forma predeterminada se encuentra habilitado para su cuenta, siempre se cifra la copia de instantánea, incluso si no habilita el cifrado aquí. Si la instantánea de origen no está cifrada y el cifrado de forma predeterminada no está habilitado para su cuenta, puede elegir habilitar o deshabilitar el cifrado. Si habilita el cifrado, pero no especifica una Clave de KMS, las instantáneas se cifran mediante la Clave de KMS de cifrado predeterminada en cada región de destino. Si especifica una Clave de KMS para la región de destino, debe tener acceso a la Clave de KMS.

9. Para agregar acciones adicionales de copia de instantáneas, elija Add new Regions (Agregar regiones nuevas).
10. Para Policy status after creation (Estado de la política después de su creación), elija Enable policy (Habilitar política) para iniciar las ejecuciones de la política a la siguiente hora programada o Disable policy (Deshabilitar política) para evitar que se ejecute la política. Si no habilita la política ahora, no se comenzarán a copiar instantáneas hasta que la habilite de forma manual después de la creación.
11. Elija Create Policy.

Command line

Utilice el comando create-lifecycle-policy (crear política de ciclo de vida) para crear una política. Para crear una política de eventos de copia entre cuentas, para `PolicyType`, especifique `EVENT_BASED_POLICY`.

Por ejemplo, el siguiente comando crea una política de eventos de copia entre cuentas en la cuenta de destino `222222222222`. La política copia instantáneas compartidas por la cuenta de origen `111111111111`. La política copia instantáneas en `sa-east-1` y `eu-west-2`. Las instantáneas copiadas en `sa-east-1` no se cifran y se retienen durante 3 días. Las instantáneas copiadas en `eu-west-2` se cifran mediante la Clave de KMS `8af79514-350d-4c52-bac8-8985e84171c7` y se conservan durante 1 mes. La política utiliza el rol de IAM predeterminado.

```
$ aws dlm create-lifecycle-policy \
    --description "Copy policy" \
    --state ENABLED \
    --execution-role-arn arn:aws:iam::222222222222:role/service-role/
AWSDataLifecycleManagerDefaultRole \
```

```
    --policy-details file://policyDetails.json
```

A continuación se muestra el contenido del archivo `policyDetails.json`.

```
{
    "PolicyType" : "EVENT_BASED_POLICY",
    "EventSource" : {
        "Type" : "MANAGED_CWE",
        "Parameters": {
            "EventType" : "shareSnapshot",
            "SnapshotOwner": ["111111111111"]
        }
    },
    "Actions" : [{
        "Name" :"Copy Snapshot to Sao Paulo and London",
        "CrossRegionCopy" : [{
            "Target" : "sa-east-1",
             "EncryptionConfiguration" : {
                 "Encrypted" : false
             },
             "RetainRule" : {
             "Interval" : 3,
            "IntervalUnit" : "DAYS"
            }
        },
        {
            "Target" : "eu-west-2",
            "EncryptionConfiguration" : {
                 "Encrypted" : true,
                 "CmkArn" : "arn:aws:kms:eu-
west-2:222222222222:key/8af79514-350d-4c52-bac8-8985e84171c7"
            },
            "RetainRule" : {
                "Interval" : 1,
                "IntervalUnit" : "MONTHS"
            }
        }]
    }]
}
```

Si se ejecuta correctamente, el comando devuelve el ID de la política recién creada. A continuación, se muestra un ejemplo del resultado.

```
{
    "PolicyId": "policy-9876543210abcdef0"
}
```

Paso 4: permitir que el rol de IAM use la Claves de KMS requerida (cuenta de destino)

Si copia instantáneas cifradas, debe conceder permisos al rol de IAM (que seleccionó en el paso anterior) para utilizar la Clave administrada por el cliente que se usó con el fin de cifrar el volumen de origen.

> **Note**
>
> Realice este paso sólo si copia instantáneas cifradas. Si copia instantáneas sin cifrar, omita este paso.

Utilice uno de los siguientes métodos para agregar las políticas necesarias al rol de IAM.

Console

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Roles (Roles). Busque y elija el rol de IAM que seleccionó al crear la política de eventos de copia entre cuentas en el paso anterior. Si opta por usar el rol predeterminado, el rol recibe un nombre AWSDataLifecycleManagerDefaultRole.
3. Elija Add inline policy (Agregar política en línea) y, a continuación, seleccione la pestaña JSON.
4. Sustituya la política existente por la siguiente y especifique el ARN de la clave de KMS que se utilizó para cifrar los volúmenes de origen y que la cuenta de origen compartió con usted en el paso 2.

   > **Note**
   >
   > Si va a copiar desde varias cuentas de origen, debe especificar el ARN de la clave de KMS correspondiente de cada cuenta de origen.

En el ejemplo siguiente, la política concede permiso al rol de IAM para usar la Clave de KMS `1234abcd-12ab-34cd-56ef-1234567890ab`, que fue compartida por la cuenta de origen `111111111111` y la Clave de KMS `4567dcba-23ab-34cd-56ef-0987654321yz`, que existe en la cuenta de destino `222222222222`.

> **Tip**
>
> Para seguir el principio de privilegios mínimos, no permita el acceso completo a `kms:CreateGrant`. En su lugar, utilice la clave `kms:GrantIsForAWSResource` condicionada para permitir al usuario crear concesiones en la clave de KMS solo cuando un AWS servicio cree la concesión en nombre del usuario, como se muestra en el siguiente ejemplo.

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
           "Action": [
               "kms:RevokeGrant",
               "kms:CreateGrant",
               "kms:ListGrants"
           ],
           "Resource": [
               "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
               "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
           ],
           "Condition": {
               "Bool": {
                   "kms:GrantIsForAWSResource": "true"
               }
           }
       },
       {
           "Effect": "Allow",
           "Action": [
```

```
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
                "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
            ]
        }
    ]
}
```

5. Elija Review policy
6. En Name (Nombre), escriba un nombre descriptivo para la política y, a continuación, elija Create policy (Crear política).

Command line

Con el uso de su editor de texto preferido, cree un nuevo archivo JSON llamado `policyDetails.json`. Agregue la siguiente política y especifique el ARN de la clave de KMS que se utilizó para cifrar los volúmenes de origen y que la cuenta de origen compartió con usted en el paso 2.

> **Note**
>
> Si va a copiar desde varias cuentas de origen, debe especificar el ARN de la clave de KMS correspondiente de cada cuenta de origen.

En el ejemplo siguiente, la política concede permiso al rol de IAM para usar la Clave de KMS `1234abcd-12ab-34cd-56ef-1234567890ab`, que fue compartida por la cuenta de origen `111111111111` y la Clave de KMS `4567dcba-23ab-34cd-56ef-0987654321yz`, que existe en la cuenta de destino `222222222222`.

> **Tip**
>
> Para seguir el principio de privilegios mínimos, no permita el acceso completo a `kms:CreateGrant`. En su lugar, utilice la clave `kms:GrantIsForAWSResource` condicionada para permitir al usuario crear concesiones en la clave KMS únicamente cuando un AWS servicio cree la concesión en nombre del usuario, como se muestra en el siguiente ejemplo.

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
           "Action": [
               "kms:RevokeGrant",
               "kms:CreateGrant",
               "kms:ListGrants"
           ],
           "Resource": [
               "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
               "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
           ],
           "Condition": {
               "Bool": {
                   "kms:GrantIsForAWSResource": "true"
               }
           }
       },
       {
           "Effect": "Allow",
           "Action": [
               "kms:Encrypt",
               "kms:Decrypt",
               "kms:ReEncrypt*",
               "kms:GenerateDataKey*",
               "kms:DescribeKey"
           ],
           "Resource": [
```

```
                "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
                "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
            ]
        }
    ]
}
```

Guarde y cierre el archivo. A continuación, utilice el comando put-role-policy (colocar una política de rol) para agregar la política al rol de IAM.

Por ejemplo

```
$ aws iam put-role-policy \
    --role-name AWSDataLifecycleManagerDefaultRole \
    --policy-name CopyPolicy \
    --policy-document file://AdminPolicy.json
```

Especificar filtros de descripción de instantáneas

Al crear la política de copia de instantáneas en la cuenta de destino, debe especificar un filtro de descripción de instantánea. El filtro de descripción de instantáneas lo habilita para especificar un nivel adicional de filtrado que permite controlar qué instantáneas se copian mediante la política. Esto significa que la política sólo copia una instantánea si la comparte una de las cuentas de origen especificadas y tiene una descripción de instantánea que coincide con el filtro especificado. En otras palabras, si una de las cuentas de curso especificadas comparte una instantánea, pero no tiene una descripción que coincida con el filtro especificado, la política no la copia.

La descripción del filtro de instantáneas debe especificarse mediante una expresión regular. Es un campo obligatorio cuando se crean políticas de eventos de copia entre cuentas mediante la consola y la línea de comandos. Las siguientes son expresiones regulares de ejemplo que se pueden utilizar:

- `.*`—Este filtro coincide con todas las descripciones de instantáneas. Si utiliza esta expresión, la política copiará todas las instantáneas compartidas por una de las cuentas de origen especificadas.
- `Created for policy: policy-0123456789abcdef0.*`—Este filtro sólo coincide con las instantáneas creadas por una política con un ID de `policy-0123456789abcdef0`. Si utiliza una expresión como esta, sólo las instantáneas compartidas con su cuenta por una de las cuentas de

origen especificadas y que hayan sido creadas por una política con el ID especificado se copiarán por la política.

- `.*production.*`—Este filtro coincide con cualquier instantánea que tenga la palabra en `production` cualquier lugar de la descripción. Si utiliza esta expresión, la política copiará todas las instantáneas compartidas por una de las cuentas de origen especificadas y que tengan el texto especificado en su descripción.

Consideraciones sobre las políticas de copia de instantáneas entre cuentas

Las siguientes consideraciones se aplican a las políticas de eventos de copia entre cuentas:

- Solo puede copiar instantáneas sin cifrar o cifradas mediante una Clave administrada por el cliente.
- Puede crear una política de eventos de copia entre cuentas para copiar instantáneas que estén compartidas fuera de Amazon Data Lifecycle Manager.
- Si desea cifrar instantáneas en la cuenta de destino, el rol de IAM seleccionado para la política de eventos de copia entre cuentas debe tener permiso a fin de usar la Clave de KMS requerida.

Recursos adicionales de

Para obtener más información, consulte el blog Cómo automatizar la copia de instantáneas cifradas de Amazon EBS en el almacenamiento de AWS cuentas AWS .

Ver, modificar y eliminar políticas de ciclo de vida

Utilice los siguientes procedimientos para ver, modificar y eliminar políticas de ciclo de vida existentes.

Temas

Ver políticas de ciclo de vida

Utilice uno de los siguientes procedimientos para ver una política de ciclo de vida.

Console

Para ver una política de ciclo de vida

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Elastic Block Store, Lifecycle Manager (Administrador de ciclo de vida).
3. Seleccione el ID de una política de ciclo de vida de la lista.

Command line

Obtener información resumida sobre las políticas de ciclo de vida

Use el comando get-lifecycle-policies.

```
aws dlm get-lifecycle-policies
```

Mostrar información acerca de una política de ciclo de vida específica

Use el comando get-lifecycle-policies. En `--policy-id`, especifique el ID de la política que desea ver.

```
aws dlm get-lifecycle-policy --policy-id policy-0123456789abcdef0
```

Modificar políticas de ciclo de vida

Consideraciones sobre la modificación de políticas

- Si modifica una política de AMI o instantánea eliminando sus etiquetas de destino, la política deja de administrar los volúmenes o las instancias que tengan esas etiquetas.
- Si modifica el nombre de una programación, la política deja de administrar las instantáneas o AMI creadas con el nombre anterior de la programación.
- Si modifica una programación de retención basada en antigüedad para utilizar un nuevo intervalo de tiempo, este último solo se utilizará para las nuevas instantáneas o AMI creadas después del cambio. La nueva programación no afecta a la programación de retención de instantáneas o las AMI creadas antes del cambio.

- No se puede cambiar la programación de retención de una política de basada en recuento a basada en antigüedad después de crearla. Para realizar este cambio, debe crear una política nueva.
- Si deshabilita una política con una programación de retención basada en la edad, las instantáneas o las AMI que están configuradas para caducar mientras la política está deshabilitada se conservan indefinidamente. Debe eliminar las instantáneas o anular el registro de las AMI manualmente. Cuando vuelve a habilitar la política, Amazon Data Lifecycle Manager reanuda la eliminación de instantáneas o anula el registro de las AMI conforme terminen los periodos de retención.
- Si deshabilita una política con una programación de retención basada en el recuento, la política deja de crear y eliminar instantáneas o AMI. Cuando vuelve a habilitar la política, Amazon Data Lifecycle Manager reanuda la creación de instantáneas y AMI, y reanuda la eliminación de instantáneas o AMI a medida que se alcanza el límite de retención.
- Si elimina una política que tiene una política habilitada para el archivado de instantáneas, Amazon Data Lifecycle Manager dejará de administrar las instantáneas que estén en el nivel de archivo en el momento de la deshabilitación de la política. Debe eliminar manualmente la instantánea si deja de ser necesaria.
- Si habilita el archivado de instantáneas según una programación basada en recuentos, la regla de archivado se aplica a todas las instantáneas nuevas que se creen y archiven según la programación así como a las instantáneas existentes que se hayan creado y archivado anteriormente según la programación.
- Si habilita el archivado de instantáneas según una programación basada en la antigüedad, la regla de archivado solo se aplica a las instantáneas nuevas que se han creado después de habilitar el archivado de instantáneas. Las instantáneas existentes que se crearon antes de habilitar el archivado de instantáneas se siguen eliminando de sus respectivos niveles de almacenamiento, de acuerdo con la programación establecida cuando dichas instantáneas se crearon y archivaron originalmente.
- Si desactiva el archivado de instantáneas de una programación basada en recuentos, dicha programación detiene inmediatamente el archivado de instantáneas. Las instantáneas que se archivaron anteriormente según la programación permanecen en el nivel de archivo y Amazon Data Lifecycle Manager no las eliminará.
- Si desactiva el archivado de instantáneas para una programación basada en la antigüedad, las instantáneas que crea la política y que están programadas para archivarse se eliminan de forma permanente en la fecha y hora programadas para el archivado, tal y como indica la etiqueta del sistema `aws:dlm:expirationTime`.

- Si desactiva el archivado de instantáneas de una programación, dicha programación detiene inmediatamente el archivado de instantáneas. Las instantáneas que se archivaron anteriormente según la programación permanecen en el nivel de archivo y Amazon Data Lifecycle Manager no las eliminará.
- Si modifica el recuento de retención de archivos para una programación basada en recuentos, el nuevo recuento de retención incluirá las instantáneas existentes que se archivaron anteriormente según la programación.
- Si modifica el periodo de retención de archivos para una programación basada en la antigüedad, el nuevo periodo de retención solo se aplicará a las instantáneas que se archiven después de modificar la regla de retención.

Utilice uno de los siguientes procedimientos para modificar una política de ciclo de vida.

Console

Para modificar una política de ciclo de vida

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Elastic Block Store, Lifecycle Manager (Administrador de ciclo de vida).
3. Seleccione una política de ciclo de vida de la lista.
4. Elija Acciones, Modificar política de ciclo de vida.
5. Modifique la configuración de la política según sea necesario. Por ejemplo, puede modificar la programación, añadir o eliminar etiquetas, o habilitar o deshabilitar la política.
6. Seleccione Modificar política.

Command line

Utilice el comando update-lifecycle-policy para modificar la información de una política de ciclo de vida. Para simplificar la sintaxis, este ejemplo hace referencia a un archivo JSON, `policyDetailsUpdated.json`, que incluye los detalles de la política.

```
aws dlm update-lifecycle-policy \
    --state DISABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole" \
```

```
    --policy-details file://policyDetailsUpdated.json
```

A continuación se muestra un ejemplo del archivo `policyDetailsUpdated.json`.

```
{
   "ResourceTypes":[
      "VOLUME"
   ],
   "TargetTags":[
      {
         "Key": "costcenter",
         "Value": "120"
      }
   ],
   "Schedules":[
      {
         "Name": "DailySnapshots",
         "TagsToAdd": [
            {
               "Key": "type",
               "Value": "myDailySnapshot"
            }
         ],
         "CreateRule": {
            "Interval": 12,
            "IntervalUnit": "HOURS",
            "Times": [
               "15:00"
            ]
         },
         "RetainRule": {
            "Count" :5
         },
         "CopyTags": false
      }
   ]
}
```

Para ver la política actualizada, use el comando `get-lifecycle-policy`. Puede ver que el estado, el valor de la etiqueta, el intervalo de instantánea y la hora de inicio de la instantánea han cambiado.

Eliminar políticas de ciclo de vida

Consideraciones sobre la modificación de políticas

- Al eliminar una política, las instantáneas o las AMI que crea esa directiva no se eliminan automáticamente. Si ya no necesita las instantáneas o las AMI, debe eliminarlas manualmente.
- Si elimina una política que tiene una política habilitada para el archivado de instantáneas, Amazon Data Lifecycle Manager dejará de administrar las instantáneas que estén en el nivel de archivo en el momento de la eliminación de la política. Debe eliminar manualmente la instantánea si deja de ser necesaria.
- Si elimina una política con una programación basada en la antigüedad y habilitada para el archivado, las instantáneas que crea la política y que están programadas para archivarse se eliminan permanentemente en la fecha y la hora de archivado programadas, según se indicada en la etiqueta del sistema `aws:dlm:expiretime`.

Utilice uno de los siguientes procedimientos para eliminar una política de ciclo de vida.

Console

Para eliminar una política de ciclo de vida

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Elastic Block Store, Lifecycle Manager (Administrador de ciclo de vida).
3. Seleccione una política de ciclo de vida de la lista.
4. Elija Acciones, Eliminar política de ciclo de vida.
5. Cuando se le pida confirmación, elija Eliminar política.

Command line

Utilice el comando delete-lifecycle-policy para eliminar una política de ciclo de vida y liberar las etiquetas de destino especificadas en la política para que se puedan reutilizar.

> **Note**
>
> Solo se pueden eliminar instantáneas creadas por Amazon Data Lifecycle Manager.

```
aws dlm delete-lifecycle-policy --policy-id policy-0123456789abcdef0
```

La Referencia de la API de Administrador de ciclo de vida de datos de Amazon ofrece descripciones y sintaxis para cada una de las acciones y tipos de datos de la API de consulta de Amazon Data Lifecycle Manager.

Como alternativa, puede utilizar uno de los AWS SDK para acceder a la API de una forma que se adapte al lenguaje de programación o la plataforma que utilice. Para obtener más información, consulte SDK de AWS.

AWS Identity and Access Management

Se requieren credenciales para acceder a Amazon Data Lifecycle Manager. Estas credenciales deben tener permisos para acceder a recursos de AWS como instancias, volúmenes, instantáneas y AMI. En las siguientes secciones, se proporcionan detalles sobre cómo se puede utilizar AWS Identity and Access Management (IAM) y se ayuda a proteger el acceso a los recursos.

Temas

- AWS políticas gestionadas
- Funciones de servicio de IAM
- Permisos para los usuarios
- Permisos para cifrado

AWS políticas gestionadas

Una política AWS gestionada es una política independiente creada y administrada por AWS. AWS las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes. AWS Las políticas administradas permiten asignar los permisos adecuados a los usuarios, grupos y roles de forma más eficiente que si tuviera que escribir las políticas usted mismo.

Sin embargo, no puede cambiar los permisos definidos en las políticas AWS administradas. AWS actualiza ocasionalmente los permisos definidos en una política AWS administrada. Cuando esto ocurre, la actualización afecta a todas las entidades principales (usuarios, grupos y roles) a los que está asociada la política.

Amazon Data Lifecycle Manager proporciona políticas AWS administradas para casos de uso comunes. Estas políticas facilitan la definición de los permisos adecuados y controlan el acceso a los recursos. Las políticas AWS gestionadas que proporciona Amazon Data Lifecycle Manager están diseñadas para adjuntarse a las funciones que se transfieran a Amazon Data Lifecycle Manager.

Temas

AWSDataLifecycleManagerServiceRole

La AWSDataLifecycleManagerServiceRolepolítica proporciona los permisos adecuados a Amazon Data Lifecycle Manager para crear y gestionar las políticas de instantáneas de Amazon EBS y las políticas de eventos de copia multicuenta.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots",
                "ec2:DeleteSnapshot",
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots",
                "ec2:EnableFastSnapshotRestores",
                "ec2:DescribeFastSnapshotRestores",
                "ec2:DisableFastSnapshotRestores",
                "ec2:CopySnapshot",
                "ec2:ModifySnapshotAttribute",
                "ec2:DescribeSnapshotAttribute",
                "ec2:ModifySnapshotTier",
                "ec2:DescribeSnapshotTierStatus"
            ],
            "Resource": "*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "events:PutRule",
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/AwsDataLifecycleRule.managed-cwe.*"
        }
    ]
}
```

AWSDataLifecycleManagerServiceRoleForAMIManagement

La AWSDataLifecycleManagerServiceRoleForAMIManagementpolítica proporciona los permisos adecuados a Amazon Data Lifecycle Manager para crear y gestionar políticas de AMI respaldadas por Amazon EBS-Click.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*::snapshot/*",
                "arn:aws:ec2:*::image/*"
            ]
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeImageAttribute",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteSnapshot",
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ResetImageAttribute",
                "ec2:DeregisterImage",
                "ec2:CreateImage",
                "ec2:CopyImage",
                "ec2:ModifyImageAttribute"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:EnableImageDeprecation",
                "ec2:DisableImageDeprecation"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        }
    ]
}
```

AWSDataLifecycleManagerSSMFullAccess

Otorga permiso a Amazon Data Lifecycle Manager para que realice las acciones de Systems Manager necesarias para ejecutar scripts previos y posteriores en todas las instancias de Amazon EC2.

> **Important**
>
> La política administrada utiliza la clave de condición `aws:ResourceTag` para restringir el acceso a documentos de SSM específicos cuando se utilizan scripts previos y posteriores. Para permitir que Amazon Data Lifecycle Manager acceda a los documentos de SSM, debe asegurarse de que sus documentos de SSM estén etiquetados con `DLMScriptsAccess:true`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSSMReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "ssm:GetCommandInvocation",
                "ssm:ListCommands",
                "ssm:DescribeInstanceInformation"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowTaggedSSMDocumentsOnly",
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:DescribeDocument",
                "ssm:GetDocument"
            ],
            "Resource": [
                "arn:aws:ssm:*:*:document/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/DLMScriptsAccess": "true"
                }
            }
        },
        {
            "Sid": "AllowSpecificAWSOwnedSSMDocuments",
            "Effect": "Allow",
```

```
            "Action": [
                "ssm:SendCommand",
                "ssm:DescribeDocument",
                "ssm:GetDocument"
            ],
            "Resource": [
                "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
                "arn:aws:ssm:*:*:document/AWSSystemsManagerSAP-
CreateDLMSnapshotForSAPHANA"
            ]
        },
        {
            "Sid": "AllowAllEC2Instances",
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ]
        }
    ]
}
```

AWS actualizaciones de políticas gestionadas

AWS los servicios mantienen y AWS actualizan las políticas gestionadas. No puede cambiar los permisos en las políticas AWS gestionadas. En ocasiones, los servicios añaden permisos adicionales a una política AWS gestionada para admitir nuevas funciones. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Lo más probable es que los servicios actualicen una política AWS administrada cuando se lanza una nueva función o cuando hay nuevas operaciones disponibles. Los servicios no eliminan los permisos de una política AWS administrada, por lo que las actualizaciones de la política no afectarán a los permisos existentes.

En la siguiente tabla se proporcionan detalles sobre las actualizaciones de las políticas AWS gestionadas de Amazon Data Lifecycle Manager desde que este servicio comenzó a realizar el seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en Historial de documentos para la guía del usuario de Amazon EBS.

Cambio	Descripción	Fecha
AWSDataLifecycleManagerSSMFullAccess— Se actualizaron los permisos de la política.	Se actualizó la política para admitir instantáneas coherentes con las aplicaciones para SAP HANA mediante el documento de SSM `AWSSystemsManagerSAP-CreateDLMSnapshotForSAPHANA` .	17 de noviembre de 2023
AWSDataLifecycleManagerSSMFullAccess— Se ha añadido una nueva política AWS gestionada.	Amazon Data Lifecycle Manager ha añadido la política AWSDataLifecycleManagerSSMFullAccess AWS gestionada.	7 de noviembre de 2023
AWSDataLifecycleManagerServiceRole— Se agregaron permisos para admitir el	Amazon Data Lifecycle Manager ha agregado las acciones `ec2:ModifySnapshotTier` y	30 de septiembre de 2022

Cambio	Descripción	Fecha
archivado de instantáneas.	`ec2:DescribeSnapshotTierStatus` a fin de conceder permiso a las políticas de instantáneas para archivar instantáneas y comprobar el estado del archivo de las instantáneas.	
AWSDataLifecycleManagerServiceRoleForAMIManagement— Se agregaron permisos para admitir la obsolescencia de la AMI.	Amazon Data Lifecycle Manager agregó las acciones `ec2:EnableImageDeprecation` y `ec2:DisableImageDeprecation` para conceder permisos a políticas de la AMI respaldadas por EBS a fin de habilitar y desactivar la obsolescencia de la AMI.	23 de agosto de 2021

Cambio	Descripción	Fecha
Amazon Data Lifecycle Manager comenzó a realizar el seguimiento de los cambios	Amazon Data Lifecycle Manager comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	23 de agosto de 2021

Funciones de servicio de IAM

Una función AWS Identity and Access Management (IAM) es similar a la de un usuario, en el sentido de que es una AWS identidad con políticas de permisos que determinan lo que la identidad puede y no puede hacer en AWS ella. No obstante, en lugar de asociarse exclusivamente a una persona, la intención es que cualquier usuario pueda asumir un rol que necesite. Una función de servicio es una función que asume un AWS servicio para realizar acciones en tu nombre. Como un servicio que realiza las operaciones de copia de seguridad en su nombre, Amazon Data Lifecycle Manager requiere transferirle un rol que debe adoptar al realizar las operaciones de políticas en su nombre. Para obtener más información acerca de los roles de IAM, consulte Roles de IAM en la guía del usuario de IAM.

El rol que transfiera a Amazon Data Lifecycle Manager debe tener una política de IAM con los permisos que permitan a Amazon Data Lifecycle Manager realizar acciones asociadas con operaciones de política, como crear instantáneas y AMI, copiar instantáneas y AMI, eliminar instantáneas y anular el registro de AMI. Se requieren permisos diferentes para cada uno de los tipos de política de Amazon Data Lifecycle Manager. Además, el rol también debe incluir a Amazon Data Lifecycle Manager como entidad de confianza, lo que permite a Amazon Data Lifecycle Manager asumir el rol.

Temas

- Funciones de servicio predeterminadas de Amazon Data Lifecycle Manager
- Funciones de servicio personalizadas para Amazon Data Lifecycle Manager

Funciones de servicio predeterminadas de Amazon Data Lifecycle Manager

Amazon Data Lifecycle Manager utiliza las siguientes funciones de servicio predeterminadas:

- AWSDataLifecycleManagerDefaultRole: función predeterminada para administrar las instantáneas. Solo confía en el servicio `dlm.amazonaws.com` para asumir el rol y permite a Amazon Data Lifecycle Manager realizar las acciones requeridas por las políticas de instantáneas y de copia de instantáneas entre cuentas en su nombre. Este rol usa la política `AWSDataLifecycleManagerServiceRole` AWS administrada.

  > **Note**
  >
  > El formato de ARN del rol varía en función de si se crea mediante la consola o la AWS CLI. Si el rol se crea mediante la consola, el formato de ARN es `arn:aws:iam::`*`account_id`*`:role/service-role/AWSDataLifecycleManagerDefaultRole`. Si el rol se creó con AWS CLI, el formato ARN es. `arn:aws:iam::`*`account_id`*`:role/AWSDataLifecycleManagerDefaultRole`

- AWSDataLifecycleManagerDefaultRoleForAMIManagement: función predeterminada para administrar las AMI. Solo confía en el servicio `dlm.amazonaws.com` para asumir el rol y permite a Amazon Data Lifecycle Manager realizar las acciones requeridas por las políticas de AMI respaldadas por EBS en su nombre. Este rol usa la política `AWSDataLifecycleManagerServiceRoleForAMIManagement` AWS administrada.

Si utiliza la consola Amazon Data Lifecycle Manager, Amazon Data Lifecycle Manager crea automáticamente el rol de AWSDataLifecycleManagerDefaultRoleservicio la primera vez que crea una política de instantáneas o copias de instantáneas entre cuentas, y crea automáticamente el rol de AWSDataLifecycleManagerDefaultRoleForAMIManagementservicio la primera vez que crea una política de AMI respaldada por EBS.

Si no utiliza la consola, puede crear de forma manual las funciones de servicio mediante el comando create-default-role. Para`--resource-type`, especifique si `snapshot` desea crear AWSDataLifecycleManagerDefaultRole o `image` crear. AWSDataLifecycleManagerDefaultRoleForAMIManagement

```
$ aws dlm create-default-role --resource-type snapshot|image
```

Si elimina las funciones de servicio predeterminadas y necesita crearlas de nuevo, puede utilizar el mismo proceso para volver a crearlas en su cuenta.

Funciones de servicio personalizadas para Amazon Data Lifecycle Manager

Como alternativa a la utilización de las funciones de servicio predeterminadas, puede crear roles de IAM personalizados con los permisos necesarios y seleccionarlos cuando cree una política de ciclo de vida.

Para crear un rol de IAM personalizado

1. Cree roles con los siguientes permisos.

   - Permisos requeridos para administrar políticas de ciclo de vida de instantáneas

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots",
                "ec2:DeleteSnapshot",
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots",
                "ec2:EnableFastSnapshotRestores",
                "ec2:DescribeFastSnapshotRestores",
                "ec2:DisableFastSnapshotRestores",
                "ec2:CopySnapshot",
                "ec2:ModifySnapshotAttribute",
                "ec2:DescribeSnapshotAttribute",
                "ec2:ModifySnapshotTier",
                "ec2:DescribeSnapshotTierStatus"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
```

```
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "events:PutRule",
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/AwsDataLifecycleRule.managed-
cwe.*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetCommandInvocation",
                "ssm:ListCommands",
                "ssm:DescribeInstanceInformation"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:DescribeDocument",
                "ssm:GetDocument"
            ],
            "Resource": [
                "arn:aws:ssm:*:*:document/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/DLMScriptsAccess": "true"
                }
            }
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "ssm:SendCommand",
                "ssm:DescribeDocument",
                "ssm:GetDocument"
            ],
            "Resource": [
                "arn:aws:ssm:*::document/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Condition": {
                "StringNotLike": {
                    "aws:ResourceTag/DLMScriptsAccess": "false"
                }
            }
        }
    ]
}
```

- Permisos requeridos para administrar políticas de ciclo de vida de AMI

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*::snapshot/*",
                "arn:aws:ec2:*::image/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
```

```
                "ec2:DescribeImageAttribute",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteSnapshot",
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ResetImageAttribute",
                "ec2:DeregisterImage",
                "ec2:CreateImage",
                "ec2:CopyImage",
                "ec2:ModifyImageAttribute"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:EnableImageDeprecation",
                "ec2:DisableImageDeprecation"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        }
    ]
}
```

Para obtener más información, consulte Creating a role (Creación de un rol) en Guía del usuario de IAM.

2. Agregue una relación de confianza a los roles.

   a. En la consola de IAM, seleccione Roles (Funciones).

   b. Seleccione los roles que ha creado y, a continuación, elija Trust relationships (Relaciones de confianza).

c. Elija Edit Trust Relationship (Editar relación de confianza), añada la siguiente política y después elija Update Trust Policy (Actualizar política de confianza).

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

Le recomendamos que utilice las claves de condición `aws:SourceAccount` y `aws:SourceArn` para protegerse contra el problema del suplente confuso. Por ejemplo, podría agregar el siguiente bloque de condición a la política de confianza anterior. `aws:SourceAccount` es el propietario de la política de ciclo de vida y `aws:SourceArn` es el ARN de la política del ciclo de vida. Si no conoce el ID de la política del ciclo de vida, puede reemplazar esa parte del ARN por un comodín (*) y, a continuación, actualizar la política de confianza después de crear la política del ciclo de vida.

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account_id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:partition:dlm:region:account_id:policy/policy_id"
    }
}
```

Permisos para los usuarios

Un usuario debe tener los siguientes permisos para utilizar Amazon Data Lifecycle Manager.

Note

- Los permisos `ec2:DescribeAvailabilityZones`, `ec2:DescribeRegions`, `kms:ListAliases` y `kms:DescribeKey` solo son necesarios para los usuarios de la consola. Si no es necesario el acceso a la consola, puede eliminar los permisos.
- El formato ARN del AWSDataLifecycleManagerDefaultRolerol varía en función de si se creó con la consola o con. AWS CLI Si el rol se crea mediante la consola, el formato de ARN es `arn:aws:iam::`*`account_id`*`:role/service-role/AWSDataLifecycleManagerDefaultRole`. Si el rol se creó con AWS CLI, el formato ARN es `arn:aws:iam::`*`account_id`*`:role/AWSDataLifecycleManagerDefaultRole` La siguiente política asume que el rol se creó con. AWS CLI

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "dlm:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::accound_id:role/service-role/
AWSDataLifecycleManagerDefaultRole",
                "arn:aws:iam::accound_id:role/service-role/
AWSDataLifecycleManagerDefaultRoleForAMIManagement"
                ]
        },
        {
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeRegions",
                "kms:ListAliases",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obtener más información, consulte Cambio de los permisos de un usuario de IAM en la Guía del usuario de IAM.

Permisos para cifrado

Tenga en cuenta lo siguiente cuando trabaje con Amazon Data Lifecycle Manager y recursos cifrados.

- Si el volumen de origen está cifrado, asegúrese de que los roles predeterminados de Amazon Data Lifecycle Manager (AWSDataLifecycleManagerDefaultRoley AWSDataLifecycleManagerDefaultRoleForAMIManagement) tengan permiso para usar las claves de KMS utilizadas para cifrar el volumen.
- Si habilita Cross Region copy (Copia entre regiones) para instantáneas no cifradas o AMI respaldadas por instantáneas no cifradas y elige habilitar el cifrado en la región de destino, asegúrese de que los roles predeterminados tengan permiso para usar la Clave de KMS necesaria a fin de realizar el cifrado en la región de destino.
- Si habilita Cross Region copy (copia entre regiones) para instantáneas cifradas o AMI respaldadas por instantáneas cifradas, asegúrese de que los roles predeterminados tengan permiso a fin de usar tanto la Claves de KMS de origen como de destino.
- Si habilita el archivado de instantáneas para las instantáneas cifradas, asegúrese de que el rol predeterminado de Amazon Data Lifecycle Manager (AWSDataLifecycleManagerDefaultRoletiene permiso) para usar la clave de KMS utilizada para cifrar la instantánea.

Para obtener más información, consulte Permitir que los usuarios de otras cuentas utilicen una clave de KMS en la Guía para desarrolladores de AWS Key Management Service .

Monitorizar el ciclo de vida de las instantáneas y las AMI

Puede utilizar las siguientes características para monitorizar el ciclo de vida de las instantáneas.

Características

- Consola y AWS CLI
- AWS CloudTrail
- Supervise sus políticas mediante CloudWatch Events
- Supervisa tus políticas con Amazon CloudWatch

Consola y AWS CLI

Puede ver las políticas de ciclo de vida con la consola de Amazon EC2 o la AWS CLI. Cada instantánea y AMI creada por una política tiene una marca temporal y etiquetas relacionadas con políticas. Puede filtrar instantáneas y las AMI mediante estas etiquetas para comprobar que las copias de seguridad se creen como lo desea. Para obtener información sobre cómo consultar las políticas de ciclo de vida con la consola, consulte Ver políticas de ciclo de vida.

AWS CloudTrail

Con ella AWS CloudTrail, puede realizar un seguimiento de la actividad de los usuarios y del uso de las API para demostrar el cumplimiento de las políticas internas y las normas reglamentarias. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.

Supervise sus políticas mediante CloudWatch Events

Amazon EBS y Amazon Data Lifecycle Manager emiten eventos relacionados con acciones de políticas de ciclo de vida. Puede utilizar AWS Lambda Amazon CloudWatch Events para gestionar las notificaciones de eventos mediante programación. Los eventos se emiten en la medida de lo posible. Para obtener más información, consulta la Guía del usuario de Amazon CloudWatch Events.

Están disponibles los siguientes eventos:

> **Note**
>
> No se emiten eventos para las acciones de política de ciclo de vida de la AMI.

- `createSnapshot`: un evento de Amazon EBS emitido cuando una acción `CreateSnapshot` se realiza correctamente o produce un error. Para obtener más información, consulte Amazon EventBridge para Amazon EBS.
- `DLM Policy State Change`: un evento de Amazon Data Lifecycle Manager emitido cuando una política de ciclo de vida pasa a tener un estado de error. El evento contiene una descripción de la causa del error.

  A continuación, se muestra un ejemplo de un evento cuando los permisos concedidos por el rol de IAM son insuficientes

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-0123456789ab",
    "detail-type": "DLM Policy State Change",
    source": "aws.dlm",
    "account": "123456789012",
    "time": "2018-05-25T13:12:22Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"
    ],
    "detail": {
        "state": "ERROR",
        "cause": "Role provided does not have sufficient permissions",
        "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/
policy-0123456789abcdef"
    }
}
```

  A continuación, se muestra un ejemplo de un evento cuando se supera el límite.

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-0123456789ab",
    "detail-type": "DLM Policy State Change",
    "source": "aws.dlm",
    "account": "123456789012",
    "time": "2018-05-25T13:12:22Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"
```

```
    ],
    "detail":{
        "state": "ERROR",
        "cause": "Maximum allowed active snapshot limit exceeded",
        "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/
policy-0123456789abcdef"
    }
}
```

- `DLM Pre Post Script Notification`: un evento que se emite cuando un script previo o posterior se inicia, se ejecuta correctamente o falla.

  A continuación, se muestra un ejemplo de un evento cuando una copia de seguridad de VSS se realiza correctamente.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "DLM Pre Post Script Notification",
    "source": "aws.dlm",
    "account": "123456789012",
    "time": "2023-10-27T22:04:52Z",
    "region": "us-east-1",
    "resources": ["arn:aws:dlm:us-east-1:123456789012:policy/
policy-01234567890abcdef"],
    "detail": {
        "script_stage": "",
        "result": "success",
        "cause": "",
        "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/
policy-01234567890abcdef",
        "execution_handler": "AWS_VSS_BACKUP",
        "source": "arn:aws:ec2:us-east-1:123456789012:instance/i-01234567890abcdef",
        "resource_type": "EBS_SNAPSHOT",
        "resources": [{
            "status": "pending",
            "resource_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
            "source": "arn:aws:ec2:us-east-1:123456789012:volume/
vol-01234567890abcdef"
        }],
        "request_id": "a1b2c3d4-a1b2-a1b2-a1b2-a1b2c3d4e5f6",
        "start_time": "2023-10-27T22:03:29.370Z",
        "end_time": "2023-10-27T22:04:51.370Z",
```

```
        "timeout_time": ""
    }
}
```

Supervisa tus políticas con Amazon CloudWatch

Puede monitorizar sus políticas de ciclo de vida de Amazon Data Lifecycle Manager mediante CloudWatch, que recopila datos sin procesar y los procesa en métricas legibles prácticamente en tiempo real. Puede utilizar estas métricas para ver exactamente cuántas instantáneas de Amazon EBS y AMI respaldadas por EBS se crean, eliminan y copian en sus políticas a lo largo del tiempo. También puede establecer alarmas que vigilen determinados umbrales y enviar notificaciones o realizar acciones cuando se cumplan dichos umbrales.

Estas métricas se conservan durante un periodo de 15 meses, de forma que pueda tener acceso a información histórica y comprender mejor el desempeño de sus políticas de ciclo de vida durante un periodo prolongado.

Para obtener más información sobre Amazon CloudWatch, consulta la Guía del CloudWatch usuario de Amazon.

Temas

- Métricas admitidas
- Vea CloudWatch las métricas de sus políticas
- Métricas de gráficos para las políticas
- Cree una CloudWatch alarma para una política
- Ejemplos de casos de uso
- Administración de políticas que notifican acciones fallidas

Métricas admitidas

El espacio de nombres de `Data Lifecycle Manager` incluye las siguientes métricas para las políticas de ciclo de vida de Amazon Data Lifecycle Manager. Las métricas admitidas difieren según el tipo de política.

Todas las métricas se pueden medir en la dimensión de `DLMPolicyId`. Las estadísticas más útiles son `sum` y `average`, y la unidad de medida es `count`.

Elija una pestaña para ver las métricas que admite ese tipo de política.

EBS snapshot policies

Métrica	Descripción
`Resources Targeted`	Número de recursos a los que se destinan las etiquetas especificadas en una instantánea o una política de AMI respaldada por EBS.
`Snapshots CreateStarted`	Número de acciones de creación de instantáneas iniciadas por una política de instantáneas. Cada acción se registra una sola vez, incluso si hay varios reintentos posteriores. Si se produce un error en una acción de creación de instantáneas, Amazon Data Lifecycle Manager envía una métrica de `Snapshots CreateFailed` .
`Snapshots CreateCompleted`	Número de instantáneas creadas por una política de instantáneas. Esto incluye reintentos exitosos dentro de los 60 minutos de la hora programada.
`Snapshots CreateFailed`	Número de instantáneas que no se pudieron crear mediante una política de instantáneas. Esto incluye reintentos fallidos en un plazo de 60 minutos a partir de la hora programada.
`Snapshots SharedCompleted`	Número de instantáneas compartidas entre cuentas por una política de instantáneas.
`Snapshots DeleteCompleted`	El número de instantáneas eliminadas por una instantánea o una política de AMI respaldada por EBS. Esta métrica se aplica únicamente a las instantáneas creadas por la política. No se aplica a las copias de instantáneas entre regiones creadas por la política. Esta métrica incluye instantáneas que se eliminan cuando una política de AMI respaldada por EBS anula el registro de las AMI.
`Snapshots DeleteFailed`	Número de instantáneas que no se pudieron eliminar mediante una instantánea o una política de AMI respaldada por EBS. Esta métrica

Métrica	Descripción
	se aplica únicamente a las instantáneas creadas por la política. No se aplica a las copias de instantáneas entre regiones creadas por la política. Esta métrica incluye instantáneas que se eliminan cuando una política de AMI respaldada por EBS anula el registro de las AMI.
`SnapshotsCopiedRegionStarted`	Número de acciones de copia de instantáneas entre regiones iniciadas por una política de instantáneas.
`SnapshotsCopiedRegionCompleted`	Número de copias de instantáneas entre regiones creadas por una política de instantáneas. Esto incluye reintentos exitosos dentro de las 24 horas siguientes a la hora programada.
`SnapshotsCopiedRegionFailed`	Número de copias de instantáneas entre regiones que no se pudieron crear mediante una política de instantáneas. Esto incluye reintentos fallidos dentro de las 24 horas siguientes a la hora programada.
`SnapshotsCopiedRegionDeleteCompleted`	Número de copias de instantáneas entre regiones eliminadas, según la regla de retención, por una política de instantáneas.
`SnapshotsCopiedRegionDeleteFailed`	Número de copias de instantáneas entre regiones que no se pudieron eliminar, según lo designado por la regla de retención, por una política de instantáneas.
`snapshotsArchiveDeletionFailed`	El número de instantáneas archivadas que no se pudieron eliminar en el nivel de archivo mediante una política de instantáneas.
`snapshotsArchiveScheduled`	El número de instantáneas programadas para ser archivadas mediante una política de instantáneas.

Métrica	Descripción
`snapshots ArchiveCompleted`	El número de instantáneas archivadas de manera correcta mediante una política de instantáneas.
`snapshots ArchiveFailed`	El número de instantáneas que no se pudieron archivar mediante una política de instantáneas.
`snapshots ArchiveDeletionCompleted`	El número de instantáneas archivadas que se pudieron eliminar en el nivel de archivo correctamente mediante una política de instantáneas.
`PreScript Started`	El número de instancias para el que se inició correctamente un script previo. Si los reintentos de scripts están habilitados, esta métrica se puede emitir varias veces por ejecución de la política.
`PreScript Completed`	El número de instancias para el que se completó correctamente un script previo. La métrica se emite incluso si el script previo se completa fuera del periodo de espera especificado. Si los reintentos de scripts están habilitados, esta métrica se puede emitir varias veces por ejecución de la política.
`PreScript Failed`	El número de instancias para el que no se completó correctamente un script previo. La métrica se emite incluso si el script previo se completa fuera del periodo de espera especificado. Si los reintentos de scripts están habilitados, esta métrica se puede emitir varias veces por ejecución de la política.
`PostScriptStarted`	El número de instancias para el que se inició correctamente un script posterior. Si los reintentos de scripts están habilitados, esta métrica se puede emitir varias veces por ejecución de la política.

Métrica	Descripción
PostScriptCompletado	El número de instancias para el que se completó correctamente un script posterior. La métrica se emite incluso si el script posterior se completa fuera del periodo de espera especificado. Si los reintentos de scripts están habilitados, esta métrica se puede emitir varias veces por ejecución de la política.
PostScriptFalló	El número de instancias con problemas para completar un script posterior. La métrica se emite incluso si el script posterior se completa fuera del periodo de espera especificado. Si los reintentos de scripts están habilitados, esta métrica se puede emitir varias veces por ejecución de la política.
`VSSBackupStarted`	El número de instancias con una copia de seguridad de VSS iniciada correctamente. Si los reintentos de scripts están habilitados, esta métrica se puede emitir varias veces por ejecución de la política.
`VSSBackupCompleted`	El número de instancias con una copia de seguridad de VSS completada correctamente. La métrica se emite incluso si la copia de seguridad de VSS se completa fuera del periodo de espera. Si los reintentos de scripts están habilitados, esta métrica se puede emitir varias veces por ejecución de la política.
`VSSBackupFailed`	El número de instancias en las que una copia de seguridad de VSS no se ha completado correctamente. La métrica se emite incluso si la copia de seguridad de VSS se completa fuera del periodo de espera. Si los reintentos de scripts están habilitados, esta métrica se puede emitir varias veces por ejecución de la política.

EBS-backed AMI policies

Las siguientes métricas se pueden utilizar con las políticas de AMI respaldadas por EBS:

Métrica	Descripción
`ResourcesTargeted`	Número de recursos a los que se destinan las etiquetas especificadas en una instantánea o una política de AMI respaldada por EBS.
`SnapshotsDeleteCompleted`	El número de instantáneas eliminadas por una instantánea o una política de AMI respaldada por EBS. Esta métrica se aplica únicamente a las instantáneas creadas por la política. No se aplica a las copias de instantáneas entre regiones creadas por la política. Esta métrica incluye instantáneas que se eliminan cuando una política de AMI respaldada por EBS anula el registro de las AMI.
`SnapshotsDeleteFailed`	Número de instantáneas que no se pudieron eliminar mediante una instantánea o una política de AMI respaldada por EBS. Esta métrica se aplica únicamente a las instantáneas creadas por la política. No se aplica a las copias de instantáneas entre regiones creadas por la política. Esta métrica incluye instantáneas que se eliminan cuando una política de AMI respaldada por EBS anula el registro de las AMI.
`SnapshotsCopiedRegionDeleteCompleted`	Número de copias de instantáneas entre regiones eliminadas, según la regla de retención, por una política de instantáneas.
`SnapshotsCopiedRegionDeleteFailed`	Número de copias de instantáneas entre regiones que no se pudieron eliminar, según lo designado por la regla de retención, por una política de instantáneas.
`ImagesCreateStarted`	El número de CreateImageacciones iniciadas por una política de AMI respaldada por EBS.

Métrica	Descripción
ImagesCreateCompleted	El número de AMI creadas por una política de AMI respaldada por EBS.
ImagesCreateFailed	Número de AMI que no se pudieron crear mediante una política de AMI respaldada por EBS.
ImagesDeregisterCompleted	Número de AMI cuyo registro fue anulado por una política de AMI respaldada por EBS.
ImagesDeregisterFailed	Número de AMI cuyo registro no pudo ser anulado por una política de AMI respaldada por EBS.
ImagesCopiedRegionStarted	Número de acciones de copia entre regiones iniciadas por una política de AMI respaldada por EBS.
ImagesCopiedRegionCompleted	Número de copias de AMI entre regiones creadas por una política de AMI respaldada por EBS.
ImagesCopiedRegionFailed	Número de copias de AMI entre regiones que no se pudieron crear mediante una política de AMI respaldada por EBS.
ImagesCopiedRegionDeregisterCompleted	El número de copias de AMI entre regiones cuyo registro se ha anulado, según lo designado por la regla de retención, mediante una política de AMI respaldada por EBS.

Métrica	Descripción
`ImagesCopiedRegionDeregisteredFailed`	Número de copias de AMI entre regiones cuyo registro no se pudo anular, según lo designado por la regla de retención, mediante una política de AMI respaldada por EBS.
`EnableImageDeprecationCompleted`	El número de AMI marcadas como obsoletas por una política de AMI respaldada por EBS.
`EnableImageDeprecationFailed`	El número de AMI que no se pudieron marcar como obsoletas mediante una política de AMI respaldada por EBS.
`EnableCopiedImageDeprecationCompleted`	El número de copias de AMI entre regiones marcadas como obsoletas por una política de AMI respaldada por EBS.
`EnableCopiedImageDeprecationFailed`	El número de copias de AMI entre regiones que no se pudieron marcar como obsoletas mediante una política de AMI respaldada por EBS.

Cross-account copy event policies

Las siguientes métricas se pueden utilizar con políticas de eventos de copia entre cuentas:

Métrica	Descripción
	El número de acciones de copia de instantáneas entre cuentas iniciadas por una política de eventos de copia entre cuentas.

Métrica	Descripción
`Snapshots CopiedAcc ountStarted`	
`Snapshots CopiedAcc ountCompleted`	El número de instantáneas copiadas de otra cuenta mediante una política de eventos de copia entre cuentas. Esto incluye reintentos exitosos dentro de las 24 horas siguientes a la hora programada.
`Snapshots CopiedAcc ountFailed`	El número de instantáneas que una política de eventos de copia entre cuentas no pudo copiar de otra cuenta. Esto incluye reintentos fallidos dentro de las 24 horas de la hora programada.
`Snapshots CopiedAcc ountDelet eCompleted`	Número de copias de instantáneas entre regiones eliminadas, según lo designado por la regla de retención, por una política de eventos de copia entre cuentas.
`Snapshots CopiedAcc ountDelet eFailed`	Número de copias de instantáneas entre regiones que no se pudieron eliminar, según lo designado por la regla de retención, mediante una política de eventos de copia entre cuentas.

Vea CloudWatch las métricas de sus políticas

Puede utilizar las herramientas de línea de comandos AWS Management Console o las de línea de comandos para enumerar las métricas que Amazon Data Lifecycle Manager envía a Amazon CloudWatch.

Amazon EC2 console

Para consultar las métricas desde la consola de Amazon EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Lifecycle Manager (Administrador de ciclo de vida).

3. Seleccione una política en la cuadrícula y, a continuación, elija la pestaña Monitoring (Monitoreo).

CloudWatch console

Para ver las métricas con la CloudWatch consola de Amazon

1. Abre la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Métricas.
3. Seleccione el espacio de nombres de EBS y, a continuación, seleccione Métricas de Data Lifecycle Manager.

AWS CLI

Para enumerar todas las métricas disponibles para Amazon Data Lifecycle Manager,

Utilice el comando list-metrics:

```
$ C:\> aws cloudwatch list-metrics \
    --namespace AWS/EBS
```

Para enumerar todas las métricas de una política específica,

Utilice el comando list-metrics y especifique la dimensión de `DLMPolicyId`.

```
$ C:\> aws cloudwatch list-metrics \
    --namespace AWS/EBS \
    --dimensions Name=DLMPolicyId,Value=policy-abcdef01234567890
```

Para presentar una métrica en todas las políticas,

Utilice el comando list-metrics y especifique la opción `--metric-name`.

```
$ C:\> aws cloudwatch list-metrics \
    --namespace AWS/EBS \
    --metric-name SnapshotsCreateCompleted
```

Métricas de gráficos para las políticas

Tras crear una política, puede abrir la consola de Amazon EC2 y ver los gráficos de monitoreo de la política en la pestaña Monitoring (Monitoreo). Cada gráfico se basa en una de las métricas de Amazon EC2 disponibles.

Se encuentran disponibles las siguientes métricas de gráficos:

- Recursos de destino (basados en `ResourcesTargeted`)
- Creación de instantáneas iniciada (basada en `SnapshotsCreateStarted`)
- Creación de instantáneas completada (basada en `SnapshotsCreateCompleted`)
- Error en la creación de instantáneas (basado en `SnapshotsCreateFailed`)
- Compartición de instantáneas completada (basada en `SnapshotsSharedCompleted`)
- Eliminación de instantáneas completada (basada en `SnapshotsDeleteCompleted`)
- Error en la eliminación de instantáneas (basado en `SnapshotsDeleteFailed`)
- Copia de instantáneas entre regiones iniciada (basada en `SnapshotsCopiedRegionStarted`)
- Copia de instantáneas entre regiones completada (basada en `SnapshotsCopiedRegionCompleted`)
- Error en la copia de instantáneas entre regiones (basada en `SnapshotsCopiedRegionFailed`)
- Eliminación de copia de instantáneas entre regiones completada (basada en `SnapshotsCopiedRegionDeleteCompleted`)
- Error en la eliminación de instantáneas entre regiones (basada en `SnapshotsCopiedRegionDeleteFailed`)
- Copia de instantáneas entre cuentas iniciada (basada en `SnapshotsCopiedAccountStarted`)
- Copia de instantáneas entre cuentas completada (basada en `SnapshotsCopiedAccountCompleted`)
- Error en la copia de instantáneas entre cuentas (basada en `SnapshotsCopiedAccountFailed`)
- Eliminación de copia de instantáneas entre cuentas completada (basada en `SnapshotsCopiedAccountDeleteCompleted`)
- Error en la eliminación de instantáneas entre cuentas (basada en `SnapshotsCopiedAccountDeleteFailed`)
- Creación de AMI iniciada (basada en `ImagesCreateStarted`)
- Creación de AMI completada (basada en `ImagesCreateCompleted`)

- Error en la creación de AMI (basado en `ImagesCreateFailed`)
- Cancelación de registro de AMI completada (basada en `ImagesDeregisterCompleted`)
- Error al cancelar el registro de AMI (basado en `ImagesDeregisterFailed`)
- Copia de AMI entre regiones iniciada (basada en `ImagesCopiedRegionStarted`)
- Copia de AMI entre regiones completada (basada en `ImagesCopiedRegionCompleted`)
- Error en la copia de AMI entre regiones (basada en `ImagesCopiedRegionFailed`)
- Cancelación de registro de copia de AMI entre regiones completada (basada en `ImagesCopiedRegionDeregisterCompleted`)
- Error al cancelar el registro de copia de AMI entre regiones (basado en `ImagesCopiedRegionDeregisteredFailed`)
- Habilitación de la obsolescencia de la AMI completada (basada en `EnableImageDeprecationCompleted`)
- Error en la habilitación de la obsolescencia de la AMI (basada en `EnableImageDeprecationFailed`)
- Habilitación de la obsolescencia de la copia entre regiones de la AMI completada (basada en `EnableCopiedImageDeprecationCompleted`)
- Error en la habilitación de la obsolescencia de la copia entre regiones de la AMI (basada en `EnableCopiedImageDeprecationFailed`)

Cree una CloudWatch alarma para una política

Puede crear una CloudWatch alarma que supervise CloudWatch las métricas de sus políticas. CloudWatch te enviará automáticamente una notificación cuando la métrica alcance el umbral que especifiques. Puede crear una CloudWatch alarma mediante la CloudWatch consola.

Para obtener más información sobre la creación de alarmas mediante la CloudWatch consola, consulta el siguiente tema de la Guía del CloudWatch usuario de Amazon.

- Cree una CloudWatch alarma basada en un umbral estático
- Cree una CloudWatch alarma basada en la detección de anomalías

Ejemplos de casos de uso

A continuación, se muestran ejemplos de casos de uso:

Temas

Ejemplo 1: métrica ResourcesTargeted

Puede utilizar la métrica `ResourcesTargeted` para monitorear el número total de recursos a los que se dirige una política específica cada vez que se ejecuta. Esto permite activar una alarma cuando el número de recursos objetivo está por debajo o por encima de un umbral esperado.

Por ejemplo, si espera que su política diaria cree copias de seguridad de no más de `50` volúmenes, puede crear una alarma de que envíe una notificación de email cuando el `sum` para `ResourcesTargeted` sea mayor a `50` a lo largo de un periodo de 1 horas. De esta forma, puede asegurarse de que no se han creado instantáneas inesperadamente a partir de volúmenes etiquetados incorrectamente.

Puede utilizar uno de los siguientes comandos para crear esta alarma:

```
$ C:\> aws cloudwatch put-metric-alarm \
    --alarm-name resource-targeted-monitor \
    --alarm-description "Alarm when policy targets more than 50 resources" \
    --metric-name ResourcesTargeted \
    --namespace AWS/EBS \
    --statistic Sum \
    --period 3600 \
    --threshold 50 \
    --comparison-operator GreaterThanThreshold \
    --dimensions "Name=DLMPolicyId,Value=policy_id" \
    --evaluation-periods 1 \
    --alarm-actions sns_topic_arn
```

Ejemplo 2: SnapshotDeleteFailed métrica

Puede utilizar la métrica `SnapshotDeleteFailed` para monitorear si hay errores al eliminar instantáneas según la regla de retención de instantáneas de la política.

Por ejemplo, si ha creado una política que debería eliminar instantáneas automáticamente cada doce horas, puede crear una alarma que notifique a su equipo de ingeniería cuando el `sum` de

`SnapshotDeletionFailed` sea mayor que `0` a lo largo de un periodo de 1 hora. Esto podría ayudar a investigar la retención inadecuada de instantáneas y a garantizar que los costos de almacenamiento de información no aumenten a causa de instantáneas innecesarias.

Puede utilizar uno de los siguientes comandos para crear esta alarma:

```
$ C:\> aws cloudwatch put-metric-alarm \
    --alarm-name snapshot-deletion-failed-monitor \
    --alarm-description "Alarm when snapshot deletions fail" \
    --metric-name SnapshotsDeleteFailed \
    --namespace AWS/EBS \
    --statistic Sum \
    --period 3600 \
    --threshold 0 \
    --comparison-operator GreaterThanThreshold \
    --dimensions "Name=DLMPolicyId,Value=policy_id" \
    --evaluation-periods 1 \
    --alarm-actions sns_topic_arn
```

Ejemplo 3: SnapshotsCopiedRegionFailed métrica

Utilice la métrica `SnapshotsCopiedRegionFailed` para identificar cuándo las políticas no pueden copiar instantáneas en otras regiones.

Por ejemplo, si la política copia instantáneas entre regiones diariamente, puede crear una alarma que envíe un SMS a su equipo de ingeniería cuando el `sum` de `SnapshotCrossRegionCopyFailed` sea mayor que `0` a lo largo de un periodo de 1 hora. Esto puede ser útil para comprobar si la política copió con éxito las instantáneas posteriores en el linaje.

Puede utilizar uno de los siguientes comandos para crear esta alarma:

```
$ C:\> aws cloudwatch put-metric-alarm \
    --alarm-name snapshot-copy-region-failed-monitor \
    --alarm-description "Alarm when snapshot copy fails" \
    --metric-name SnapshotsCopiedRegionFailed \
    --namespace AWS/EBS \
    --statistic Sum \
    --period 3600 \
    --threshold 0 \
    --comparison-operator GreaterThanThreshold \
    --dimensions "Name=DLMPolicyId,Value=policy_id" \
    --evaluation-periods 1 \
```

```
    --alarm-actions sns_topic_arn
```

Administración de políticas que notifican acciones fallidas

Para obtener más información sobre qué hacer cuando una de sus políticas informa un valor inesperado distinto de cero para una métrica de acción fallida, consulte ¿Qué debo hacer si Amazon Data Lifecycle Manager informa de acciones fallidas en las CloudWatch métricas? AWS Artículo del Knowledge Center.

Resolución de problemas

La siguiente documentación lo puede ayudar a solucionar los problemas que puedan presentarse.

Temas

- Error: Role with name already exists

Error: **`Role with name already exists`**

Descripción

Aparece el mensaje de error `Role with name AWSDataLifecycleManagerDefaultRole already exists` o `Role with name AWSDataLifecycleManagerDefaultRoleForAMIManagement already exists` cuando intenta crear una política con la consola.

Causa

El formato de ARN del rol predeterminado varía en función de si se crea mediante la consola o la AWS CLI. Si bien los ARN son diferentes, los roles usan el mismo nombre de rol, lo que genera un conflicto de nombres de roles entre la consola y la AWS CLI.

Solución

Para resolver este problema, siga estos pasos:

1. (En el caso de políticas instantáneas habilitadas únicamente para scripts previos y posteriores) Adjunte manualmente la política AWSDataLifecycleManagerSSMFullAccess AWS gestionada a la función de AWSDataLifecycleManagerDefaultRoleIAM. Para obtener más información, consulte Adición de permisos de identidad de IAM.

2. Al crear su política de Amazon Data Lifecycle Manager, para el rol de IAM, seleccione Elegir otro rol y, a continuación, seleccione AWSDataLifecycleManagerDefaultRole(para una política instantánea) o AWSDataLifecycleManagerDefaultRoleForAMIManagement(para una política de AMI).
3. Siga creando la política como de costumbre.

Usar las API directas de EBS para acceder al contenido de una instantánea de EBS

Puede utilizar las API directas Amazon Elastic Block Store (Amazon EBS) para crear instantáneas de EBS, escribir datos directamente en las instantáneas, leer datos en las instantáneas e identificar las diferencias o cambios entre dos instantáneas. Si es un proveedor de software independiente (ISV) que ofrece servicios de copia de seguridad para Amazon EBS, las API directas de EBS permiten que realice un seguimiento de los cambios incrementales en los volúmenes de EBS a través de instantáneas de forma más eficiente y económica. Esto se puede hacer sin tener que crear nuevos volúmenes a partir de instantáneas y utilizar después instancias Amazon Elastic Compute Cloud (Amazon EC2) para comparar las diferencias.

Puede crear instantáneas incrementales directamente a partir de datos locales en volúmenes de EBS y en la nube para utilizarlos para una recuperación de desastres rápida. Con la capacidad de escribir y leer instantáneas, puede escribir los datos locales en una instantánea de EBS durante un desastre. A continuación, tras la recuperación, puede restaurarla de nuevo en la instantánea AWS o de forma local a partir de ella. Ya no es necesario crear y mantener mecanismos complejos para copiar datos desde y hacia Amazon EBS.

Esta guía del usuario proporciona información general sobre los elementos que componen las API directas de EBS y ejemplos de cómo usarlos de manera eficaz. Para obtener más información acerca de las acciones, los tipos de datos, los parámetros y los errores de las API, consulte la referencia de API directas de EBS. Para obtener más información sobre las AWS regiones, los puntos de enlace y las cuotas de servicio compatibles para las API directas de EBS, consulte los puntos de enlace y las cuotas de servicio de Amazon EBS en. Referencia general de AWS

Contenido

Comprender las API directas de EBS

A continuación, se indican los conceptos clave que debe conocer antes de empezar a trabajar con las API directas de EBS.

Instantáneas

Las instantáneas son el mecanismo principal para realizar copias de seguridad de los datos de los volúmenes de EBS. Con API directas de EBS, también puede realizar copias de seguridad de los datos de los discos locales en instantáneas. Para ahorrar costos de almacenamiento, las instantáneas sucesivas son incrementales y solo contienen los datos del volumen modificados desde la instantánea anterior. Para obtener más información, consulte Instantáneas de Amazon EBS.

> **Note**
>
> Las API directas de EBS no admiten instantáneas públicas ni locales en Outposts.

Bloques

Un bloque es un fragmento de datos dentro de una instantánea. Cada instantánea puede contener miles de bloques. Todos los bloques de una instantánea tienen un tamaño fijo.

Índices de bloque

Un índice de bloques es un índice lógico en unidades de bloques de 512 KiB. Para identificar el índice de bloques, divida el desplazamiento lógico de los datos en el volumen lógico por el tamaño de bloque (desplazamiento lógico de datos/524288). El desplazamiento lógico de los datos debe estar alineado con 512 KiB.

Tokens de bloque

Un token de bloque es el hash de identificación de un bloque dentro de una instantánea y se utiliza para localizar los datos del bloque. Los tokens de bloque devueltos por las API directas de EBS son temporales. Cambian según la fecha de caducidad especificada para ellas o si se ejecuta otra ListSnapshotBlocks instantánea o se solicita la misma. ListChangedBlocks

Suma de comprobación

Una suma de comprobación es un dato de pequeño tamaño derivado de un bloque de datos con el fin de detectar errores que se introdujeron durante su transmisión o almacenamiento. Las API directas de EBS utilizan sumas de comprobación para validar la integridad de los datos. Cuando lee datos de una instantánea de EBS, el servicio proporciona sumas de comprobación SHA256 codificadas en Base64 para cada bloque de datos transmitido, que puede utilizar para la validación. Cuando escribe datos en una instantánea de EBS, debe proporcionar una suma de comprobación SHA256 codificada en Base64 para cada bloque de datos transmitido. El servicio valida los datos recibidos utilizando la suma de comprobación proporcionada. Para obtener más información, consulte Usar sumas de comprobación más adelante en esta guía.

Cifrado

El cifrado protege los datos al convertirlos en código ilegible que solo pueden descifrar las personas que tienen acceso a la Clave de KMS utilizada para cifrarlos. Puede usar las API directas de EBS para leer y escribir instantáneas cifradas, pero hay algunas limitaciones. Para obtener más información, consulte Usar cifrado más adelante en esta guía.

Acciones de API

Las API directas de EBS constan de seis acciones. Hay tres acciones de lectura y tres acciones de escritura. Las acciones de lectura son:

- ListSnapshotBloques: devuelve los índices de bloques y los símbolos de bloque de los bloques de la instantánea especificada
- ListChangedBloques: devuelve los índices de bloques y los símbolos de bloque de los bloques que son diferentes entre dos instantáneas especificadas del mismo volumen y linaje de instantáneas.
- GetSnapshotBloque: devuelve los datos de un bloque para el ID de instantánea, el índice de bloque y el token de bloque especificados.

Las acciones de escritura son:

- StartSnapshot— inicia una instantánea, ya sea como una instantánea incremental de una existente o como una nueva instantánea. La instantánea iniciada permanece en estado pendiente hasta que se complete con la CompleteSnapshot acción.
- PutSnapshotBloquear: añade datos a una instantánea iniciada en forma de bloques individuales. Debe especificar una suma de comprobación de codificación Base64 SHA256 para el bloque

de datos transmitido. El servicio convalida la suma de comprobación una vez completada la transmisión. La solicitud presenta error si la suma de comprobación calculada por servicio no coincide con lo que especificó.

- CompleteSnapshot— completa una instantánea iniciada que se encuentra en estado pendiente. La instantánea se puede cambiar a estado completo.

Permisos de IAM para las API directas de EBS

Un usuario debe tener las siguientes políticas para utilizar las API directas de EBS. Para obtener más información, consulte Cambio de los permisos de un usuario de IAM.

Para obtener más información sobre las claves de contexto de condición, acciones y recursos de las API directas de EBS para su uso en las políticas de permisos de IAM, consulteAcciones, recursos y claves de condición para Amazon Elastic Block Store en la Referencia de autorizaciones de servicio.

> **Important**
>
> Tenga cuidado al asignar las siguientes políticas a los usuarios de . Al asignar estas políticas, puede conceder acceso a un usuario al que se le deniegue el acceso al mismo recurso a través de las API de Amazon EC2, como CopySnapshot las CreateVolume acciones o.

Permisos para leer instantáneas

La siguiente política permite utilizar las API de lectura directa de EBS en todas las instantáneas de una región específica. AWS En la política, sustituya *<Región>* por la región de la instantánea.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ebs:GetSnapshotBlock"
            ],
            "Resource": "arn:aws:ec2:<Region>::snapshot/*"
        }
    ]
```

```
}
```

La siguiente política permite utilizar las API directas de EBS de lectura en instantáneas con una etiqueta clave-valor específica. En la política, reemplace *<Key>* por el valor de clave de la etiqueta y *<Value>* por el valor de la etiqueta.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ebs:GetSnapshotBlock"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*",
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "aws:ResourceTag/<Key>": "<Value>"
                }
            }
        }
    ]
}
```

La siguiente directiva permite que todas las API directas de EBS de lectura se utilicen en todas las instantáneas de la cuenta solo dentro de un intervalo de tiempo específico. Esta política autoriza el uso de las API directas de EBS basadas en la clave de condición global `aws:CurrentTime`. En la política, asegúrese de reemplazar el intervalo de fecha y hora mostrado por el intervalo de fecha y hora de la política.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ebs:GetSnapshotBlock"
            ],
```

```
            "Resource": "arn:aws:ec2:*::snapshot/*",
            "Condition": {
                "DateGreaterThan": {
                    "aws:CurrentTime": "2018-05-29T00:00:00Z"
                },
                "DateLessThan": {
                    "aws:CurrentTime": "2020-05-29T23:59:59Z"
                }
            }
        }
    ]
}
```

Para obtener más información, consulte Cambio de los permisos de un usuario de IAM en la Guía del usuario de IAM.

Permisos para escribir instantáneas

La siguiente política permite utilizar las API directas de escritura de EBS en todas las instantáneas de una región específica. AWS En la política, sustituya *<Región>* por la región de la instantánea.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:StartSnapshot",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:<Region>::snapshot/*"
        }
    ]
}
```

La siguiente política permite que las API directas de EBS de escritura se utilicen en instantáneas con una etiqueta clave-valor específica. En la política, reemplace *<Key>* por el valor de clave de la etiqueta y *<Value>* por el valor de la etiqueta.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:StartSnapshot",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*",
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "aws:ResourceTag/<Key>": "<Value>"
                }
            }
        }
    ]
}
```

La siguiente política permite que se utilicen las API directas de EBS. También permite la acción `StartSnapshot` solo si se especifica un ID de instantánea principal. Por lo tanto, esta política bloquea la capacidad de iniciar nuevas instantáneas sin utilizar una instantánea principal.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ebs:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ebs:ParentSnapshot": "arn:aws:ec2:*::snapshot/*"
                }
            }
        }
    ]
}
```

La siguiente política permite que se utilicen las API directas de EBS. También permite que solo se cree la clave de etiqueta de `user` para una nueva instantánea. Esta política también garantiza que el usuario tenga acceso para crear etiquetas. La acción `StartSnapshot` es la única acción que puede especificar etiquetas.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ebs:*",
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "user"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

La siguiente política permite que todas las API directas de EBS de escritura se utilicen en todas las instantáneas de la cuenta solo dentro de un intervalo de tiempo específico. Esta política autoriza el uso de las API directas de EBS basadas en la clave de condición global `aws:CurrentTime`. En la política, asegúrese de reemplazar el intervalo de fecha y hora mostrado por el intervalo de fecha y hora de la política.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:StartSnapshot",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*",
            "Condition": {
                "DateGreaterThan": {
                    "aws:CurrentTime": "2018-05-29T00:00:00Z"
                },
```

```
                "DateLessThan": {
                    "aws:CurrentTime": "2020-05-29T23:59:59Z"
                }
            }
        }
    ]
}
```

Para obtener más información, consulte Cambio de los permisos de un usuario de IAM en la Guía del usuario de IAM.

Permisos de uso AWS KMS keys

La siguiente política concede permiso para descifrar una instantánea cifrada mediante una clave de KMS específica. También concede permiso para cifrar instantáneas nuevas mediante la clave de KMS predeterminada para el cifrado de EBS. En la política, <Region>sustitúyala por la región de la clave de KMS, *< AccountId >* por el ID de la AWS cuenta de la clave de KMS y *< KeyId >* por el ID de la clave de KMS.

> **Note**
>
> De forma predeterminada, todos los responsables de la cuenta tienen acceso a la clave de KMS AWS administrada predeterminada para el cifrado de Amazon EBS y pueden usarla para las operaciones de cifrado y descifrado de EBS. Si utiliza una clave administrada por el cliente, debe crear una política de claves nueva o modificar la política de clave existente para la clave administrada por el cliente para conceder acceso a la entidad principal a la clave administrada por el cliente. Para obtener más información, consulte Políticas de claves en AWS KMS en la Guía para desarrolladores de AWS Key Management Service .

> **Tip**
>
> Para seguir el principio de privilegios mínimos, no permita el acceso completo a `kms:CreateGrant`. En su lugar, utilice la clave `kms:GrantIsForAWSResource` condicionada para permitir al usuario crear concesiones en la clave de KMS únicamente cuando un AWS servicio cree la concesión en nombre del usuario, como se muestra en el siguiente ejemplo.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:GenerateDataKey",
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:ReEncrypt*",
                "kms:CreateGrant",
                "ec2:CreateTags",
                "kms:DescribeKey"
            ],
            "Resource": "arn:aws:kms:<Region>:<AccountId>:key/<KeyId>",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

Para obtener más información, consulte Cambio de los permisos de un usuario de IAM en la Guía del usuario de IAM.

Use las API directas de EBS

En los siguientes temas se muestra cómo leer y escribir instantáneas mediante las API directas de EBS. Puede leer y escribir instantáneas únicamente con las AWS CLI AWS API y AWS los SDK. Para obtener más información, consulte:

- Instalación AWS CLI y configuración del AWS CLI
- Referencia de las API directas de EBS
- AWS SDK

> **Important**
>
> Las API directas de EBS requieren una AWS firma de la versión 4 de Signature. Para obtener más información, consulte Usar la firma de Signature Version 4.

Temas

Leer instantáneas mediante las API directas de EBS

En los siguientes pasos se describe cómo utilizar las API directas de EBS para leer instantáneas:

1. Utilice la ListSnapshotBlocks acción para ver todos los índices de bloques y los símbolos de bloques en una instantánea. O bien, utilice la ListChangedBlocks acción para ver solo los índices de bloques y los símbolos de bloques que son diferentes entre dos instantáneas del mismo volumen y linaje de instantáneas. Estas acciones le ayudan a identificar los tokens de bloque y los índices de bloque de bloques para los que es posible que desee obtener datos.
2. Utilice la GetSnapshotBlock acción y especifique el índice de bloque y el token de bloque del bloque del que desea obtener datos.

En los siguientes ejemplos, se muestra cómo leer instantáneas mediante las API directas de EBS.

Temas

- Obtener datos de bloque de una instantánea

Listado de bloques en una instantánea

AWS CLI

El siguiente comando de ejemplo list-snapshot-blocks devuelve los índices de bloque y los tokens de bloque de bloques que están en la instantánea `snap-0987654321`. El parámetro `--starting-block-index` limita los resultados a índices de bloque mayores que `1000` y el parámetro `--max-results` limita los resultados a los primeros `100` bloques.

```
aws ebs list-snapshot-blocks --snapshot-id snap-0987654321 --starting-block-
index 1000 --max-results 100
```

La siguiente respuesta de ejemplo para el comando anterior enumera los índices de bloque y los tokens de bloque en la instantánea. Utilice el comando `get-snapshot-block` y especifique el índice de bloque y el token de bloque del bloque para el que desea obtener datos. Los tokens de bloque son válidos hasta el tiempo de caducidad indicado.

```
{
      "Blocks": [
          {
              "BlockIndex": 1001,
              "BlockToken": "AAABAV3/
PNhXOynVdMYHUpPsetaSvjLB1dtIGfbJv5OJ0sX855EzGTWos4a4"
          },
          {
              "BlockIndex": 1002,
              "BlockToken": "AAABATGQIgwr0WwIuqIMjCA/Sy7e/
YoQFZsHejzGNvjKauzNgzeI13YHBfQB"
          },
          {
              "BlockIndex": 1007,
              "BlockToken": "AAABAZ9CTuQtUvp/
dXqRWw4d07eOgTZ3jvn6hiW30W9duM8MiMw6yQayzF2c"
          },
          {
              "BlockIndex": 1012,
              "BlockToken": "AAABAQdzxhw0rVV6PNmsfo/
YRIxo9JPR85XxPf1BLjg0Hec6pygYr6laE1p0"
          },
```

```
          {
              "BlockIndex": 1030,
              "BlockToken": "AAABAaYvPax6mv+iGWLdTUjQtFWouQ7Dqz6nSD9L
+CbXnvpkswA6iDID523d"
          },
          {
              "BlockIndex": 1031,
              "BlockToken": "AAABATgWZC0XcFwUKvTJbUXMiSPg59KVxJGL
+BWBClkw6spzCxJVqDVaTskJ"
          },
          ...
      ],
      "ExpiryTime": 1576287332.806,
      "VolumeSize": 32212254720,
      "BlockSize": 524288
  }
```

AWS API

La siguiente solicitud de ejemplo de ListSnapshotbloques devuelve los índices de bloques y los símbolos de bloque de los bloques que están en una instantáneasnap-0acEXAMPLEcf41648. El parámetro `startingBlockIndex` limita los resultados a índices de bloque mayores que `1000` y el parámetro `maxResults` limita los resultados a los primeros `100` bloques.

```
GET /snapshots/snap-0acEXAMPLEcf41648/blocks?maxResults=100&startingBlockIndex=1000
 HTTP/1.1
  Host: ebs.us-east-2.amazonaws.com
  Accept-Encoding: identity
  User-Agent: <User agent parameter>
  X-Amz-Date: 20200617T231953Z
  Authorization: <Authentication parameter>
```

La siguiente respuesta de ejemplo para la solicitud anterior enumera los índices de bloque y los tokens de bloque en la instantánea. Usa la GetSnapshotBlock acción y especifica el índice de bloque y el token de bloque del bloque del que deseas obtener datos. Los tokens de bloque son válidos hasta el tiempo de caducidad indicado.

```
HTTP/1.1 200 OK
  x-amzn-RequestId: d6e5017c-70a8-4539-8830-57f5557f3f27
  Content-Type: application/json
  Content-Length: 2472
  Date: Wed, 17 Jun 2020 23:19:56 GMT
```

```
  Connection: keep-alive

  {
      "BlockSize": 524288,
      "Blocks": [
          {
              "BlockIndex": 0,
              "BlockToken": "AAUBAcuWqOCnDNuKle11s7IIX6jp6FYcC/q8oT93913HhvLvA
+3JRrSybp/0"
          },
          {
              "BlockIndex": 1536,
              "BlockToken":
 "AAUBAWudwfmofcrQhGVlLwuRKm2b8ZXPiyrgoykTRC6IU1NbxKWDY1pPjvnV"
          },
          {
              "BlockIndex": 3072,
              "BlockToken":
 "AAUBAV7p6pC5fKAC7TokoNCtAnZhqq27u6YEXZ3MwRevBkDjmMx6iuA6tsBt"
          },
          {
              "BlockIndex": 3073,
              "BlockToken":
 "AAUBAbqt9zpqBUEvtO2HINAfFaWToOwlPjbIsQOlx6JUN/0+iMQl0NtNbnX4"
          },
          ...
      ],
      "ExpiryTime": 1.59298379649E9,
      "VolumeSize": 3
  }
```

Listado de bloques que son diferentes entre dos instantáneas

Tenga en cuenta lo siguiente al realizar solicitudes paginadas para enumerar los bloques modificados entre dos instantáneas:

- La respuesta puede incluir una o varias matrices `ChangedBlocks` vacías. Por ejemplo:
  - Instantánea 1: instantánea completa con 1000 bloques con índices de bloques `0` - 999.
  - Instantánea 2: instantánea incremental con solo un bloque modificado con un índice de bloques 999.

Listar los bloques modificados para estas instantáneas con `StartingBlockIndex = 0` y `MaxResults = 100` devuelve una matriz vacía de `ChangedBlocks`. Debe solicitar los resultados restantes mediante `nextToken` hasta que devuelva el bloque modificado en el décimo conjunto de resultados, el cual incluye bloques con índices de bloque `900` - 999.

- La respuesta puede omitir bloques no escritos en las instantáneas. Por ejemplo:
  - Instantánea 1: instantánea completa con 1000 bloques con índices de bloques `2000` - 2999.
  - Instantánea 2: instantánea incremental con solo un bloque modificado con el índice de bloques `2000`.

  Al listar los bloques modificados para estas instantáneas con `StartingBlockIndex = 0` y `MaxResults = 100`, la respuesta omite los índices de bloque `0` - 1999 e incluye el índice de bloques `2000`. La respuesta no incluirá matrices `ChangedBlocks` vacías.

AWS CLI

El siguiente comando de ejemplo list-changed-blocks devuelve los índices de bloque y los tokens de bloque de bloques que son diferentes entre instantáneas `snap-1234567890` y `snap-0987654321`. El parámetro `--starting-block-index` limita los resultados a índices de bloque mayores que `0` y el parámetro `--max-results` limita los resultados a los primeros `500` bloques.

```
aws ebs list-changed-blocks --first-snapshot-id snap-1234567890 --second-snapshot-
id snap-0987654321 --starting-block-index 0 --max-results 500
```

La respuesta de ejemplo siguiente del comando anterior muestra que los índices de bloque 0, 6000, 6001, 6002 y 6003 son diferentes entre las dos instantáneas. Además, los índices de bloque 6001, 6002 y 6003 solo existen en el primer ID de instantánea especificado y no en el segundo ID de instantánea, porque no hay un segundo token de bloque en la respuesta.

Utilice el comando `get-snapshot-block` y especifique el índice de bloque y el token de bloque del bloque para el que desea obtener datos. Los tokens de bloque son válidos hasta el tiempo de caducidad indicado.

```
{
      "ChangedBlocks": [
          {
              "BlockIndex": 0,
```

```
            "FirstBlockToken": "AAABAVahm9SO60Dyi0ORySzn2ZjGjW/
KN3uygGlS0QOYWesbzBbDnX2dGpmC",
            "SecondBlockToken":
 "AAABAf8o0o6UFi1rDbSZGIRaCEdDyBu9TlvtCQxxoKV8qrUPQP7vcM6iWGSr"
        },
        {
            "BlockIndex": 6000,
            "FirstBlockToken": "AAABAbYSiZvJ0/
R9tz8suI8dSzecLjN4kkazK8inFXVintPkdaVFLfCMQsKe",
            "SecondBlockToken":
 "AAABAZnqTdzFmKRpsaMAsDxviVqEI/3jJzI2crq2eFDCgHmyNf777elD9oVR"
        },
        {
            "BlockIndex": 6001,
            "FirstBlockToken": "AAABASBpSJ2UAD3PLxJnCt6zun4/
T4sU25Bnb8jB5Q6FRXHFqAIAqE04hJoR"
        },
        {
            "BlockIndex": 6002,
            "FirstBlockToken": "AAABASqX4/
NWjvNceoyMUljcRd0DnwbSwNnes1UkoP62CrQXvn47BY5435aw"
        },
        {
            "BlockIndex": 6003,
            "FirstBlockToken":
 "AAABASmJ0O5JxAOce25rF4P1sdRtyIDsX12tFEDunnePYUKOf4PBROuICb2A"
        },
        ...
    ],
    "ExpiryTime": 1576308931.973,
    "VolumeSize": 32212254720,
    "BlockSize": 524288,
    "NextToken": "AAADARqElNng/sV98CYk/bJDCXeLJmLJHnNSkHvLzVaO0zsPH/QM3Bi3zF//
O6Mdi/BbJarBnp8h"
  }
```

AWS API

La siguiente solicitud de ejemplo de ListChangedbloques devuelve los índices de bloque y los símbolos de bloque de los bloques que son diferentes entre las instantáneas `snap-0acEXAMPLEcf41648` y. `snap-0c9EXAMPLE1b30e2f` El parámetro `startingBlockIndex` limita los resultados a índices de bloque mayores que `0` y el parámetro `maxResults` limita los resultados a los primeros `500` bloques.

```
GET /snapshots/snap-0c9EXAMPLE1b30e2f/changedblocks?
firstSnapshotId=snap-0acEXAMPLEcf41648&maxResults=500&startingBlockIndex=0 HTTP/1.1
  Host: ebs.us-east-2.amazonaws.com
  Accept-Encoding: identity
  User-Agent: <User agent parameter>
  X-Amz-Date: 20200617T232546Z
  Authorization: <Authentication parameter>
```

La respuesta de ejemplo siguiente para la solicitud anterior muestra que los índices de bloque `0`, `3072`, `6002` y `6003` son diferentes entre las dos instantáneas. Además, los índices de bloque `6002` y `6003` solo existen en el primer ID de instantánea especificado y no en el segundo ID de instantánea, porque no hay un segundo token de bloque en la respuesta.

Utilice la acción `GetSnapshotBlock` y especifique el índice de bloque y el token de bloque del bloque para el que desea obtener los datos. Los tokens de bloque son válidos hasta el tiempo de caducidad indicado.

```
HTTP/1.1 200 OK
  x-amzn-RequestId: fb0f6743-6d81-4be8-afbe-db11a5bb8a1f
  Content-Type: application/json
  Content-Length: 1456
  Date: Wed, 17 Jun 2020 23:25:47 GMT
  Connection: keep-alive

  {
      "BlockSize": 524288,
      "ChangedBlocks": [
          {
              "BlockIndex": 0,
              "FirstBlockToken": "AAUBAVaWqOCnDNuKle11s7IIX6jp6FYcC/
tJuVT1GgP23AuLntwiMdJ+OJkL",
              "SecondBlockToken": "AAUBASxzy0Y0b33JVRLoYm3NOresCxn5RO+HVFzXW3Y/
RwfFaPX2Edx8QHCh"
          },
          {
              "BlockIndex": 3072,
              "FirstBlockToken":
 "AAUBAcHp6pC5fKAC7TokoNCtAnZhqq27u6fxRfZOLEmeXLmHBf2R/Yb24MaS",
              "SecondBlockToken":
 "AAUBARGCaufCqBRZC8tEkPYGGkSv3vqvOjJ2xKDi3ljDFiytUxBLXYgTmkid"
          },
          {
```

```
            "BlockIndex": 6002,
            "FirstBlockToken": "AAABASqX4/
NWjvNceoyMUljcRd0DnwbSwNnes1UkoP62CrQXvn47BY5435aw"
        },
        {
            "BlockIndex": 6003,
            "FirstBlockToken":
 "AAABASmJ0O5JxAOce25rF4P1sdRtyIDsX12tFEDunnePYUKOf4PBROuICb2A"
        },
        ...
    ],
    "ExpiryTime": 1.592976647009E9,
    "VolumeSize": 3
 }
```

Obtener datos de bloque de una instantánea

AWS CLI

El siguiente comando de ejemplo get-snapshot-block devuelve los datos en el índice de bloque `6001` con token de bloque `AAABASBpSJ2UAD3PLxJnCt6zun4/T4sU25Bnb8jB5Q6FRXHFqAIAqE04hJoR`, en la instantánea `snap-1234567890`. Los datos binarios se envían al archivo `data` en el directorio `C:\Temp` de un equipo con Windows. Si ejecuta el comando en un equipo Linux o Unix, reemplace la ruta de salida por `/tmp/data` para enviar los datos al archivo `data` en el directorio `/tmp`.

```
aws ebs get-snapshot-block --snapshot-id snap-1234567890 --block-index 6001 --block-
token AAABASBpSJ2UAD3PLxJnCt6zun4/T4sU25Bnb8jB5Q6FRXHFqAIAqE04hJoR C:/Temp/data
```

La respuesta de ejemplo siguiente para el comando anterior muestra el tamaño de los datos devueltos, la suma de comprobación para validar los datos y el algoritmo de la suma de comprobación. Los datos binarios se guardan automáticamente en el directorio y archivo especificados en el comando de la solicitud.

```
{
    "DataLength": "524288",
    "Checksum": "cf0Y6/Fn0oFa4VyjQPOa/iD0zhTflPTKzxGv2OKowXc=",
    "ChecksumAlgorithm": "SHA256"
 }
```

AWS API

La siguiente solicitud de ejemplo de GetSnapshotbloque devuelve los datos del índice de bloques `3072` con el token del bloque`AAUBARGCaufCqBRZC8tEkPYGGkSv3vqvOjJ2xKDi3ljDFiytUxBLXYgTmkid`, en forma de instantánea. `snap-0c9EXAMPLE1b30e2f`

```
GET /snapshots/snap-0c9EXAMPLE1b30e2f/blocks/3072?
blockToken=AAUBARGCaufCqBRZC8tEkPYGGkSv3vqvOjJ2xKDi3ljDFiytUxBLXYgTmkid HTTP/1.1
  Host: ebs.us-east-2.amazonaws.com
  Accept-Encoding: identity
  User-Agent: <User agent parameter>
  X-Amz-Date: 20200617T232838Z
  Authorization: <Authentication parameter>
```

La siguiente respuesta de ejemplo para la solicitud anterior muestra el tamaño de los datos devueltos, la suma de comprobación para validar los datos y el algoritmo utilizado para generar la suma de comprobación. Los datos binarios se transmiten en el cuerpo de la respuesta y se representan como *`BlockData`*en el siguiente ejemplo.

```
HTTP/1.1 200 OK
  x-amzn-RequestId: 2d0db2fb-bd88-474d-a137-81c4e57d7b9f
  x-amz-Data-Length: 524288
  x-amz-Checksum: Vc0yY2j3qg8bUL9I6GQuI2orTudrQRBDMIhcy7bdEsw=
  x-amz-Checksum-Algorithm: SHA256
  Content-Type: application/octet-stream
  Content-Length: 524288
  Date: Wed, 17 Jun 2020 23:28:38 GMT
  Connection: keep-alive

  BlockData
```

Escribir instantáneas mediante las API directas de EBS

En los siguientes pasos se describe cómo utilizar las API directas de EBS para escribir instantáneas incrementales:

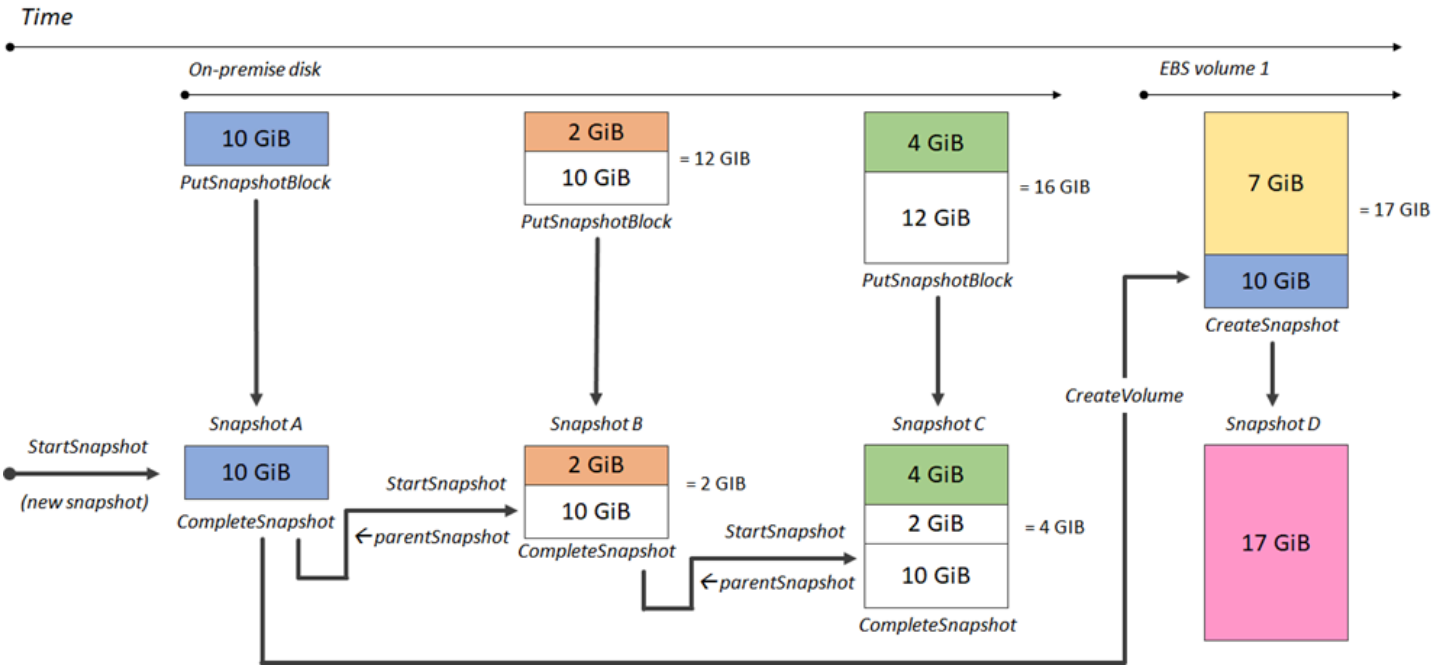
1. Utilice la StartSnapshot acción y especifique un ID de instantánea principal para iniciar una instantánea como una instantánea incremental de una existente, u omita el ID de instantánea

principal para iniciar una nueva instantánea. Esta acción devuelve el nuevo ID de instantánea, que está en estado pendiente.

2. Utilice la PutSnapshotBlock acción y especifique el ID de la instantánea pendiente para añadirle datos en forma de bloques individuales. Debe especificar una suma de comprobación de codificación Base64 SHA256 para el bloque de datos transmitido. El servicio calcula la suma de comprobación de los datos recibidos y la valida con la suma de comprobación especificada. La acción devuelve un error si las sumas de comprobación no coinciden.
3. Cuando haya terminado de añadir datos a la instantánea pendiente, utilice la CompleteSnapshot acción para iniciar un flujo de trabajo asíncrono que selle la instantánea y la mueva a un estado completo.

Repita estos pasos para crear una nueva instantánea incremental utilizando la instantánea creada anteriormente como principal.

Por ejemplo, en el siguiente diagrama, la instantánea A es la primera nueva instantánea iniciada. La instantánea A se utiliza como instantánea principal para iniciar la instantánea B. La instantánea B se utiliza como instantánea principal para iniciar y crear la instantánea C. Las instantáneas A, B y C son instantáneas incrementales. La instantánea A se utiliza para crear el volumen 1 de EBS. La instantánea D se crea a partir del volumen 1 de EBS. La instantánea D es una instantánea incremental de A; no es una instantánea incremental de B o C.



En los siguientes ejemplos, se muestra cómo escribir instantáneas mediante las API directas de EBS.

Temas

- Iniciar una instantánea
- Inclusión de datos en una instantánea
- Completar una instantánea

Iniciar una instantánea

AWS CLI

El siguiente comando de ejemplo start-snapshot inicia una instantánea de 8 GiB, utilizando la instantánea `snap-123EXAMPLE1234567` como instantánea principal. La nueva instantánea será una instantánea incremental de la instantánea principal. La instantánea se mueve a un estado de error si no hay solicitudes PUT o completas realizadas para la instantánea dentro del periodo de tiempo de espera de `60` minutos especificado. El token de cliente `550e8400-e29b-41d4-a716-446655440000` garantiza la idempotencia de la solicitud. Si se omite el token del cliente, el AWS SDK generará uno automáticamente. Para obtener más información acerca de la idempotencia, consulte Idempotencia para la API StartSnapshot .

```
aws ebs start-snapshot --volume-size 8 --parent-snapshot snap-123EXAMPLE1234567 --
timeout 60 --client-token 550e8400-e29b-41d4-a716-446655440000
```

La siguiente respuesta de ejemplo al comando anterior muestra el ID de la instantánea, el ID de la cuenta de AWS , el estado, el tamaño del volumen en GiB y el tamaño de los bloques de la instantánea. La instantánea se inicia en un estado `pending`. Especifique el ID de instantánea en los comandos `put-snapshot-block` siguientes para escribir datos en la instantánea y, a continuación, utilice el comando `complete-snapshot` para completar la instantánea y cambiar su estado a `completed`.

```
{
    "SnapshotId": "snap-0aaEXAMPLEe306d62",
    "OwnerId": "111122223333",
    "Status": "pending",
    "VolumeSize": 8,
    "BlockSize": 524288
}
```

AWS API

La siguiente solicitud de StartSnapshotejemplo inicia una instantánea de 8 GiB, utilizando la instantánea `snap-123EXAMPLE1234567` como instantánea principal. La nueva instantánea será una instantánea incremental de la instantánea principal. La instantánea se mueve a un estado de error si no hay solicitudes PUT o completas realizadas para la instantánea dentro del periodo de tiempo de espera de `60` minutos especificado. El token de cliente `550e8400-e29b-41d4-a716-446655440000` garantiza la idempotencia de la solicitud. Si se omite el token del cliente, el AWS SDK generará uno automáticamente. Para obtener más información acerca de la idempotencia, consulte Idempotencia para la API StartSnapshot .

```
POST /snapshots HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T040724Z
Authorization: <Authentication parameter>

{
    "VolumeSize": 8,
    "ParentSnapshot": snap-123EXAMPLE1234567,
    "ClientToken": "550e8400-e29b-41d4-a716-446655440000",
    "Timeout": 60
}
```

La siguiente respuesta de ejemplo a la solicitud anterior muestra el ID de la instantánea, el ID de la cuenta de AWS , el estado, el tamaño del volumen en GiB y el tamaño de los bloques de la instantánea. La instantánea se inicia en un estado pendiente. Especifique el ID de instantánea en una solicitud `PutSnapshotBlocks` posterior para escribir datos en la instantánea.

```
HTTP/1.1 201 Created
x-amzn-RequestId: 929e6eb9-7183-405a-9502-5b7da37c1b18
Content-Type: application/json
Content-Length: 181
Date: Thu, 18 Jun 2020 04:07:29 GMT
Connection: keep-alive

{
    "BlockSize": 524288,
    "Description": null,
    "OwnerId": "138695307491",
```

```
    "Progress": null,
    "SnapshotId": "snap-052EXAMPLEc85d8dd",
    "StartTime": null,
    "Status": "pending",
    "Tags": null,
    "VolumeSize": 8
}
```

Inclusión de datos en una instantánea

AWS CLI

El siguiente comando de ejemplo put-snapshot escribe 524288 Bytes de datos para bloquear el índice 1000 en la instantánea snap-0aaEXAMPLEe306d62. La suma de comprobación Q0D3gmEQ0XATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM= codificada en Base64 se generó utilizando el algoritmo SHA256. Los datos que se transmiten están en el archivo /tmp/data.

```
aws ebs put-snapshot-block --snapshot-id snap-0aaEXAMPLEe306d62
 --block-index 1000 --data-length 524288 --block-data /tmp/data --
checksum Q0D3gmEQ0XATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM= --checksum-algorithm SHA256
```

La respuesta de ejemplo siguiente para el comando anterior confirma la longitud de los datos, la suma de comprobación y el algoritmo de suma de comprobación para los datos recibidos por el servicio.

```
{
    "DataLength": "524288",
    "Checksum": "Q0D3gmEQ0XATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM=",
    "ChecksumAlgorithm": "SHA256"
}
```

AWS API

La siguiente solicitud de PutSnapshotejemplo escribe 524288 bytes de datos en el índice de bloques de 1000 la instantáneasnap-052EXAMPLEc85d8dd. La suma de comprobación Q0D3gmEQ0XATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM= codificada en Base64 se generó utilizando el algoritmo SHA256. Los datos se transmiten en el cuerpo de la solicitud y se representan como *BlockData*en el siguiente ejemplo.

```
PUT /snapshots/snap-052EXAMPLEc85d8dd/blocks/1000 HTTP/1.1
```

```
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
x-amz-Data-Length: 524288
x-amz-Checksum: QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM=
x-amz-Checksum-Algorithm: SHA256
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T042215Z
X-Amz-Content-SHA256: UNSIGNED-PAYLOAD
Authorization: <Authentication parameter>

          BlockData
```

La siguiente respuesta de ejemplo para la solicitud anterior confirma la longitud de los datos, la suma de comprobación y el algoritmo de suma de comprobación para los datos recibidos por el servicio.

```
HTTP/1.1 201 Created
x-amzn-RequestId: 643ac797-7e0c-4ad0-8417-97b77b43c57b
x-amz-Checksum: QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM=
x-amz-Checksum-Algorithm: SHA256
Content-Type: application/json
Content-Length: 2
Date: Thu, 18 Jun 2020 04:22:12 GMT
Connection: keep-alive

{}
```

Completar una instantánea

AWS CLI

El siguiente comando de ejemplo complete-snapshot completa la instantánea `snap-0aaEXAMPLEe306d62`. El comando especifica que 5 bloques se escribieron en la instantánea. La suma de comprobación `6D3nmwi5f2F0wlh7xX8QprrJBFzDX8aacdOcA3KCM3c=` representa la suma de comprobación del conjunto completo de datos escritos en una instantánea. Para obtener más información acerca de las sumas de comprobación, consulte Usar sumas de comprobación anteriormente en esta guía.

```
aws ebs complete-snapshot --snapshot-id snap-0aaEXAMPLEe306d62 --changed-blocks-
count 5 --checksum 6D3nmwi5f2F0wlh7xX8QprrJBFzDX8aacdOcA3KCM3c= --checksum-
algorithm SHA256 --checksum-aggregation-method LINEAR
```

A continuación, se muestra una respuesta de ejemplo para el comando anterior.

```
{
    "Status": "pending"
}
```

AWS API

En el siguiente CompleteSnapshotejemplo, la solicitud completa la instantáneasnap-052EXAMPLEc85d8dd. El comando especifica que 5 bloques se escribieron en la instantánea. La suma de comprobación 6D3nmwi5f2F0wlh7xX8QprrJBFzDX8aacdOcA3KCM3c= representa la suma de comprobación del conjunto completo de datos escritos en una instantánea.

```
POST /snapshots/completion/snap-052EXAMPLEc85d8dd HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
x-amz-ChangedBlocksCount: 5
x-amz-Checksum: 6D3nmwi5f2F0wlh7xX8QprrJBFzDX8aacdOcA3KCM3c=
x-amz-Checksum-Algorithm: SHA256
x-amz-Checksum-Aggregation-Method: LINEAR
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T043158Z
Authorization: <Authentication parameter>
```

La siguiente es una respuesta de ejemplo para la solicitud anterior.

```
HTTP/1.1 202 Accepted
x-amzn-RequestId: 06cba5b5-b731-49de-af40-80333ac3a117
Content-Type: application/json
Content-Length: 20
Date: Thu, 18 Jun 2020 04:31:50 GMT
Connection: keep-alive

{"Status":"pending"}
```

Usar cifrado

Al iniciar una nueva instantánea con ella StartSnapshot, el estado del cifrado depende de los valores que especifique para Encrypted, KmsKeyArn e ParentSnapshotId, y de si su AWS cuenta está habilitada para el cifrado de forma predeterminada.

> **Note**
>
> - Es posible que necesite permisos de IAM adicionales para usar las API directas de EBS con el cifrado. Para obtener más información, consulte Permisos de uso AWS KMS keys.
> - Si el cifrado de Amazon EBS está activado de forma predeterminada en su AWS cuenta, no podrá crear instantáneas sin cifrar.
> - Si el cifrado de Amazon EBS está activado de forma predeterminada en su AWS cuenta, no podrá iniciar una nueva instantánea con una instantánea principal no cifrada. Primero debe cifrar la instantánea principal copiándola. Para obtener más información, consulte Copia de una instantánea de Amazon EBS.

Temas

Resultados del cifrado: instantánea principal no cifrada

En la siguiente tabla, se describe el resultado de cifrado para cada combinación posible de configuraciones al momento de especificar una instantánea principal no cifrada.

ParentSnapshotID	Encriptado	KmsKeyArn	Cifrado de forma predeterminada	Resultado
Sin cifrar	Omitido	Omitido	Habilitado	Error en la solicitud respecto a `ValidationException` .

ParentSnapshotID	Encriptado	KmsKeyArn	Cifrado de forma predeterminada	Resultado
			Deshabilitad	La instantánea no está cifrada.
		Especificado	Habilitado	
			Deshabilitad	
Sin cifrar	True	Omitido	Habilitado	Error en la solicitud respecto a `ValidationException` .
			Deshabilitad	
		Especificado	Habilitado	
			Deshabilitad	
Sin cifrar	False	Omitido	Habilitado	Error en la solicitud respecto a `ValidationException` .
			Deshabilitad	
		Especificado	Habilitado	
			Deshabilitad	

Resultados del cifrado: instantánea principal cifrada

En la siguiente tabla, se describe el resultado de cifrado para cada combinación posible de configuraciones al momento de especificar una instantánea principal cifrada.

ParentSnapshotId	Encriptado	KmsKeyArn	Cifrado de forma predeterminada	Resultado
Encriptado	Omitido	Omitido	Habilitado	La instantánea se cifra con la misma clave de KMS que la instantánea principal.
			Deshabilitad	
		Especificado	Habilitado	Error en la solicitud respecto a `ValidationException` .
			Deshabilitad	
Encriptado	True	Omitido	Habilitado	Error en la solicitud respecto a `ValidationException` .
			Deshabilitad	
		Especificado	Habilitado	
			Deshabilitad	
Encriptado	False	Omitido	Habilitado	Error en la solicitud respecto a `ValidationException` .
			Deshabilitad	
		Especificado	Habilitado	
			Deshabilitad	

Resultados del cifrado: sin una instantánea principal

En las siguientes tablas, se describe el resultado del cifrado para cada combinación posible de configuraciones cuando no se utiliza una instantánea principal.

ParentSnapshotId	Encriptado	KmsKeyArn	Cifrado de forma predeterminada	Resultado
Omitido	True	Omitido	Habilitado	La instantánea se cifra con la clave de KMS predeterminada de su cuenta. *
			Deshabilitad	
		Especificado	Habilitado	La instantánea se cifra con la clave KMS especificada para KmsKeyArn.
			Deshabilitad	
Omitido	False	Omitido	Habilitado	Error en la solicitud respecto a `ValidationException` .
			Deshabilitad	La instantánea no está cifrada.
		Especificado	Habilitado	Error en la solicitud respecto a `ValidationException` .
			Deshabilitad	
Omitido	Omitido	Omitido	Habilitado	La instantánea se cifra con la clave de KMS predeterminada de su cuenta. *
			Deshabilitad	La instantánea no está cifrada.
		Especificado	Habilitado	La instantánea se cifra con la clave KMS especificada para KmsKeyArn.
			Deshabilitad	

* Esta clave de KMS predeterminada puede ser una clave administrada por el cliente o la clave de KMS AWS administrada predeterminada para el cifrado de Amazon EBS.

Usar la firma de Signature Version 4

La versión 4 de Signature es el proceso para añadir información de autenticación a AWS las solicitudes enviadas por HTTP. Por motivos de seguridad, la mayoría de las solicitudes AWS deben

firmarse con una clave de acceso, que consiste en un identificador de clave de acceso y una clave de acceso secreta. Estas dos claves comúnmente se denominan credenciales de seguridad. Para obtener información sobre cómo obtener credenciales para su cuenta, consulte Credenciales de seguridad de AWS.

Si tiene la intención de crear manualmente solicitudes HTTP, debe aprender a firmarlas. Cuando utilizas el AWS Command Line Interface (AWS CLI) o uno de los AWS SDK para realizar solicitudes AWS, estas herramientas firman automáticamente las solicitudes por ti con la clave de acceso que especifiques al configurar las herramientas. Si usa estas herramientas, no tiene que aprender a firmar las solicitudes personalmente.

Para obtener más información, consulte Firmar las solicitudes de AWS API en la Guía del usuario de IAM.

Usar sumas de comprobación

La GetSnapshotBlock acción devuelve datos que se encuentran en un bloque de una instantánea y añade datos a un bloque de una instantánea. PutSnapshotBlock Los datos de bloque que se transmiten no se firman como parte del proceso de firma de Signature Version 4. Como resultado, las sumas de comprobación se utilizan para validar la integridad de los datos de la siguiente manera:

- Al utilizar la GetSnapshotBlock acción, la respuesta proporciona una suma de control SHA256 codificada en Base64 para los datos del bloque que utilizan el encabezado X-AMZ-Checksum, y el algoritmo de suma de comprobación utiliza el encabezado X-AMZ-Checksum-Algorithm. Utilice la suma de comprobación devuelta para validar la integridad de los datos. Si la suma de comprobación que genera no coincide con la proporcionada por Amazon EBS, debe considerar que los datos no son válidos y volver a intentar su solicitud.
- Al utilizar la PutSnapshotBlock acción, la solicitud debe proporcionar una suma de comprobación SHA256 codificada en Base64 para los datos del bloque mediante el encabezado X-AMZ-checksum y el algoritmo de suma de comprobación mediante el encabezado X-AMZ-checksum-algorithm. La suma de comprobación que proporcione se valida con una suma de comprobación generada por Amazon EBS para validar la integridad de los datos. Si las sumas de comprobación no se corresponden, la solicitud devuelve un error.
- Al usar la CompleteSnapshot acción, la solicitud puede proporcionar opcionalmente una suma de verificación SHA256 agregada codificada en Base64 para todo el conjunto de datos agregado a la instantánea. Proporcione la suma de comprobación mediante el encabezado x-amz-Checksum, el algoritmo de suma de comprobación mediante el encabezado x-amz-Checksum-Algorithm y el método de agregación de suma de comprobación mediante el encabezado x-amz-Checksum-

Aggregation-Method. Para generar la suma de comprobación agregada mediante el método de agregación lineal, organice las sumas de comprobación para cada bloque escrito en orden ascendente de su índice de bloque, concaténelas para formar una sola cadena y, a continuación, genere la suma de comprobación en toda la cadena utilizando el algoritmo SHA256.

Las sumas de comprobación de estas acciones forman parte del proceso de firma Signature Version 4.

Idempotencia para la API StartSnapshot

La idempotencia garantiza que una solicitud de API se complete solo una vez. Con una solicitud idempotente, los reintentos posteriores devuelven el resultado de la solicitud original correcta y no tienen ningún efecto adicional.

La StartSnapshotAPI admite la idempotencia mediante un token de cliente. Un token de cliente es una cadena única que se especifica cuando se realiza una solicitud de API. Si vuelve a intentar una solicitud de API con el mismo token de cliente y los mismos parámetros de solicitud después de que se haya completado correctamente, se devuelve el resultado de la solicitud original. Si vuelve a intentar una solicitud con el mismo token de cliente, pero cambia uno o más de los parámetros de solicitud, se devuelve el error `ConflictException`.

Si no especificas tu propio token de cliente, los AWS SDK generan automáticamente un token de cliente para la solicitud, a fin de garantizar que sea idempotente.

Un token de cliente puede ser cualquier cadena que incluya hasta 64 caracteres ASCII. No debe reutilizar los mismos tokens de cliente para diferentes solicitudes.

Para realizar una StartSnapshot solicitud idempotente con tu propio token de cliente mediante la API

Especifique el parámetro de solicitud `ClientToken`.

```
POST /snapshots HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T040724Z
Authorization: <Authentication parameter>

{
    "VolumeSize": 8,
    "ParentSnapshot": snap-123EXAMPLE1234567,
```

```
    "ClientToken": "550e8400-e29b-41d4-a716-446655440000",
    "Timeout": 60
}
```

Para realizar una StartSnapshot solicitud idempotente con tu propio token de cliente, utiliza la AWS CLI

Especifique el parámetro de solicitud `client-token`.

```
$ C:\> aws ebs start-snapshot --region us-east-2 --volume-size 8 --parent-
snapshot snap-123EXAMPLE1234567 --timeout 60 --client-token 550e8400-e29b-41d4-
a716-446655440000
```

Reintentos de error

Los SDK de AWS implementan la lógica de reintentos automáticos para las solicitudes que devuelven respuestas a errores. Puede configurar los ajustes de reintento para los SDK de AWS . Para obtener más información, consulte la documentación del SDK.

Puede configurar la AWS CLI para reintentar automáticamente algunas solicitudes fallidas. Para obtener más información sobre cómo configurar los reintentos para el AWS CLI, consulte los AWS CLI reintentos en la Guía del usuario.AWS Command Line Interface

La API de consulta de AWS no admite la lógica de reintentos para solicitudes fallidas. Si utiliza solicitudes HTTP o HTTPS, debe implementar la lógica de reintentos en la aplicación del cliente.

En la tabla siguiente, se muestran las posibles respuestas de error de la API. Algunos errores de la API son reintentables. La aplicación cliente siempre debe reintentar solicitudes fallidas que reciban un error reintentable.

Error	Código de respuesta	Descripción	Lanzada por	¿Reintentable?
`InternalServerException`	500	Se produjo un error en la solicitud debido a un problema de red o AWS del servidor.	Todas las API	Sí

Error	Código de respuesta	Descripción	Lanzada por	¿Reintentable?
`ThrottlingException`	400	El número de solicitudes de API ha superado el límite máximo permitido de limitación de solicitudes de API para la cuenta.	Todas las API	Sí
`RequestThrottleException`	400	El número de solicitudes de API ha superado el límite máximo permitido de limitación de solicitudes de API para la instantánea.	GetSnapshotBlock | PutSnapshotBlock	Sí
`ValidationException` con el mensaje “`Failed to read block data`”	400	El bloque de datos proporcionado era ilegible.	PutSnapshotBloquear	Sí

Error	Código de respuesta	Descripción	Lanzada por	¿Reintentable?
`ValidationException` con cualquier otro mensaje	400	La sintaxis de la solicitud tiene un formato incorrecto o la entrada no cumple las restricciones especificadas en el Servicio de AWS.	Todas las API	No
`ResourceNotFoundException`	404	El ID de instantánea especificado no existe.	Todas las API	No
`ConflictException`	409	El token de cliente especificado se usó anteriormente en una solicitud similar que tenía parámetros de solicitud diferentes. Para obtener más información, consulte Idempotencia para la API StartSnapshot .	StartSnapshot	No

Error	Código de respuesta	Descripción	Lanzada por	¿Reintentable?
`AccessDeniedException`	403	No tiene permiso para realizar la operación solicitada.	Todas las API	No
`ServiceQuotaExceededException`	402	La solicitud falló porque, de cumplirse, se superarían una o más cuotas de servicio dependientes de su cuenta.	Todas las API	No
`InvalidSignatureException`	403	La firma de autorización de la solicitud ha caducado. Solo puede reintentar la solicitud después de actualizar la firma de autorización.	Todas las API	No

Optimizar el rendimiento

Puede ejecutar solicitudes de API simultáneamente. Suponiendo que la PutSnapshotBlock latencia es de 100 ms, un hilo puede procesar 10 solicitudes en un segundo. Además, suponiendo que su aplicación cliente crea múltiples hilos y conexiones (por ejemplo, 100 conexiones), puede realizar 1000 (10 * 100) solicitudes por segundo en total. Esto corresponderá a un rendimiento de alrededor de 500 MB por segundo.

La siguiente lista contiene algunas cosas que debe buscar en su aplicación:

- ¿Cada hilo usa una conexión separada? Si las conexiones están limitadas en la aplicación, varios subprocesos esperarán a que la conexión esté disponible y observará un menor rendimiento.
- ¿Hay algún tiempo de espera en la aplicación entre dos solicitudes PUT? Esto reducirá el rendimiento efectivo de un subproceso.
- El límite de ancho de banda de la instancia: si otras aplicaciones comparten el ancho de banda de la instancia, esto podría limitar el rendimiento disponible para PutSnapshotBlock las solicitudes.

Asegúrese de tomar nota de otras cargas de trabajo que pudieran estar ejecutándose en la cuenta para evitar cuellos de botella. También debe crear mecanismos de reintento en sus flujos de trabajo de API directas de EBS para controlar las limitaciones controladas, los tiempos de espera y la falta de disponibilidad del servicio.

Revise las cuotas de servicio de las API directas de EBS para determinar las solicitudes de API máximas que puede ejecutar por segundo. Para obtener más información, consulte Puntos de enlace y cuotas de Amazon Elastic Block Store en la Referencia general de AWS .

Puntos de conexión del servicio de las API directas de EBS

Un punto final es una URL que sirve como punto de entrada para un servicio AWS web. Las API directas de EBS admiten los siguientes tipos de puntos de conexión:

- Puntos de conexión IPv4
- Puntos de conexión de doble pila compatibles con IPv4 e IPv6
- Puntos de conexión FIPS

Al hacer una solicitud, puede especificar el punto de conexión y la región que se van a utilizar. Si no especifica un punto de conexión, se utilizará de forma predeterminada el punto de conexión IPv4. Para utilizar un tipo de punto de conexión diferente, debe especificarlo en la solicitud. Para ver ejemplos prácticos, consulte Especificación de puntos de conexión.

Para obtener más información sobre las regiones, consulte Regiones y zonas de disponibilidad en la Guía del usuario de Amazon EC2. Para obtener una lista de los puntos de conexión para las API directas de EBS, consulte Puntos de conexión para las API directas de EBS en Referencia general de Amazon Web Services.

Temas

- Puntos de conexión IPv4

- Puntos de conexión de doble pila (IPv4 e IPv6)
- Puntos de conexión FIPS
- Especificación de puntos de conexión

Puntos de conexión IPv4

Los puntos de conexión IPv4 solo son compatibles con el tráfico IPv4. Los puntos de conexión IPv4 están disponibles para todas las regiones.

Las API directas de EBS solo admiten puntos de enlace IPv4 regionales que puede utilizar para realizar sus solicitudes. Debe especificar la región como parte del nombre del punto final. Los nombres de los puntos finales utilizan la siguiente convención de nomenclatura:

- `ebs.region.amazonaws.com`

Por ejemplo, para dirigir las solicitudes al punto final de `us-east-2` IPv4, debe especificarlo `ebs.us-east-2.amazonaws.com` como punto final. Para obtener una lista de los puntos de conexión para las API directas de EBS, consulte Puntos de conexión para las API directas de EBS en Referencia general de Amazon Web Services.

Precios

No se le cobrarán los datos transferidos directamente entre las API directas de EBS y las instancias de Amazon EC2 que utilicen un punto de conexión IPv4 en la misma región. Sin embargo, si hay servicios intermedios, como AWS PrivateLink puntos de conexión, NAT Gateway o Amazon VPC Transit Gateways, se le cobrarán los costos asociados.

Puntos de conexión de doble pila (IPv4 e IPv6)

Los puntos de conexión de doble pila admiten tráfico IPv4 e IPv6. Los puntos de conexión de doble pila están disponibles para todas las regiones.

Para utilizar IPv6, debe usar un punto de conexión de doble pila. Cuando hace una solicitud a un punto de conexión de doble pila, la URL del punto de conexión se resuelve en una dirección IPv6 o IPv4, según el protocolo que utilicen la red y el cliente.

Las API directas de EBS solo admiten puntos de conexión regionales de doble pila, lo que significa que debe especificar la región como parte del nombre del punto de conexión. Los nombres de puntos de conexión de doble pila utilizan la siguiente convención de nomenclatura:

- `ebs.region.api.aws`

Por ejemplo, el nombre del punto de conexión de doble pila para la región `eu-west-1` es `ebs.eu-west-1.api.aws`. Para obtener una lista de los puntos de conexión para las API directas de EBS, consulte Puntos de conexión para las API directas de EBS en Referencia general de Amazon Web Services.

Precios

No se le cobrarán los datos transferidos directamente entre las API directas de EBS y las instancias de Amazon EC2 que utilicen un punto de conexión de doble pila en la misma región. Sin embargo, si hay servicios intermedios, como AWS PrivateLink puntos de conexión, NAT Gateway o Amazon VPC Transit Gateways, se le cobrarán los costos asociados.

Puntos de conexión FIPS

Las API directas de EBS proporcionan puntos de conexión IPv4 y de doble pila (IPv4 e IPv6) validados por FIPS para las regiones siguientes:

- `us-east-1`: Este de EE. UU. (Norte de Virginia)
- `us-east-2`: Este de EE. UU. (Ohio)
- `us-west-1`: Oeste de EE. UU. (Norte de California)
- `us-west-2`: Oeste de EE. UU. (Oregón)
- `ca-central-1`: Canadá (centro)

Los puntos de conexión IPv4 FIPS utilizan la siguiente convención de nomenclatura: `ebs-fips.region.amazonaws.com`. Por ejemplo, el punto de conexión IPv4 FIPS para `us-east-1` es `ebs-fips.us-east-1.amazonaws.com`.

Los puntos de conexión FIPS de doble pila utilizan la siguiente convención de nomenclatura: `ebs-fips.region.api.aws`. Por ejemplo, el punto de conexión FIPS de doble pila para `us-east-1` es `ebs-fips.us-east-1.api.aws`.

Para obtener más información acerca de los puntos de conexión de FIPS, consulte Puntos de conexión de la FIPS en Referencia general de Amazon Web Services.

Especificación de puntos de conexión

En esta sección, se proporcionan algunos ejemplos de cómo especificar un punto de conexión al hacer una solicitud.

AWS CLI

En los siguientes ejemplos, se muestra cómo especificar un punto de conexión para la región `us-east-2` mediante la AWS CLI.

- Doble pila

```
aws ebs list-snapshot-blocks --snapshot-id snap-0987654321 --starting-block-index
 1000 --endpoint-url https://ebs.us-east-2.api.aws
```

- IPv4

```
aws ebs list-snapshot-blocks --snapshot-id snap-0987654321 --starting-block-index
 1000 --endpoint-url https://ebs.us-east-2.amazonaws.com
```

AWS SDK for Java 2.x

En los siguientes ejemplos, se muestra cómo especificar un punto de conexión para la región `us-east-2` mediante la AWS SDK for Java 2.x.

- Doble pila

```
AwsClientBuilder.EndpointConfiguration config = new
 AwsClientBuilder.EndpointConfiguration("https://ebs.us-east-2.api.aws", "us-
east-2");
AmazonEBS ebs = AmazonEBSClientBuilder.standard()
    .withEndpointConfiguration(config)
    .build();
```

- IPv4

```
AwsClientBuilder.EndpointConfiguration config = new
 AwsClientBuilder.EndpointConfiguration("https://ebs.us-east-2.amazonaws.com",
 "us-east-2");
AmazonEBS ebs = AmazonEBSClientBuilder.standard()
    .withEndpointConfiguration(config)
```

```
    .build();
```

AWS SDK for Go

En los siguientes ejemplos, se muestra cómo especificar un punto de conexión para la región `us-east-2` mediante la AWS SDK for Go.

- Doble pila

```
sess := session.Must(session.NewSession())
svc := ebs.New(sess, &aws.Config{
    Region: aws.String(endpoints.UsEast1RegionID),
    Endpoint: aws.String("https://ebs.us-east-2.api.aws")
})
```

- IPv4

```
sess := session.Must(session.NewSession())
svc := ebs.New(sess, &aws.Config{
    Region: aws.String(endpoints.UsEast1RegionID),
    Endpoint: aws.String("https://ebs.us-east-2.amazonaws.com")
})
```

Precios de las API directas de EBS

Temas

Precios de las API

El precio que se paga para usar las API directas de EBS depende de las solicitudes que se realicen. Para obtener más información, consulte Precios Amazon EBS.

- ListChangedLos bloques y ListSnapshotBlocks las API se cobran por solicitud. Por ejemplo, si realizas 100 000 solicitudes de ListSnapshotBlocks API en una región que cobra 0,0006$ por cada 1000 solicitudes, se te cobrarán 0,06$ (0,0006$ por cada 1000 solicitudes x 100).

- GetSnapshotEl bloqueo se cobra por cada bloque devuelto. Por ejemplo, si realizas 100 000 solicitudes a la GetSnapshotBlock API en una región que cobra 0,003$ por cada 1000 bloques devueltos, se te cobrarán 0,30$ (0,003$ por cada 1000 bloques devueltos x 100).
- PutSnapshotEl bloqueo se cobra por bloque escrito. Por ejemplo, si realizas 100 000 solicitudes a la PutSnapshotBlock API en una región que cobra 0,006$ por cada 1000 bloques escritos, se te cobrarán 0,60$ (0,006$ por cada 1000 bloques escritos x 100).

Costes de red

Costes de transferencia de datos

Los datos transferidos directamente entre las API directas de EBS y las instancias de Amazon EC2 de la AWS misma región son gratuitos cuando se utilizan puntos de enlace que no son de FIPS. Para obtener más información, consulte puntos de conexión de servicio de AWS. Si hay otros AWS servicios en el proceso de transferencia de datos, se le cobrarán los costos de procesamiento de datos asociados. Estos servicios incluyen, pero no se limitan a, PrivateLink puntos finales, NAT Gateway y Transit Gateway.

Puntos de enlace de interfaz de VPC

Si utiliza las API directas de EBS desde instancias AWS Lambda o funciones de Amazon EC2 en subredes privadas, puede utilizar los puntos de enlace de la interfaz de VPC, en lugar de utilizar puertas de enlace NAT, para reducir los costes de transferencia de datos de la red. Para obtener más información, consulte Uso de los puntos de enlace de la VPC con las API directas de EBS.

Uso de los puntos de enlace de la VPC con las API directas de EBS

Puede establecer una conexión privada entre la VPC y las API directas de EBS mediante la creación de un punto de conexión de VPC de interfaz basado en AWS PrivateLink Puede acceder a las API directas de EBS como si estuvieran en su VPC, sin necesidad de utilizar una puerta de enlace de Internet, un dispositivo NAT, una conexión VPN ni una conexión de AWS Direct Connect . Las instancias de la VPC no necesitan direcciones IP públicas para comunicarse con las API directas de EBS.

Creamos una interfaz de red de punto de conexión en cada subred habilitada para el punto de conexión de interfaz.

Para obtener más información, consulte Acceso directo AWS PrivateLink en la Servicios de AWSAWS PrivateLink guía.

Consideraciones sobre los puntos de enlace de la VPC de las API directas de EBS

Antes de configurar un punto de conexión de VPC de interfaz para las API directas de EBS, consulte Considerations (Consideraciones) en la Guía de AWS PrivateLink .

De forma predeterminada, se permite el acceso completo a las API directas de EBS a través del punto de enlace. Puede controlar el acceso al punto final de la interfaz mediante políticas de punto final de la VPC. Puede adjuntar una política de punto final a su punto final de VPC que controle el acceso a las API directas de EBS. La política especifica la siguiente información:

- El principal que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos con los que se pueden realizar las acciones.

Para obtener más información, consulte Control del acceso a servicios con puntos de enlace de la VPC en la Guía del usuario de Amazon VPC.

El siguiente es un ejemplo de una política de puntos finales para las API directas de EBS. Cuando se adjunta a un punto final, esta política otorga acceso a todas las acciones de las API directas de EBS en todos los recursos, excepto las instantáneas etiquetadas con la clave `Environment` y el valor. `Test`

```
{
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "ebs:*",
            "Principal": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Environment": "Test"
                }
            }
        },
```

```
        {
            "Effect": "Allow",
            "Action": "ebs:*",
            "Principal": "*",
            "Resource": "*"
        }
    ]
}
```

Creación de un punto de enlace de la VPC de interfaz para las API directas de EBS

Puede crear un punto de enlace de la VPC para el servicio de API directas de EBS mediante la consola de Amazon VPC o la AWS Command Line Interface (AWS CLI). Para obtener más información, consulte Create a VPC endpoint (Creación de un punto de conexión de VPC) en la Guía de AWS PrivateLink .

Cree un punto de enlace de la VPC para las API directas de EBS mediante el siguiente nombre de servicio:

- `com.amazonaws.region.ebs`

Si habilita el DNS privado para el punto de conexión, puede efectuar solicitudes de API a las API directas de EBS utilizando su nombre de DNS predeterminado para la región como, por ejemplo, `ebs.us-east-1.amazonaws.com`.

Registre las llamadas de API para las API directas de EBS con AWS CloudTrail

El servicio de API directas de EBS está integrado con. AWS CloudTrail CloudTrail es un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio. CloudTrail captura todas las llamadas a las API realizadas en las API directas de EBS como eventos. Si crea un registro, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon Simple Storage Service (Amazon S3). Si no configura una ruta, podrá ver los eventos de administración más recientes en la CloudTrail consola, en el historial de eventos. Los eventos de datos no se capturan en el historial de eventos. Puede usar la información recopilada CloudTrail para determinar la solicitud que se realizó a las API directas de EBS, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información al respecto CloudTrail, consulte la Guía del AWS CloudTrail usuario.

Información sobre las API directas de EBS en CloudTrail

CloudTrail está habilitada en su AWS cuenta al crear la cuenta. Cuando se produce una actividad de eventos admitida en las API directas de EBS, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los eventos recientes en su AWS cuenta. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para obtener un registro continuo de los eventos de su AWS cuenta, incluidos los eventos de las API directas de EBS, cree un registro. Un registro permite CloudTrail enviar los archivos de registro a un bucket de S3. De forma predeterminada, al crear una ruta en la consola, la ruta se aplica a todas AWS las regiones. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al depósito de S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail Integraciones y servicios compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Acciones de la API admitidas

En el caso de las API directas de EBS, puede CloudTrail utilizarlas para registrar dos tipos de eventos:

- Eventos de administración: los eventos de administración proporcionan visibilidad de las operaciones de administración que se realizan en las instantáneas de su AWS cuenta. Las siguientes acciones de la API se registran de forma predeterminada como eventos de administración en registros de seguimiento:
  - StartSnapshot
  - CompleteSnapshot

  Para obtener más información sobre el registro de los eventos de administración, consulte Registrar los eventos de administración para las rutas en la Guía del CloudTrail usuario.

- Datos de eventos: estas instantáneas proporcionan visibilidad de las operaciones realizadas en una instantánea o dentro de ella. Las siguientes acciones de API se pueden registrar opcionalmente como eventos de datos en registros de seguimiento:
  - ListSnapshotBloques
  - ListChangedBloques
  - GetSnapshotBlock
  - PutSnapshotBloquear

  El registro de los eventos de datos está deshabilitado de forma predeterminada cuando crea un registro de seguimiento. Solo puede utilizar Selectores de eventos avanzados para registrar eventos de datos en llamadas directas a la API de EBS. Para obtener más información, consulte Registrar eventos de datos para senderos en la Guía del CloudTrail usuario.

  > **Note**
  >
  > Si realiza una acción en una instantánea que se comparte con usted, los eventos de datos no se envían a la AWS cuenta propietaria de la instantánea.

Información de identidad

Cada entrada de registro o evento contiene información acerca de quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales del usuario raíz o del usuario.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte al CloudTrail usuario IdentityElement.

Comprender las entradas del archivo de registros de las API directas de EBS

Un seguimiento es una configuración que permite la entrega de eventos como archivos de registro a un bucket de S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye

información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

A continuación se muestran ejemplos de entradas de CloudTrail registro.

StartSnapshot


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2020-07-03T23:27:26Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "StartSnapshot",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "PostmanRuntime/7.25.0",
    "requestParameters": {
        "volumeSize": 8,
        "clientToken": "token",
        "encrypted": true
    },
    "responseElements": {
        "snapshotId": "snap-123456789012",
        "ownerId": "123456789012",
        "status": "pending",
        "startTime": "Jul 3, 2020 11:27:26 PM",
        "volumeSize": 8,
        "blockSize": 524288,
        "kmsKeyArn": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "requestID": "be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
    "eventID": "6e12345-2a4e-417c-aa78-7594fEXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

CompleteSnapshot


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2020-07-03T23:28:24Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "CompleteSnapshot",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "PostmanRuntime/7.25.0",
    "requestParameters": {
        "snapshotId": "snap-123456789012",
        "changedBlocksCount": 5
    },
    "responseElements": {
        "status": "completed"
    },
    "requestID": "be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
    "eventID": "6e12345-2a4e-417c-aa78-7594fEXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```


ListSnapshotBlocks


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
```

```
    "eventTime": "2021-06-03T00:32:46Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "ListSnapshotBlocks",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "snapshotId": "snap-abcdef01234567890",
        "maxResults": 100,
        "startingBlockIndex": 0
    },
    "responseElements": null,
    "requestID": "example6-0e12-4aa9-b923-1555eexample",
    "eventID": "example4-218b-4f69-a9e0-2357dexample",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}
```


ListChangedBlocks


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
        "userName": "user"
    },
    "eventTime": "2021-06-02T21:11:46Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "ListChangedBlocks",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "firstSnapshotId": "snap-abcdef01234567890",
        "secondSnapshotId": "snap-9876543210abcdef0",
        "maxResults": 100,
        "startingBlockIndex": 0
    },
    "responseElements": null,
    "requestID": "example0-f4cb-4d64-8d84-72e1bexample",
    "eventID": "example3-fac4-4a78-8ebb-3e9d3example",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        },
       {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-9876543210abcdef0"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}
```

GetSnapshotBlock


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-02T20:43:05Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "GetSnapshotBlock",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "snapshotId": "snap-abcdef01234567890",
        "blockIndex": 1,
        "blockToken": "EXAMPLEiL5E3pMPFpaDWjExM2/mnSKh1mQfcbjwe2mM7EwhrgCdPAEXAMPLE"
    },
    "responseElements": null,
    "requestID": "examplea-6eca-4964-abfd-fd9f0example",
    "eventID": "example6-4048-4365-a275-42e94example",
    "readOnly": true,
    "resources": [
        {
          "accountId": "123456789012",
          "type": "AWS::EC2::Snapshot",
          "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
```

```
}
```

PutSnapshotBlock


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-02T21:09:17Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "PutSnapshotBlock",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "snapshotId": "snap-abcdef01234567890",
        "blockIndex": 1,
        "dataLength": 524288,
        "checksum": "exampleodSGvFSb1e3kxWUgbOQ4TbzPurnsfVexample",
        "checksumAlgorithm": "SHA256"
    },
    "responseElements": {
        "checksum": "exampleodSGvFSb1e3kxWUgbOQ4TbzPurnsfVexample",
        "checksumAlgorithm": "SHA256"
    },
    "requestID": "example3-d5e0-4167-8ee8-50845example",
    "eventID": "example8-4d9a-4aad-b71d-bb31fexample",
    "readOnly": false,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
```

```
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}
```

Preguntas frecuentes

¿Se puede acceder a una instantánea usando las API directas de EBS si tiene un estado pendiente?

No. Solo se puede acceder a la instantánea si tiene un estado completado.

¿Devuelven las API directas de EBS los índices de bloque en orden numérico?

Sí. Los índices de bloque devueltos son únicos y están en orden numérico.

¿Puedo enviar una solicitud con un valor de MaxResults parámetro inferior a 100?

No. El valor mínimo de MaxResult parámetro que puede utilizar es 100. Si envías una solicitud con un valor de MaxResult parámetro inferior a 100 y hay más de 100 bloques en la instantánea, la API devolverá al menos 100 resultados.

¿Puedo ejecutar solicitudes de API simultáneamente?

Puede ejecutar solicitudes de API simultáneamente. Asegúrese de tomar nota de otras cargas de trabajo que pudieran estar ejecutándose en la cuenta para evitar cuellos de botella. También debe crear mecanismos de reintento en sus flujos de trabajo de API directas de EBS para controlar las limitaciones controladas, los tiempos de espera y la falta de disponibilidad del servicio. Para obtener más información, consulte Optimizar el rendimiento.

Revise las cuotas de servicio de las API directas de EBS para determinar las solicitudes de API que puede ejecutar por segundo. Para obtener más información, consulte Puntos de enlace y cuotas de Amazon Elastic Block Store en la Referencia general de AWS .

Al ejecutar la ListChangedBlocks acción, ¿es posible obtener una respuesta vacía aunque haya bloques en la instantánea?

Sí. Si los bloques modificados son escasos en la instantánea, la respuesta puede estar vacía, pero la API devolverá un valor de token de página siguiente. Utilice el valor del token de página

siguiente para continuar con la siguiente página de resultados. Sabrá que ha llegado a la última página de resultados cuando la API devuelva un valor null de token de página siguiente.

Si el NextToken parámetro se especifica junto con otro StartingBlockIndex parámetro, ¿cuál de los dos se utiliza?

NextToken Se usa y StartingBlockIndex se ignora.

¿Cuánto tiempo son válidos los tokens de bloque y los tokens de siguiente página?

Los tokens de bloque son válidos durante siete días, y los tokens de siguiente página son válidos durante 60 minutos.

¿Se admiten instantáneas cifradas?

Sí. Se puede acceder a las instantáneas cifradas mediante las API directas de EBS.

Para acceder a una instantánea cifrada, el usuario debe tener acceso a la clave KMS utilizada para cifrar la instantánea y a la acción de AWS KMS desencriptación. Consulte la Permisos de IAM para las API directas de EBS sección anterior de esta guía para ver la AWS KMS política que se debe asignar a un usuario.

¿Se admiten instantáneas públicas?

No se admiten instantáneas públicas.

¿Son compatibles las instantáneas locales de Amazon EBS con Outposts?

Outposts no admite las instantáneas locales de Amazon EBS.

¿El bloque de enumeración de instantáneas devuelve todos los índices de bloque y tokens de bloque de una instantánea o solo aquellos que tienen datos escritos en ellos?

Devuelve solo los índices y los tokens de bloque que tienen datos escritos en ellos.

¿Puedo obtener un historial de todas las llamadas a la API realizadas por las API directas de EBS en mi cuenta a los fines de realizar tareas de análisis de seguridad y solución de problemas operativos?

Sí. Para recibir un historial de llamadas a la API de las API directas de EBS realizadas en su cuenta, active AWS CloudTrail en la AWS Management Console. Para obtener más información, consulte Registre las llamadas de API para las API directas de EBS con AWS CloudTrail.

Seguridad en Amazon Elastic Block Store

En AWS, la seguridad en la nube es la máxima prioridad. Como cliente de AWS, se beneficiará de una arquitectura de red y de centros de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta servicios de AWS en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los Programas de conformidad de AWS . Para obtener información sobre los programas de conformidad que se aplican a Amazon Elastic Block Store, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad se determina según el servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le permite comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Amazon EBS. En los siguientes temas, se mostrará cómo configurar Amazon EBS para satisfacer sus objetivos de seguridad y conformidad. También puede aprender a utilizar otros servicios de AWS que ayudan a monitorear y proteger los recursos de Amazon EBS.

Temas

Protección de datos en Amazon Elastic Block Store

El modelo de responsabilidad compartida de AWS se aplica a la protección de datos en Amazon Elastic Block Store. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta la totalidad de Nube de AWS. Usted es responsable de mantener

el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog AWS Shared Responsibility Model and GDPR en el Blog de seguridad de AWS.

Con fines de protección de datos, recomendamos proteger las credenciales de la cuenta de Cuenta de AWS y configurar cuentas de usuario individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos de AWS. Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad del usuario con AWS CloudTrail.
- Utilice las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-2 al acceder a AWS a través de una interfaz de la línea de comandos o una API, utilice un punto de conexión de FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con Amazon EBS u otros Servicios de AWS mediante la consola, la API, la AWS CLI o los SDK de AWS. Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Temas

- Seguridad de datos de Amazon EBS

Seguridad de datos de Amazon EBS

Los volúmenes de Amazon EBS se presentan como dispositivos de bloques sin formatear y sin procesar. Estos dispositivos son dispositivos lógicos que se crean en la infraestructura de EBS, y el servicio Amazon EBS garantiza que los dispositivos estén vacíos de forma lógica (es decir, los bloques sin procesar se establecen en cero o contienen datos criptográficamente pseudoaleatorios) antes de cualquier uso o reutilización por parte de un cliente.

Si tiene procedimientos que requieren que todos los datos se borren mediante un método específico, ya sea después o antes de su uso (o ambos), como los que se detallan en DoD 5220.22-M (National Industrial Security Program Operating Manual) o NIST 800-88 (Guidelines for Media Sanitization), puede hacerlo en Amazon EBS. Esa actividad de bloques se reflejará en los medios de almacenamiento subyacentes del servicio Amazon EBS.

Cifrado en reposo y en tránsito

El cifrado de Amazon EBS es una solución de cifrado que le permite cifrar los volúmenes de Amazon EBS y las instantáneas de Amazon EBS mediante claves criptográficas de AWS Key Management Service. Las operaciones de cifrado de EBS se producen en los servidores que alojan instancias de Amazon EC2, lo que garantiza la seguridad tanto de los datos en reposo como de los datos en tránsito entre la instancia y su volumen adjunto y cualquier instantánea posterior. Para obtener más información, consulte Cifrado de Amazon EBS.

Administración de claves de KMS

Cuando crea un volumen o instantánea de Amazon EBS cifrado, se especifica una clave de AWS Key Management Service. De manera predeterminada, Amazon EBS utiliza la clave de KMS administrada de AWS para Amazon EBS en su cuenta y región (`aws/ebs`). Sin embargo, puede especificar una clave de KMS administrada por el cliente que puede crear y administrar. Usar su propia clave de KMS administrada por el cliente le da más flexibilidad, incluida la capacidad de crear, rotar y deshabilitar claves de KMS.

Para utilizar una clave de KMS administrada por el cliente, debe dar permiso a los usuarios para usar la clave KMS. Para obtener más información, consulte Permisos para los usuarios.

> **Important**
>
> Amazon EBS solo admite claves de KMS simétricas. No se puede utilizar una clave de KMS asimétrica para cifrar un volumen e instantánea de Amazon EBS. Para obtener ayuda para determinar si una clave de KMS es simétrica o asimétrica, consulte Identificación de claves de KMS asimétricas.

Para cada volumen, Amazon EBS pide AWS KMS para generar una clave de datos única cifrada bajo la clave KMS que especifique. Amazon EBS almacena la clave de datos cifrada con el volumen. A continuación, al adjuntar el volumen a una instancia de Amazon EC2, Amazon EBS llama a AWS KMS para descifrar la clave de datos. Amazon EBS utiliza la clave de datos de texto no cifrado en la memoria del hipervisor para cifrar toda la E/S al volumen. Para obtener más información, consulte Cómo funciona el cifrado de EBS.

Administración de identidades y accesos para Amazon Elastic Block Store

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda a los administradores a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan a qué personas se puede autenticar (pueden iniciar sesión) y autorizar (tienen permisos) para utilizar los recursos de Amazon EBS. IAM es un servicio de Servicio de AWS que se puede utilizar sin cargo adicional.

Temas

Público

La forma en que utilice AWS Identity and Access Management (IAM) varía en función del trabajo que realice en Amazon EBS.

Usuario de servicio: si utiliza el servicio de Amazon EBS para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Amazon EBS para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica de Amazon EBS, consulte Solucionar problemas de identidad y acceso de Amazon EBS.

Administrador de servicio: si está a cargo de los recursos de Amazon EBS en su empresa, probablemente tenga acceso completo a Amazon EBS. Es su trabajo determinar a qué características y recursos de Amazon EBS deben tener acceso los usuarios de su servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información acerca de cómo la empresa puede utilizar IAM con Amazon EBS, consulte Cómo funciona Amazon Elastic Block Store con IAM.

Administrador de IAM: si es administrador de IAM, es posible que desee obtener más información sobre cómo escribir políticas para administrar el acceso a Amazon EBS. Para ver ejemplos de políticas basadas en identidad de Amazon EBS que puede utilizar en IAM, consulte Ejemplos de políticas basadas en identidades de Amazon Elastic Block Store.

Autenticación con identidades

La autenticación es la manera de iniciar sesión en AWS mediante credenciales de identidad. Debe estar autenticado (haber iniciado sesión en AWS) como Usuario raíz de la cuenta de AWS, como un usuario de IAM o asumiendo un rol de IAM.

Puede iniciar sesión en AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (del IAM Identity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accede a AWS mediante la federación, está asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en la AWS Management Console o en el portal de acceso a AWS. Para obtener más información sobre el inicio de sesión en AWS, consulte Cómo iniciar sesión en su Cuenta de AWS en la Guía del usuario de AWS Sign-In.

Si accede a AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de la línea de comandos (CLI) para firmar criptográficamente las solicitudes mediante el uso de las credenciales. Si no utiliza las herramientas de AWS, debe firmar usted mismo las solicitudes. Para obtener más información sobre el método recomendado para firmar solicitudes, consulte Firma de solicitudes API de AWS en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, AWS le recomienda el uso de la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.

Usuario raíz de cuenta de Cuenta de AWS

Cuando se crea una cuenta de Cuenta de AWS, se comienza con una identidad de inicio de sesión que tiene acceso completo a todos los servicios y recursos de Servicios de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la Cuenta de AWS y se accede a ella iniciando sesión con el correo electrónico y la contraseña que utilizó para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, solicite que los usuarios humanos, incluidos los que requieren acceso de administrador, utilicen la federación con un proveedor de identidades para acceder a los servicios de Servicios de AWS utilizando credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidad web, el AWS Directory Service, el directorio del Identity Center, o cualquier usuario que acceda a Servicios de AWS utilizando credenciales proporcionadas a través de una fuente de identidad. Cuando identidades federadas acceden a las Cuentas de AWS, asumen roles y los roles proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en el IAM Identity Center o puede conectarse y sincronizar con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus aplicaciones y Cuentas de AWS. Para más información, consulte ¿Qué es IAM Identity Center? en la Guía del usuario de AWS IAM Identity Center.

Usuarios y grupos de IAM

Un usuario de IAM es una identidad en su Cuenta de AWS que dispone de permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad de tu cuenta de Cuenta de AWS que dispone de permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente un rol de IAM en la AWS Management Console cambiando de roles. Puede asumir un rol llamando a una operación de la AWS CLI o de la API de AWS, o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. El Centro de identidades de IAM correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder sus identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center.
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. No obstante, con algunos Servicios de AWS se puede asociar una política directamente a un recurso (en lugar de utilizar un rol como representante). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.
- Acceso entre servicios: algunos servicios de Servicios de AWS utilizan características de otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado a servicios.
  - Reenviar sesiones de acceso (FAS): cuando utiliza un rol o un usuario de IAM para llevar a cabo acciones en AWS, se le considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el Servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio

desde IAM. Para más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

- Rol vinculado al servicio: un rol vinculado al servicio es un tipo de rol de servicio que está vinculado a un Servicio de AWS. El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en la Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puede utilizar un rol de IAM que le permita administrar credenciales temporales para las aplicaciones que se ejecutan en una instancia EC2 y realizan solicitudes a la AWS CLI o a la API de AWS. Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar un rol de AWS a una instancia EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia adjuntado a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

Para controlar el acceso en AWS, se crean políticas y se adjuntan a identidades o recursos de AWS. Una política es un objeto de AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando una entidad principal (sesión de rol, usuario o usuario raíz) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan en AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de IAM. A continuación, el administrador puede agregar las políticas de IAM a los roles y los usuarios pueden asumir esos roles.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con dicha política puede obtener información del usuario de la AWS Management Console, AWS CLI o la API de AWS.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede asociar a varios usuarios, grupos y roles de su Cuenta de AWS. Las políticas administradas incluyen las políticas administradas de AWS y las políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Las entidades principales pueden incluir cuentas, usuarios, roles, usuarios federados o Servicios de AWS.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No se puede utilizar políticas de IAM administradas por AWS en una política basada en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3, AWS WAF y Amazon VPC son ejemplos de servicios que admiten las ACL. Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite otros tipos de políticas adicionales menos frecuentes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifique el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicio (SCP): las SCP son políticas de JSON que especifican los permisos máximos de una organización o una unidad organizativa en AWS Organizations. AWS Organizations es un servicio que le permite agrupar y administrar de manera centralizada varias cuentas de Cuentas de AWS que posea su empresa. Si habilita todas las características en una empresa, entonces podrá aplicar políticas de control de servicio (SCP) a una o todas sus cuentas. Una SCP limita los permisos para las entidades de las cuentas de miembros, incluido cada Usuario raíz de la cuenta de AWS. Para más información sobre Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para obtener información acerca de cómo AWS decide si permitir o no una

solicitud cuando hay varios tipos de políticas implicados, consulte Lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona Amazon Elastic Block Store con IAM

Antes de utilizar IAM para administrar el acceso a Amazon EBS, obtenga información sobre qué características de IAM se encuentran disponibles para su uso con Amazon EBS.

Características de IAM que puede utilizar con Amazon Elastic Block Store

Característica de IAM	Soporte de Amazon EBS
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de políticas	Sí
ACL	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	Sí
Roles vinculados al servicio	No

Para obtener una perspectiva general sobre cómo funcionan Amazon EBS y otros servicios de AWS con la mayoría de las características de IAM, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en identidad para Amazon EBS

Compatibilidad con las políticas basadas en identidades	Sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en identidad para Amazon EBS

Para ver ejemplos de políticas basadas en identidad de Amazon EBS, consulte Ejemplos de políticas basadas en identidades de Amazon Elastic Block Store.

Políticas basadas en recursos de Amazon EBS

Compatibilidad con las políticas basadas en recursos	No

Las políticas basadas en recursos son documentos de políticas JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Las entidades principales pueden incluir cuentas, usuarios, roles, usuarios federados o servicios de Servicios de AWS.

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando la entidad principal y el recurso se encuentran en Cuentas de AWS diferentes, un administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para más información, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Acciones de políticas para Amazon EBS

Admite acciones de políticas	Sí

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones de la política generalmente tienen el mismo nombre que la operación de API AWS asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de acciones de Amazon EBS, consulte Acciones, recursos y claves de condición en la Referencia de autorizaciones de servicio.

Las acciones de políticas de Amazon EBS utilizan el siguiente prefijo antes de la acción:

```
ec2
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
  "ec2:action1",
  "ec2;:action2"
```

```
]
```

Para ver ejemplos de políticas basadas en identidad de Amazon EBS, consulte Ejemplos de políticas basadas en identidades de Amazon Elastic Block Store.

Recursos de políticas para Amazon EBS

Admite recursos de políticas	Sí

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de los tipos de recursos de Amazon EBS y sus ARN, consulte Recursos definidos por Amazon Elastic Block Store en la Referencia de autorizaciones de servicio. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por Amazon Elastic Block Store.

Algunas acciones de la API de Amazon EBS admiten varios recursos. Para especificar varios recursos en una única instrucción, separe los ARN con comas. Por ejemplo, `DescribeVolumes` accede a vol-01234567890abcdef y vol-09876543210fedcba, por lo que una entidad principal debe tener permisos para acceder a ambos recursos.

```
"Resource": [
  "arn:aws:ec2:us-east-1:123456789012:volume/vol-01234567890abcdef",
  "arn:aws:ec2:us-east-1:123456789012:volume/vol-09876543210fedcba"
]
```

Claves de condición de políticas para Amazon EBS

Admite claves de condición de políticas específicas del servicio	Sí

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación lógica `AND`. Si especifica varios valores para una única clave de condición, AWS evalúa la condición con una operación `OR` lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del usuario de IAM.

Por ejemplo, la siguiente condición permite a la entidad principal realizar una acción en un volumen solo si el tipo de volumen es `gp2`.

```
"Condition":{
  "StringLikeIfExists":{
    "ec2:VolumeType":"gp2"
  }
}
```

A fin de conocer una lista completa de acciones de políticas para Amazon EBS, consulte Acciones, recursos y claves de condición en la Referencia de autorizaciones de servicio. Para obtener más

información acerca de las acciones y los recursos con los que puede utilizar una clave de condición, consulte Acciones definidas por Amazon Elastic Block Store.

ACL en Amazon EBS

Admite las ACL	No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con Amazon EBS

Admite ABAC (etiquetas en las políticas)	Parcial

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a entidades de IAM (usuarios o roles) y a muchos recursos de AWS. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte ¿Qué es ABAC? en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con Amazon EBS

Compatible con el uso de credenciales temporales	Sí

Algunos Servicios de AWS no funcionan cuando inicia sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre qué Servicios de AWS funcionan con credenciales temporales, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en la AWS Management Console con cualquier método, excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accede a AWS utilizando el enlace de inicio de sesión único (SSO) de la empresa, ese proceso crea automáticamente credenciales temporales. También crea automáticamente credenciales temporales cuando inicia sesión en la consola como usuario y luego cambia de rol. Para más información sobrel cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puede crear credenciales temporales de forma manual mediante la AWS CLI o la API de AWS. A continuación, puede usar esas credenciales temporales para acceder a AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de usar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Permisos de entidad principal entre servicios para Amazon EBS

Admite Forward access sessions (FAS)	Sí

Cuando utiliza un usuario o un rol de IAM para llevar a cabo acciones en AWS, se lo considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el Servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Roles de servicio para Amazon EBS

Compatible con roles de servicio	Sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de Amazon EBS. Edite los roles de servicio solo cuando reciba la orientación de Amazon EBS.

Roles vinculados a servicios para Amazon EBS

Compatible con roles vinculados al servicio	No

Un rol vinculado al servicio es un tipo de rol de servicio que está vinculado a un Servicio de AWS. El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en la Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en identidades de Amazon Elastic Block Store

De forma predeterminada, los usuarios y roles no tienen permiso para crear o modificar los recursos de Amazon EBS. Tampoco pueden realizar tareas mediante la AWS Management Console, la AWS Command Line Interface (AWS CLI) o la API de AWS. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de

IAM. A continuación, el administrador puede agregar las políticas de IAM a los roles y los usuarios pueden asumir esos roles.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por Amazon EBS, incluido el formato de los ARN para cada tipo de recurso, consulte Acciones, recursos y claves de condición para Amazon Elastic Block Store en la Referencia de autorizaciones de servicio.

Temas

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidad determinan si alguien puede crear, acceder o eliminar los recursos de Amazon EBS de la cuenta. Estas acciones pueden generar costes adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas administradas de AWS y continúe con los permisos de privilegio mínimo: a fin de comenzar a conceder permisos a los usuarios y las cargas de trabajo, utilice las políticas administradas de AWS, que conceden permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Se recomienda definir políticas administradas por el cliente de AWS específicas para los casos de uso a fin de reducir aún más los permisos. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía del usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.

- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puede usar condiciones para conceder acceso a acciones de servicios si se emplean a través de un Servicio de AWS determinado, como por ejemplo AWS CloudFormation. Para más información, consulte Elementos de política JSON de IAM: condición en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Política de validación de Analizador de acceso de IAM en la Guía de usuario de IAM.
- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesita usuarios raíz o de IAM en su Cuenta de AWS, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de la consola de Amazon EBS

Para acceder a la consola de Amazon Elastic Block Store, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver los detalles sobre los recursos de Amazon EBS en la Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que conceda permisos mínimos para la consola a los usuarios que solo realizan llamadas a la AWS CLI o a la API de AWS. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para asegurarse de que los usuarios y los roles puedan seguir utilizando la consola de Amazon EBS, asocie también `ConsoleAccess` de Amazon EBS o la política administrada `ReadOnly` de AWS

a las entidades. Para más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para realizar esta acción en la consola o mediante programación con la AWS CLI o la API de AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Trabajar con volúmenes

Ejemplos

- Ejemplo: Adjuntar y separar volúmenes
- Ejemplo: Crear un volumen
- Ejemplo: Crear un volumen con etiquetas
- Por ejemplo: trabajo con volúmenes desde la consola de Amazon EC2

Ejemplo: Adjuntar y separar volúmenes

Cuando para una acción de una API el intermediario tiene que especificar varios recursos, usted debe crear una instrucción de política que permita a los usuarios obtener acceso a todos los recursos necesarios. Si necesita utilizar un elemento `Condition` con uno o varios de estos recursos, debe crear varias instrucciones, tal y como se muestra en este ejemplo.

La siguiente política permite a los usuarios adjuntar volúmenes con la etiqueta "`volume_user`=iam-user-name" a instancias con la etiqueta "`department=dev`" y separar dichos volúmenes de dichas instancias. Si asocia esta política a un grupo de IAM, la variable de política de `aws:username` da a cada usuario del grupo permiso para asociar o desasociar volúmenes de las instancias con una etiqueta llamada `volume_user` que tiene su nombre de usuario como valor.

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/department": "dev"
        }
      }
   },
   {
      "Effect": "Allow",
```

```
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/volume_user": "${aws:username}"
        }
      }
    }
  ]
}
```

Ejemplo: Crear un volumen

La siguiente política permite a los usuarios utilizar la acción CreateVolume de la API. Se permite al usuario crear un volumen únicamente si este está cifrado y si el tamaño del volumen es inferior a 20 GiB.

```
{
  "Version": "2012-10-17",
  "Statement": [
         {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateVolume"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition":{
         "NumericLessThan": {
             "ec2:VolumeSize" : "20"
          },
          "Bool":{
              "ec2:Encrypted" : "true"
          }
       }
    }
  ]
}
```

Ejemplo: Crear un volumen con etiquetas

La siguiente política contiene la clave de condición `aws:RequestTag` que exige a los usuarios que etiqueten todos los volúmenes que creen con las etiquetas `costcenter=115` y `stack=prod`. Si los usuarios no transmiten estas etiquetas en concreto o si no especifican ninguna etiqueta, la solicitud dará un error.

En las acciones de creación de recursos que aplican etiquetas, los usuarios también deben tener permisos para utilizar la acción `CreateTags`. La segunda instrucción utiliza la clave de condición `ec2:CreateAction` para permitir a los usuarios crear etiquetas únicamente en el contexto de `CreateVolume`. Los usuarios no pueden etiquetar volúmenes que ya existen ni otros recursos.

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Sid": "AllowCreateTaggedVolumes",
      "Effect": "Allow",
      "Action": "ec2:CreateVolume",
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/costcenter": "115",
          "aws:RequestTag/stack": "prod"
         }
       }
     },
     {
       "Effect": "Allow",
       "Action": [
         "ec2:CreateTags"
       ],
       "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
       "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "CreateVolume"
         }
       }
     }
  ]
}
```

La siguiente política permite a los usuarios crear un volumen sin tener que especificar etiquetas. La acción `CreateTags` solo se evalúa si se especifican etiquetas en la solicitud `CreateVolume`. Si los usuarios especifican etiquetas, la etiqueta tiene que ser `purpose=test`. No se permite ninguna otra etiqueta en la solicitud.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVolume",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
         "StringEquals": {
             "aws:RequestTag/purpose": "test",
             "ec2:CreateAction" : "CreateVolume"
          },
         "ForAllValues:StringEquals": {
             "aws:TagKeys": "purpose"
          }
       }
    }
  ]
}
```

Por ejemplo: trabajo con volúmenes desde la consola de Amazon EC2

La siguiente política concede a los usuarios permiso para ver y crear volúmenes, además de adjuntar volúmenes a instancias específicas y separarlos de ellas mediante la consola de Amazon EC2.

Los usuarios pueden adjuntar cualquier volumen a instancias que tienen la etiqueta "`purpose=test`" y también separar volúmenes de dichas instancias. Para adjuntar un volumen mediante la consola de Amazon EC2, es conveniente que los usuarios tengan permiso para utilizar la acción `ec2:DescribeInstances`, ya que esto les permite seleccionar una instancia en una lista rellenada previamente en el cuadro de diálogo Attach Volume (Asociar volumen). Sin embargo, esto

también permite a los usuarios ver todas las instancias de la página Instances (Instancia[s]) de la consola, por lo que puede omitir esta acción.

En la primera instrucción, la acción `ec2:DescribeAvailabilityZones` es necesaria para garantizar que un usuario pueda seleccionar una zona de disponibilidad al crear un volumen.

Los usuarios no pueden etiquetar los volúmenes que crean (ni durante la creación de volúmenes ni después).

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVolumes",
        "ec2:DescribeAvailabilityZones",
        "ec2:CreateVolume",
        "ec2:DescribeInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": "arn:aws:ec2:region:111122223333:instance/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/purpose": "test"
        }
     }
   },
   {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": "arn:aws:ec2:region:111122223333:volume/*"
   }
   ]
```

```
}
```

Trabajar con instantáneas

A continuación se incluyen políticas de ejemplo para `CreateSnapshot` (instantánea de un punto en el tiempo de un volumen de EBS) y `CreateSnapshots` (instantáneas de varios volúmenes).

Ejemplos

- Ejemplo: Crear una instantánea
- Ejemplo: Crear instantáneas
- Ejemplo: Crear una instantánea con etiquetas
- Ejemplo: Creación de instantáneas de varios volúmenes con etiquetas
- Ejemplo: Copia de instantáneas
- Ejemplo: Modificar la configuración de permisos de las instantáneas

Ejemplo: Crear una instantánea

La siguiente política permite a los clientes utilizar la acción CreateSnapshot de la API. El cliente puede crear instantáneas únicamente si este está cifrado y si el tamaño del volumen es inferior a 20 GiB.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*"
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1:account-id:volume/*",
         "Condition":{
            "NumericLessThan":{
               "ec2:VolumeSize":"20"
            },
            "Bool":{
```

```
                "ec2:Encrypted":"true"
            }
         }
      }
   ]
}
```

Ejemplo: Crear instantáneas

La siguiente política permite a los clientes utilizar la acción CreateSnapshots de la API. El cliente puede crear instantáneas solo si todos los volúmenes de la instancia son de tipo GP2.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":[
"arn:aws:ec2:us-east-1::snapshot/*",
"arn:aws:ec2:*:*:instance/*"
   ]
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1:*:volume/*",
         "Condition":{
            "StringLikeIfExists":{
               "ec2:VolumeType":"gp2"
             }
     }

      }
   ]
}
```

Ejemplo: Crear una instantánea con etiquetas

La siguiente política incluye la clave de condición `aws:RequestTag` que exige al cliente aplicar las etiquetas `costcenter=115` y `stack=prod` a cualquier instantánea nueva. Si los usuarios no transmiten estas etiquetas en concreto o si no especifican ninguna etiqueta, la solicitud dará un error.

En las acciones de creación de recursos que aplican etiquetas, los clientes también deben tener permisos para utilizar la acción `CreateTags`. La tercera instrucción utiliza la clave de condición `ec2:CreateAction` para permitir a los clientes crear etiquetas únicamente en el contexto de `CreateSnapshot`. Los clientes no pueden etiquetar volúmenes que ya existen ni otros recursos.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1:account-id:volume/*"
      },
      {
         "Sid":"AllowCreateTaggedSnapshots",
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/costcenter":"115",
               "aws:RequestTag/stack":"prod"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "ec2:CreateAction":"CreateSnapshot"
            }
         }
      }
   ]
}
```

Ejemplo: Creación de instantáneas de varios volúmenes con etiquetas

La siguiente política incluye la clave de condición `aws:RequestTag` que exige al cliente aplicar las etiquetas `costcenter=115` y `stack=prod` al crear un conjunto de instantáneas de varios

volúmenes. Si los usuarios no transmiten estas etiquetas en concreto o si no especifican ninguna etiqueta, la solicitud dará un error.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":[
"arn:aws:ec2:us-east-1::snapshot/*",
"arn:aws:ec2:*:*:instance/*",
"arn:aws:ec2:*:*:volume/*"

   ]
      },
      {
         "Sid":"AllowCreateTaggedSnapshots",
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/costcenter":"115",
               "aws:RequestTag/stack":"prod"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "ec2:CreateAction":"CreateSnapshots"
            }
         }
      }
   ]
}
```

La siguiente política permite a los clientes crear una instantánea sin tener que especificar etiquetas. La acción `CreateTags` se evalúa solo si se especifican etiquetas en la solicitud `CreateSnapshot`

o `CreateSnapshots`. Las etiquetas se pueden omitir en la solicitud. Si se especifica una etiqueta, la etiqueta debe ser `purpose=test`. No se permite ninguna otra etiqueta en la solicitud.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/purpose":"test",
               "ec2:CreateAction":"CreateSnapshot"
            },
            "ForAllValues:StringEquals":{
               "aws:TagKeys":"purpose"
            }
         }
      }
   ]
}
```

La siguiente política permite a los clientes crear conjuntos de instantáneas de varios volúmenes sin tener que especificar etiquetas. La acción `CreateTags` se evalúa solo si se especifican etiquetas en la solicitud `CreateSnapshot` o `CreateSnapshots`. Las etiquetas se pueden omitir en la solicitud. Si se especifica una etiqueta, la etiqueta debe ser `purpose=test`. No se permite ninguna otra etiqueta en la solicitud.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"*"
      },
```

```
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/purpose":"test",
               "ec2:CreateAction":"CreateSnapshots"
            },
            "ForAllValues:StringEquals":{
               "aws:TagKeys":"purpose"
            }
         }
      }
   ]
}
```

La siguiente política permite crear instantáneas solo si el volumen de origen se etiqueta con `User:username` para el cliente y la propia instantánea se etiqueta con `Environment:Dev` y `User:username`. El cliente puede añadir etiquetas adicionales a la instantánea.

```
{
   "Version":"2012-10-17",
   "Statement": [
           {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1:account-id:volume/*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/User":"${aws:username}"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/Environment":"Dev",
               "aws:RequestTag/User":"${aws:username}"
            }
```

```
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*"
      }
   ]
}
```

La siguiente política de `CreateSnapshots` permite crear instantáneas solo si el volumen de origen se etiqueta con `User:`*`username`* para el cliente y la propia instantánea se etiqueta con `Environment:Dev` y `User:`*`username`*.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1:*:instance/*",
 },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1:account-id:volume/*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/User":"${aws:username}"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/Environment":"Dev",
               "aws:RequestTag/User":"${aws:username}"
            }
         }
      },
```

```
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*"
      }
   ]
}
```

La siguiente política permite la eliminación de una instantánea solo si la instantánea está etiquetada con User:nombre de usuario para el cliente.

```
{
   "Version":"2012-10-17",
   "Statement": [
            {
         "Effect":"Allow",
         "Action":"ec2:DeleteSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/User":"${aws:username}"
            }
         }
      }
   ]
}
```

La siguiente política permite a un cliente crear una instantánea, pero deniega la acción si la instantánea que se está creando tiene una clave de etiqueta `value=stack`.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":[
            "ec2:CreateSnapshot",
            "ec2:CreateTags"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Deny",
```

```
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "ForAnyValue:StringEquals":{
               "aws:TagKeys":"stack"
            }
         }
      }
   ]
}
```

La siguiente política permite a un cliente crear instantáneas, pero deniega la acción si las instantáneas que se están creando tienen una clave de etiqueta `value=stack`.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":[
            "ec2:CreateSnapshots",
            "ec2:CreateTags"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Deny",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "ForAnyValue:StringEquals":{
               "aws:TagKeys":"stack"
            }
         }
      }
   ]
}
```

La siguiente política le permite combinar varias acciones en una sola política. Solo puede crear una instantánea (en el contexto de `CreateSnapshots`) cuando la instantánea se crea en la región `us-east-1`. Solo puede crear instantáneas (en el contexto de `CreateSnapshots`) cuando las instantáneas se crean en la región `us-east-1` y cuando el tipo de instancia es `t2*`.

```
{
   "Version":"2012-10-17",
   "Statement": [
          {
         "Effect":"Allow",
         "Action":[
            "ec2:CreateSnapshots",
            "ec2:CreateSnapshot",
            "ec2:CreateTags"
         ],
         "Resource": [
            "arn:aws:ec2:*:*:instance/*",
            "arn:aws:ec2:*:*:snapshot/*",
            "arn:aws:ec2:*:*:volume/*"
         ],
         "Condition":{
            "StringEqualsIgnoreCase": {
              "ec2:Region": "us-east-1"
            },
            "StringLikeIfExists": {
              "ec2:InstanceType": ["t2.*"]
            }
         }
      }
   ]
}
```

Ejemplo: Copia de instantáneas

Los permisos de nivel de recursos especificados para la acción CopySnapshot sólo se aplican a la nueva instantánea. No se pueden especificar para la instantánea de origen.

La siguiente política de ejemplo permite a las entidades copiar instantáneas sólo si la nueva instantánea se crea con la clave de etiqueta de `purpose` y un valor de etiqueta de `production` (`purpose=production`).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCopySnapshotWithTags",
            "Effect": "Allow",
```

```
            "Action": "ec2:CopySnapshot",
            "Resource": "arn:aws:ec2:*:account-id:snapshot/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/purpose": "production"
                }
            }
        }
    ]
}
```

Ejemplo: Modificar la configuración de permisos de las instantáneas

La siguiente política permite la modificación de una instantánea solo si la instantánea está etiquetada con `User:username`, donde *username* es el nombre de usuario de la cuenta de AWS del cliente. La solicitud falla si no se cumple esta condición.

```
{
   "Version":"2012-10-17",
   "Statement": [
           {
         "Effect":"Allow",
         "Action":"ec2:ModifySnapshotAttribute",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/user-name":"${aws:username}"
            }
         }
      }
   ]
}
```

Solucionar problemas de identidad y acceso de Amazon EBS

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que es posible que surjan cuando se trabaja con Amazon EBS e IAM.

Problemas

- No tengo autorización para realizar una acción en Amazon EBS
- No tengo autorización para realizar la operación iam:PassRole
- Quiero permitir a personas externas a mi Cuenta de AWS el acceso a mis recursos de Amazon EBS

No tengo autorización para realizar una acción en Amazon EBS

Si la AWS Management Console le indica que no tiene autorización para llevar a cabo una acción, debe ponerse en contacto con su administrador para recibir ayuda. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

El siguiente ejemplo, el error se produce cuando el usuario de IAM denominado `mateojackson` intenta utilizar la consola para ver detalles de un volumen, pero no tiene permisos de `ec2:DescribeVolumes`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:DescribeVolumes on resource: volume-id
```

En este caso, Mateo pide a su administrador de AWS que le permita describir el volumen.

No tengo autorización para realizar la operación iam:PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, sus políticas deben actualizarse para permitirle pasar un rol a Amazon EBS.

Algunos Servicios de AWS le permiten transferir un rol existente a dicho servicio en lugar de crear un nuevo rol de servicio o uno vinculado al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Amazon EBS. Sin embargo, la acción requiere que el servicio cuente con permisos que concede un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador de AWS. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir a personas externas a mi Cuenta de AWS el acceso a mis recursos de Amazon EBS

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para saber si Amazon EBS admite estas características, consulte Cómo funciona Amazon Elastic Block Store con IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos de las Cuentas de AWS de su propiedad, consulte Proporcionar acceso a un usuario de IAM a otra Cuenta de AWS de la que es propietario en la Guía del usuario de IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos a Cuentas de AWS de terceros, consulte Proporcionar acceso a Cuentas de AWS que son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante la federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (federación de identidades) en la Guía del usuario de IAM.
- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Validación de conformidad para Amazon Elastic Block Store

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

  > **Note**
  >
  > No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos

de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.

- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en Amazon Elastic Block Store

La infraestructura global de AWS se divide en Regiones de AWS y zonas de disponibilidad. Las Regiones de AWS proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que conmutan automáticamente entre zonas sin interrupción. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre las Regiones de AWS y las zonas de disponibilidad, consulte la Infraestructura global de AWS.

Además de la infraestructura global de AWS, Amazon EBS ofrece varias características que le brindan ayuda con sus necesidades de resiliencia y copia de seguridad de los datos.

- Automatización de las instantáneas de EBS con Amazon Data Lifecycle Manager
- Copia de las instantáneas de EBS en las regiones

Monitoreo de Amazon Elastic Block Store

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Amazon Elastic Block Store y sus demás AWS soluciones. AWS proporciona las siguientes herramientas de supervisión para vigilar Amazon EBS, informar cuando algo va mal y tomar medidas automáticas cuando sea necesario:

- AWS CloudTrailcaptura las llamadas a la API y los eventos relacionados realizados por usted o en su nombre Cuenta de AWS y entrega los archivos de registro a un bucket de Amazon S3 que especifique. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron las llamadas. Para más información, consulte la Guía del usuario de AWS CloudTrail.
- Amazon CloudWatch monitorea tus AWS recursos y las aplicaciones en las que AWS ejecutas en tiempo real. Puede recopilar métricas y realizar un seguimiento de las métricas, crear paneles personalizados y definir alarmas que le advierten o que toman medidas cuando una métrica determinada alcanza el umbral que se especifique. Por ejemplo, puede CloudWatch hacer un seguimiento del uso de la CPU u otras métricas de sus instancias de Amazon EC2 y lanzar automáticamente nuevas instancias cuando sea necesario. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.
- Amazon se EventBridge puede utilizar para automatizar sus AWS servicios y responder automáticamente a los eventos del sistema, como los problemas de disponibilidad de las aplicaciones o los cambios de recursos. Los eventos de AWS los servicios se entregan EventBridge prácticamente en tiempo real. Puede crear reglas sencillas para indicar qué eventos le resultan de interés, así como qué acciones automatizadas se van a realizar cuando un evento cumple una de las reglas. Para obtener más información, consulta la Guía EventBridge del usuario de Amazon.

Temas

AWS CloudTrail para Amazon EBS

Amazon Elastic Block Store (Amazon EBS) se integra a AWS CloudTrail, un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un servicio de AWS en Amazon EBS. CloudTrail captura todas las llamadas a la API de Amazon EBS como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de Amazon EBS y las llamadas de código hacia las operaciones de la API de Amazon EBS. Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos de Amazon EBS. Si no configura un registro de seguimiento, puede ver los eventos más recientes en la consola de CloudTrail en el Historial de eventos. Mediante la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a Amazon EBS, la dirección IP desde la que se realizó la solicitud, quién realizó la solicitud, cuándo se realizó y otros detalles adicionales.

Para más información sobre CloudTrail, consulte la Guía del usuario de AWS CloudTrail.

Información de Amazon EBS en CloudTrail

CloudTrail se habilita en su Cuenta de AWS cuando se crea la cuenta. Cuando se produce una actividad en Amazon EBS, dicha actividad se registra en un evento de CloudTrail junto con los eventos de los demás servicios de AWS en el Historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para más información, consulte Viewing events with CloudTrail Event history.

Para mantener un registro continuo de los eventos de su Cuenta de AWS, incluidos los eventos de Amazon EBS, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También es posible configurar otros servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- Servicios e integraciones compatibles con CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de registro de CloudTrail de varias regiones y Recibir archivos de registro de CloudTrail de varias cuentas

CloudTrail registra todas las acciones de la API de Amazon EBS Por ejemplo, las llamadas a las acciones CreateVolume, DeleteVolume y CreateSnapshot generan entradas en los archivos de registro de CloudTrail.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario de AWS Identity and Access Management (IAM) o credenciales de usuario raíz.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para más información, consulte Elemento userIdentity de CloudTrail.

Descripción de las entradas de los archivos de registro de Amazon EBS

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros en un bucket de Amazon S3 que especifique. Los archivos de registro de CloudTrail pueden contener una o varias entradas de registro. Un evento representa una solicitud específica realizada desde un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de registro de CloudTrail que ilustra la acción CreateVolume.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "Root",
        "principalId": "AROAJABCHBVMHREXAMPLE:root",
        "arn": "123456789012",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE"
    },
    "eventTime": "2024-02-08T08:02:21Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "CreateVolume",
    "awsRegion": "us-east-1",
```

```
    "sourceIPAddress": "12.12.123.123",
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7botocore/1.4.1",
    "requestParameters": {
        "size": "100",
        "zone": "us-east-1a",
        "volumeType": "gp3",
        "iops": "3000",
        "encrypted": true,
        "masterEncryptionKeyId": "arn:aws:kms:us-east-1:123456789012:key/12345678-
a202-4b72-8030-example23456",
        "throughput": "125",
        "clientToken": "12345678-2427-4336-a555-e8607example"
    },
    "responseElements": {
        "requestId": "12345678-4229-4cfd-9cb1-0b094example",
        "volumeId": "vol-01234567890abcdef",
        "size": "100",
        "zone": "us-east-1a",
        "status": "creating",
        "createTime": 1707379341000,
        "volumeType": "gp3",
        "iops": 3000,
        "encrypted": true,
        "masterEncryptionKeyId": "arn:aws:kms:us-east-1:123456789012:key/12345678-
a202-4b72-8030-example23456",
        "tagSet": {},
        "multiAttachEnabled": false,
        "throughput": 125
    },
    "requestID": "12345678-4229-4cfd-9cb1-0b094example",
    "eventID": "12345678-4b33-4c18-90a1-76d4bexample",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```

CloudWatch Métricas de Amazon para Amazon EBS

Las CloudWatch métricas de Amazon son datos estadísticos que puede utilizar para ver, analizar y configurar alarmas sobre el comportamiento operativo de sus volúmenes.

Los datos se encuentran disponibles automáticamente en periodos de 1 minuto sin costo alguno.

Al obtener datos de CloudWatch, puede incluir un parámetro de `Period` solicitud para especificar la granularidad de los datos devueltos. Este periodo es diferente al que utilizamos cuando recopilamos los datos (periodos de 1 minuto). Recomendamos que especifique un periodo en la solicitud que sea igual o superior al periodo de obtención para asegurarse de que los datos devueltos sean válidos.

Puede obtener los datos mediante la CloudWatch API o la consola Amazon EC2. La consola toma los datos sin procesar de la CloudWatch API y muestra una serie de gráficos basados en los datos. En función de sus necesidades, es posible que prefiera utilizar los datos de la API o los gráficos de la consola.

Temas

Métricas para los volúmenes de Amazon EBS

El espacio de nombres de `AWS/EBS` incluye las siguientes métricas para los volúmenes de EBS que se han adjuntado a todo tipo de instancias. Todos los tipos de volúmenes de Amazon EBS envían automáticamente métricas de 1 minuto a una CloudWatch instancia, pero solo cuando el volumen está adjunto a una instancia.

Para obtener información sobre el espacio en disco disponible del sistema operativo en una instancia, consulte Ver espacio libre en disco.

> **Note**
>
> Algunas de estas métricas tienen diferencias en las instancias creadas en el sistema Nitro. Para obtener una lista de estos tipos de instancias, consulte Instancias creadas en el sistema Nitro.

Métrica	Descripción	Unidades	Dimensiones	Estadísticas significativas
`VolumeReadBytes`	Proporciona información sobre las operaciones de lectura realizadas en un periodo especificado. • La estadística `Sum` registra el número total de bytes transferidos durante el periodo. • La estadística `Average` informa el tamaño promedio de cada operación de lectura durante el periodo, excepto en volúmenes asociados a una instancia Nitro, donde el promedio corresponde al del periodo especificado. • La estadística `SampleCount` informa el número total de operaciones	Bytes	`VolumeId`	• `Average` • `Sum` • `SampleCount` • `Minimum` | `Maximum`: solo para los volúmenes asociados a instancias basadas en Nitro

Métrica	Descripción	Unidades	Dimensiones	Estadísticas significativas
	de lectura durante el periodo, excepto en volúmenes asociados a una instancia basada en Nitro, donde el número de muestras representa el número de puntos de datos usados en el cálculo estadístico. **Note** Para las instancias Xen, los datos solo se registran cuando existe una actividad de lectura en el volumen.			

Métrica	Descripción	Unidades	Dimensiones	Estadísticas significativas
`VolumeWriteBytes`	Proporciona información sobre las operaciones de escritura realizadas en un periodo especificado • La estadística `Sum` registra el número total de bytes transferidos durante el periodo. • La estadística `Average` informa del tamaño medio de cada operación de escritura durante el periodo, excepto en volúmenes asociados a una instancia basada en Nitro, donde la media corresponde a la del periodo especificado. • La estadística `SampleCount` informa del tamaño medio de las operaciones de escritura durante el periodo, excepto en volúmenes asociados a una instancia basada en Nitro, donde el número de muestras	Bytes	`VolumeId`	• `Average` • `Sum` • `SampleCount` • `Minimum` | `Maximum`: solo para los volúmenes asociados a instancias basadas en Nitro

Métrica	Descripción	Unidades	Dimensiones	Estadísticas significativas
	representa el número de puntos de datos usados en el cálculo estadístico. **Note** Para las instancias Xen, los datos solo se registran cuando existe una actividad de escritura en el volumen.			
`VolumeReadOps`	Número total de operaciones de lectura realizadas en un periodo especificado. Las operaciones de lectura se contabilizan una vez finalizadas. Para calcular el promedio de operaciones de lectura por segundo (IOPS de lectura) del periodo, divida el total de operaciones del periodo por el número de segundos de ese periodo.	Recuento	`VolumeId`	• `Average` • `Sum` • `Minimum` | `Maximum`: solo para los volúmenes asociados a instancias basadas en Nitro

Métrica	Descripción	Unidades	Dimensiones	Estadísticas significativas
`VolumeWriteOps`	Número total de operaciones de escritura en un periodo especificado. Las operaciones de escritura se contabilizan una vez finalizadas. Para calcular el promedio de operaciones de escritura por segundo (IOPS de escritura) del periodo, divida el total de operaciones de escritura del periodo por el número de segundos de ese periodo.	Recuento	`VolumeId`	• `Average` • `Sum` • `Minimum` | `Maximum`: solo para los volúmenes asociados a instancias basadas en Nitro

Métrica	Descripción	Unidades	Dimensiones	Estadísticas significativas
`VolumeTotalReadTime`	**Note** No compatible con volúmenes habilitados para Multi-Attach. Para las instancias Xen, los datos solo se registran cuando existe una actividad de lectura en el volumen. Número total de segundos empleados por todas las operaciones de lectura que se realizaron en el periodo especificado. Si se envían varias solicitudes al mismo tiempo, este total puede ser mayor que la duración del periodo. Por ejemplo, para un periodo de 1 minuto (60 segundos): si se completaron 150 operaciones durante el periodo y cada operación	Segundos	`VolumeId`	• `Average`: sin importancia para los volúmenes asociados a instancias basadas en Nitro • `Sum` • `Minimum` | `Maximum`: solo para los volúmenes asociados a instancias basadas en Nitro

Métrica	Descripción	Unidades	Dimensiones	Estadísticas significativas
	tardó 1 segundo, el valor sería de 150 segundos.			

Métrica	Descripción	Unidades	Dimensiones	Estadísticas significativas
`VolumeTotalWriteTime`	**Note** No compatible con volúmenes habilitados para Multi-Attach. Para las instancias Xen, los datos solo se registran cuando existe una actividad de escritura en el volumen. Número total de segundos empleados por todas las operaciones de escritura que se realizaron en el periodo especificado. Si se envían varias solicitudes al mismo tiempo, este total puede ser mayor que la duración del periodo. Por ejemplo, para un periodo de 1 minuto (60 segundos): si se completaron 150 operaciones durante el periodo y cada operación	Segundos	`VolumeId`	• `Average`: sin importancia para los volúmenes asociados a instancias basadas en Nitro • `Sum` • `Minimum` | `Maximum`: solo para los volúmenes asociados a instancias basadas en Nitro

Métrica	Descripción	Unidades	Dimensiones	Estadísticas significativas
	tardó 1 segundo, el valor sería de 150 segundos.			
`VolumeIdleTime`	**Note** No compatible con volúmenes habilitados para Multi-Attach. Número total de segundos en un periodo de tiempo especificado en el que no se emitieron operaciones de lectura o escritura.	Segundos	`VolumeId`	• `Average`: sin importancia para los volúmenes asociados a instancias basadas en Nitro • `Sum` • `Minimum` | `Maximum`: solo para los volúmenes asociados a instancias basadas en Nitro

Métrica	Descripción	Unidades	Dimensiones	Estadísticas significativas
`VolumeQueueLength`	Número de solicitudes de operaciones de lectura y escritura a la espera de realizarse en un periodo de tiempo especificado.	Recuento	`VolumeId`	• `Average` • `Sum`: sin importancia para los volúmenes asociados a instancias Nitro • `Minimum` | `Maximum`: solo para los volúmenes asociados a instancias Nitro

Métrica	Descripción	Unidades	Dimensiones	Estadísticas significativas
`VolumeStalledIOCheck`	**Note** Solo para instancias de Nitro. No se publica para los volúmenes adjuntos a Amazon ECS y AWS Fargate las tareas. Indica si un volumen ha superado o no un control de E/S estancado en el último minuto. Esta métrica puede ser `0` (aprobada) o 1 (no aprobada). Para obtener más información, consulte. Supervise las características de E/S mediante CloudWatch	Recuento	`VolumeId` | `InstanceId`	• Sum • Media • Mínimo • Máximo

Métrica	Descripción	Unidades	Dimensiones	Estadísticas significativas
`VolumeThroughputPercentage`	**Note** Solo volúmenes SSD de las IOPS aprovisionadas. No compatible con volúmenes habilitados para Multi-Attach. El porcentaje de operaciones de E/S por segundo (IOPS) enviadas del total de IOPS provisionadas para un volumen de Amazon EBS. Los volúmenes de SSD de IOPS provisionadas ofrecen su rendimiento aprovisionado el 99,9 % del tiempo. Durante una operación de escritura, si no hay otras solicitudes de E/S pendientes en un minuto, el valor de la métrica será del 100%. Además, el rendimiento de E/S de un volumen se puede	Porcentaje	`VolumeId`	• `Average` • `Minimum` | `Maximum`

Métrica	Descripción	Unidades	Dimensiones	Estadísticas significativas
	degradar temporalmente debido a una acción que ha realizado (como crear una instantánea de un volumen durante un pico de uso, ejecutar el volumen en una instancia que no está optimizada para EBS u obtener acceso a los datos del volumen por primera vez).			

Métrica	Descripción	Unidades	Dimensiones	Estadísticas significativas
`VolumeConsumedReadWriteOps`	**Note** Solo volúmenes SSD de las IOPS aprovisionadas. La cantidad total de operaciones de lectura y escritura (normalizadas a las unidades de capacidad de 256 K) usadas en el periodo de tiempo especificado. Las operaciones de E/S menores de 256 K se cuentan como 1 IOPS consumida. Las operaciones de E/S mayores de 256 K se cuentan como unidades de capacidad de 256 K. Por ejemplo, una operación de E/S de 1024 K se contaría como 4 IOPS consumidas.	Recuento	`VolumeId`	• `Average` • `Sum` • `Minimum` | `Maximum`

Métrica	Descripción	Unidades	Dimensiones	Estadísticas significativas
`BurstBalance`	**Note** `gp2st1`, y solo para `sc1` volúmenes. Proporciona información sobre el porcentaje de créditos de E/S (para `gp2`) o créditos de rendimiento (para `st1` y `sc1`) que quedan en el bucket por ráfaga. Los datos CloudWatch solo se notifican cuando el volumen está activo. Si el volumen no está adjuntado, no se registran datos. Si el rendimiento de la línea de base del volumen excede el rendimiento por ráfagas máximo, no se gastan nunca créditos. Si el volumen está asociado a una instancia creada en Nitro System, no se informa del saldo de ráfagas. Para otras	Porcentaje	`VolumeId`	• `Average` • `Sum`: sin importancia para los volúmenes asociados a instancias Nitro. • `Minimum` | `Maximum`

Métrica	Descripción	Unidades	Dimensiones	Estadísticas significativas
	instancias, el saldo de ráfagas registrado es del 100 %. Para obtener más información, consulte Rendimiento del volumen gp2.			

Métricas para las instancias Nitro

El espacio de nombres de `AWS/EC2` incluye métricas adicionales de Amazon EBS para los volúmenes que se han adjuntado a instancias basadas en Nitro que no son instancias bare metal.

Métrica	Descripción	Unidad	Estadísticas significativas
`EBSReadOps`	Operaciones de lectura completadas de todos los volúmenes de Amazon EBS conectados a la instancia en un periodo especificado. Para calcular el promedio de operaciones de E/S de lectura por segundo (IOPS de lectura) del periodo, divida el total de operaciones del periodo por el número de segundos de ese periodo. Si utiliza el monitoreo básico (5 minutos), puede dividir este número por 300 para calcular la IOPS de lectura. Si utiliza el monitoreo detallado (1 minuto), divídalo por 60. También puede usar la función matemática CloudWatch métrica `DIFF_TIME` para encontrar las operaciones por segundo. Por ejemplo, si ha representado gráficamente `EBSReadOps` CloudWatch comom1, la fórmula	Recuento	• Sum • Media • Mínimo • Máximo

Métrica	Descripción	Unidad	Estadísticas significativas
	matemática métrica `m1/(DIFF_TIME(m1))` devuelve la métrica en operaciones/segundo. Para obtener más información `DIFF_TIME` y otras funciones matemáticas métricas, consulte Uso de la matemática métrica en la Guía del CloudWatch usuario de Amazon.		
`EBSWriteOps`	Operaciones de escritura completadas en todos los volúmenes de EBS conectados a la instancia en un periodo especificado. Para calcular el promedio de operaciones de E/S de escritura por segundo (IOPS de escritura) del periodo, divida el total de operaciones del periodo por el número de segundos de ese periodo. Si utiliza el monitoreo básico (5 minutos), puede dividir este número por 300 para calcular la IOPS de escritura. Si utiliza el monitoreo detallado (1 minuto), divídalo por 60. También puede utilizar la función matemática CloudWatch métrica `DIFF_TIME` para encontrar las operaciones por segundo. Por ejemplo, si ha representado gráficamente `EBSWriteOps` CloudWatch como `m1`, la fórmula matemática métrica `m1/(DIFF_TIME(m1))` devuelve la métrica en operaciones/segundo. Para obtener más información `DIFF_TIME` y otras funciones matemáticas métricas, consulte Uso de la matemática métrica en la Guía del CloudWatch usuario de Amazon.	Recuento	• Sum • Media • Mínimo • Máximo

Métrica	Descripción	Unidad	Estadísticas significativas
`EBSReadBytes`	Bytes leídos de todos los volúmenes de EBS conectados a la instancia en un periodo especificado. El número registrado es el número de bytes leídos durante el periodo. Si utiliza el monitoreo básico (5 minutos), puede dividir este número por 300 para conocer los bytes de lectura por segundo. Si utiliza el monitoreo detallado (1 minuto), divídalo por 60. También puede utilizar la función matemática CloudWatch métrica `DIFF_TIME` para encontrar los bytes por segundo. Por ejemplo, si ha representado gráficamente `EBSReadBytes` CloudWatch como`m1`, la fórmula matemática métrica `m1/(DIFF_TIME(m1))` devuelve la métrica en bytes/segundo. Para obtener más informaci ón `DIFF_TIME` y otras funciones matemátic as métricas, consulte Uso de la matemática métrica en la Guía del CloudWatch usuario de Amazon.	Bytes	• Sum • Media • Mínimo • Máximo

Métrica	Descripción	Unidad	Estadísticas significativas
`EBSWriteBytes`	Bytes escritos en todos los volúmenes de EBS conectados a la instancia en un periodo especificado. El número registrado es el número de bytes escritos durante el periodo. Si utiliza el monitoreo básico (5 minutos), puede dividir este número por 300 para conocer los bytes de escritura por segundo. Si utiliza el monitoreo detallado (1 minuto), divídalo por 60. También puede utilizar la función matemática CloudWatch métrica `DIFF_TIME` para encontrar los bytes por segundo. Por ejemplo, si ha representado gráficamente `EBSWriteBytes` CloudWatch como`m1`, la fórmula matemática métrica `m1/(DIFF_TIME(m1))` devuelve la métrica en bytes/segundo. Para obtener más información `DIFF_TIME` y otras funciones matemáticas métricas, consulte Uso de la matemática métrica en la Guía del CloudWatch usuario de Amazon.	Bytes	• Sum • Media • Mínimo • Máximo

Métrica	Descripción	Unidad	Estadísticas significativas
`EBSIOBalance%`	Proporciona información sobre el porcentaje de créditos restantes de E/S en el bucket por ráfaga. Esta métrica solo está disponible para la monitorización básica. Esta métrica solo está disponible para algunos tamaños de instancia `*.4xlarge` y otros más pequeños que alcancen su rendimiento máximo durante solo 30 minutos al menos una vez cada 24 horas. Para obtener más información, consulte EBS optimizado de forma predeterminada. La estadística `Sum` no es aplicable a esta métrica.	Porcentaje	• Mínimo • Máximo
`EBSByteBalance%`	Proporciona información sobre el porcentaje de créditos restantes de desempeño en el bucket por ráfaga. Esta métrica solo está disponible para la monitorización básica. Esta métrica solo está disponible para algunos tamaños de instancia `*.4xlarge` y otros más pequeños que alcancen su rendimiento máximo durante solo 30 minutos al menos una vez cada 24 horas. Para obtener más información, consulte EBS optimizado de forma predeterminada. La estadística `Sum` no es aplicable a esta métrica.	Porcentaje	• Mínimo • Máximo

Métricas para la restauración rápida de instantáneas

El espacio de nombres AWS/EBS incluye las siguientes métricas para la restauración rápida de instantáneas.

Métrica	Descripción	Unidades	Dimensiones	Estadísticas significativas
FastSnapshotRestoreCreditsBucketSize	El número máximo de volumen crea créditos que se pueden acumular. Esta métrica se notifica por instantánea y zona de disponibilidad.	Recuento	SnapshotId | AvailabilityZone	• Average • Minimum | Maximum **Note** La estadística más significativa es Average. Los resultados de las estadísticas Minimum y Maximum son las mismas que para Average y se pueden utilizar en su lugar.
FastSnapshotRestoreCreditsBalance	El número de volumen crea créditos disponibles. Esta métrica se notifica por instantánea y zona de disponibilidad.	Recuento	SnapshotId | AvailabilityZone	• Average • Minimum | Maximum **Note** La estadística más significativa es Average. Los resultados de las estadísti

Métrica	Descripción	Unidades	Dimensiones	Estadísticas significativas
				cas `Minimum` y `Maximum` son las mismas que para `Average` y se pueden utilizar en su lugar.

Gráficos de la consola de Amazon EC2

Después de crear un volumen, puede ver los gráficos de monitorización del volumen en la consola de Amazon EC2. Seleccione un volumen en la página Volumes (Volúmenes) de la consola y elija Monitoring (Monitorización). La siguiente tabla muestra los gráficos que aparecen. La columna de la derecha describe cómo se utilizan las métricas de datos sin procesar de la CloudWatch API para producir cada gráfico. El periodo para todos los gráficos es de 5 minutos.

Gráfico	Descripción con métricas sin formato
Rendimiento de lectura (KiB/s)	`Sum(VolumeReadBytes) / Period / 1024`
Rendimiento de escritura (KiB/s)	`Sum(VolumeWriteBytes) / Period / 1024`
Operaciones de lectura (Ops/s)	`Sum(VolumeReadOps) / Period`
Operaciones de escritura (Ops/s)	`Sum(VolumeWriteOps) / Period`
Longitud de cola media (operaciones)	`Avg(VolumeQueueLength)`
% tiempo inactivo	`Sum(VolumeIdleTime) / Period × 100`
Tamaño de lectura promedio (KiB/op)	`Avg(VolumeReadBytes) / 1024` Para las instancias basadas en Nitro, la siguiente fórmula obtiene el tamaño medio de lectura mediante la matemática CloudWatchmétrica:

Gráfico	Descripción con métricas sin formato
	`(Sum(VolumeReadBytes) / Sum(VolumeReadOps)) / 1024` Las `VolumeReadOps` métricas `VolumeReadBytes` y están disponibles en la consola de CloudWatch EBS.

Tamaño de escritura promedio (KiB/op)	`Avg(VolumeWriteBytes) / 1024`
	
	Para las instancias basadas en Nitro, la siguiente fórmula obtiene el tamaño medio de escritura mediante CloudWatch la matemática métrica:
	
	`(Sum(VolumeWriteBytes) / Sum(VolumeWriteOps)) / 1024`
	
	Las `VolumeWriteOps` métricas `VolumeWriteBytes` y están disponibles en la consola de CloudWatch EBS.

Latencia de lectura promedio (ms/op)	`Avg(VolumeTotalReadTime) × 1000`
	
	Para las instancias basadas en Nitro, la siguiente fórmula obtiene la latencia media de lectura mediante CloudWatch Metric Math:
	
	`(Sum(VolumeTotalReadTime) / Sum(VolumeReadOps)) × 1000`
	
	Las `VolumeReadOps` métricas `VolumeTotalReadTime` y están disponibles en la consola de CloudWatch EBS.

Gráfico	Descripción con métricas sin formato

Latencia de escritura promedio (ms/op)	`Avg(VolumeTotalWriteTime) × 1000`
	
	Para las instancias basadas en Nitro, la siguiente fórmula obtiene la latencia de escritura media mediante CloudWatch la matemática métrica:
	
	`(Sum(VolumeTotalWriteTime) / Sum(VolumeWriteOps)) * 1000`
	
	Las `VolumeWriteOps` métricas `VolumeTotalWriteTime` y están disponibles en la consola de CloudWatch EBS.

Para los gráficos de latencia media y los gráficos de tamaño medio, la media se calcula para el número total de operaciones (lectura o escritura, lo que corresponda al gráfico) completadas durante el periodo.

Amazon EventBridge para Amazon EBS

Amazon EBS envía eventos a Amazon EventBridge para las acciones realizadas en volúmenes e instantáneas. Con EventBridge él, puede establecer reglas que activen acciones programáticas en respuesta a estos eventos. Por ejemplo, puede crear una regla que envíe una notificación a su correo electrónico cuando se active una instantánea para la restauración rápida de instantáneas.

Los eventos de EventBridge se representan como objetos JSON. Los campos que son únicos del evento se encuentran en la sección "detail" del objeto JSON. El campo "event" contiene el nombre del evento. El campo "result" contiene el estado completad de la acción que desencadenó el evento. Para obtener más información, consulta los patrones de EventBridge eventos de Amazon en la Guía del EventBridge usuario de Amazon.

Para obtener más información, consulta ¿Qué es Amazon EventBridge? en la Guía del EventBridge usuario de Amazon.

Eventos

- Eventos de volumen de EBS
- Eventos de modificación del volumen de EBS

- Eventos de instantánea de EBS
- Eventos del archivo de instantáneas de EBS
- Eventos de restauración rápida de instantáneas de EBS
- Se utiliza AWS Lambda para gestionar eventos EventBridge

Eventos de volumen de EBS

Amazon EBS envía los eventos al EventBridge momento en que se producen los siguientes eventos de volumen.

Eventos

- Crear volumen (CreateVolume)
- Eliminar volumen (deleteVolume)
- Asociar o volver a asociar volumen (attachVolume, reattachVolume)
- Separar volumen (DetachVolume)

Crear volumen (CreateVolume)

El `createVolume` evento se envía a su AWS cuenta cuando se completa una acción para crear un volumen. Sin embargo, no se guarda, registra o archiva. Este evento tiene un resultado de `available` o `failed`. La creación no se realizará correctamente si AWS KMS key se proporciona un mensaje no válido, como se muestra en los ejemplos siguientes.

Datos de evento

La lista siguiente es un ejemplo de un objeto JSON emitido por EBS para un evento `createVolume` correcto.

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Volume Notification",
   "source": "aws.ec2",
   "account": "012345678901",
   "time": "yyyy-mm-ddThh:mm:ssZ",
   "region": "us-east-1",
```

```
   "resources": [
      "arn:aws:ec2:us-east-1:012345678901:volume/vol-01234567"
   ],
   "detail": {
      "result": "available",
      "cause": "",
      "event": "createVolume",
      "request-id": "01234567-0123-0123-0123-0123456789ab"
   }
}
```

La lista siguiente es un ejemplo de un objeto JSON emitido por EBS después de que un evento `createVolume` diera error. La causa del error fue una Clave de KMS deshabilitada.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "sa-east-1",
  "resources": [
    "arn:aws:ec2:sa-east-1:0123456789ab:volume/vol-01234567",
  ],
  "detail": {
    "event": "createVolume",
    "result": "failed",
    "cause": "arn:aws:kms:sa-
east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is disabled.",
    "request-id": "01234567-0123-0123-0123-0123456789ab",
  }
}
```

A continuación se ofrece un ejemplo de un objeto JSON emitido por EBS después de que un evento `createVolume` diera error. La causa del error fue una importación pendiente de una Clave de KMS.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
```

```
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "sa-east-1",
  "resources": [
    "arn:aws:ec2:sa-east-1:0123456789ab:volume/vol-01234567",
  ],
  "detail": {
    "event": "createVolume",
    "result": "failed",
    "cause": "arn:aws:kms:sa-
east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is pending import.",
    "request-id": "01234567-0123-0123-0123-0123456789ab",
  }
}
```

Eliminar volumen (deleteVolume)

El `deleteVolume` evento se envía a tu AWS cuenta cuando se completa una acción para eliminar un volumen. Sin embargo, no se guarda, registra o archiva. Este evento da como resultado `deleted`. Si la eliminación no se completa, el evento no se enviará nunca.

Datos de evento

La lista siguiente es un ejemplo de un objeto JSON emitido por EBS para un evento `deleteVolume` correcto.

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Volume Notification",
   "source": "aws.ec2",
   "account": "012345678901",
   "time": "yyyy-mm-ddThh:mm:ssZ",
   "region": "us-east-1",
   "resources": [
      "arn:aws:ec2:us-east-1:012345678901:volume/vol-01234567"
   ],
   "detail": {
      "result": "deleted",
      "cause": "",
      "event": "deleteVolume",
      "request-id": "01234567-0123-0123-0123-0123456789ab"
   }
```

```
}
```

Asociar o volver a asociar volumen (attachVolume, reattachVolume)

El evento `attachVolume` o `reattachVolume` se envía a la cuenta de AWS cuando no se logra asociar o volver a asociar un volumen a una instancia. Sin embargo, no se guarda, registra o archiva. Si utiliza una Clave de KMS para cifrar un volumen de EBS y la Clave de KMS deja de ser válida, EBS emitirá un evento si esa Clave de KMS se utiliza posteriormente para asociar o volver a asociar a una instancia, como se muestra en los ejemplos a continuación.

Datos de evento

La lista siguiente es un ejemplo de un objeto JSON emitido por EBS después de que un evento `attachVolume` diera error. La causa del error fue una eliminación pendiente de una Clave de KMS.

> **Note**
>
> AWS puede intentar volver a conectarse a un volumen tras un mantenimiento rutinario del servidor.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
  "arn:aws:ec2:us-east-1:0123456789ab:volume/vol-01234567",
  "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab"
  ],
  "detail": {
    "event": "attachVolume",
    "result": "failed",
    "cause": "arn:aws:kms:us-
east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is pending deletion.",
    "request-id": ""
  }
}
```

La lista siguiente es un ejemplo de un objeto JSON emitido por EBS después de que un evento `reattachVolume` diera error. La causa del error fue una eliminación pendiente de una Clave de KMS.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
  "arn:aws:ec2:us-east-1:0123456789ab:volume/vol-01234567",
  "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab"
  ],
  "detail": {
    "event": "reattachVolume",
    "result": "failed",
    "cause": "arn:aws:kms:us-
east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is pending deletion.",
    "request-id": ""
  }
}
```

Separar volumen (DetachVolume)

El `detachVolume` evento se envía a su AWS cuenta cuando se separa un volumen de una instancia de Amazon EC2.

Datos de evento

El siguiente es un ejemplo de un `detachVolume` evento exitoso.

```
{
  "version":"0",
  "id":"2ec37298-1234-e436-70fc-c96b1example",
  "detail-type":"AWS API Call via CloudTrail",
  "source":"aws.ec2",
  "account":"123456789012",
  "time":"2024-03-18T16:35:52Z",
  "region":"us-east-1",
  "resources":[],
```

```
  "detail":
  {
    "eventVersion":"1.09",
    "userIdentity":
    {
      "type":"IAMUser",
      "principalId":"AIDAJT12345SQ2EXAMPLE",
      "arn":"arn:aws:iam::123456789012:user/administrator",
      "accountId":"123456789012",
      "accessKeyId":"AKIAJ67890A6EXAMPLE",
      "userName":"administrator"
    },
    "eventTime":"2024-03-18T16:35:52Z",
    "eventSource":"ec2.amazonaws.com",
    "eventName":"DetachVolume",
    "awsRegion":"us-east-1",
    "sourceIPAddress":"12.12.123.12",
    "userAgent":"aws-cli/2.7.12 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
ec2.detach-volume",
    "requestParameters":
    {
      "volumeId":"vol-072577c46bexample",
      "force":false
    },
    "responseElements":
    {
      "requestId":"1234513a-6292-49ea-83f8-85e95example",
      "volumeId":"vol-072577c46bexample",
      "instanceId":"i-0217f7eb3dexample",
      "device":"/dev/sdb",
      "status":"detaching",
      "attachTime":1710776815000
    },
    "requestID":"1234513a-6292-49ea-83f8-85e95example",
    "eventID":"1234551d-a15a-43eb-9e69-c983aexample",
    "readOnly":false,
    "eventType":"AwsApiCall",
    "managementEvent":true,
    "recipientAccountId":"123456789012",
    "eventCategory":"Management",
    "tlsDetails":
    {
      "tlsVersion":"TLSv1.3",
      "cipherSuite":"TLS_AES_128_GCM_SHA256",
```

```
      "clientProvidedHostHeader":"ec2.us-east-1.amazonaws.com"
    }
  }
}
```

Eventos de modificación del volumen de EBS

Amazon EBS envía `modifyVolume` eventos EventBridge cuando se modifica un volumen. Sin embargo, no se guarda, registra o archiva.

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Volume Notification",
   "source": "aws.ec2",
   "account": "012345678901",
   "time": "yyyy-mm-ddThh:mm:ssZ",
   "region": "us-east-1",
   "resources": [
      "arn:aws:ec2:us-east-1:012345678901:volume/vol-03a55cf56513fa1b6"
   ],
   "detail": {
      "result": "optimizing",
      "cause": "",
      "event": "modifyVolume",
      "request-id": "01234567-0123-0123-0123-0123456789ab"
   }
}
```

Eventos de instantánea de EBS

Amazon EBS envía los eventos al EventBridge momento en que se producen los siguientes eventos de volumen.

Eventos

- Crear instantánea (createSnapshot)
- Crear instantáneas (createSnapshots)
- Copiar instantánea (copySnapshot)
- Compartir instantánea (shareSnaphot)

Crear instantánea (createSnapshot)

El `createSnapshot` evento se envía a su AWS cuenta cuando se completa una acción para crear una instantánea. Sin embargo, no se guarda, registra o archiva. Este evento tiene un resultado de `succeeded` o `failed`.

Datos de evento

La lista siguiente es un ejemplo de un objeto JSON emitido por EBS para un evento `createSnapshot` correcto. En la sección `detail`, el campo `source` contiene el ARN del volumen de origen. Los campos `startTime` y `endTime` indican el inicio y la finalización de la creación de la instantánea.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
     "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "createSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::us-west-2:volume/vol-01234567",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ"  }
}
```

Crear instantáneas (createSnapshots)

El `createSnapshots` evento se envía a su AWS cuenta cuando se completa una acción para crear una instantánea de varios volúmenes. Este evento tiene un resultado de `succeeded` o `failed`.

Datos de evento

La lista siguiente es un ejemplo de un objeto JSON emitido por EBS para un evento `createSnapshots` correcto. En la sección `detail`, el campo `source` contiene los ARN de los volúmenes de origen del conjunto de instantáneas de varios volúmenes. Los campos `startTime` y `endTime` indican el inicio y la finalización de la creación de la instantánea.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Multi-Volume Snapshots Completion Status",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
    "arn:aws:ec2::us-east-1:snapshot/snap-012345678"
  ],
  "detail": {
    "event": "createSnapshots",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "snapshots": [
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
        "source": "arn:aws:ec2::us-east-1:volume/vol-01234567",
        "status": "completed"
      },
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-012345678",
        "source": "arn:aws:ec2::us-east-1:volume/vol-012345678",
        "status": "completed"
      }
    ]
  }
}
```

La lista siguiente es un ejemplo de un objeto JSON emitido por EBS después de que un evento `createSnapshots` diera error. La causa del error fue que no se pudieron completar una o varias instantáneas para el conjunto de instantáneas de varios volúmenes. Los valores de `snapshot_id`

son los ARN de las instantáneas erróneas. `startTime` y `endTime` representan la hora de inicio y de fin de la acción create-snapshots.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Multi-Volume Snapshots Completion Status",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
    "arn:aws:ec2::us-east-1:snapshot/snap-012345678"
  ],
"detail": {
    "event": "createSnapshots",
    "result": "failed",
    "cause": "Snapshot snap-01234567 is in status error",
   "request-id": "",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "snapshots": [
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
        "source": "arn:aws:ec2::us-east-1:volume/vol-01234567",
        "status": "error"
      },
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-012345678",
        "source": "arn:aws:ec2::us-east-1:volume/vol-012345678",
        "status": "error"
      }
    ]
  }
}
```

Copiar instantánea (copySnapshot)

El `copySnapshot` evento se envía a su AWS cuenta cuando se completa una acción para copiar una instantánea. Sin embargo, no se guarda, registra o archiva. Este evento tiene un resultado de `succeeded` o `failed`.

Si está copiando la instantánea entre regiones, el evento se emite en la región de destino.

Datos de evento

La lista siguiente es un ejemplo de un objeto JSON emitido por EBS tras un evento `copySnapshot` correcto. El valor de `snapshot_id` es el ARN de la instantánea recién creada. En la sección `detail`, el valor de `source` es el ARN de la instantánea de origen. `startTime` y `endTime` representan cuándo comenzó y finalizó la acción copy-snapshot. `incremental` indica si la instantánea es una instantánea incremental (`true`) o una instantánea completa (`false`).

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "copySnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "incremental": "true"
  }
}
```

La lista siguiente es un ejemplo de un objeto JSON emitido por EBS después de que un evento `copySnapshot` diera error. La causa del error fue un ID de instantánea de origen no válido. El valor de `snapshot_id` es el ARN de la instantánea con errores. En la sección `detail`, el valor de `source` es el ARN de la instantánea de origen. `startTime` y `endTime` representan la hora de inicio y de fin de la acción copy-snapshot.

```
{
```

```
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "copySnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

Compartir instantánea (shareSnaphot)

El `shareSnapshot` evento se envía a tu AWS cuenta cuando otra cuenta comparte una instantánea con ella. Sin embargo, no se guarda, registra o archiva. El resultado siempre es `succeeded`.

Datos de evento

A continuación se muestra un ejemplo de un objeto JSON emitido por EBS tras la finalización de un evento `shareSnapshot`. En la `detail` sección, el valor de `source` es el número de AWS cuenta del usuario que compartió la instantánea contigo. `startTime`y `endTime` representan cuándo comenzó y finalizó la acción de compartir la instantánea. El evento `shareSnapshot` solo se activa cuando se comparte una instantánea privada con otro usuario. Si se comparte una instantánea pública, no se desencadena el evento.

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
```

```
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "shareSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": 012345678901,
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

Eventos del archivo de instantáneas de EBS

Amazon EBS emite eventos relacionados con acciones de archivo de instantáneas. Para obtener más información, consulte Monitorear el archivo de instantáneas.

Eventos de restauración rápida de instantáneas de EBS

Amazon EBS envía los eventos EventBridge cuando cambia el estado de restauración rápida de una instantánea. Los eventos se emiten en la medida de lo posible.

El siguiente es un ejemplo de los datos de este evento.

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Fast Snapshot Restore State-change Notification",
   "source": "aws.ec2",
   "account": "123456789012",
   "time": "yyyy-mm-ddThh:mm:ssZ",
   "region": "us-east-1",
   "resources": [
      "arn:aws:ec2:us-east-1::snapshot/snap-03a55cf56513fa1b6"
   ],
   "detail": {
      "snapshot-id": "snap-1234567890abcdef0",
```

```
      "state": "optimizing",
      "zone": "us-east-1a",
      "message": "Client.UserInitiated - Lifecycle state transition",
   }
}
```

Los valores posibles de `state` son `enabling`, `optimizing`, `enabled`, `disabling` y `disabled`.

Los valores posibles para `message` son los siguientes:

`Client.InvalidSnapshot.InvalidState - The requested snapshot transitioned to an invalid state (Error)`

Falló una solicitud para habilitar la restauración rápida de instantáneas y el estado pasó a `disabling` o `disabled`. La restauración rápida de instantáneas no se puede habilitar para esta instantánea.

`Client.UserInitiated`

El estado cambió satisfactoriamente a `enabling` o `disabling`.

`Client.UserInitiated - Lifecycle state transition`

El estado cambió satisfactoriamente a `optimizing`, `enabled` o `disabled`.

`Server.InsufficientCapacity - There was insufficient capacity available to satisfy the request`

Falló una solicitud para habilitar la restauración rápida de instantáneas por capacidad insuficiente y el estado pasó a`disabling` o `disabled`. Espere e inténtelo de nuevo.

`Server.InternalError - An internal error caused the operation to fail`

Falló una solicitud para habilitar la restauración rápida de instantáneas por un error interno y el estado pasó a`disabling` o `disabled`. Espere e inténtelo de nuevo.

`Client.InvalidSnapshot.InvalidState - The requested snapshot was deleted or access permissions were revoked`

El estado de restauración rápida de la instantánea ha pasado a `disabling` o `disabled` porque el propietario de la instantánea eliminó o dejó de compartir la instantánea. La restauración rápida de instantáneas no se puede habilitar para una instantánea que se ha eliminado o que ya no se comparte con usted.

Se utiliza AWS Lambda para gestionar eventos EventBridge

Puede utilizar Amazon EBS y Amazon EventBridge para automatizar el flujo de trabajo de copia de seguridad de datos. Esto requiere que cree una política de IAM, una AWS Lambda función para gestionar el evento y una EventBridge regla que haga coincidir los eventos entrantes y los dirija a la función Lambda.

En el procedimiento siguiente se usa el evento `createSnapshot` para copiar automáticamente una instantánea completada en otra región para la recuperación de desastres.

Para copiar una instantánea completada en otra región

1. Cree una política de IAM, como la que se muestra en el siguiente ejemplo, para proporcionar permisos para usar la `CopySnapshot` acción y escribir en el registro. EventBridge Asigne la política al usuario que gestionará el EventBridge evento.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CopySnapshot"
      ],
      "Resource": "*"
    }
  ]
}
```

2. Defina una función en Lambda que estará disponible en la EventBridge consola. El ejemplo de función Lambda que aparece a continuación, escrito en Node.js, se invoca EventBridge cuando Amazon EBS emite un `createSnapshot` evento coincidente (lo que indica que se

ha completado una instantánea). Cuando se le llama, la función copia la instantánea de `us-east-2` en `us-east-1`.

```
// Sample Lambda function to copy an EBS snapshot to a different Region

var AWS = require('aws-sdk');
var ec2 = new AWS.EC2();

// define variables
var destinationRegion = 'us-east-1';
var sourceRegion = 'us-east-2';
console.log ('Loading function');

//main function
exports.handler = (event, context, callback) => {

    // Get the EBS snapshot ID from the event details
    var snapshotArn = event.detail.snapshot_id.split('/');
    const snapshotId = snapshotArn[1];
    const description = `Snapshot copy from ${snapshotId} in ${sourceRegion}.`;
    console.log ("snapshotId:", snapshotId);

    // Load EC2 class and update the configuration to use destination Region to
 initiate the snapshot.
    AWS.config.update({region: destinationRegion});
    var ec2 = new AWS.EC2();

    // Prepare variables for ec2.modifySnapshotAttribute call
    const copySnapshotParams = {
        Description: description,
        DestinationRegion: destinationRegion,
        SourceRegion: sourceRegion,
        SourceSnapshotId: snapshotId
    };

    // Execute the copy snapshot and log any errors
    ec2.copySnapshot(copySnapshotParams, (err, data) => {
        if (err) {
            const errorMessage = `Error copying snapshot ${snapshotId} to Region
 ${destinationRegion}.`;
            console.log(errorMessage);
            console.log(err);
            callback(errorMessage);
```

```
        } else {
            const successMessage = `Successfully started copy of snapshot
 ${snapshotId} to Region ${destinationRegion}.`;
            console.log(successMessage);
            console.log(data);
            callback(null, successMessage);
        }
    });
};
```

Para asegurarse de que la función Lambda esté disponible en la EventBridge consola, créela en la región en la que se producirá el EventBridge evento. Para obtener más información, consulte la Guía para desarrolladores de AWS Lambda.

3. Abre la EventBridge consola de Amazon en https://console.aws.amazon.com/events/.
4. En el panel de navegación, elija Rules (Reglas) y, a continuación, elija Create rule (Crear regla).
5. En Step 1: Define rule detail (Paso 1: definición de detalles de reglas), haga lo siguiente:
   a. Introduzca valores para Name (Nombre) y Description (Descripción).
   b. En Event bus (Bus de eventos), mantenga la opción de default (Valor predeterminado).
   c. Asegúrese de que la opción Enable the rule on the selected event bus (Habilitar la regla en el bus de eventos seleccionado) esté activada.
   d. En Event type (Tipo de evento), seleccione Rule with an event pattern (Regla con un patrón de evento).
   e. Elija Siguiente.
6. En Step 2: Build event pattern (Paso 2: crear patrón de eventos), haga lo siguiente:
   a. En Fuente del evento, selecciona AWS eventos o eventos EventBridge asociados.
   b. En la sección Patrón de eventos, en Origen del evento, asegúrese de que la opción Servicio de AWS esté seleccionada y, en Servicio de AWS , seleccione EC2.
   c. En Event type, seleccione EBS Snapshot Notification (Notificación de instantáneas de EBS), seleccione Specific event(s) (Eventos específicos) y, a continuación, elija createSnapshot.
   d. Seleccione Specific result(s) (Resultados específicos) y luego elija succeeded.
   e. Elija Siguiente.
7. En Step 3: Select targets (Paso 3: seleccionar destinos), haga lo siguiente:
   a. En Tipos de destino, seleccione Servicio de AWS .

b. En Select target (Seleccionar destino), elija Lambda function (Función Lambda) y, en Function (Función), seleccione la función creada anteriormente.

c. Elija Next (Siguiente).

8. En Step 4: Configure tags (Paso 4: configurar etiquetas), especifique las etiquetas para la regla si es necesario y, a continuación, seleccione Next.
9. En Step 5: Review and create (Paso 5: revisar y crear), revise la regla y, a continuación, elija Create rule.

La regla debería aparecer ahora en la pestaña Rules (Reglas). En el ejemplo mostrado, el evento que ha configurado debería activarlo EBS la próxima vez que copie una instantánea.

Amazon GuardDuty para Amazon EBS

Amazon GuardDuty es un servicio de detección de amenazas que ayuda a proteger sus cuentas, contenedores, cargas de trabajo y los datos de su AWS entorno. Mediante modelos de aprendizaje automático (ML) y funciones de detección de anomalías y amenazas, monitorea GuardDuty continuamente las diferentes fuentes de registro y la actividad en tiempo de ejecución para identificar y priorizar los posibles riesgos de seguridad y las actividades maliciosas en su entorno.

La función Malware Protection incluida GuardDuty analiza los volúmenes de Amazon EBS asociados a sus instancias de Amazon EC2 y cargas de trabajo de contenedores para detectar posibles amenazas. GuardDuty ofrece dos formas de hacerlo:

- Habilitar la protección contra malware: cuando se GuardDuty genera un hallazgo que indica la posible presencia de malware en una instancia de Amazon EC2 o en la carga de trabajo de un contenedor, se iniciará automáticamente un análisis de malware en el recurso potencialmente comprometido.
- Utilice el análisis de malware bajo demanda sin activar la protección contra malware: proporcione el nombre del recurso de Amazon (ARN) de su instancia de Amazon EC2 para iniciar un análisis bajo demanda.

Para obtener más información, consulta la Guía del GuardDuty usuario de Amazon.

Cuotas para Amazon EBS

Su Cuenta de AWS tiene cuotas predeterminadas —anteriormente conocidas como “límites”— para cada servicio de Servicio de AWS. A menos que se indique lo contrario, cada cuota es específica de la región de . Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar.

Para ver las cuotas de Amazon EBS, abra la Consola de Service Quotas. En el panel de navegación, elija Servicios de AWS y seleccione Amazon Elastic Block Store (Amazon EBS). Para solicitar un aumento de cuota, consulte Solicitud de aumento de cuota en la Guía del usuario de Service Quotas.

Su Cuenta de AWS incluye las siguientes cuotas relacionadas con Amazon EBS.

Nombre	Valor predeterminado	Ajusta	Descripción
Instantáneas archivadas por volumen	Cada región admitida: 25	Sí	Número máximo de instantáneas archivadas por volumen.
Solicitudes de CompletesNapshot por cuenta	Cada región admitida: 10 por segundo	No	Número máximo de solicitudes de Completes Snapshot permitidas por cuenta.
Copias de instantáneas simultáneas por región de destino	Cada región admitida: 20	No	Número máximo de copias de instantáneas simultáneas en una única región de destino.
Instantáneas simultáneas por volumen de HDD en frío (sc1)	Cada región admitida: 1	No	Número máximo de instantáneas simultáneas por volumen de HDD en frío (sc1) en esta región.
Instantáneas simultáneas por volumen de SSD de uso general (gp2)	Cada región admitida: 5	No	Número máximo de instantáneas simultáneas por volumen de SSD de

Nombre	Valor predeterminado	Ajusta	Descripción
			uso general (gp2) en esta región.
Instantáneas simultáneas por volumen de SSD de uso general (gp3)	Cada región admitida: 5	No	Número máximo de instantáneas simultáneas por volumen de SSD de uso general (gp3) en esta región.
Instantáneas simultáneas por volumen magnético (estándar)	Cada región admitida: 5	No	Número máximo de instantáneas simultáneas por volumen magnético (estándar) en esta región.
Instantáneas simultáneas por volumen de SSD de IOPS aprovisionadas (io1)	Cada región admitida: 5	No	Número máximo de instantáneas simultáneas por volumen de SSD de IOPS aprovisionadas (io1) en esta región.
Instantáneas simultáneas por volumen de SSD de IOPS aprovisionadas (io2)	Cada región admitida: 5	No	Número máximo de instantáneas simultáneas por volumen de SSD de IOPS aprovisionadas (io2) en esta región.
Instantáneas simultáneas por volumen de HDD con rendimiento optimizado (st1)	Cada región admitida: 1	No	Número máximo de instantáneas simultáneas por volumen de HDD con rendimiento optimizado (st1) en esta región.

Nombre	Valor predeterminado	Ajusta	Descripción
Restauración rápida de instantáneas	us-east-1: 5 us-east-2: 5 us-west-1: 5 us-west-2: 5 af-south-1: 5 ap-east-1: 5 ap-northeast-1: 5 ap-northeast-2: 5 ap-northeast-3: 5 ap-south-1: 5 ap-southeast-1: 5 ap-southeast-2: 5 ap-southeast-3: 5 ca-central-1: 5 eu-central-1: 5 eu-north-1: 5 eu-south-1: 5 eu-west-1: 5 eu-west-2: 5 eu-west-3: 5	Sí	El número máximo de instantáneas que puede activarse para la restauración rápida de instantáneas en esta región.

Nombre	Valor predeterminado	Ajusta	Descripción
	me-south-1: 5 sa-east-1: 5 Cada una de las regiones admitidas: 5		
Solicitudes de GetSnapshotBlock por cuenta	Cada región admitida: 1000 por segundo	Sí	Número máximo de solicitudes de GetSnapshotBlock permitidas por cuenta.
Solicitudes de GetSnapshotBlock por instantánea	Cada región admitida: 1000 por segundo	No	Número máximo de solicitudes de GetSnapshotBlock permitidas por instantánea.
IOPS para volúmenes de SSD de IOPS aprovisionadas (io1)	Cada región admitida: 300 000	Sí	Número máximo agregado de IOPS que se puede aprovisionar en los volúmenes SSD (io1) de IOPS aprovisionadas en esta región.
IOPS para volúmenes de SSD de IOPS aprovisionadas (io2)	Cada región admitida: 100 000	Sí	Número máximo agregado de IOPS que se puede aprovisionar en los volúmenes SSD (io2) de IOPS aprovisionadas en esta región.

Nombre	Valor predeterminado	Ajusta	Descripción
Modificaciones de IOPS para volúmenes de SSD de IOPS aprovisionadas (io1)	Cada región admitida: 500 000	Sí	Número máximo agregado de IOPS que se puede solicitar en modificaciones de volúmenes SSD (io1) de IOPS aprovisionadas en esta región.
Modificaciones de IOPS para volúmenes de SSD de IOPS aprovisionadas (io2)	Cada región admitida: 100 000	Sí	IOPS máximas actuales (desde) y solicitadas (hasta) para las solicitudes de modificación de volumen en los volúmenes de SSD (io2) de IOPS aprovisionadas de esta región.
Archivos de instantáneas en curso por cuenta	Cada región admitida: 25	Sí	Número máximo de archivos de instantáneas simultáneas en curso por cuenta.
Restauraciones de instantáneas en curso del archivo por cuenta	Cada región admitida: 5	Sí	El Número máximo de archivos de instantáneas simultáneas se restaura del archivo por cuenta.
Solicitudes de ListChangedBlocks por cuenta	Cada región admitida: 50 por segundo	No	Número máximo de solicitudes de ListChangedBlocks permitidas por cuenta.

Nombre	Valor predeterminado	Ajusta	Descripción
Solicitudes de ListSnapshotBlocks por cuenta	Cada región admitida: 50 por segundo	No	Número máximo de solicitudes de ListSnapshotBlocks permitidas por cuenta.
Instantáneas pendientes por cuenta	Cada región admitida: 100	No	Número máximo de instantáneas pendientes por cuenta.
Solicitudes de PutSnapshotBlock por cuenta	Cada región admitida: 1000 por segundo	Sí	Número máximo de solicitudes de PutSnapshotBlock permitidas por cuenta.
Solicitudes de PutSnapshotBlock por instantánea	Cada región admitida: 1000 por segundo	No	Número máximo de solicitudes de PutSnapshotBlock permitidas por instantánea.
Instantáneas por región	Cada región admitida: 100 000	Sí	Número máximo de instantáneas por región
Solicitudes de StartSnapshot por cuenta	Cada región admitida: 10 por segundo	No	Número máximo de solicitudes de StartSnapshot permitidas por cuenta.

Nombre	Valor predeterminado	Ajusta	Descripción
Almacenamiento de volúmenes de HDD en frío (sc1) en TiB	af-south-1: 300 ap-east-1: 300 eu-south-1: 300 me-south-1: 300 Cada una de las demás regiones admitidas: 50	Sí	Cantidad máxima agregada de almacenamiento, en TiB, que se puede aprovisionar en volúmenes de HDD en frío (sc1) aprovisionados en esta región.
Almacenamiento de volúmenes de SSD de uso general (gp2), en TiB	af-south-1: 300 ap-east-1: 300 eu-south-1: 300 me-south-1: 300 Cada una de las demás regiones admitidas: 50	Sí	Cantidad máxima agregada de almacenamiento, en TiB, que se puede aprovisionar en los volúmenes de SSD de uso general (gp2) en esta región.
Almacenamiento de volúmenes de SSD de uso general (gp3), en TiB	af-south-1: 300 ap-east-1: 300 eu-south-1: 300 me-south-1: 300 Cada una de las demás regiones admitidas: 50	Sí	Cantidad máxima agregada de almacenamiento, en TiB, que se puede aprovisionar en los volúmenes de SSD de uso general (gp3) en esta región.

Nombre	Valor predeterminado	Ajusta	Descripción
Almacenamiento para volúmenes magnéticos (estándar), en TiB	af-south-1: 300 ap-east-1: 300 eu-south-1: 300 me-south-1: 300 Cada una de las demás regiones admitidas: 50	Sí	Cantidad máxima agregada de almacenamiento, en TiB, que se puede aprovisionar en volúmenes magnéticos (estándar) aprovisionados en esta región.
Almacenamiento de volúmenes de SSD de IOPS aprovisionadas (io1), en TiB	af-south-1: 300 ap-east-1: 300 eu-south-1: 300 me-south-1: 300 Cada una de las demás regiones admitidas: 50	Sí	Cantidad máxima agregada de almacenamiento, en TiB, que se puede aprovisionar en los volúmenes SSD (io1) de IOPS aprovisionadas en esta región.
Almacenamiento de volúmenes de SSD de IOPS aprovisionadas (io2), en TiB	Cada región admitida: 20	Sí	Cantidad máxima agregada de almacenamiento, en TiB, que se puede aprovisionar en los volúmenes SSD (io2) de IOPS aprovisionadas en esta región.

Nombre	Valor predeterminado	Ajusta	Descripción
Almacenamiento de volúmenes de HDD con rendimiento optimizado (st1), en TiB	af-south-1: 300 ap-east-1: 300 eu-south-1: 300 me-south-1: 300 Cada una de las demás regiones admitidas: 50	Sí	Cantidad máxima agregada de almacenamiento, en TiB, que se puede aprovisionar en volúmenes de HDD con rendimiento optimizado (st1) aprovisionados en esta región.
Modificaciones de almacenamiento para volúmenes de HDD en frío (sc1), en TiB	Cada región admitida: 500	Sí	Cantidad máxima agregada de almacenamiento, en TiB, que se puede solicitar en modificaciones de volúmenes de HDD en frío (sc1) en esta región.
Modificaciones de almacenamiento de volúmenes de SSD de uso general (gp2), en TiB	Cada región admitida: 500	Sí	Cantidad máxima agregada de almacenamiento, en TiB, que se puede solicitar en modificaciones de volúmenes de SSD de uso general (gp2) en esta región.

Nombre	Valor predeterminado	Ajusta	Descripción
Modificaciones de almacenamiento de volúmenes de SSD de uso general (gp3), en TiB	Cada región admitida: 500	Sí	Cantidad máxima agregada de almacenamiento, en TiB, que se puede solicitar en modificaciones de volúmenes de SSD de uso general (gp3) en esta región.
Modificaciones de almacenamiento para volúmenes magnéticos (estándar), en TiB	Cada región admitida: 500	Sí	Cantidad máxima agregada de almacenamiento, en TiB, que se puede solicitar en modificaciones de volúmenes de volúmenes magnéticos (estándar) en esta región.
Modificaciones de almacenamiento de volúmenes de SSD de IOPS aprovisionadas (io1), en TiB	Cada región admitida: 500	Sí	Cantidad máxima agregada de almacenamiento, en TiB, que se puede solicitar en modificaciones de volúmenes SSD (io1) de IOPS aprovisionadas en esta región.

Nombre	Valor predeterminado	Ajusta	Descripción
Modificaciones de almacenamiento de volúmenes de SSD de IOPS aprovisionadas (io2), en TiB	Cada región admitida: 20	Sí	Cantidad máxima agregada de almacenamiento, en TiB, que se puede solicitar en modificaciones de volúmenes SSD (io2) de IOPS aprovisionadas en esta región.
Modificaciones de almacenamiento de volúmenes de HDD con rendimiento optimizado (st1), en TiB	Cada región admitida: 500	Sí	Cantidad máxima agregada de almacenamiento, en TiB, que se puede solicitar en modificaciones de volúmenes de HDD con rendimiento optimizado para el procesamiento (st1) en esta región.

Consideraciones

- Sus cuotas pueden cambiar con el tiempo. Amazon EBS supervisa constantemente el almacenamiento aprovisionado y el uso de IOPS en cada región y podría aumentar automáticamente las cuotas, por región, en función de su uso. Aunque Amazon EBS aumenta automáticamente las cuotas en función del uso, puede solicitar un aumento de la cuota si es necesario. Por ejemplo, si tiene intención de utilizar más almacenamiento de gp3 en el este de EE. UU. (Norte de Virginia) del que permite su cuota actual, puede solicitar un aumento de la cuota para ese tipo de volumen en esa región antes del uso planeado.
- La cuota de instantáneas simultáneas por región de destino no se puede ajustar mediante Service Quotas. Sin embargo, puede solicitar un aumento de esta cuota poniéndose en contacto con AWS Support.
- Las cuotas de modificaciones de IOPS y de almacenamiento se aplican al valor actual agregado (por tamaño o IOPS, según la cuota) de los volúmenes que pueden modificarse simultáneamente.

Puede realizar solicitudes de modificación simultáneas para los volúmenes que tengan un valor actual combinado (por tamaño o IOPS) hasta alcanzar la cuota. Por ejemplo, si su cuota de modificaciones de IOPS para los volúmenes de SSD (io1) de IOPS aprovisionadas es igual o inferior a `50,000`, puede realizar solicitudes de modificación de IOPS simultáneas para cualquier número de volúmenes de `io1`, siempre que sus IOPS actuales combinadas sean iguales o inferiores a `50,000`. Si tiene tres volúmenes de `io1` aprovisionados con `20,000` IOPS cada uno, puede solicitar modificaciones de IOPS para dos volúmenes simultáneamente (`20,000 * 2 < 50,000`). Si envía una solicitud de modificación de IOPS simultánea para el tercer volumen, sobrepasa su cuota y esa solicitud no es válida (`20,000 * 3 > 50,000`).

Historial de documentos para la guía del usuario de Amazon EBS

En la siguiente tabla se describen las versiones de la documentación de Amazon EBS.

Cambio	Descripción	Fecha
Habilite las políticas predeterminadas de Amazon Data Lifecycle Manager en todas las cuentas	Puede utilizarlas AWS CloudFormation StackSets para habilitar las políticas predeterminadas de Amazon Data Lifecycle Manager en una AWS organización o en AWS cuentas específicas.	26 de abril de 2024
AWSDataLifecycleManagerSSMFullAccess AWS política gestionada	Se actualizó la política para admitir instantáneas coherentes con las aplicaciones para SAP HANA mediante el documento de SSM `AWSSystemsManagerSAP-CreateDLMSnapshotForSAPHANA` .	17 de noviembre de 2023
VolumeStalledmétrica ioCheck	Puede utilizar la métrica `VolumeStalledIOCheck` para comprobar si un volumen ha superado o no una comprobación de E/S estancada en el último minuto.	16 de noviembre de 2023
Políticas predeterminadas de Amazon Data Lifecycle Manager	Ahora puede crear políticas predeterminadas de Amazon Data Lifecycle Manager para instantáneas de EBS y las AMI respaldadas por EBS a fin de	16 de noviembre de 2023

	realizar copias de seguridad de todos los volúmenes e instancias de una región.	
Bloqueo de instantáneas de Amazon EBS	Puede bloquear las instantáneas de Amazon EBS para protegerlas contra eliminaciones accidentales o malintencionadas o almacenarlas en formato WORM durante un periodo específico.	15 de noviembre de 2023
Bloqueo del acceso público de instantáneas	Ahora puede usar el bloqueo del acceso público de las instantáneas para impedir que se compartan públicamente.	9 de noviembre de 2023
Scripts previos y posteriores de Amazon Data Lifecycle Manager	Ahora puede usar scripts previos y posteriores en sus políticas de instantáneas de Amazon Data Lifecycle Manager para automatizar el ciclo de vida de las instantáneas coherentes con las aplicaciones.	7 de noviembre de 2023
Reservas de NVMe	Los volúmenes `io2` habilitados para Multi-Attach admiten reservas de NVMe, que son un conjunto de protocolos de protección de almacenamiento estándar del sector.	18 de septiembre de 2023

Pruebas de fallos en Amazon EBS	AWS FIS Utilícela para detener temporalmente la E/S entre un volumen de EBS y las instancias a las que está conectado para comprobar cómo gestionan sus cargas de trabajo las interrupciones de E/S.	27 de enero de 2023
Volúmenes `io2` Block Express	Puede modificar el tamaño y las IOPS aprovisionadas de los volúmenes `io2` Block Express y puede habilitarlos para restaurar instantáneas de manera rápida.	31 de mayo de 2022
Papelera de reciclaje para instantáneas de Amazon EBS	La papelera de reciclaje para instantáneas de Amazon EBS es una característica de recuperación de instantáneas que le permite restaurar instantáneas eliminadas accidentalmente.	29 de noviembre de 2021
Archivo de instantáneas de Amazon EBS	El archivo de instantáneas de Amazon EBS es un nuevo nivel de almacenamiento que se puede utilizar para el almacenamiento de bajo costo y a largo plazo de las instantáneas de acceso poco frecuente.	29 de noviembre de 2021

CloudWatch métricas de Amazon Data Lifecycle Manager	Puede supervisar sus políticas de Amazon Data Lifecycle Manager mediante Amazon CloudWatch.	28 de julio de 2021
CloudTrail eventos de datos para las API directas de EBS	En las PutSnapshotBlock API ListSnapshotBlocks ListChangedBlocks GetSnapshotBlock,, y se pueden registrar eventos de datos. CloudTrail	27 de julio de 2021
Volúmenes `io2` Block Express	Ahora, los volúmenes `io2` Block Express están, en general, disponibles.	19 de julio de 2021
Instantáneas locales de Amazon EBS en Outposts	Ahora puede utilizar Instantáneas locales de Amazon EBS en Outposts para almacenar instantáneas de volúmenes en un Outpost localmente en Amazon S3 en el propio Outpost.	4 de febrero de 2021
Compatibilidad con Multi-Attach para volúmenes io2	Ahora puede habilitar volúmenes SSD de IOPS provisionadas (`io2`) para Amazon EBS Multi-Attach.	18 de diciembre de 2020
Administrador de vida útil de datos de Amazon	Utilice Amazon Data Lifecycle Manager para automatizar el proceso de compartir instantáneas y copiarlas en todas AWS las cuentas.	17 de diciembre de 2020

Volúmenes gp3	Un nuevo tipo de volumen SSD de uso general de Amazon EBS. Puede especificar las IOPS provisionadas y el rendimiento al crear o modificar el volumen.	1 de diciembre de 2020
Tamaño de los volúmenes de HDD con rendimiento optimizado y de HDD en frío	Los volúmenes de HDD de rendimiento optimizado (`st1`) y de HDD en frío (`sc1`) pueden variar en tamaño de 125 GiB a 16 TiB.	30 de noviembre de 2020
Administrador de vida útil de datos de Amazon	Puede utilizar Amazon Data Lifecycle Manager para automatizar la creación, retención y eliminación de AMI respaldadas por EBS.	9 de noviembre de 2020
Administrador de vida útil de datos de Amazon	Las políticas de Amazon Data Lifecycle Manager se pueden configurar con hasta cuatro programaciones.	17 de septiembre de 2020
Volúmenes (io2) SSD de IOPS provisionadas para Amazon EBS	Los volúmenes SSD de IOPS provisionadas (`io2`) están diseñados para proporcionar una durabilidad del volumen del 99,999 por ciento con una AFR no superior al 0,001 por ciento.	24 de agosto de 2020
Restauración rápida de instantáneas	Puede habilitar la restauración rápida de instantáneas para las instantáneas que se compartan con usted.	21 de julio de 2020

Amazon EBS Multi-Attach	Ahora puede asociar un único volumen SSD de IOPS provisionadas (io1) a un máximo de 16 instancias basadas en Nitro que se encuentren en la misma zona de disponibilidad.	14 de febrero de 2020
Restauración rápida de instantáneas de Amazon EBS	Puede habilitar las restauraciones rápidas de instantáneas en una instantánea de EBS para garantizar que los volúmenes de EBS creados desde la instantánea se inicialicen por completo durante la creación y proporcionen al instante todo su rendimiento aprovisionado.	20 de noviembre de 2019
Instantáneas de varios volúmenes de Amazon EBS	Puede realizar instantáneas exactas point-in-time, coordinadas con los datos y coherentes con los fallos de varios volúmenes de EBS conectados a una instancia EC2.	29 de mayo de 2019
Cifrado de Amazon EBS de manera predeterminada	Después de habilitar el cifrado de forma predeterminada en una región, todos los volúmenes de EBS nuevos que cree en la región se cifrarán al utilizar la Clave de KMS predeterminada para el cifrado de EBS.	23 de mayo de 2019

Automatización del ciclo de vida de instantáneas	Puede usar Amazon Data Lifecycle Manager para automatizar la creación y eliminación de instantáneas de los volúmenes de EBS.	12 de julio de 2018
Modificaciones en volúmenes de EBS asociados	Con la mayoría de los volúmenes de EBS adjuntos a la mayoría de las instancias de EC2, puede modificar el tamaño, el tipo y el IOPS del volumen sin separarlo ni detener la instancia.	13 de febrero de 2017
Copie instantáneas cifradas de Amazon EBS entre Cuentas de AWS	Ahora puede copiar instantáneas cifradas de EBS entre Cuentas de AWS.	21 de junio de 2016
Tipos de volúmenes de HDD de rendimiento optimizado y de HDD en frío	Ahora puede crear volúmenes de HDD de rendimiento optimizado (st1) y HDD en frío (sc1).	19 de abril de 2016
Tipo de volumen SSD de uso general	Los volúmenes SSD de uso general ofrecen almacenamiento económico que resulta ideal para una gran variedad de cargas de trabajo. Estos volúmenes ofrecen latencias en milisegundos de un solo dígito, la posibilidad de ampliar a 3000 IOPS durante periodos prolongados y un rendimiento de referencia de 3 IOPS/GiB. El tamaño de un volumen SSD de uso general puede variar de 1 GiB a 1 TiB.	16 de junio de 2014

Cifrado de Amazon EBS	Cifrado de Amazon EBS ofrece un cifrado perfecto de volúmenes de datos de EBS e instantáneas, lo que elimina la necesidad de crear y mantener una infraestructura de administración de claves segura. El cifrado de EBS permite la seguridad de los datos en reposo mediante el cifrado de los datos con Claves administradas por AWS. El cifrado se produce en los servidores que alojan las instancias de EC2, por lo que los datos se cifran a medida que circulan entre las instancia s de EC2 y el almacenamiento de EBS.	21 de mayo de 2014
Copias de instantáneas incrementales	Ahora puede realizar copias de instantáneas increment ales.	11 de junio de 2013
Copia de instantáneas de EBS	Puede utilizar copias de instantáneas para crear copias de seguridad de los datos, para crear nuevos volúmenes de Amazon EBS o para crear imágenes de máquina de Amazon (AMI).	17 de diciembre de 2012

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.