aws

Guía del usuario de Lustre

# FSx para Lustre

# FSx para Lustre: Guía del usuario de Lustre

# Table of Contents

# ¿Qué es Amazon FSx para Lustre?

FSx para Lustre hace que sea fácil y rentable lanzar y ejecutar el popular sistema de archivos Lustre de alto rendimiento. Utiliza Lustre para cargas de trabajo en las que la velocidad es importante, como el machine learning, la computación de alto rendimiento (HPC), el procesamiento de vídeo y el modelado financiero.

El sistema de archivos Lustre de código abierto está diseñado para aplicaciones que requieren un almacenamiento rápido, en las que desea que el almacenamiento esté a la altura del procesamiento. Lustre se creó para resolver el problema de procesar de forma rápida y económica los crecientes conjuntos de datos del mundo. Es un sistema de archivos muy utilizado diseñado para los ordenadores más rápidos del mundo. Proporciona latencias inferiores a un milisegundo, hasta cientos de GBps de rendimiento y hasta millones de IOPS. Para obtener más información, consulte el sitio web de Lustre.

Como servicio totalmente gestionado, Amazon FSx facilita el uso de Lustre para cargas de trabajo en las que la velocidad de almacenamiento es importante. FSx para Lustre elimina la complejidad tradicional de configurar y administrar los sistemas de archivos Lustre, lo que le permite poner en marcha y ejecutar un sistema de archivos de alto rendimiento probado en cuestión de minutos. También ofrece múltiples opciones de implementación para que pueda optimizar los costes en función de las necesidades.

FSx para Lustre es compatible con POSIX, por lo que puede utilizar las aplicaciones actuales basadas en Linux sin tener que realizar ningún cambio. FSx para Lustre proporciona una interfaz de sistema de archivos nativa y funciona como cualquier sistema de archivos con el sistema operativo Linux. También proporciona read-after-write coherencia y admite el bloqueo de archivos.

Temas

- Precios de Amazon FSx para Lustre
- Amazon FSx para Lustre
- ¿Es la primera vez que usa Amazon FSx para Lustre?

## Múltiples opciones de implementación

Amazon FSx para Lustre ofrece una selección de sistemas de archivos temporales y persistentes para adaptarse a las diferentes necesidades de procesamiento de datos. Los sistemas de archivos temporales son ideales para el almacenamiento temporal y el procesamiento de datos de corto plazo. Los datos no se replican y no persisten si un servidor de archivos falla. Los sistemas de archivos persistentes son ideales para el almacenamiento de largo plazo y las cargas de trabajo centradas en el rendimiento. En los sistemas de archivos persistentes, los datos se replican y los servidores de archivos se sustituyen si fallan. Para obtener más información, consulte Opciones de implementación para sistemas de archivos de FSx para Lustre.

## Múltiples opciones de almacenamiento

Amazon FSx para Lustre ofrece una selección de tipos de almacenamiento en unidades de estado sólido (SSD) y unidades de disco duro (HDD) optimizados para diferentes requisitos de procesamiento de datos:

- Opciones de almacenamiento en SSD: para cargas de trabajo de baja latencia e intensivas en IOPS que suelen tener operaciones de archivos pequeñas y aleatorias, elija una de las opciones de almacenamiento en SSD.
- Opciones de almacenamiento en disco duro: para cargas de trabajo con un rendimiento intensivo que suelen tener operaciones de archivos secuenciales de gran tamaño, elija una de las opciones de almacenamiento en disco duro.

Si aprovisiona un sistema de archivos con la opción de almacenamiento en disco duro, también puede aprovisionar una caché SSD de solo lectura con un tamaño del 20 por ciento de la capacidad de almacenamiento de su disco duro. Esto proporciona latencias inferiores a un milisegundo e IOPS más altas para los archivos a los que se accede con frecuencia. Tanto los sistemas de archivos basados en SSD como los basados en HDD se aprovisionan con servidores de metadatos basados en SSD. Como resultado, todas las operaciones de metadatos, que representan la mayoría de las operaciones del sistema de archivos, se entregan con latencias inferiores a un milisegundo.

Para obtener más información sobre el rendimiento de estas opciones de almacenamiento, consulte Rendimiento de Amazon FSx para Lustre.

# FSx para Lustre y repositorios de datos

Puede vincular los sistemas de archivos de FSx para Lustre a los repositorios de datos de Amazon S3 o en las instalaciones de datos locales.

## Integración con el repositorio de datos FSx para Lustre S3

FSx para Lustre se integra con Amazon S3, lo que le facilita el procesamiento de conjuntos de datos en la nube mediante el sistema de archivos de alto rendimiento Lustre. Cuando se encuentra vinculado a un bucket de Amazon S3, un sistema de archivos de FSx para Lustre presenta de forma transparente los objetos de S3 como archivos. Amazon FSx importa listados de todos los archivos existentes en el bucket de S3 al crear el sistema de archivos. Amazon FSx también puede importar listados de archivos añadidos al repositorio de datos una vez creado el sistema de archivos. Puede configurar las preferencias de importación para que se ajusten a las necesidades de su flujo de trabajo. El sistema de archivos también le permite volver a escribir los datos del sistema de archivos en S3. Las tareas de repositorio de datos simplifican la transferencia de datos y metadatos entre el sistema de archivos de FSx para Lustre y su repositorio de datos duradero en Amazon S3. Para obtener más información, consulte Uso de repositorios de datos con Amazon FSx para Lustre y Tareas de repositorio de datos.

## FSx para Lustre y repositorios datos en las instalaciones locales

Con Amazon FSx para Lustre, puede dividir sus cargas de trabajo de procesamiento de datos en las instalaciones locales a la Nube de AWS con la importación datos mediante AWS Direct Connect o AWS VPN. Para obtener más información, consulte Uso de Amazon FSx con sus datos en las instalaciones.

# Acceso a sistemas de archivos de FSx para Lustre

Puede mezclar y combinar los tipos de instancia de procesamiento y la Imagen de máquina de Amazon (AMI) de Linux que están conectadas a un único sistema de archivos de FSx para Lustre.

Se puede acceder a los sistemas de archivos de Amazon FSx para Lustre desde cargas de trabajo de procesamiento que se ejecutan en instancias Amazon Elastic Compute Cloud (Amazon EC2), en

contenedores Docker de Amazon Elastic Container Service (Amazon ECS) y contenedores que se ejecutan en Amazon Elastic Kubernetes Service (Amazon EKS).

- Amazon EC2: accede a su sistema de archivos desde sus instancias de procesamiento de Amazon EC2 mediante el cliente Lustre de código abierto. Las instancias de Amazon EC2 pueden acceder a su sistema de archivos desde otras zonas de disponibilidad dentro de la misma Amazon Virtual Private Cloud (Amazon VPC), siempre y cuando la configuración de red permita el acceso a través de subredes dentro de la VPC. Una vez montado el sistema de archivos Amazon FSx para Lustre, puede trabajar con los archivos y directorios como haría con cualquier sistema de archivos local.
- Amazon EKS: puede acceder a Amazon FSx para Lustre desde contenedores que se ejecutan en Amazon EKS mediante el controlador CSI FSx para Lustre de código abierto, tal y como se describe en la Guía del usuario de Amazon EKS. Los contenedores que se ejecutan en Amazon EKS pueden utilizar volúmenes persistentes (PV) de alto rendimiento respaldados por Amazon FSx para Lustre.
- Amazon ECS: puede acceder a Amazon FSx para Lustre desde contenedores Docker de Amazon ECS en instancias de Amazon EC2. Para obtener más información, consulte Montaje de Amazon Elastic Container Service.

Amazon FSx para Lustre es compatible con las AMI basadas en Linux más populares, incluidas Amazon Linux 2 y Amazon Linux, Red Hat Enterprise Linux (RHEL), CentOS, Ubuntu y SUSE Linux. El cliente Lustre se incluye en Amazon Linux 2 y Amazon Linux. Para RHEL, CentOS y Ubuntu, un repositorio de clientes de AWS Lustre proporciona clientes que son compatibles con estos sistemas operativos.

Utilizando FSx para Lustre, puede dividir sus cargas de trabajo de procesamiento de datos intensivo en las instalaciones a la Nube de AWS con la importación datos mediante AWS Direct Connect o AWS Virtual Private Network. Puede acceder a su sistema de archivos Amazon FSx en las instalaciones, copiar los datos en su sistema de archivos según sea necesario y ejecutar cargas de trabajo de procesamiento de datos intensivo en instancias en la nube.

Para obtener más información sobre los clientes, las instancias de procesamiento y los entornos desde los que puede acceder a los sistemas de archivos de FSx para Lustre, consulte Acceso a sistemas de archivo.

# Integración a los servicios de AWS

Amazon FSx for Lustre se integra con SageMaker Amazon como fuente de datos de entrada. Cuando se utiliza SageMaker con FSx for Lustre, sus trabajos de formación en aprendizaje automático se aceleran al eliminar el paso inicial de descarga de Amazon S3. Además, el costo total de propiedad (TCO) se reduce al evitar la descarga repetitiva de objetos comunes para trabajos iterativos en el mismo conjunto de datos, lo que ahorra en costos de solicitudes de S3. Para obtener más información, consulte ¿Qué es? SageMaker en la Guía para SageMaker desarrolladores de Amazon. Para ver un tutorial sobre cómo utilizar Amazon FSx for Lustre como fuente de datos, consulte Acelere la formación en Amazon SageMaker con Amazon FSx SageMaker for Lustre y los sistemas de archivos Amazon EFS en el blog Machine Learning. AWS

FSx para Lustre se integra con AWS Batch utilizando de plantillas de lanzamiento de EC2. AWS Batch le permite ejecutar cargas de trabajo de procesamiento por lotes en Nube de AWS, incluidas las de computación de alto rendimiento (HPC), machine learning (ML) y otras cargas de trabajo asíncronas. AWS Batch dimensiona las instancias de forma automática y dinámica en función de los requisitos de recursos del trabajo. Para obtener más información, consulte AWS Batch en la Guía del usuario de AWS Batch.

FSx para Lustre se integra con AWS ParallelCluster. AWS ParallelCluster es una herramienta de gestión de clústeres de código abierto compatible con AWS que se utiliza para implementar y gestionar clústeres de HPC. Puede crear automáticamente los sistemas de archivos de FSx para Lustre o utilizar los sistemas de archivos existentes durante el proceso de creación del clúster.

# Seguridad y conformidad

Los sistemas de archivos de FSx para Lustre admiten el cifrado en reposo y en tránsito. Amazon FSx cifra automáticamente los datos en reposo del sistema de archivos mediante claves administradas en AWS Key Management Service (AWS KMS). Los datos en tránsito también se cifran automáticamente en algunos sistemas de archivos Regiones de AWS cuando se accede a ellos desde instancias Amazon EC2 compatibles. Para obtener más información sobre el cifrado de datos en FSx for LustreRegiones de AWS, incluidos los casos en los que se admite el cifrado de datos en tránsito, consulte. Cifrado de datos en Amazon FSx para Lustre Se ha evaluado que Amazon FSx cumple con las certificaciones ISO, PCI-DSS y SOC, y cumple con los requisitos de la HIPAA. Para obtener más información, consulte Seguridad en FSx para Lustre.

# Suposición

En esta guía, hacemos las siguientes suposiciones:

- Si utiliza Amazon Elastic Compute Cloud (Amazon EC2), suponemos que está familiarizado con ese servicio. Para obtener más información sobre cómo utilizar Amazon EC2, consulte la Documentación de Amazon EC2.
- Suponemos que está familiarizado con el uso de Amazon Virtual Private Cloud (Amazon VPC). Para obtener más información sobre cómo utilizar Amazon VPC, consulte la Guía del usuario de Amazon VPC.
- Suponemos que no ha cambiado las reglas del grupo de seguridad predeterminado de su VPC en función del servicio Amazon VPC. Si lo ha hecho, asegúrese de añadir las reglas necesarias para permitir el tráfico de red desde la instancia de Amazon EC2 al sistema de archivos de Amazon FSx para Lustre. Para obtener más información, consulte Control de acceso al sistema de archivos con Amazon VPC.

# Precios de Amazon FSx para Lustre

Con Amazon FSx para Lustre, no hay costes iniciales de hardware o software. Solo paga por los recursos utilizados, sin compromisos mínimos, costos de configuración ni tarifas adicionales. Para obtener información sobre los precios y tarifas asociados al servicio, consulte Precios de Amazon FSx para Lustre.

# Amazon FSx para Lustre

Si tiene problemas al utilizar Amazon FSx para Lustre, consulte los foros.

# ¿Es la primera vez que usa Amazon FSx para Lustre?

Si es la primera vez que utiliza Amazon FSx para Lustre, le recomendamos que lea las siguientes secciones en orden:

1. Si está preparado para crear su primer sistema de archivos Amazon FSx para Lustre, inténtelo Introducción a Amazon FSx para Lustre.
2. Para obtener más información sobre el desempeño, consulte Rendimiento de Amazon FSx para Lustre.

3. Para obtener información sobre cómo vincular su sistema de archivos a un repositorio de datos de bucket de Amazon S3, consulte Uso de repositorios de datos con Amazon FSx para Lustre.
4. Para ver los detalles de seguridad de Amazon FSx para Lustre, consulte Seguridad en FSx para Lustre.
5. Para obtener información sobre los límites de escalabilidad de Amazon FSx para Lustre, incluidos el rendimiento y el tamaño del sistema de archivos, consulte Cuotas.
6. Para obtener información sobre la API de Amazon FSx para Lustre, consulte la referencia de la API de Amazon FSx para Lustre.

# Configuración de Amazon FSx para Lustre

Antes de usar Amazon FSx para Lustre por primera vez, complete las tareas de la sección Inscribirse en Amazon Web Services. Para completar la Explicación introductoria, asegúrese de que el bucket de Amazon S3 que va a vincular a su sistema de archivos tenga los permisos que se indican en Agregar permisos para utilizar repositorios de datos en Amazon S3.

Temas



## Inscribirse en Amazon Web Services

Para configurar AWS, lleve a cabo las siguientes tareas:

1. Registro para obtener una Cuenta de AWS
2. Crear un usuario administrativo

### Registro para obtener una Cuenta de AWS

Si no dispone de una Cuenta de AWS, siga estos pasos para crear una.

Cómo registrarse en 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.

   Al registrarse en una Cuenta de AWS, se crea un Usuario raíz de la cuenta de AWS. 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 administrativo y utilice únicamente el usuario raíz para realizar tareas que requieran acceso de usuario raíz.

AWS le enviará un correo electrónico de confirmación luego de completar 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.

## Crear un usuario administrativo

Después de registrarse para obtener una Cuenta de AWS, proteja su Usuario raíz de la cuenta de AWS, habilite AWS IAM Identity Center y cree un usuario administrativo para no utilizar el usuario raíz en las tareas cotidianas.

Protección de su Usuario raíz de la cuenta de AWS

1. Inicie sesión en la AWS Management Console como propietario de cuenta, elija Usuario raíz e ingrese el email de su Cuenta de AWS. 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 raíz de la Cuenta de AWS (consola) en la Guía del usuario de IAM.

Creación de un usuario administrativo

1. Activar IAM Identity Center

   Para conocer las instrucciones, consulte Habilitar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center.
2. En IAM Identity Center, otorga acceso administrativo a un usuario administrativo.

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

Cómo iniciar sesión como usuario administrativo

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

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

# Agregar permisos para utilizar repositorios de datos en Amazon S3

Amazon FSx para Lustre está profundamente integrado con Amazon S3. Esta integración significa que las aplicaciones que acceden a su sistema de archivos de FSx para Lustre también pueden acceder sin problemas a los objetos almacenados en su bucket de Amazon S3 vinculado. Para obtener más información, consulte Uso de repositorios de datos con Amazon FSx para Lustre.

Para utilizar repositorios de datos, primero debe permitir a Amazon FSx para Lustre determinados permisos de IAM en un rol asociado a la cuenta de su usuario administrador.

Para integrar una política en línea para un rol utilizando la consola

1. Inicie sesión en la consola de IAM AWS Management Console y ábrala en https://console.aws.amazon.com//iam/.
2. Seleccione Roles en el panel de navegación.
3. En la lista, seleccione el nombre del rol en el que incrustará una política.
4. Elija la pestaña Permisos.
5. Desplácese a la parte inferior de la página y seleccione Agregar política en línea.

> **Note**
>
> No puede integrar una política insertada en un rol vinculado a un servicio en IAM. Dado que el servicio vinculado define si puede modificar los permisos del rol, podría añadir las políticas adicionales del servicio desde la consola, la API o la AWS CLI. Para ver la documentación del rol vinculado al servicio de un servicio, consulte Servicios que funcionan con IAM AWS y elija Sí en la columna Rol vinculado a servicio del servicio.

6. Seleccione Creación de políticas con el editor visual
7. Agregue la siguiente declaración de política de permisos.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
```

```
        "Action": [
            "iam:CreateServiceLinkedRole",
            "iam:AttachRolePolicy",
            "iam:PutRolePolicy"
        ],
        "Resource": "arn:aws:iam::*:role/aws-service-role/s3.data-
source.lustre.fsx.amazonaws.com/*"
    }
}
```

Una vez que cree una política insertada, se integra automáticamente en su rol. Para obtener más información acerca de los roles vinculados a servicios, consulte Uso de roles vinculados a servicios para Amazon FSx.

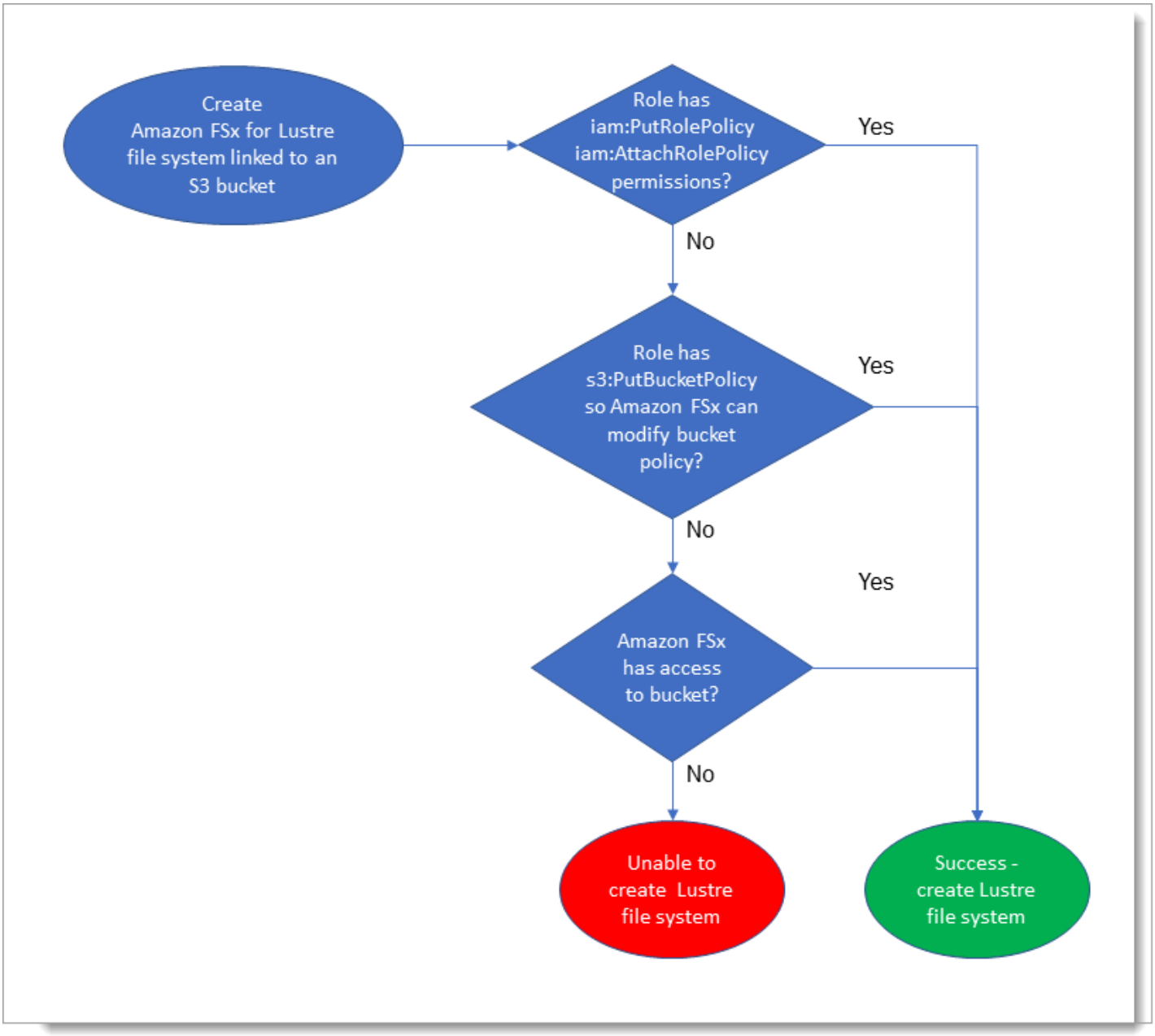
## Cómo FSx para Lustre comprueba el acceso a los buckets S3 vinculados

Si el rol de IAM que utiliza para crear el sistema de archivos de FSx para Lustre no tiene los permisos `iam:AttachRolePolicy` y `iam:PutRolePolicy`, Amazon FSx comprueba si puede actualizar su política de bucket de S3. Amazon FSx puede actualizar su política de bucket si el permiso `s3:PutBucketPolicy` está incluido en su rol de IAM para permitir que el sistema de archivos de Amazon FSx importe o exporte datos a su bucket de S3. Si se le permite modificar la política del bucket, Amazon FSx agrega los siguientes permisos a la política del bucket:

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:PutObject`
- `s3:Get*`
- `s3:List*`
- `s3:PutBucketNotification`
- `s3:PutBucketPolicy`
- `s3:DeleteBucketPolicy`

Si Amazon FSx no puede modificar la política de bucket, comprueba si la política de bucket existente concede a Amazon FSx acceso al bucket.

Si todas estas opciones fallan, entonces la solicitud para crear el sistema de archivos falla. El siguiente diagrama ilustra las comprobaciones que realiza Amazon FSx para determinar si un sistema de archivos puede acceder al bucket de S3 al que se vinculará.




## Siguiente paso

Para empezar a utilizar FSx para Lustre, consulte Introducción a Amazon FSx para Lustre para obtener instrucciones para crear sus recursos Amazon FSx para Lustre.

# Introducción a Amazon FSx para Lustre

A continuación, puede aprender cómo empezar a utilizar Amazon FSx para Lustre. Estos pasos le explicarán cómo crear un sistema de archivos Amazon FSx para Lustre y cómo acceder a él desde sus instancias informáticas. Opcionalmente, también muestran cómo usar el sistema de archivos de Amazon FSx para Lustre para procesar los datos del bucket de Amazon S3 con las aplicaciones basadas en archivos.

Este ejercicio introductorio incluye los siguientes pasos.

Temas



## Requisitos previos

Para realizar este ejercicio introductorio, necesitará lo siguiente:

- Una AWS cuenta con los permisos necesarios para crear un sistema de archivos Amazon FSx for Lustre y una instancia de Amazon EC2. Para obtener más información, consulte Configuración de Amazon FSx para Lustre.
- Cree un grupo de seguridad de Amazon VPC para asociarlo a su sistema de archivos FSx for Lustre y no lo cambie después de crear el sistema de archivos. Para obtener más información, consulte Para crear un grupo de seguridad para el sistema de archivos Amazon FSx.
- Una instancia de Amazon EC2 que ejecuta una versión de Linux compatible en su nube privada virtual (VPC) basada en el servicio Amazon VPC. Para este ejercicio de introducción, le recomendamos que utilice Amazon Linux 2023. Instalará el cliente Lustre en esta instancia EC2 y montará su sistema de archivos de FSx para Lustre en la instancia EC2. Para obtener más información sobre la creación de una instancia EC2, consulte Introducción: lanzar una instancia o Lance su instancia en la Guía del usuario de Amazon EC2 para instancias de Linux.

El cliente Lustre es compatible con Amazon Linux; Amazon Linux 2; Amazon Linux 2023; CentOS y Red Hat Enterprise Linux 7.7 a 7.9, 8.2 a 8.9, 9.0 y 9.3; Rocky Linux 8.4 a 8.9, 9.0 y 9.3; SUSE Linux Enterprise Server 12 SP3, SP4 y SP5; y Ubuntu 18.04, 20.04 y 22.04. Para obtener más información, consulte Compatibilidad entre el sistema de archivos de Lustre y el núcleo del cliente.

Al crear la instancia de Amazon EC2 para este ejercicio introductorio, tenga en cuenta lo siguiente:

- Le recomendamos que cree la instancia en la VPC predeterminada.
- Se recomienda que utilice el grupo de seguridad predeterminado al crear la instancia EC2.

- Cada sistema de archivos de FSx para Lustre requiere una dirección IP para el servidor de metadatos (MDS) y una dirección IP para cada servidor de almacenamiento (OSS).
  - Los sistemas de archivos SSD persistentes se aprovisionan con 2,4 TiB de almacenamiento por OSS.
  - Los sistemas de archivos HDD persistentes con 12 MB/s/TiB de capacidad de rendimiento se aprovisionan con 6 TiB de almacenamiento por OSS.
  - Los sistemas de archivos HDD persistentes con 40 MB/s/TiB de capacidad de rendimiento se aprovisionan con 1,8 TiB de almacenamiento por OSS.
  - Los sistemas de archivos Scratch_2 se aprovisionan con 2,4 TiB de almacenamiento por OSS.
  - Los sistemas de archivos Scratch_1 se aprovisionan con 3,6 TiB de almacenamiento por OSS.
- Un bucket de Amazon S3 que almacena los datos para que los procese su carga de trabajo. El bucket S3 será el repositorio de datos duradero vinculado a su sistema de archivos de FSx para Lustre.
- Determine qué tipo de sistema de archivos Amazon FSx para Lustre desea crear, scratch o persistent. Para obtener más información, consulte Opciones de implementación para sistemas de archivos de FSx para Lustre .

## Cree su sistema de archivos FSx for Lustre

A continuación, cree su sistema de archivos en la consola.

Para crear su sistema de archivos

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel, elija Create file system (Crear sistema de archivos) para iniciar el asistente de creación de sistemas de archivos.

3. Elija FSx para Lustre y luego elija Siguiente para abrir la página Crear sistema de archivos.
4. Proporcione la información en la sección de Información del sistema de archivos:

   - En File system name-optional (Nombre del sistema de archivos (opcional), introduzca un nombre para su sistema de archivos. Puede utilizar hasta 256 letras Unicode, espacios en blanco y números, además de los caracteres especiales + - = . _ : /.
   - Para Tipo de implementación y almacenamiento, elija una de las siguientes opciones:

     El almacenamiento SSD proporciona cargas de trabajo de baja latencia e intensivas en IOPS que suelen tener operaciones de archivos pequeñas y aleatorias. El almacenamiento en HDD proporciona cargas de trabajo de alto rendimiento que suelen tener grandes operaciones de archivos secuenciales.

     Para obtener más información acerca de los tipos de almacenamiento, consulte Múltiples opciones de almacenamiento.

     Para obtener más información sobre los tipos de implementación, consulte Opciones de implementación para sistemas de archivos de FSx para Lustre.

     Para obtener más información sobre Regiones de AWS dónde está disponible el cifrado de datos en tránsito, consulteCifrado de datos en tránsito.

     - Elija el tipo de implementación Persistent, SSD (SSD persistente) para un almacenamiento a largo plazo y para cargas de trabajo sensibles a la latencia que requieren los niveles más altos de IOPS/rendimiento. Los servidores de archivos tienen una alta disponibilidad, los datos se replican automáticamente dentro de la zona de disponibilidad del sistema de archivos y permiten cifrar los datos en tránsito. Persistent, SSD utiliza Persistent 2, la última generación de sistemas de archivos persistentes.
     - Elija el tipo de implementación Persistent, HDD (HDD persistente) para el almacenamiento a largo plazo y para cargas de trabajo centradas en el rendimiento que no sean sensibles a la latencia. Los servidores de archivos son de alta disponibilidad, los datos se replican automáticamente dentro de la zona de disponibilidad del sistema de archivos y este tipo admite el cifrado de datos en tránsito. Persistent, HDD utiliza el tipo de implementación Persistent 1.

       Elija with SSD cache (con caché SSD) para crear una caché SSD con un tamaño equivalente al 20 por ciento de la capacidad de almacenamiento de su disco duro para proporcionar latencias inferiores al milisegundo y mayores IOPS para los archivos a los que se accede con frecuencia.

  - Elija el tipo de implementación Scratch, SSD para el almacenamiento temporal y el tratamiento de datos a corto plazo. Scratch, SSD, utiliza los sistemas de archivos Scratch 2 y ofrece el cifrado de datos en tránsito.
- Elija la cantidad de rendimiento por unidad de almacenamiento que desee para su sistema de archivos. Esta opción solo es válida para los tipos de implementación persistentes.

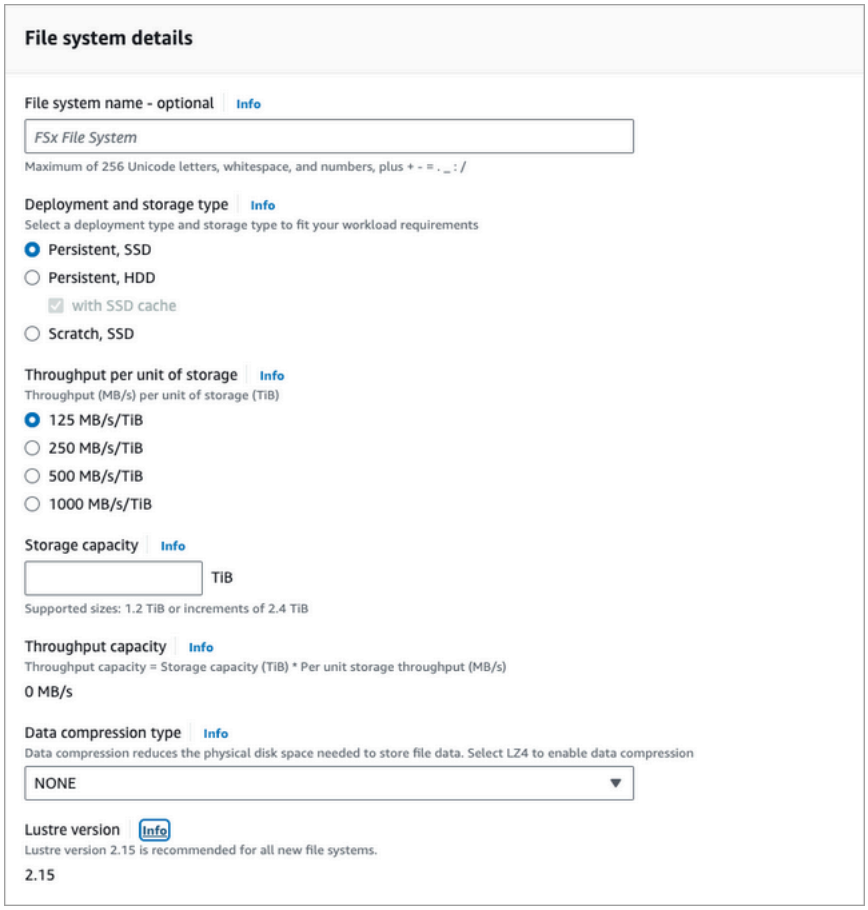
  El rendimiento por unidad de almacenamiento es la cantidad de rendimiento de lectura y escritura por cada 1 tebibyte (TiB) de almacenamiento aprovisionado, en MB/s/TiB. Usted paga la cantidad de rendimiento aprovisionada:

  - Para almacenamiento SSD persistente, elija un valor de 125, 250, 500 o 1000 MB/s/TiB.
  - Para almacenamiento SSD persistente, elija un valor de 12 o 40 MB/s/TiB.

  Puede aumentar o disminuir la cantidad de rendimiento por unidad de almacenamiento según sea necesario después de crear el sistema de archivos. Para obtener más información, consulte Administración de la capacidad de rendimiento.
- Para la capacidad de almacenamiento, defina la cantidad de capacidad de almacenamiento del sistema de archivos en TiB:
  - Para un tipo de implementación SSD persistente, configúrelo en un valor de 1,2 TiB, 2,4 TiB o incrementos de 2,4 TiB.
  - Para un tipo de implementación HDD persistente este valor puede ser incrementos de 6,0 TiB para sistemas de archivos de 12 MB/s/TiB e incrementos de 1,8 TiB para sistemas de archivos de 40 MB/s/TiB.

  Puede aumentar la capacidad de almacenamiento según sea necesario en cualquier momento después de crear el sistema de archivos. Para obtener más información, consulte Administración de la capacidad de almacenamiento.
- En el tipo de compresión de datos, seleccione NINGUNO para desactivar la compresión de datos o elija LZ4 para activar la compresión de datos con el algoritmo LZ4. Para obtener más información, consulte Compresión de datos de Lustre.

Todos los sistemas de archivos de FSx para Lustre se basan en la versión 2.15 de Lustre cuando se crean mediante la consola de Amazon FSx.



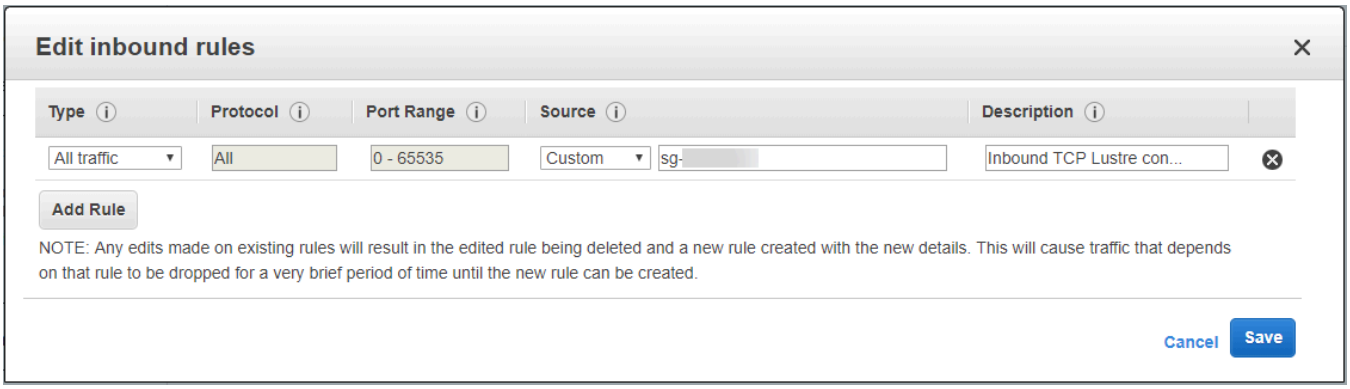

5. En la sección Network & security, proporcione la siguiente información de red y grupo de seguridad:

   - Para la nube privada virtual (VPC), elija la VPC que desea asociar con su sistema de archivos. Para este ejercicio introductorio, elija la misma VPC que eligió para la instancia de Amazon EC2.
   - Para los grupos de seguridad VPC, el ID para el grupo de seguridad por defecto para su VPC debe estar ya añadido. Si no está utilizando el grupo de seguridad predeterminado, asegúrese de que la siguiente regla de entrada se agregue al grupo de seguridad que está utilizando para este ejercicio introductorio.

| Tipo | Protocolo | Rango de puerto | Origen | Descripción |
|---|---|---|---|---|
| Todos los TCP | TCP | 0-65535 | Personalizado *the_ID_of _this_sec* | Regla de tráfico entrante de Lustre |

| Tipo | Protocolo | Rango de puerto | Origen | Descripción |
|---|---|---|---|---|
| | | | *urity_gro up* | |

La siguiente captura de pantalla muestra un ejemplo de edición de reglas de entrada.




> **Important**
>
> Asegúrese de que el grupo de seguridad que está utilizando sigue las instrucciones de configuración que se proporcionan en. Control de acceso al sistema de archivos con Amazon VPC Debe configurar el grupo de seguridad para permitir el tráfico entrante en los puertos 988 y 1018-1023 desde el propio grupo de seguridad o la subred CIDR completa, que es necesaria para permitir que los hosts del sistema de archivos se comuniquen entre sí.

- En Subred, elija cualquier valor de la lista de subredes disponibles.

6. Para la sección de Cifrado, las opciones disponibles varían según el tipo de sistema de archivos que vaya a crear:

   - En el caso de un sistema de archivos persistente, puede elegir una clave de cifrado AWS Key Management Service (AWS KMS) para cifrar los datos del sistema de archivos en reposo.
   - En el caso de un sistema de archivos temporal, los datos en reposo se cifran mediante claves gestionadas por AWS.
   - Para los sistemas de archivos scratch 2 y persistentes, los datos en tránsito se cifran automáticamente cuando se obtiene acceso al sistema de archivos desde un tipo de instancia

de Amazon EC2 compatible. Para obtener más información, consulte Cifrado de datos en tránsito.

7. En la sección Importar/Exportar repositorios de datos (opcional), la vinculación del sistema de archivos a los repositorios de datos de Amazon S3 está deshabilitada de forma predeterminada. Para obtener información sobre cómo activar esta opción y crear una asociación de repositorio de datos a un bucket de S3 existente, consulte Para vincular un bucket de S3 al crear un sistema de archivos (consola).

   > **Important**
   >
   > - Al seleccionar esta opción también se deshabilitan las copias de seguridad y no podrá habilitarlas mientras crea el sistema de archivos.
   > - Si vincula uno o varios sistemas de archivos de Amazon FSx para Lustre a un bucket de Amazon S3, no elimine el bucket de Amazon S3 hasta que se hayan eliminado todos los sistemas de archivos vinculados.

8. Para el Registro: opcional, el registro está activado de forma predeterminada. Cuando está habilitada, los errores y las advertencias de la actividad del repositorio de datos en su sistema de archivos se registran en Amazon CloudWatch Logs. Para obtener información sobre la configuración de los registros, consulte Administración de registros.
9. En Copia de seguridad y mantenimiento - opcional, puede hacer lo siguiente.

   Para copias de seguridad automáticas diarias:

   - Desactive la Copia de seguridad automática diaria. Esta opción está habilitada de forma predeterminada, a menos que haya activado Importar/Exportar repositorios de datos.
   - Establezca la hora de inicio de la ventana de copia de seguridad automática diaria.
   - Establezca el Período de retención de la copia de seguridad automática, de 1 a 35 días.

   Para obtener más información, consulte Trabajo con copias de seguridad.
10. Defina la hora de inicio de la Ventana de mantenimiento semanal o manténgala en el valor predeterminado Sin preferencia.
11. En el caso de Root Squash (opcional), el Root Squash está deshabilitado de forma predeterminada. Para obtener información sobre cómo habilitar y configurar root squash, consultePara habilitar root squash al crear un sistema de archivos (consola).

12. Cree las etiquetas que desee aplicar a su sistema de archivos.
13. Seleccione Siguiente para mostrar la página de Resumen de creación del sistema de archivos.
14. Revise la configuración de su sistema de archivos Amazon FSx para Lustre y seleccione Crear sistema de archivos.

Ahora que creó su sistema de archivos, anote el nombre de dominio completo y su nombre de montaje para un paso posterior. Puede encontrar el nombre de dominio completo y el nombre de montaje de un sistema de archivos seleccionando el nombre del sistema de archivos en el panel Caches y luego seleccionando Adjuntar.

## Instale y configure el cliente Lustre

Antes de poder acceder a su sistema de archivos Amazon FSx for Lustre desde su instancia de Amazon EC2, debe hacer lo siguiente:

- Compruebe que la instancia EC2 cumpla con los requisitos mínimos del núcleo.
- Actualice el núcleo si es necesario.
- Descargue e instale el cliente Lustre.

Para comprobar la versión del núcleo y descargar el cliente Lustre

1. Abra una ventana de terminal en su instancia EC2.
2. Determine qué kernel se está ejecutando actualmente en su instancia de procesamiento mediante la ejecución del siguiente comando.

   ```
   uname -r
   ```

3. Realice una de las acciones siguientes:

   - Si el comando devuelve `6.1.79-99.167.amzn2023.x86_64` para instancias EC2 basadas en x86, o `6.1.79-99.167.amzn2023.aarch64` o superior para instancias EC2 basadas en Graviton2, descargue e instale el cliente Lustre con el siguiente comando.

     ```
     sudo dnf install -y lustre-client
     ```

   - Si el comando devuelve un resultado inferior `6.1.79-99.167.amzn2023.x86_64` para instancias EC2 basadas en x86, o inferior que `6.1.79-99.167.amzn2023.aarch64` para

instancias EC2 basadas en Graviton2, actualice el kernel y reinicie su instancia de Amazon EC2 ejecutando el siguiente comando.

```
sudo dnf -y update kernel && sudo reboot
```

Compruebe que el kernel se haya actualizado usando el comando uname -r. Luego, descargue e instale el cliente Lustre como se ha descrito anteriormente.

Para obtener información sobre la instalación del cliente Lustre en otras distribuciones de Linux, consulte Instalación del cliente Lustre.

## Monte el sistema de archivos.

Para montar el sistema de archivos, debe crear un directorio de montaje o punto de montaje y, a continuación, montar el sistema de archivos en el cliente y comprobar que el cliente puede acceder al sistema de archivos.

Para montar el sistema de archivos

1. Haga un directorio para el punto de montaje con el siguiente comando.

   ```
   sudo mkdir -p /mnt/fsx
   ```

2. Monte el sistema de archivos de Amazon FSx para Lustre en el directorio que ha creado. Utilice el siguiente comando y sustituya los siguientes elementos:

   - Sustituya *file_system_dns_name* por el nombre del sistema de nombres de dominio (DNS) del sistema de archivos real.
   - *mountname*Sustitúyalo por el nombre de montaje del sistema de archivos, que puede obtener ejecutando el describe-file-systems AWS CLI comando o la operación de DescribeFileSystemsAPI.

   ```
   sudo mount -t lustre -o relatime,flock file_system_dns_name@tcp:/mountname /mnt/fsx
   ```

   Este comando monta el sistema de archivos con dos opciones: `-o relatime` y `flock`:

- `relatime` – Si bien la opción `atime` mantiene los datos `atime` (tiempos de acceso al inodo) cada vez que se accede a un archivo, la opción `relatime` también mantiene los datos `atime`, pero no para cada vez que se accede a un archivo. Con la opción `relatime` habilitada, los datos `atime` se escriben en el disco solo si el archivo se ha modificado desde que los datos `atime` se actualizaron por última vez (`mtime`), o si se accedió al archivo por última vez hace más de un cierto tiempo (6 horas por defecto). El uso de la opción `relatime` o `atime` optimizará los procesos de liberación de archivos.

  > **Note**
  >
  > Si su carga de trabajo requiere una precisión exacta del tiempo de acceso, puede montar con la opción de montaje `atime`. Sin embargo, hacerlo puede afectar al rendimiento de la carga de trabajo al aumentar el tráfico de red necesario para mantener valores de tiempo de acceso precisos.
  > Si su carga de trabajo no requiere tiempo de acceso a metadatos, el uso de la opción de montaje `noatime` para desactivar las actualizaciones del tiempo de acceso puede proporcionar una ganancia de rendimiento. Tenga en cuenta que los procesos centrados `atime` como la liberación de archivos o la liberación de la validez de los datos serán imprecisos en su liberación.

- `flock` – Permite el bloqueo de archivos para su sistema de archivos. Si no quiere activar el bloqueo de archivos, utilice el comando `mount` sin `flock`.

3. Compruebe que el comando de montaje se haya realizado correctamente listando el contenido del directorio en el que ha montado el sistema de archivos `/mnt/fsx`, mediante el siguiente comando.

```
ls /mnt/fsx
import-path  lustre
$
```

También puede utilizar el comando `df`, a continuación.

```
df
Filesystem                   1K-blocks    Used  Available Use% Mounted on
devtmpf                       1001808       0    1001808   0% /dev
tmpfs                         1019760       0    1019760   0% /dev/shm
tmpfs                         1019760     392    1019368   1% /run
```

```
tmpfs                           1019760       0    1019760   0% /sys/fs/cgroup
/dev/xvda1                      8376300 1263180    7113120  16% /
123.456.789.0@tcp:/mountname  3547698816   13824 3547678848   1% /mnt/fsx
tmpfs                            203956       0     203956   0% /run/user/1000
```

Los resultados muestran el sistema de archivos Amazon FSx montado en /mnt/fsx.

## Ejecutar el flujo de trabajo

Ahora que se creó y montó su sistema de archivos en una instancia informática, puede utilizarlo para ejecutar su carga de trabajo informática de alto rendimiento.

Puede crear una asociación de repositorio de datos para vincular su sistema de archivos a un repositorio de datos de Amazon S3, Para obtener más información, consulte Vincular su sistema de archivos a un bucket de S3.

Una vez que haya vinculado su sistema de archivos a un repositorio de datos de Amazon S3, podrá exportar los datos que haya escrito en su sistema de archivos de vuelta a su bucket de Amazon S3 en cualquier momento. Desde un terminal en una de sus instancias informáticas, ejecute el siguiente comando para exportar un archivo a su bucket de Amazon S3.

```
sudo lfs hsm_archive file_name
```

Para obtener más información sobre cómo ejecutar este comando en una carpeta o una gran colección de archivos rápidamente, consulte Exportación de archivos mediante comandos de HSM.

## Eliminar recursos

Cuando haya terminado este ejercicio, debe seguir estos pasos para limpiar sus recursos y proteger su AWS cuenta.

Para limpiar los recursos

1. Si desea realizar una exportación final, ejecute el siguiente comando.

   ```
   nohup find /mnt/fsx -type f -print0 | xargs -0 -n 1 sudo lfs hsm_archive &
   ```

2. En la consola de Amazon EC2, termine la instancia. Para obtener más información, consulte Terminar la instancia en la Guía del usuario de Amazon EC2 para instancias de Linux.

3. En la consola de Amazon FSx para Lustre, elimine su sistema de archivos con el siguiente procedimiento:

   a. En el panel de navegación, elija File systems (Sistema de archivos).
   b. Elija el sistema de archivos que desea eliminar de la lista de sistemas de archivos del panel.
   c. En Acciones, seleccione Eliminar sistema de archivos.
   d. En el cuadro de diálogo que aparece, elija si desea realizar una copia de seguridad final del sistema de archivos. A continuación, indique el ID del sistema de archivos para confirmar la eliminación. Seleccione Delete file system (Eliminar sistema de archivos).

4. Si ha creado un bucket de Amazon S3 para este ejercicio y no desea conservar los datos exportados, puede eliminarlo. Para obtener más información, consulte Eliminación de un bucket en la Guía del usuario de Amazon Simple Storage Service.

# Opciones de implementación para sistemas de archivos de FSx para Lustre

FSx para Lustre proporciona un sistema de archivos en paralelo de alto rendimiento que almacena datos en varios servidores de archivos de red para maximizar el rendimiento y reducir los cuellos de botella. Estos servidores tienen varios discos. Para distribuir la carga, Amazon FSx particiona los datos del sistema de archivos en trozos más pequeños y los distribuye por los discos y servidores mediante un proceso llamado fragmentación. Para obtener más información sobre la fragmentación de datos de FSx para Lustre, consulte. Fragmentación de datos en su sistema de archivos

Se recomienda vincular un repositorio de datos a largo plazo altamente duradero que resida en Amazon S3 con su sistema de archivos de alto rendimiento FSx para Lustre.

En este escenario, almacena sus conjuntos de datos en el repositorio de datos de Amazon S3 vinculado. Cuando crea su sistema de archivos de FSx para Lustre, lo vincula a su repositorio de datos de S3. En este punto, los objetos del bucket de S3 se muestran como archivos y directorios en el sistema de archivos de FSx. A continuación, Amazon FSx copia automáticamente el contenido del archivo de S3 a su sistema de archivos Lustre cuando se accede a un archivo por primera vez en el sistema de archivos Amazon FSx. Después de que se ejecute la carga de trabajo informática, o en cualquier momento, puede utilizar una tarea de repositorio de datos para exportar los cambios de nuevo a S3. Para obtener más información, consulte Uso de repositorios de datos con Amazon FSx para Lustre y Uso de las tareas del repositorio de datos para exportar los cambios.

## Opciones de implementación para sistemas de archivos de FSx para Lustre

Amazon FSx para Lustre proporciona dos opciones de implementación del sistema de archivos: scratch y persistente.

> **Note**
>
> Ambas opciones de implementación admiten el almacenamiento en unidades de estado sólido (SSD). Sin embargo, el almacenamiento en unidad de disco duro (HDD) solo se admite en uno de los tipos de implementación persistente.

Puede elegir el tipo de implementación del sistema de archivos cuando cree un nuevo sistema de archivos, utilizando la AWS Management Console, AWS Command Line Interface (AWS CLI) o la API Amazon FSx para Lustre. Para obtener más información, consulte Cree su sistema de archivos FSx for Lustre y consulte la CreateFileSystemreferencia de la API de Amazon FSx.

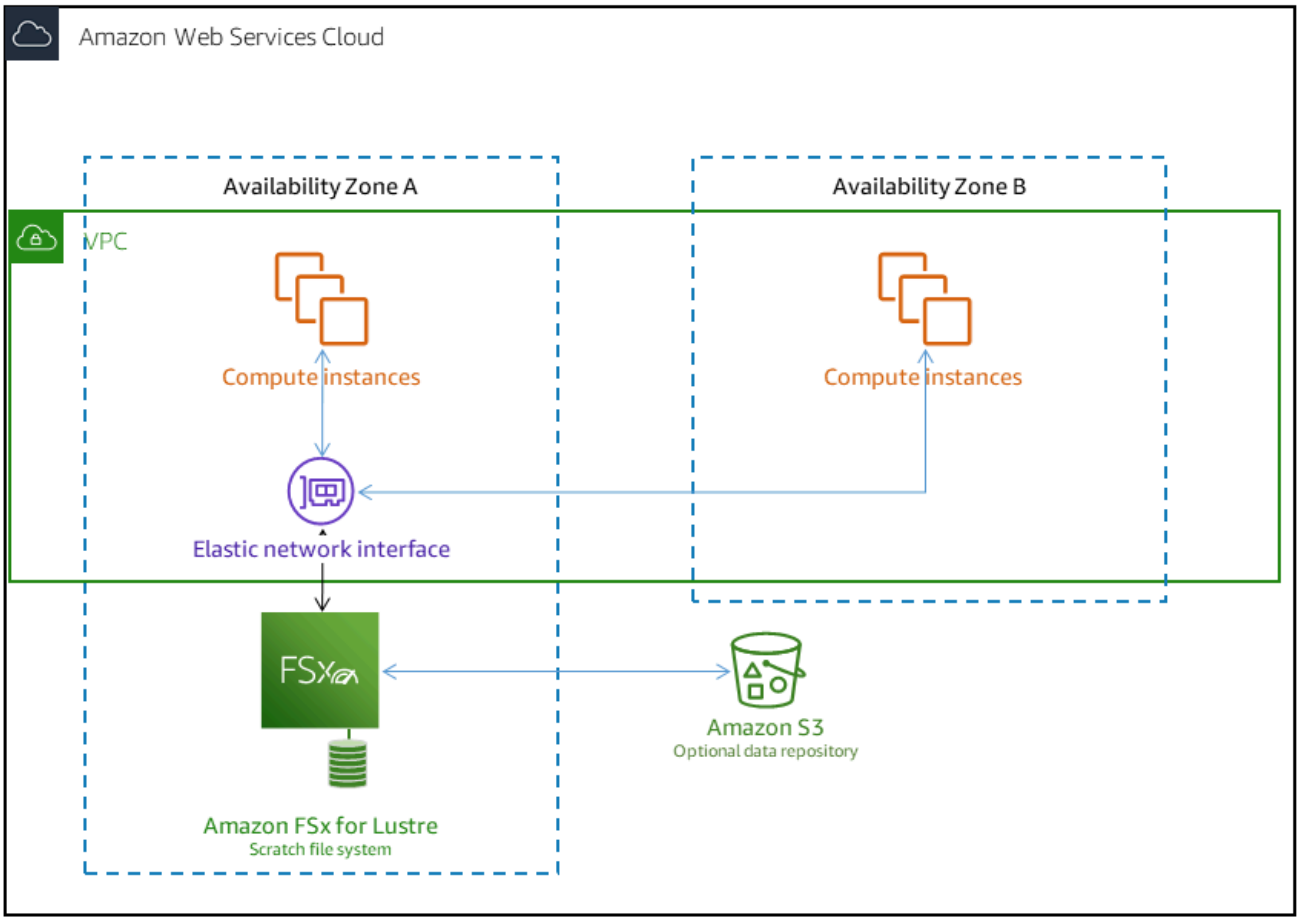
El cifrado de datos en reposo se habilita automáticamente al crear un sistema de archivos de Amazon FSx para Lustre, independientemente del tipo de implementación que utilice. Scratch 2 y los sistemas de archivos persistentes cifran automáticamente los datos en tránsito cuando se accede a ellos desde instancias de Amazon EC2 que soportan el cifrado en tránsito. Para obtener más información sobre el cifrado, consulte Cifrado de datos en Amazon FSx para Lustre.

## Sistemas de archivos Scratch

Los sistemas de archivos Scratch están diseñados para el almacenamiento temporal y el procesamiento de datos a corto plazo. Los datos no se replican y no persisten si falla un servidor de archivos. Los sistemas de archivos Scratch proporcionan un alto rendimiento en ráfagas de hasta seis veces el rendimiento de referencia de 200 MBps por TiB de capacidad de almacenamiento. Para obtener más información, consulte Rendimiento agregado del sistema de archivos.

Utilice los sistemas de archivos scratch cuando necesite un almacenamiento de costo optimizado para cargas de trabajo de procesamiento intensivo a corto plazo.

En el siguiente diagrama, se muestra la arquitectura de un entorno de Amazon FSx para Lustre.




En un sistema de archivos scratch, los servidores de archivos no se sustituyen si fallan y los datos no se replican. Si un servidor de archivos o un disco de almacenamiento deja de estar disponible en un sistema de archivos scratch, los archivos almacenados en otros servidores siguen siendo accesibles. Si los clientes intentan acceder a datos que están en el servidor o disco no disponible, los clientes experimentan un error de E/S inmediato.

La siguiente tabla ilustra la disponibilidad o durabilidad para la que están diseñados los sistemas de archivos scratch de tamaños de ejemplo, en el transcurso de un día y una semana. Dado que los sistemas de archivos más grandes tienen más servidores de archivos y más discos, las probabilidades de fallo aumentan.

| Tamaño del sistema de archivos (TiB) | Número de servidores de archivos | Disponibilidad/durabilidad a lo largo de un día | Disponibilidad/durabilidad a lo largo de una semana |
|---|---|---|---|
| 1.2 | 2 | 99,9% | 99,4% |
| 2.4 | 2 | 99,9% | 99,4% |
| 4.8 | 3 | 99,8% | 99,2% |
| 9,6 | 5 | 99,8% | 98,6% |
| 50,4 | 22 | 99,1% | 93,9% |

# Sistemas de archivos persistentes

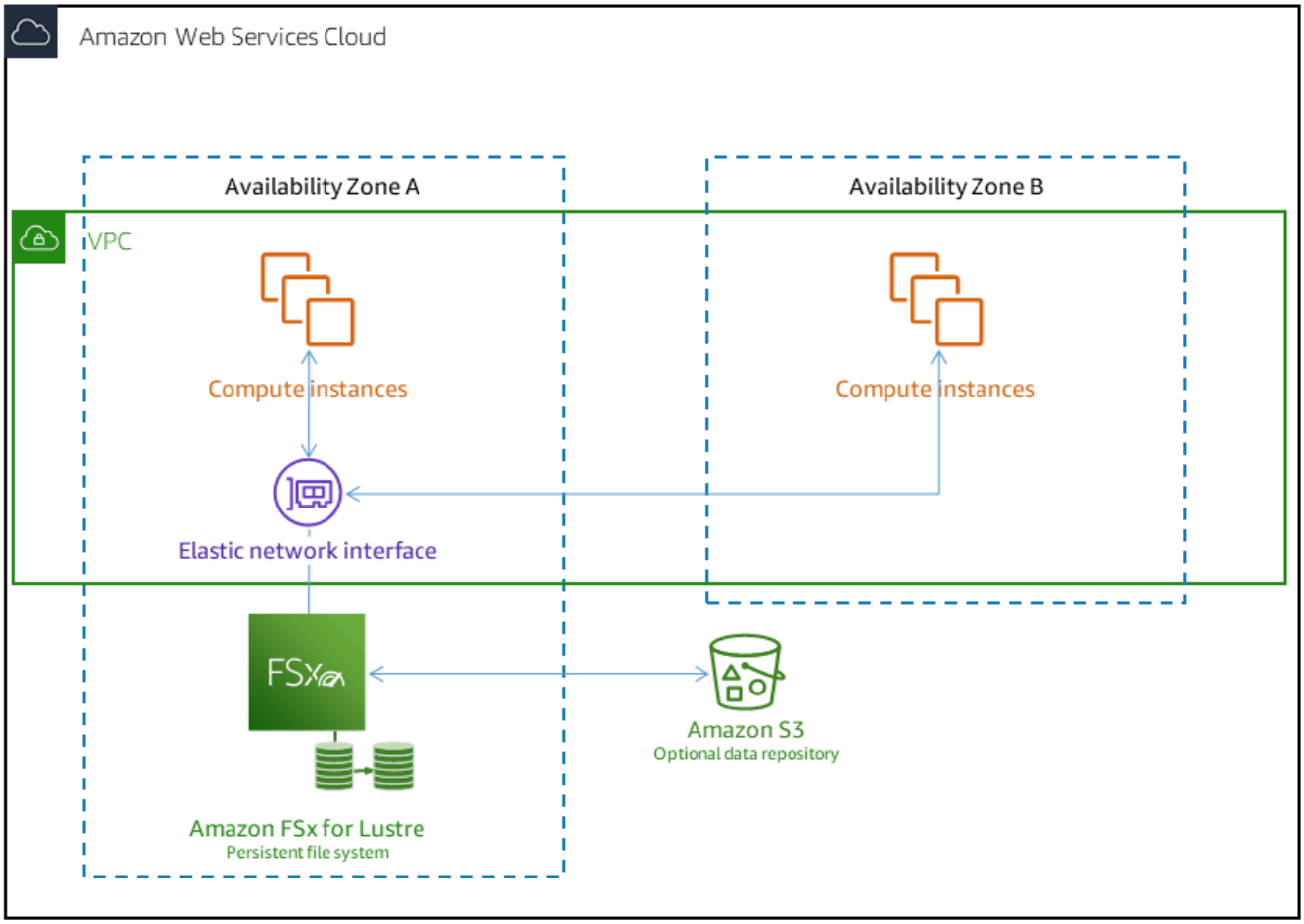
Los sistemas de archivos persistentes están diseñados para cargas de trabajo y almacenamiento a largo plazo. Los servidores de archivos son de alta disponibilidad, y los datos se replican automáticamente dentro de la misma Zona de Disponibilidad en la que se encuentra el sistema de archivos. Los volúmenes de datos adjuntos a los servidores de archivos se replican de forma independiente de los servidores de archivos a los que están conectados.

Amazon FSx monitorea de forma continua los sistemas de archivos persistentes para detectar errores de hardware y reemplaza automáticamente los componentes de la infraestructura en caso de que se produzca un error. En un sistema de archivos persistente, si un servidor de archivos deja de estar disponible, se reemplaza automáticamente a los pocos minutos de producirse el fallo. Durante ese tiempo, las solicitudes de datos de ese servidor por parte del cliente se vuelven a intentar de forma transparente y, finalmente, se realizan correctamente una vez que se reemplaza el servidor de archivos. Los datos de los sistemas de archivos persistentes se replican en los discos y cualquier disco que falle se reemplaza automáticamente de forma transparente.

Utilice sistemas de archivos persistentes para el almacenamiento a largo plazo y para cargas de trabajo centradas en el rendimiento que se ejecutan durante períodos prolongados o indefinidamente, y que podrían ser sensibles a las interrupciones en la disponibilidad.

El siguiente diagrama muestra la arquitectura de un sistema de archivos persistente Amazon FSx para Lustre, con servidores de archivos y volúmenes de datos replicados y de alta disponibilidad dentro de una única zona de disponibilidad.

Los tipos de implementación persistentes cifran automáticamente los datos en tránsito cuando se obtiene acceso a ellos desde instancias de Amazon EC2 que soportan el cifrado en tránsito.




Amazon FSx para Lustre soporta dos tipos de implementación persistente, Persistent_1 y Persistent_2.

## Tipo de implementación Persistent 1

Los tipos de implementación Persistent_1 se pueden construir sobre Lustre 2.10 o 2.12, y admiten tipos de almacenamiento SSD (unidad de estado sólido) y HDD (unidad de disco duro). El tipo de implementación Persistent_1 es adecuado para casos de uso que requieren almacenamiento a largo plazo y tienen cargas de trabajo centradas en el rendimiento que no son sensibles a la latencia.

Para un sistema de archivos Persistent_1 con almacenamiento SSD, el rendimiento por unidad de almacenamiento es de 50, 100 o 200 MB/s por tebibyte (TiB). Para almacenamiento HDD, el rendimiento de Persistent_1 por unidad de almacenamiento es de 12 o 40 MB/s por TiB.

Solo puede crear tipos de implementación Persistent_1 utilizando AWS CLI y la API de Amazon FSx.

## Tipo de implementación Persistent 2

Persistent_2 es la última generación del tipo de implementación Persistent, y es el más adecuado para casos de uso que requieren almacenamiento a largo plazo, y tienen cargas de trabajo sensibles a la latencia que requieren los más altos niveles de IOPS y rendimiento. Los tipos de implementación de Persistent_2 se basan en la versión 2.12 de Lustre y admiten almacenamiento en SSD. Admiten mayores niveles de rendimiento por unidad de almacenamiento en comparación con los sistemas de archivos Persistent_1, con opciones de 125, 250, 500 y 1000 MB/s/TiB.

Puede crear tipos de implementación Persistent_2 usando la consola Amazon FSx, AWS Command Line Interface y la API.

### Regiones disponibles

Los tipos de implementación Persistent_1 y Persistent_2 están disponibles en Regiones de AWS:

| Región de AWS | Persistent_1 | Persistent_2 |
|---|---|---|
| US East (Ohio) | ✓ | ✓ |
| Este de EE. UU. (Norte de Virginia) | ✓ | ✓ |
| Oeste de EE. UU. (Norte de California) | ✓ | |
| Oeste de EE. UU. (Los Ángeles) | ✓ | |
| Oeste de EE. UU. (Oregón) | ✓ | ✓ |
| África (Ciudad del Cabo) | ✓ | |
| Asia-Pacífico (Hong Kong) | ✓ | ✓ |
| Asia-Pacífico (Hyderabad) | ✓ | |
| Asia-Pacífico (Yakarta) | ✓ | |
| Asia-Pacífico (Melbourne) | ✓ | |
| Asia-Pacífico (Bombay) | ✓ | ✓ |

| Región de AWS | Persistent_1 | Persistent_2 |
|---|---|---|
| Asia-Pacífico (Osaka) | ✓ | |
| Asia-Pacífico (Seúl) | ✓ | ✓ |
| Asia-Pacífico (Singapur) | ✓ | ✓ |
| Asia-Pacífico (Sídney) | ✓ | ✓ |
| Asia-Pacífico (Tokio) | ✓ | ✓ |
| Canadá (Centro) | ✓ | ✓ |
| Europa (Fráncfort) | ✓ | ✓ |
| Europa (Irlanda) | ✓ | ✓ |
| Europa (Londres) | ✓ | ✓ |
| Europa (Milán) | ✓ | |
| Europa (París) | ✓ | |
| Europa (España) | ✓ | |
| Europa (Estocolmo) | ✓ | ✓ |
| Europa (Zúrich) | ✓ | |
| Israel (Tel Aviv) | ✓ | |
| Medio Oriente (Baréin) | ✓ | |
| Medio Oriente (EAU) | ✓ | |
| América del Sur (São Paulo) | ✓ | |
| AWS GovCloud (Este de EE. UU.) | ✓ | |
| AWS GovCloud (Estados Unidos-Oeste) | ✓ | |

Para obtener más información sobre el rendimiento de FSx para Lustre, consulte Rendimiento agregado del sistema de archivos.

# Uso de repositorios de datos con Amazon FSx para Lustre

Amazon FSx para Lustre proporciona sistemas de archivos de alto rendimiento optimizados para un procesamiento rápido de las cargas de trabajo. Puede soportar cargas de trabajo como el machine learning, la computación de alto rendimiento (HPC), el procesamiento de vídeo, la modelización financiera y la Electronic Design Automation (EDA). Estas cargas de trabajo suelen requerir que los datos se presenten mediante una interfaz de sistema de archivos de escalabilidad y de alta velocidad para el acceso a los datos. A menudo, los conjuntos de datos que se utilizan para estas cargas de trabajo se almacenan en repositorios de datos de largo plazo en Amazon S3. FSx para Lustre está integrado de forma nativa con Amazon S3, lo que facilita el procesamiento de conjuntos de datos con el sistema de archivos Lustre.

> **Note**
>
> Las copias de seguridad de los sistemas de archivos no se admiten en los sistemas de archivos que están vinculados a un repositorio de datos. Para más información, consulte Trabajo con copias de seguridad.

Temas

# Información general de los repositorios de datos

Cuando utiliza Amazon FSx para Lustre con repositorios de datos, puede ingresar y procesar grandes volúmenes de datos de archivos en un sistema de archivos de alto rendimiento mediante tareas de importación e importación automáticas de repositorios de datos. Al mismo tiempo, puede escribir los resultados en sus repositorios de datos mediante tareas automáticas de exportación o exportación de repositorios de datos. Con estas características, puede reiniciar su carga de trabajo en cualquier momento utilizando los datos más recientes almacenados en su repositorio de datos.

> **Note**
>
> Las asociaciones de repositorios de datos, la exportación automática y la compatibilidad con varios repositorios de datos no están disponibles en los sistemas de archivos FSx para Lustre 2.10 o los sistemas de archivo `Scratch 1`.

FSx para Lustre está profundamente integrado con Amazon S3. Esta integración significa que puede acceder sin problemas a los objetos almacenados en sus buckets de Amazon S3 desde las aplicaciones que montan su sistema de archivos FSx para Lustre. También puede ejecutar sus cargas de trabajo de procesamiento intensivo en instancias de Amazon EC2 en Nube de AWS y exportar los resultados a su repositorio de datos una vez finalizada la carga de trabajo.

Para acceder a los objetos del repositorio de datos de Amazon S3 como archivos y directorios del sistema de archivos, los metadatos de los archivos y directorios deben cargarse en el sistema de archivos. Puede cargar metadatos desde un repositorio de datos vinculado al crear una asociación de repositorios de datos.

Además, puede importar metadatos de archivos y directorios de sus repositorios de datos vinculados al sistema de archivos mediante la importación automática o mediante una tarea de importación del repositorio de datos. Al activar la importación automática para una asociación de repositorios de datos, el sistema de archivos importa automáticamente los metadatos de los archivos a medida que se crean, modifican o eliminan archivos en el repositorio de datos de S3. Como alternativa, puede importar metadatos para archivos y directorios nuevos o modificados mediante una tarea de importación del repositorio de datos.

> **Note**
>
> Las tareas automáticas de importación e importación del repositorio de datos se pueden utilizar simultáneamente en un sistema de archivos.

También puede exportar los archivos y los metadatos asociados del sistema de archivos al repositorio de datos mediante la exportación automática o mediante una tarea de exportación del repositorio de datos. Al activar la exportación automática en una asociación de repositorio de datos, el sistema de archivos exporta automáticamente los datos y metadatos de los archivos cuando estos se crean, modifican o eliminan. Como alternativa, puede exportar archivos o directorios mediante una tarea de exportación de repositorios de datos. Cuando utiliza una tarea de repositorio de datos de exportación, se exportan los datos y metadatos de los archivos que se crearon o modificaron desde la última tarea de este tipo.

> **Note**
>
> - Las tareas de exportación automática y exportación de repositorio de datos no pueden utilizarse simultáneamente en un sistema de archivos.
> - Las asociaciones de repositorios de datos solo exportan archivos, enlaces simbólicos y directorios normales. Esto significa que todos los demás tipos de archivos (FIFO especial, bloque especial, especial de caracteres y conector) no se exportarán como parte de los procesos de exportación, como las tareas automáticas de exportación y exportación del repositorio de datos.

FSx para Lustre también admite cargas de trabajo de ampliación en la nube con sistemas de archivos en las instalaciones, ya que permite copiar datos de clientes en las instalaciones mediante AWS Direct Connect o VPN.

> **Important**
>
> Si ha vinculado uno o más sistemas de archivos FSx para Lustre a un repositorio de datos en Amazon S3, no elimine el bucket de Amazon S3 hasta que haya eliminado o desvinculado todos los sistemas de archivos enlazados.

# Soporte de metadatos POSIX para repositorios de datos

Amazon FSx para Lustre transfiere automáticamente los metadatos de la Interfaz de Sistema Operativo Portátil (POSIX) para archivos, directorios y enlaces simbólicos (enlaces simbólicos) al importar y exportar datos a y desde un repositorio de datos enlazados en Amazon S3. Al exportar los cambios del sistema de archivos a su repositorio de datos vinculado, FSx para Lustre también exporta los cambios en los metadatos POSIX como metadatos de objetos S3. Esto significa que si otro sistema de archivos FSx para Lustre importa los mismos archivos de S3, los archivos tendrán los mismos metadatos POSIX en ese sistema de archivos, incluidos la propiedad y los permisos.

FSx para Lustre importa solo objetos de S3 que tienen claves de objeto compatibles con POSIX, como las siguientes.

```
mydir/
mydir/myfile1
mydir/mysubdir/
mydir/mysubdir/myfile2.txt
```

FSx para Lustre almacena los directorios y enlaces simbólicos como objetos independientes en el repositorio de datos enlazados de S3. En el caso de los directorios, FSx para Lustre crea un objeto S3 con un nombre clave que termina con una barra diagonal (“/”), de la siguiente manera:

- La clave de objeto S3 `mydir/` se asigna al directorio FSx para Lustre `mydir/`.
- La clave de objeto S3 `mydir/mysubdir/` se asigna al directorio FSx para Lustre `mydir/mysubdir/`.

Para los enlaces simbólicos, FSx para Lustre utiliza el siguiente esquema de Amazon S3:

- Clave de objeto S3: la ruta al enlace, relativa al directorio de montaje de FSx para Lustre
- Datos del objeto S3: la ruta de destino de este enlace simbólico
- Metadatos del objeto S3: los metadatos del enlace simbólico

FSx para Lustre almacena los metadatos POSIX, incluida la propiedad, los permisos y las marcas de tiempo de los archivos, directorios y enlaces simbólicos, en objetos S3 de la siguiente manera:

- `Content-Type`: el encabezado de la entidad HTTP que se utiliza para indicar el tipo de medio del recurso para los navegadores web.

- `x-amz-meta-file-permissions`: el tipo de archivo y los permisos del formato `<octal file type><octal permission mask>`, de acuerdo con los `st_mode` de la Página del manual de Linux stat (2).

  > **Note**
  >
  > FSx para Lustre no importa ni retiene información `setuid`.

- `x-amz-meta-file-owner`: el ID de usuario (UID) del propietario expresado en forma de número entero.
- `x-amz-meta-file-group`: el ID de grupo (GID) expresado en forma de número entero.
- `x-amz-meta-file-atime`: el tiempo de acceso por última vez en nanosegundos desde el comienzo de la era de Unix. Termine el valor de tiempo con `ns`; de lo contrario, FSx para Lustre interpreta el valor como milisegundos.
- `x-amz-meta-file-mtime`: el tiempo de la última modificación en nanosegundos desde el comienzo de la era de Unix. Termine el valor de tiempo con `ns`; de lo contrario, FSx para Lustre interpreta el valor como milisegundos.
- `x-amz-meta-user-agent`: el agente de usuario, ignorado durante la importación de FSx para Lustre. Durante la exportación, FSx para Lustre establece este valor en `aws-fsx-lustre`.

Al importar objetos de S3 que no tienen permisos POSIX asociados, el permiso POSIX predeterminado que FSx para Lustre asigna a un archivo es `755`. Este permiso permite el acceso de lectura y ejecución para todos los usuarios y el acceso de escritura para el propietario del archivo.

> **Note**
>
> FSx para Lustre no retiene ningún metadato personalizado definido por el usuario en los objetos de S3.

## Enlaces duros y exportación a S3

Si la exportación automática (con políticas NUEVAS y CAMBIADAS) está habilitada en una DRA de su sistema de archivos, cada enlace duro contenido en la DRA se exporta a Amazon S3 como un objeto S3 independiente para cada enlace duro. Si se modifica un archivo con varios enlaces duros

en el sistema de archivos, se actualizan todas las copias de S3, independientemente del enlace duro que se haya utilizado al cambiar el archivo.

Si los enlaces duros se exportan a S3 mediante tareas de repositorio de datos (DRT), cada enlace físico contenido en las rutas especificadas para el DRT se exporta a S3 como un objeto S3 independiente para cada enlace duro. Si se modifica un archivo con varios enlaces duros en el sistema de archivos, se actualizan todas las copias en S3 en el momento en que se exporta el enlace duro respectivo, independientemente del enlace duro que se haya utilizado al modificar el archivo.

> **Important**
>
> Cuando un nuevo sistema de archivos FSx para Lustre se vincula a un bucket de S3 al que anteriormente otro sistema de archivos FSx para Lustre, AWS DataSync o puerta de enlace de archivo Amazon FSx exportaba previamente los enlaces duros, los enlaces duros se importan posteriormente como archivos independientes en el nuevo sistema de archivos.

## Enlaces duros y archivos liberados

Un archivo liberado es un archivo cuyos metadatos están presentes en el sistema de archivos, pero cuyo contenido solo se almacena en S3. Para más información sobre los archivos liberados, consulte Liberación de archivos.

> **Important**
>
> El uso de enlaces duros en un sistema de archivos que tiene asociaciones de repositorios de datos (DRA) está sujeto a las siguientes limitaciones:
>
> - Al eliminar y volver a crear un archivo liberado que tiene varios enlaces duros, es posible que se sobrescriba el contenido de todos los enlaces duros.
> - Al eliminar un archivo liberado, se eliminará el contenido de todos los enlaces duros que se encuentren fuera de una asociación de repositorios de datos.
> - La creación de un enlace duro a un archivo liberado cuyo objeto S3 correspondiente se encuentre en las clases de almacenamiento S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive no creará un objeto nuevo en S3 para el enlace duro.

# Tutorial: adjuntar permisos POSIX al cargar objetos a un bucket de Amazon S3

El siguiente procedimiento presenta el proceso de carga de objetos en Amazon S3 con permisos POSIX. De este modo, podrá importar los permisos POSIX al crear un sistema de archivos Amazon FSx vinculado a ese bucket de S3.

Para cargar objetos con permisos POSIX a Amazon S3

1. Desde su ordenador o máquina local, utilice los siguientes comandos de ejemplo para crear un directorio de prueba (`s3cptestdir`) y un archivo (`s3cptest.txt`) que se cargarán en el bucket de S3.

   ```
   $ mkdir s3cptestdir
   $ echo "S3cp metadata import test" >> s3cptestdir/s3cptest.txt
   $ ls -ld s3cptestdir/ s3cptestdir/s3cptest.txt
   drwxr-xr-x 3 500 500 96 Jan 8 11:29 s3cptestdir/
   -rw-r--r-- 1 500 500 26 Jan 8 11:29 s3cptestdir/s3cptest.txt
   ```

   El archivo y el directorio recién creados tienen un ID de usuario (UID) y un ID de grupo (GID) del propietario del archivo de 500 y los permisos que se muestran en el ejemplo anterior.

2. Llame a la API de Amazon S3 para crear el directorio `s3cptestdir` con permisos de metadatos. Debe especificar el nombre del directorio con una barra diagonal (/) al final. Para obtener información acerca de los metadatos POSIX soportados, consulte Soporte de metadatos POSIX para repositorios de datos.

   Reemplace *bucket_name* con el nombre real de su bucket de Amazon S3.

   ```
   $ aws s3api put-object --bucket bucket_name --key s3cptestdir/ --metadata '{"user-
   agent":"aws-fsx-lustre" , \
         "file-atime":"1595002920000000000ns" , "file-owner":"500" , "file-
   permissions":"0100664","file-group":"500" , \
         "file-mtime":"1595002920000000000ns"}'
   ```

3. Compruebe que los permisos POSIX estén etiquetados en los metadatos del objeto S3.

   ```
   $ aws s3api head-object --bucket bucket_name --key s3cptestdir/
   {
       "AcceptRanges": "bytes",
       "LastModified": "Fri, 08 Jan 2021 17:32:27 GMT",
   ```

```
    "ContentLength": 0,
    "ETag": "\"d41d8cd98f00b204e9800998ecf8427e\"",
    "VersionId": "bAlhCoWq7aIEjc3R6Myc6UOb8sHHtJkR",
    "ContentType": "binary/octet-stream",
    "Metadata": {
        "user-agent": "aws-fsx-lustre",
        "file-atime": "1595002920000000000ns",
        "file-owner": "500",
        "file-permissions": "0100664",
        "file-group": "500",
        "file-mtime": "1595002920000000000ns"
    }
}
```

4. Cargue el archivo de prueba (creado en el paso 1) desde su ordenador al bucket de S3 con permisos de metadatos.

```
$ aws s3 cp s3cptestdir/s3cptest.txt s3://bucket_name/s3cptestdir/s3cptest.txt \
      --metadata '{"user-agent":"aws-fsx-lustre" , "file-
atime":"1595002920000000000ns" , \
      "file-owner":"500" , "file-permissions":"0100664","file-group":"500" , "file-
mtime":"1595002920000000000ns"}'
```

5. Compruebe que los permisos POSIX estén etiquetados en los metadatos del objeto S3.

```
$ aws s3api head-object --bucket bucket_name --key s3cptestdir/s3cptest.txt
{
    "AcceptRanges": "bytes",
    "LastModified": "Fri, 08 Jan 2021 17:33:35 GMT",
    "ContentLength": 26,
    "ETag": "\"eb33f7e1f44a14a8e2f9475ae3fc45d3\"",
    "VersionId": "w9ztRoEhB832m8NC3a_JTlTyIx7Uzql6",
    "ContentType": "text/plain",
    "Metadata": {
        "user-agent": "aws-fsx-lustre",
        "file-atime": "1595002920000000000ns",
        "file-owner": "500",
        "file-permissions": "0100664",
        "file-group": "500",
        "file-mtime": "1595002920000000000ns"
    }
}
```

6. Compruebe los permisos en el sistema de archivos Amazon FSx vinculado al bucket de S3.

```
$ sudo lfs df -h /fsx
UUID                       bytes        Used   Available Use% Mounted on
3rnxfbmv-MDT0000_UUID       34.4G        6.1M       34.4G   0% /fsx[MDT:0]
3rnxfbmv-OST0000_UUID        1.1T        4.5M        1.1T   0% /fsx[OST:0]

filesystem_summary:          1.1T        4.5M        1.1T   0% /fsx

$ cd /fsx/s3cptestdir/
$ ls -ld s3cptestdir/
drw-rw-r-- 2 500 500 25600 Jan  8 17:33 s3cptestdir/

$ ls -ld s3cptestdir/s3cptest.txt
-rw-rw-r-- 1 500 500 26 Jan 8 17:33 s3cptestdir/s3cptest.txt
```

Tanto el directorio `s3cptestdir` como el archivo `s3cptest.txt` tienen permisos POSIX importados.

## Vincular su sistema de archivos a un bucket de S3

Puede vincular su sistema de archivos de Amazon FSx para Lustre con los repositorios de datos de Amazon S3. Puede crear el enlace al crear el sistema de archivos o en cualquier momento después de crearlo.

Un vínculo entre un directorio del sistema de archivos y un bucket o prefijo de S3 se denomina asociación de repositorio de datos (DRA). Puede configurar un máximo de 8 asociaciones de repositorios de datos en un sistema de ficheros FSx para Lustre. Se pueden poner en cola un máximo de 8 solicitudes de DRA, pero solo se puede trabajar con una solicitud a la vez para el sistema de archivos. Cada DRA debe tener un único directorio de sistema de archivos FSx para Lustre y un único bucket de S3 o prefijo asociado a él.

> **Note**
>
> Las asociaciones de repositorios de datos, la exportación automática y la compatibilidad con varios repositorios de datos no están disponibles en los sistemas de archivos FSx para Lustre 2.10 o los sistemas de archivo `Scratch 1`.

Para acceder a los objetos del repositorio de datos S3 como archivos y directorios en el sistema de archivos, los metadatos de archivos y directorios deben cargarse en el sistema de archivos. Puede cargar los metadatos de un repositorio de datos vinculado al crear la DRA o cargar los metadatos de los lotes de archivos y directorios a los que desee acceder mediante el sistema de archivos FSx para Lustre más adelante mediante una tarea de importación de repositorio de datos, o utilizar la exportación automática para cargar los metadatos automáticamente cuando se añaden, modifican o eliminan objetos del repositorio de datos.

Puede configurar una DRA solo para la importación automática, solo para la exportación automática o para ambas. Una asociación de repositorios de datos configurada con importación y exportación automáticas propaga los datos en ambas direcciones entre el sistema de archivos y el bucket de S3 vinculado. A medida que realiza cambios en los datos del repositorio de datos de S3, FSx para Lustre detecta los cambios y, a continuación, los importa automáticamente a su sistema de archivos. A medida que crea, modifica o elimina archivos, FSx para Lustre exporta automáticamente los cambios a Amazon S3 de forma asíncrona una vez que su aplicación termina de modificar el archivo.

> **Important**
>
> - Si modifica el mismo archivo tanto en el sistema de archivos como en el bucket de S3, debe garantizar la coordinación a nivel de la aplicación para evitar conflictos. FSx para Lustre no evita escrituras conflictivas en varias ubicaciones.
> - En el caso de los archivos marcados con un atributo inmutable, FSx para Lustre no puede sincronizar los cambios entre su sistema de archivos FSx para Lustre y un bucket de S3 vinculado al sistema de archivos. Si se establece un indicador inmutable durante un período de tiempo prolongado, se puede reducir el rendimiento del movimiento de datos entre Amazon FSx y S3.

Al crear una asociación de repositorios de datos, puede configurar las siguientes propiedades:

- Ruta del sistema de archivos: introduzca una ruta local en el sistema de archivos que apunte a un directorio (por ejemplo`/ns1/`) o subdirectorio (por ejemplo`/ns1/subdir/`) que se asignará one-to-one con la ruta del repositorio de datos especificada a continuación. Se requiere la barra diagonal que aparece al principio del nombre. Dos asociaciones de repositorios de datos no pueden tener rutas de sistema de archivos superpuestas. Por ejemplo, si un repositorio de datos está asociado a la ruta del sistema de archivos `/ns1`, no se puede vincular otro repositorio de datos con la ruta del sistema de archivos `/ns1/ns2`.

> **Note**
>
> Si especifica solo una barra diagonal (/) como ruta del sistema de archivos, a este solo se puede vincular un repositorio de datos. Solo puede especificar "/" como la ruta del sistema de archivos del primer repositorio de datos asociado a un sistema de archivos.

- Data repository path: introduzca una ruta en el repositorio de datos de S3. La ruta puede ser un bucket de S3 o un prefijo con el formato `s3://myBucket/myPrefix/`. Esta propiedad especifica desde qué parte del repositorio de datos S3 se importarán o exportarán los archivos. FSx para Lustre añadirá una "/" final a la ruta del repositorio de datos si no la proporciona. Por ejemplo, si proporciona una ruta de repositorio de datos de `s3://myBucket/myPrefix`, FSx para Lustre la interpretará como `s3://myBucket/myPrefix/`.

  Dos asociaciones de repositorios de datos no pueden tener rutas de repositorios de datos superpuestas. Por ejemplo, si un repositorio de datos con la ruta `s3://myBucket/myPrefix/` está vinculado al sistema de archivos, no se puede crear otra asociación de repositorio de datos con la ruta de repositorio de datos `s3://myBucket/myPrefix/mySubPrefix`.
- Import metadata from repository: puede seleccionar esta opción para importar metadatos de todo el repositorio de datos inmediatamente después de crear la asociación de repositorios de datos. Como alternativa, puede ejecutar una tarea de importación del repositorio de datos para cargar todos o un subconjunto de los metadatos del repositorio de datos vinculado al sistema de archivos en cualquier momento después de crear la asociación de repositorios de datos.
- Import settings: elija una política de importación que especifique el tipo de objetos actualizados (cualquier combinación de objetos nuevos, modificados y eliminados) que se importarán automáticamente desde el bucket de S3 vinculado a su sistema de archivos. La importación automática (nueva, modificada, eliminada) se activa de forma predeterminada cuando se añade un repositorio de datos desde la consola, pero se desactiva de forma predeterminada cuando se utiliza la AWS CLI o la API de Amazon FSx.
- Export settings: elija una política de exportación que especifique el tipo de objetos actualizados (cualquier combinación de nuevos, modificados y eliminados) que se exportarán automáticamente al bucket de S3. La exportación automática (nuevos, modificados, eliminados) se activa de forma predeterminada al añadir un repositorio de datos desde la consola, pero se desactiva de forma predeterminada al utilizar la AWS CLI o la API de Amazon FSx.

La configuración de la File system path y la Data repository path proporcionan un mapeo 1:1 entre las rutas de Amazon FSx y las claves de objeto de S3.

## Soporte regional y de cuenta para los buckets de S3 enlazados

Al crear enlaces a buckets de S3, tenga en cuenta las siguientes limitaciones de compatibilidad de cuentas y regiones:

- La exportación automática admite configuraciones entre regiones. El sistema de archivos Amazon FSx y el bucket de S3 vinculado pueden estar ubicados en la misma Región de AWS o en una Regiones de AWS distinta.
- La importación automática no admite configuraciones entre regiones. Tanto el sistema de archivos de Amazon FSx como el bucket de S3 vinculado deben estar ubicados en la misma Región de AWS.
- Tanto la exportación automática como la importación automática admiten configuraciones entre cuentas. El sistema de archivos Amazon FSx y el bucket de S3 vinculado pueden estar ubicados en la misma Cuenta de AWS o en una Cuentas de AWS distinta.

## Crear un enlace a un bucket de S3

Los siguientes procedimientos le guiarán por el proceso de creación de una asociación de repositorios de datos para un sistema de archivos FSx para Lustre con un bucket de S3 existente, mediante la AWS Management Console y la AWS Command Line Interface (AWS CLI). Para obtener información sobre cómo añadir permisos a un bucket de S3 para vincularlo a su sistema de archivos, consulte Agregar permisos para utilizar repositorios de datos en Amazon S3.

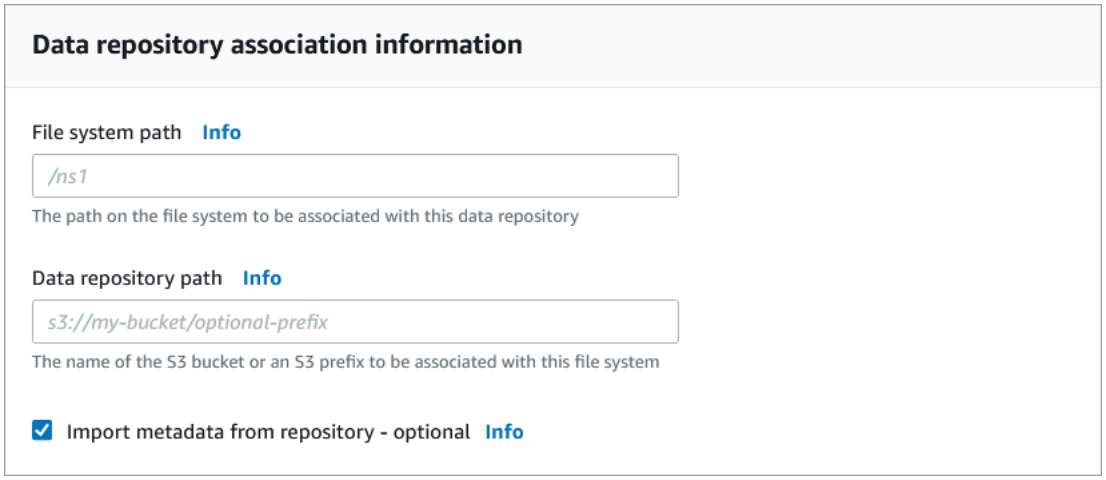
> **Note**
>
> Los repositorios de datos no se pueden vincular a sistemas de archivos que tengan habilitadas las copias de seguridad del sistema de archivos. Deshabilite las copias de seguridad antes de vincularlas a un repositorio de datos.

Para vincular un bucket de S3 al crear un sistema de archivos (consola)

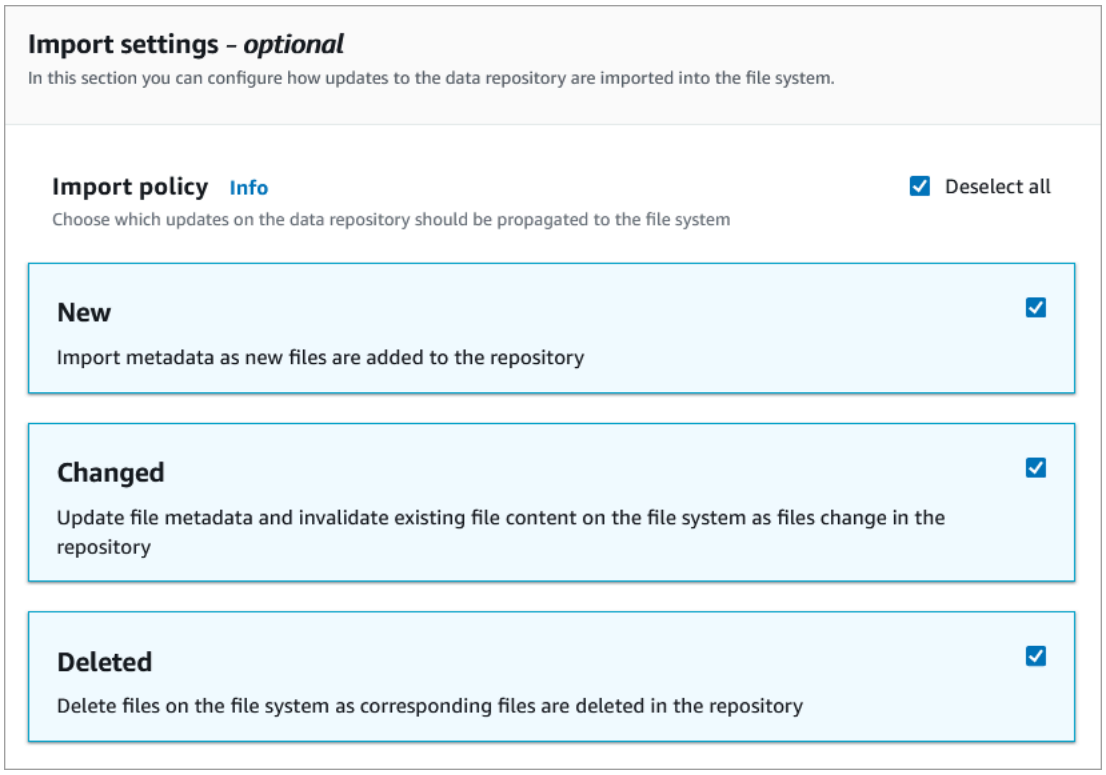
1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Siga el procedimiento para crear un nuevo sistema de archivos que se describe en Cree su sistema de archivos FSx for Lustre en la sección Primeros pasos.

3. Abra la sección Data Repository Import/Export - optional. De forma predeterminada, esta característica está deshabilitada.
4. Elija Import data from and export data to S3.
5. En el cuadro de diálogo de Data repository association information, proporcione información para los siguientes campos.

   - File system path: introduzca el nombre de un directorio de alto nivel (como `/ns1`) o subdirectorio (como `/ns1/subdir`) dentro del sistema de archivos de Amazon FSx que se asociará con el repositorio de datos de S3. Se requiere la barra diagonal inicial en la ruta. Dos asociaciones de repositorios de datos no pueden tener rutas de sistema de archivos superpuestas. Por ejemplo, si un repositorio de datos está asociado a la ruta del sistema de archivos `/ns1`, no se puede vincular otro repositorio de datos con la ruta del sistema de archivos `/ns1/ns2`. La configuración de la File system path debe ser única en todas las asociaciones de repositorios de datos del sistema de archivos.
   - Data repository path: introduzca la ruta de un bucket o prefijo de S3 existente para asociarlo a su sistema de archivos (por ejemplo, `s3://my-bucket/my-prefix/`). Dos asociaciones de repositorios de datos no pueden tener rutas de repositorios de datos superpuestas. Por ejemplo, si un repositorio de datos con la ruta `s3://myBucket/myPrefix/` está vinculado al sistema de archivos, no se puede crear otra asociación de repositorio de datos con la ruta de repositorio de datos `s3://myBucket/myPrefix/mySubPrefix`. La configuración de la File system path debe ser única en todas las asociaciones de repositorios de datos del sistema de archivos.
   - Import metadata from repository: seleccione esta propiedad para ejecutar, de manera opcional, una tarea de importación de repositorios de datos para importar metadatos inmediatamente después de crear el vínculo.

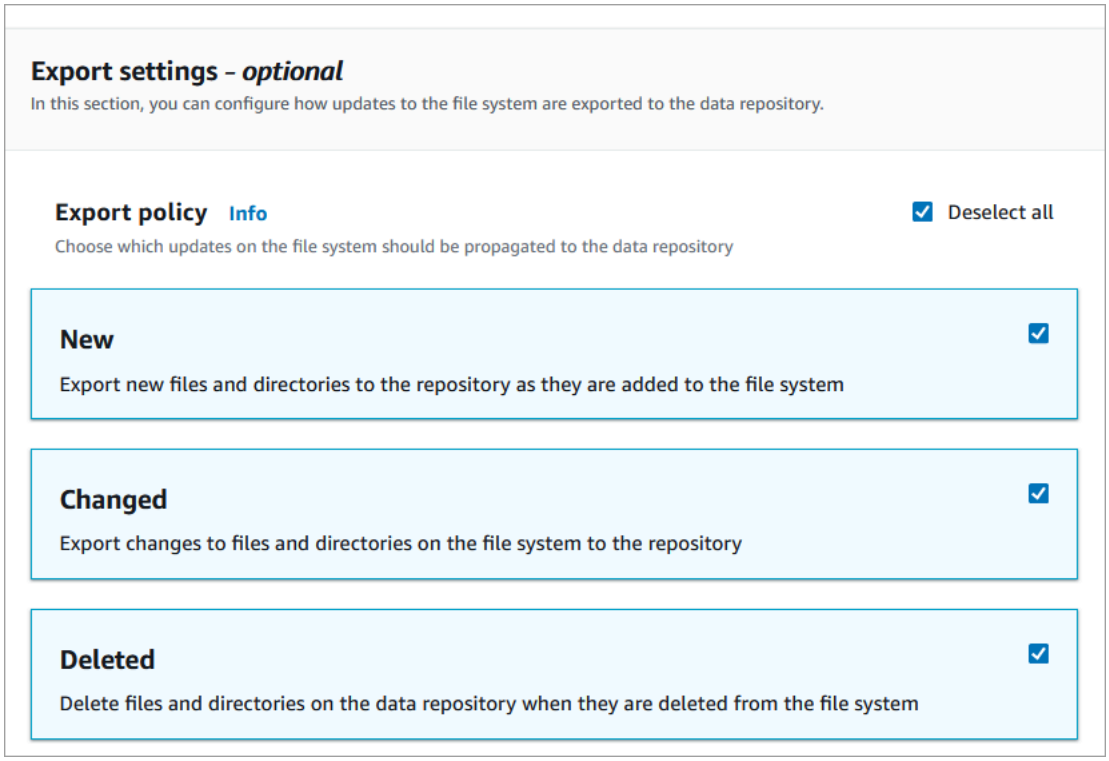



6. En el caso de los Import settings - optional, defina Import Policy que determine cómo se mantienen actualizados los listados de archivos y directorios al añadir, cambiar o eliminar objetos del bucket de S3. Por ejemplo, elija New para importar los metadatos a su sistema de archivos para los nuevos objetos creados en el bucket de S3. Para obtener más información sobre las políticas de importación, consulte Importe automáticamente actualizaciones desde un bucket de S3.




7. Para Export policy, defina una política de exportación que determine cómo se exportarán sus archivos al bucket de S3 vinculado a medida que añada, modifique o elimine objetos del sistema

de archivos. Por ejemplo, elija Changed para exportar los objetos cuyo contenido o metadatos se hayan modificado en su sistema de archivos. Para obtener más información acerca de las políticas de exportación, consulte Exporte automáticamente las actualizaciones a su bucket de S3.




8. Continúe con la siguiente sección del asistente de creación del sistema de archivos.

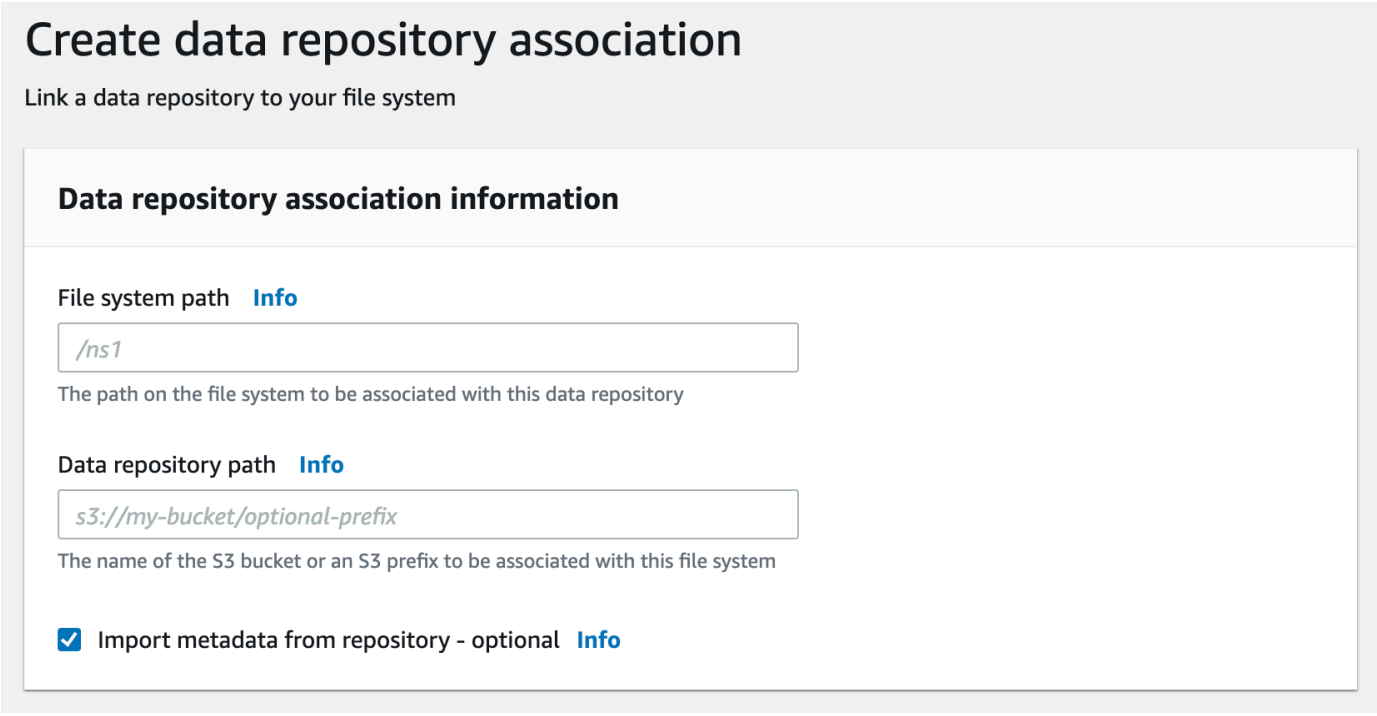
Para vincular un bucket de S3 a un sistema de archivos existente (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel, elija File systems y, a continuación, seleccione el sistema de archivos para el que desee crear una asociación de repositorios de datos.
3. Seleccione la pestaña Data repository.
4. En el panel Data repository associations, elija Create data repository association.
5. En el cuadro de diálogo de Data repository association information, proporcione información para los siguientes campos.

   - File system path: introduzca el nombre de un directorio de alto nivel (como `/ns1`) o subdirectorio (como `/ns1/subdir`) dentro del sistema de archivos de Amazon FSx que se asociará con el repositorio de datos de S3. Se requiere la barra diagonal inicial en la ruta. Dos asociaciones de repositorios de datos no pueden tener rutas de sistema de archivos

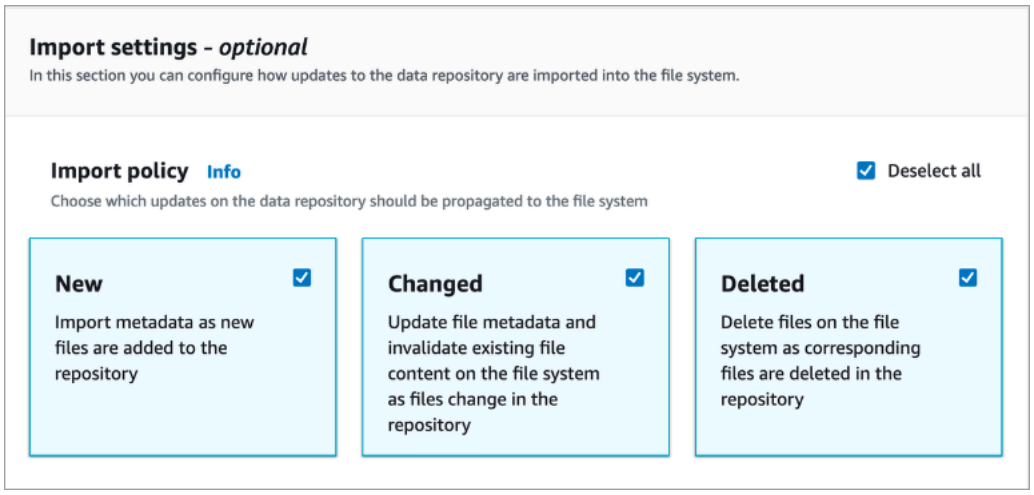
superpuestas. Por ejemplo, si un repositorio de datos está asociado a la ruta del sistema de archivos `/ns1`, no se puede vincular otro repositorio de datos con la ruta del sistema de archivos `/ns1/ns2`. La configuración de la File system path debe ser única en todas las asociaciones de repositorios de datos del sistema de archivos.

- Data repository path: introduzca la ruta de un bucket o prefijo de S3 existente para asociarlo a su sistema de archivos (por ejemplo, `s3://my-bucket/my-prefix/`). Dos asociaciones de repositorios de datos no pueden tener rutas de repositorios de datos superpuestas. Por ejemplo, si un repositorio de datos con la ruta `s3://myBucket/myPrefix/` está vinculado al sistema de archivos, no se puede crear otra asociación de repositorio de datos con la ruta de repositorio de datos `s3://myBucket/myPrefix/mySubPrefix`. La configuración de la File system path debe ser única en todas las asociaciones de repositorios de datos del sistema de archivos.
- Import metadata from repository: seleccione esta propiedad para ejecutar, de manera opcional, una tarea de importación de repositorios de datos para importar metadatos inmediatamente después de crear el vínculo.

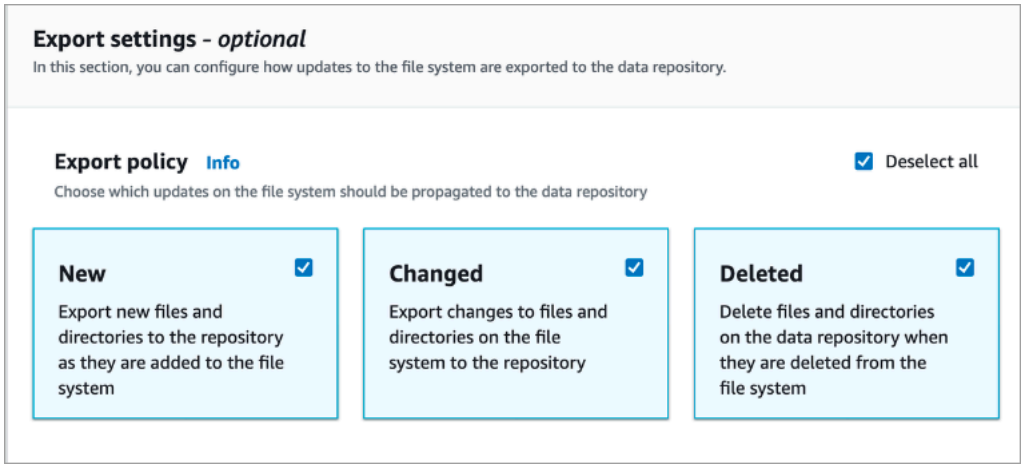



6. En el caso de los Import settings - optional, defina Import Policy que determine cómo se mantienen actualizados los listados de archivos y directorios al añadir, cambiar o eliminar objetos del bucket de S3. Por ejemplo, elija New para importar los metadatos a su sistema de archivos para los nuevos objetos creados en el bucket de S3. Para obtener más información

acerca de las políticas de importación, consulte Importe automáticamente actualizaciones desde un bucket de S3.




7. Para Export policy, defina una política de exportación que determine cómo se exportarán sus archivos al bucket de S3 vinculado a medida que añada, modifique o elimine objetos del sistema de archivos. Por ejemplo, elija Changed para exportar los objetos cuyo contenido o metadatos se hayan modificado en su sistema de archivos. Para obtener más información acerca de las políticas de exportación, consulte Exporte automáticamente las actualizaciones a su bucket de S3.




8. Elija Create.

Para vincular su sistema de archivos a un bucket de S3 (AWS CLI)

El siguiente ejemplo crea una asociación de repositorios de datos que vincula un sistema de archivos Amazon FSx a un bucket de S3, con una política de importación que importa todos los archivos nuevos o modificados al sistema de archivos y una política de exportación que exporta los archivos nuevos, modificados o eliminados al bucket de S3 vinculado.

- Para crear una asociación de repositorios de datos, utilice el comando de la CLI de Amazon FSx `create-data-repository-association`, como se muestra a continuación.

```
$ aws fsx create-data-repository-association \
      --file-system-id fs-0123456789abcdef0 \
      --file-system-path /ns1/path1/ \
      --data-repository-path s3://mybucket/myprefix/ \
      --s3
 "AutoImportPolicy={Events=[NEW,CHANGED,DELETED]},AutoExportPolicy={Events=[NEW,CHANGED,DEL
```

Amazon FSx devuelve inmediatamente la descripción en formato JSON de la DRA. La DRA se crea de forma asíncrona.

Puede utilizar este comando para crear una asociación de repositorios de datos incluso antes de que el sistema de archivos haya terminado de crearse. La solicitud se pondrá en cola y la asociación de repositorios de datos se creará cuando el sistema de archivos esté disponible.

## Actualización de la configuración de asociación de repositorios de datos

Puede actualizar la configuración de una asociación de repositorios de datos existente mediante la AWS Management Console, la AWS CLI y la API de Amazon FSx, tal y como se muestra en los siguientes procedimientos.

> **Note**
>
> No puede actualizar la `File system path` o la `Data repository path` de una DRA una vez creado. Si desea cambiar la `File system path` o la `Data repository path`, debe eliminar la DRA y volver a crearlo.

Para actualizar la configuración de una asociación de repositorios de datos existente (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel, elija File systems y, a continuación, seleccione el sistema de archivos que desea administrar.
3. Elija la pestaña Data repository.
4. En el panel Data repository associations, elija la asociación de repositorios de datos que desea modificar.

5. Elija Update. Aparece un cuadro de diálogo de edición para la asociación del repositorio de datos.
6. Para Import settings - optional, puede actualizar su Import Policy. Para obtener más información sobre las políticas de importación, consulte Importe automáticamente actualizaciones desde un bucket de S3.
7. Para Export settings - optional, puede actualizar su política de exportación. Para más información sobre políticas de exportación, consulte Exporte automáticamente las actualizaciones a su bucket de S3.
8. Seleccione Actualizar.

Para actualizar la configuración de una asociación de repositorios de datos existente (CLI)

- Para actualiza una asociación de repositorios de datos, utilice el comando de la CLI de Amazon FSx `update-data-repository-association`, como se muestra a continuación.

```
$ aws fsx update-data-repository-association \
      --association-id 'dra-872abab4b4503bfc2' \
      --s3
 "AutoImportPolicy={Events=[NEW,CHANGED,DELETED]},AutoExportPolicy={Events=[NEW,CHANGED,DEL
```

Después de actualizar correctamente las políticas de importación y exportación de la asociación de repositorios de datos, Amazon FSx devuelve la descripción de la asociación de repositorios de datos actualizada en formato JSON.

## Eliminación de una asociación a un bucket de S3

Los siguientes procedimientos le guiarán a través del proceso de eliminación de una asociación de repositorio de datos de un sistema de archivos de Amazon FSx existente a un bucket de S3 existente, mediante la AWS Management Console y la AWS Command Line Interface (AWS CLI). Al eliminar la asociación de repositorios de datos, se desvincula el sistema de archivos del bucket de S3.

Para eliminar un vínculo de un sistema de archivos a un bucket de S3 (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel, elija File systems y, a continuación, seleccione el sistema de archivos del que desee eliminar una asociación de repositorios de datos.

3. Elija la pestaña Data repository.
4. En el panel Data repository associations, elija la asociación de repositorios de datos que desea eliminar.
5. En Actions, elija Delete association.
6. (Opcional) En el cuadro de diálogo Delete, puede elegir Delete data in file system para eliminar físicamente los datos del sistema de archivos que corresponden a la asociación del repositorio de datos.
7. Elija Delete para eliminar la asociación de repositorios de datos del sistema de archivos.

Para eliminar un vínculo de un sistema de archivos a un bucket de S3 (AWS CLI)

En el siguiente ejemplo, se elimina una asociación de repositorios de datos que vincula un sistema de archivos Amazon FSx a un bucket de S3. El parámetro `--association-id` especifica el ID de la asociación de repositorios de datos que se va a eliminar.

- Para eliminar una asociación de repositorios de datos, utilice el comando de la CLI de Amazon FSx `delete-data-repository-association`, como se muestra a continuación.

```
$ aws fsx delete-data-repository-association \
      --association-id dra-872abab4b4503bfc \
      --delete-data-in-file-system false
```

Después de eliminar correctamente la asociación de repositorios de datos, Amazon FSx devuelve su descripción en formato JSON.

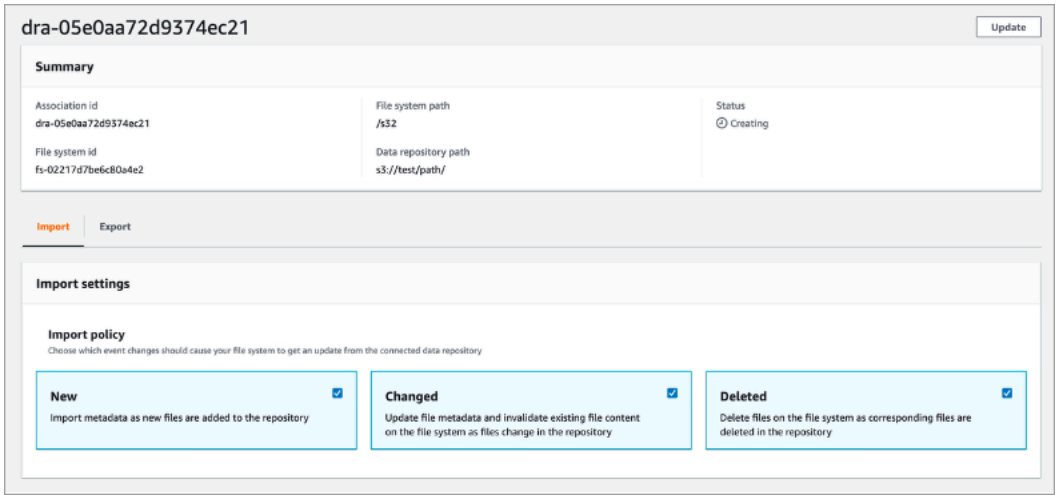
## Visualización de los detalles de asociación del repositorio de datos

Puede ver los detalles de una asociación de repositorios de datos con la consola de FSx para Lustre, la AWS CLI y la API. Los detalles incluyen el ID de asociación de la DRA, la ruta del sistema de archivos, la ruta del repositorio de datos, la configuración de importación, la configuración de exportación, el estado y el ID del sistema de archivos asociado.

Para ver los detalles de la DRA (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel, elija File systems y, a continuación, seleccione el sistema de archivos del que desee ver los detalles de una asociación de repositorios de datos.

3. Elija la pestaña Data repository.
4. En el panel Data repository associations, elija la asociación de repositorios de datos que desea ver. Aparece la página de Summary, que muestra los detalles de la DRA.




Para ver los detalles de la DRA (CLI)

- Para ver los detalles de una asociación de repositorio de datos específica, utilice el comando CLI de Amazon FSx `describe-data-repository-associations`, como se muestra a continuación.

```
$ aws fsx describe-data-repository-associations \
      --association-ids dra-872abab4b4503bfc2
```

  Amazon FSx devuelve la descripción de la asociación del repositorio de datos en formato JSON.

## Estado del ciclo de vida de la asociación de repositorios

El estado del ciclo de vida de la asociación del repositorio de datos proporciona información de estado sobre una DRA específica. Una asociación de repositorios de datos puede tener los siguientes Lifecycle states:

- Creating: Amazon FSx crea la asociación de repositorios de datos entre el sistema de archivos y el repositorio de datos vinculado. El repositorio de datos no está disponible.
- Available: la asociación de repositorios de datos está disponible para su uso.
- Updating: la asociación de repositorios de datos está siendo objeto de una actualización iniciada por el cliente que podría afectar a su disponibilidad.

- Deleting: se está procediendo a una eliminación de la asociación de repositorios de datos iniciada por el cliente.
- Misconfigured: Amazon FSx no puede importar automáticamente las actualizaciones del bucket de S3 ni exportarlas automáticamente al bucket de S3 hasta que se corrija la configuración de asociación del repositorio de datos.
- Failed: la asociación del repositorio de datos está en un estado terminal que no se puede recuperar (por ejemplo, porque se elimina la ruta del sistema de archivos o se elimina el bucket de S3).

Puede ver el estado del ciclo de vida de una asociación de repositorios de datos mediante la consola de Amazon FSx, la AWS Command Line Interface y la API de Amazon FSx. Para más información, consulte Visualización de los detalles de asociación del repositorio de datos.

## Trabajo con buckets de Amazon S3 cifrados del lado del servidor

FSx para Lustre admite buckets de Amazon S3 que utilizan cifrado del lado del servidor con claves administradas de S3 (SSE-S3) y con AWS KMS keys almacenadas en AWS Key Management Service (SSE-KMS).

Si desea que Amazon FSx cifre los datos al escribir en su bucket de S3, debe configurar el cifrado predeterminado de su bucket de S3 en SSE-S3 o SSE-KMS. Para obtener más información, consulte Configuración del cifrado predeterminado en la Guía del usuario de Amazon S3. Al escribir archivos en su bucket de S3, Amazon FSx sigue la política de cifrado predeterminada de su bucket de S3.

De forma predeterminada, Amazon FSx admite buckets de S3 cifrados mediante SSE-S3. Si desea vincular su sistema de archivos Amazon FSx a un bucket de S3 cifrado mediante el cifrado SSE-KMS, debe añadir una declaración a su política de claves gestionadas por el cliente que permita a Amazon FSx cifrar y descifrar los objetos de su bucket de S3 mediante su clave de KMS.

La siguiente declaración permite a un sistema de archivos Amazon FSx específico cifrar y descifrar objetos para un bucket de S3 específico, *bucket_name*.

```
{
    "Sid": "Allow access through S3 for the FSx SLR to use the KMS key on the objects
 in the given S3 bucket",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::aws_account_id:role/aws-service-role/s3.data-
source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_fsx_file_system_id"
```

```
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:CallerAccount": "aws_account_id",
            "kms:ViaService": "s3.bucket-region.amazonaws.com"
        },
        "StringLike": {
            "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::bucket_name/*"
        }
    }
}
```

**Note**

Si utiliza un KMS con una CMK para cifrar su bucket de S3 con las claves de bucket de S3 habilitadas, establezca el `EncryptionContext` en la ARN del bucket, no en el ARN del objeto, como en este ejemplo:

```
"StringLike": {
    "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::bucket_name"
}
```

La siguiente declaración de política permite que todos los sistemas de archivos de Amazon FSx de su cuenta se vinculen a un bucket de S3 específico.

```
{
    "Sid": "Allow access through S3 for the FSx SLR to use the KMS key on the objects
 in the given S3 bucket",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
```

```
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:CallerAccount": "aws_account_id",
            "kms:ViaService": "s3.bucket-region.amazonaws.com"
        },
        "StringLike": {
            "aws:userid": "*:FSx",
            "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::bucket_name/*"
        }
    }
}
```

## Acceder a los buckets de Amazon S3 cifrados del lado del servidor en una Cuenta de AWS distinta

Después de crear un sistema de archivos FSx para Lustre vinculado a un bucket de Amazon S3 cifrado, debe conceder al rol vinculado al servicio (SLR) `AWSServiceRoleForFSxS3Access_fs-01234567890` acceso a la clave de KMS utilizada para cifrar el bucket de S3 antes de leer o escribir datos del bucket de S3 vinculado. Puede utilizar un rol de IAM que ya tenga permisos para acceder a la clave de KMS.

> **Note**
>
> Este rol de IAM debe estar en la cuenta en la que se creó el sistema de archivos FSx para Lustre (que es la misma cuenta que el SLR de S3), no en la cuenta a la que pertenece la clave de KMS o el bucket de S3.

Utiliza el rol de IAM para llamar a la siguiente AWS KMS API a fin de crear una concesión para el SLR de S3, de modo que el SLR obtenga permiso para acceder a los objetos de S3. Para encontrar la ARN asociado a su SLR, busque sus roles de IAM utilizando el ID del sistema de archivos como cadena de búsqueda.

```
$ aws kms create-grant --region fs_account_region \
      --key-id arn:aws:kms:s3_bucket_account_region:s3_bucket_account:key/key_id \
      --grantee-principal arn:aws:iam::fs_account_id:role/aws-service-role/s3.data-
source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_file-system-id \
      --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

Para obtener más información acerca de los roles vinculados a servicios, consulte Uso de roles vinculados a servicios para Amazon FSx.

## Importación de cambios desde su repositorio de datos

Puede importar los cambios en los datos y los metadatos POSIX desde un repositorio de datos vinculado a su sistema de archivos Amazon FSx. Los metadatos POSIX asociados incluyen la propiedad, los permisos y las marcas de tiempo.

Para importar cambios al sistema de archivos, utilice alguno de los métodos siguientes:

- Configure el sistema de archivos para importar automáticamente los archivos nuevos, modificados o eliminados del repositorio de datos vinculado. Para más información, consulte Importe automáticamente actualizaciones desde un bucket de S3.
- Seleccione la opción de importar metadatos al crear una asociación de repositorios de datos. Esto iniciará una tarea de importación del repositorio de datos inmediatamente después de crear la asociación de repositorios de datos.
- Utilice una tarea de repositorio de datos de importación bajo demanda. Para más información, consulte Uso de las tareas del repositorio de datos para importar los cambios.

Las tareas automáticas de importación e importación del repositorio de datos se pueden ejecutar al mismo tiempo.

Al activar la importación automática para una asociación de repositorio de datos, el sistema de archivos actualiza automáticamente los metadatos de archivo a medida que se crean, modifican o eliminan objetos en S3. Si selecciona la opción de importar metadatos al crear una asociación de repositorios de datos, el sistema de archivos importa los metadatos de todos los objetos del repositorio de datos. Al importar mediante una tarea de importación de un repositorio de datos, el sistema de archivos solo importa los metadatos de los objetos que se crearon o modificaron desde la última importación.

FSx para Lustre copia automáticamente el contenido de un archivo del repositorio de datos y lo carga en el sistema de archivos cuando la aplicación accede por primera vez al archivo del sistema de archivos. Este movimiento de datos lo gestiona FSx para Lustre y es transparente para sus aplicaciones. Las lecturas posteriores de estos archivos se realizan directamente desde el sistema de archivos con latencias inferiores a un milisegundo.

También puede precargar todo el sistema de archivos o un directorio dentro de su sistema de archivos. Para más información, consulte Precargar los archivos en el sistema de archivos. Si solicita la precarga de varios archivos simultáneamente, FSx para Lustre carga los archivos del repositorio de datos de Amazon S3 en paralelo.

FSx para Lustre importa solo objetos de S3 que tienen claves de objeto compatibles con POSIX. Tanto las tareas de importación automática como las de importación del repositorio de datos importan metadatos POSIX. Para más información, consulte Soporte de metadatos POSIX para repositorios de datos.

> **Note**
>
> FSx para Lustre no admite la importación de metadatos para enlaces simbólicos (symlinks) desde las clases de almacenamiento S3 Glacier Flexible Retrieval y S3 Glacier. Se pueden importar los metadatos de los objetos S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive que no sean enlaces simbólicos (es decir, se crea un inodo en el sistema de archivos FSx para Lustre con los metadatos correctos). Sin embargo, para leer estos datos del sistema de archivos, primero debe restaurar el objeto S3 Glacier Flexible Retrieval o S3 Glacier Flexible Archive. No se admite la importación de datos de archivos directamente desde objetos de Amazon S3 en la clase de almacenamiento S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive a FSx para Lustre.

## Importe automáticamente actualizaciones desde un bucket de S3

Puede configurar FSx para Lustre para que actualice automáticamente los metadatos del sistema de archivos a medida que se añadan, modifiquen o eliminen objetos del bucket de S3. FSx para Lustre crea, actualiza o elimina la lista de archivos y directorios correspondiente al cambio en S3. Si el objeto modificado del bucket de S3 ya no contiene sus metadatos, FSx para Lustre mantiene los valores de metadatos actuales del archivo, incluidos los permisos actuales.

> **Note**
>
> El sistema de archivos FSx para Lustre y el bucket de S3 vinculado deben estar ubicados en la misma Región de AWS para poder importar automáticamente las actualizaciones.

Puede configurar la importación automática al crear la asociación de repositorios de datos y actualizar la configuración de importación automática en cualquier momento mediante la consola de administración de FSx, la AWS CLI o la API de AWS.

> **Note**
>
> Puede configurar tanto la importación automática como la exportación automática en la misma asociación de repositorios de datos. En este tema se describe únicamente la característica de importación automática.

> **Important**
>
> - Si se modifica un objeto en S3 con todas las políticas de importación automática activadas y la exportación automática desactivada, el contenido de ese objeto siempre se importa al archivo correspondiente del sistema de archivos. Si ya existe un archivo en la ubicación de destino, se sobrescribe.
> - Si se modifica un archivo tanto en el sistema de archivos como en S3, con todas las políticas de importación y exportación automáticas activadas, el otro podría sobrescribir el archivo del sistema de archivos o el objeto de S3. No se garantiza que una edición posterior en una ubicación sobrescriba una edición anterior en otra ubicación. Si modifica el mismo archivo tanto en el sistema de archivos como en el bucket de S3, debe garantizar la coordinación a nivel de la aplicación para evitar conflictos. FSx para Lustre no evita escrituras conflictivas en varias ubicaciones.

La política de importación especifica cómo desea que FSx para Lustre actualice su sistema de archivos a medida que cambie el contenido del bucket de S3 vinculado. Una asociación de repositorios de datos puede tener una de las siguientes políticas de importación:

- New: FSx para Lustre actualiza automáticamente los metadatos de archivos y directorios solo cuando se agregan nuevos objetos al repositorio de datos de S3 vinculado.
- Changed: FSx para Lustre actualiza automáticamente los metadatos de archivos y directorios solo cuando un objeto existente en el repositorio de datos es modificado.
- Deleted: FSx para Lustre actualiza automáticamente los metadatos de archivos y directorios solo cuando un objeto del repositorio de datos es eliminado.
- Any combination of New, Changed, and Deleted: FSx para Lustre actualiza automáticamente los metadatos de archivos y directorios cuando se produce alguna de las acciones especificadas en el repositorio de datos de S3. Por ejemplo, puede especificar que el sistema de archivos se actualice cuando se añada un objeto (New) o se elimine (Deleted) del repositorio de S3, pero que no se actualice cuando se cambie un objeto.
- No policy configured: FSx para Lustre no actualiza los metadatos de los archivos y directorios del sistema de archivos cuando se agregan, modifican o eliminan objetos del repositorio de datos de S3. Si no configura una política de importación, la importación automática se deshabilita para la asociación de repositorios de datos. Aún puede importar manualmente los cambios en los metadatos mediante una tarea de importación del repositorio de datos, tal y como se describe en Uso de las tareas del repositorio de datos para importar los cambios.

> **Important**
>
> La importación automática no sincronizará las siguientes acciones de S3 con el sistema de archivos FSx para Lustre vinculado:
>
> - Eliminar un objeto mediante los vencimientos del ciclo de vida de los objetos de S3
> - Eliminación permanente de la versión actual del objeto en un bucket con control de versiones habilitado
> - Anular la eliminación de un objeto en un bucket con control de versiones habilitado

Para la mayoría de los casos de uso, se recomienda configurar una política de importación de New, Changed y Deleted. Esta política garantiza que todas las actualizaciones realizadas en el repositorio de datos de S3 vinculado se importen automáticamente a su sistema de archivos.

Cuando establece una política de importación para actualizar los metadatos de los archivos y directorios del sistema de archivos en función de los cambios en el repositorio de datos de S3 vinculado, FSx para Lustre crea una configuración de notificación de eventos en el bucket de S3

vinculado. La configuración de notificación de eventos se denomina `FSx`. No modifique o elimine la configuración de notificación de eventos `FSx` en el bucket S3; si lo hace, impedirá la importación automática de los metadatos actualizados de los archivos y directorios a su sistema de archivos.

Cuando FSx para Lustre actualiza una lista de archivos que ha cambiado en el repositorio de datos de S3 vinculado, sobrescribe el archivo local con la versión actualizada, incluso si el archivo tiene la escritura bloqueada.

FSx para Lustre hará todo lo posible por actualizar su sistema de archivos. FSx para Lustre no puede actualizar el sistema de archivos en las siguientes situaciones:

- Si FSx para Lustre no tiene permiso para abrir el objeto de S3 nuevo o modificado. En este caso, FSx para Lustre omite el objeto y continúa. El estado del ciclo de vida de la DRA no se ve afectado.
- Si FSx para Lustre no tiene permisos a nivel de bucket, como para `GetBucketAcl`. Esto hará que el estado del ciclo de vida del repositorio de datos se convierta en Misconfigured. Para más información, consulte Estado del ciclo de vida de la asociación de repositorios.
- Si se elimina o modifica la configuración de notificación de eventos `FSx` en el bucket S3 vinculado. Esto hará que el estado del ciclo de vida del repositorio de datos se convierta en Misconfigured. Para más información, consulte Estado del ciclo de vida de la asociación de repositorios.

Se recomienda activar el registro en CloudWatch los registros para registrar la información sobre los archivos o directorios que no se hayan podido importar automáticamente. Las advertencias y los errores del registro contienen información sobre el motivo del error. Para más información, consulte Registros de eventos del repositorio de datos.

## Requisitos previos

Se requieren las siguientes condiciones para que FSx para Lustre importe automáticamente los archivos nuevos, modificados o eliminados del bucket de S3 vinculado:

- El sistema de archivos y su bucket de S3 vinculado se encuentran en la misma Región de AWS.
- El bucket de S3 no tiene el Lifecycle state mal configurado. Para más información, consulte Estado del ciclo de vida de la asociación de repositorios.
- Su cuenta tiene los permisos necesarios para configurar y recibir notificaciones de eventos en el bucket de S3 vinculado.

## Tipos de cambios de archivos compatibles

FSx para Lustre admite la importación de los siguientes cambios en los archivos y directorios que se producen en el bucket de S3 vinculado:

- Cambios en el contenido de los archivos.
- Cambios en los metadatos de los archivos o directorios.
- Cambios en el destino o los metadatos del enlace simbólico.
- Eliminaciones de archivos y directorios. Si elimina un objeto del bucket de S3 vinculado que corresponde a un directorio del sistema de archivos (es decir, un objeto con un nombre clave que termina con una barra diagonal), FSx para Lustre elimina el directorio correspondiente del sistema de archivos solo si está vacío.

## Actualización de la configuración de importación

Puede establecer la configuración de importación de un sistema de archivos para un bucket de S3 vinculado al crear la asociación de repositorios de datos. Para más información, consulte Crear un enlace a un bucket de S3.

También puede actualizar la configuración de importación en cualquier momento, incluida la política de importación. Para más información, consulte Actualización de la configuración de asociación de repositorios de datos.

## Monitorización de la importación automática

Si la velocidad de cambio en su bucket de S3 supera la velocidad a la que la importación automática puede procesar estos cambios, los cambios de metadatos correspondientes que se importen a su sistema de archivos FSx para Lustre se retrasarán. Si esto ocurre, puede utilizar la métrica `AgeOfOldestQueuedMessage` para monitorizar la antigüedad del cambio más antiguo que espera ser procesado mediante la importación automática. Para obtener más información sobre esta métrica, consulte Métricas de AutoImport y AutoExport.

Si el retraso en la importación de los cambios de metadatos supera los 14 días (medido con la métrica `AgeOfOldestQueuedMessage`), los cambios del bucket de S3 que no se hayan procesado mediante la importación automática no se importarán a su sistema de archivos. Además, el ciclo de vida de la asociación del repositorio de datos se marca como MISCONFIGURED y la importación automática se detiene. Si tiene habilitada la exportación automática, la exportación automática

seguirá monitorizando los cambios en su sistema de archivos FSx para Lustre. Sin embargo, los cambios adicionales no se sincronizan desde el sistema de archivos FSx para Lustre a S3.

Para que la asociación de repositorios de datos pase del estado de ciclo de vida MISCONFIGURED al estado de ciclo de vida AVAILABLE, debe actualizar la asociación de repositorios de datos. Puede actualizar la asociación del repositorio de datos mediante el comando update-data-repository-associationCLI (o la operación de UpdateDataRepositoryAssociationAPI correspondiente). El único parámetro de solicitud que necesita es el `AssociationID` de la asociación de repositorios de datos que desea actualizar.

Cuando el estado del ciclo de vida de la asociación de repositorios de datos cambie a AVAILABLE, se reiniciará la importación automática (y la exportación automática si está habilitada). Al reiniciarse, la exportación automática reanuda la sincronización de los cambios del sistema de archivos a S3. Para sincronizar los metadatos de los objetos nuevos y modificados de S3 con el sistema de archivos FSx para Lustre que no se importaron o que proceden de cuando la asociación de repositorios de datos estaba mal configurada, ejecute una tarea de importación de repositorio de datos. Las tareas de importación del repositorio de datos no sincronizan las eliminaciones del bucket de S3 con el sistema de archivos FSx para Lustre. Si desea sincronizar completamente S3 con su sistema de archivos (incluidas las eliminaciones), debe volver a crear el sistema de archivos.

Para garantizar que los retrasos en la importación de los cambios en los metadatos no superen los 14 días, le recomendamos que configure una alarma en la métrica `AgeOfOldestQueuedMessage` y reduzca la actividad en su bucket de S3 si la métrica `AgeOfOldestQueuedMessage` supera el umbral de alarma. En el caso de un sistema de archivos FSx para Lustre conectado a un bucket de S3 con una sola partición que envíe de forma continua el máximo número de cambios posibles desde S3, con solo la importación automática ejecutándose en el sistema de archivos FSx para Lustre, la importación automática puede procesar una acumulación de cambios de S3 de 7 horas en un plazo de 14 días.

Además, con una sola acción de S3, puede generar más cambios de los que la importación automática procesará en 14 días. Algunos ejemplos de este tipo de acciones son, entre otros, las subidas de AWS Snowball a S3 y las eliminaciones a gran escala. Si realiza un cambio a gran escala en su bucket de S3 y desea que se sincronice con su sistema de archivos FSx para Lustre para evitar que los cambios de importación automática superen los 14 días, debe eliminar el sistema de archivos y volver a crearlo una vez que se haya completado el cambio de S3.

Si su métrica `AgeOfOldestQueuedMessage` está aumentando, revise el bucket de S3 `GetRequests`, `PutRequests`, `PostRequests` y `DeleteRequests`, y las métricas para ver si hay

cambios de actividad que puedan provocar un aumento en la frecuencia o el número de cambios que se envían a la importación automática. Para obtener información sobre las métricas de S3 disponibles, consulte Monitorización de Amazon S3 en la Guía del usuario de Amazon S3.

Para obtener una lista de todas las métricas de FSx para Lustre, consulte Supervisión con Amazon CloudWatch.

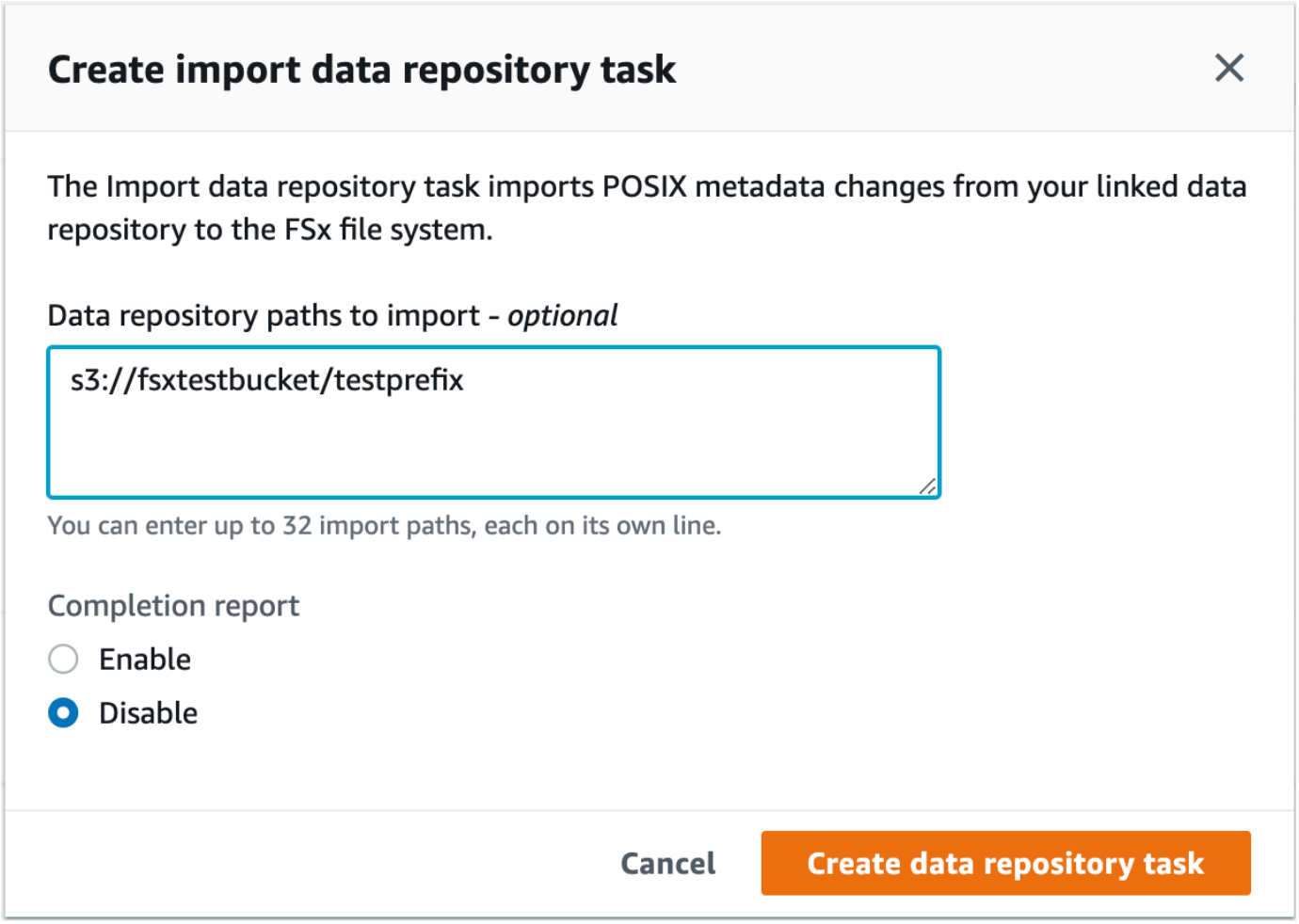
## Uso de las tareas del repositorio de datos para importar los cambios

La tarea de importación del repositorio de datos importa los metadatos de los objetos nuevos o modificados en el repositorio de datos de S3, lo que crea una nueva lista de archivos o directorios para cualquier objeto nuevo del repositorio de datos de S3. Para cualquier objeto que se haya modificado en el repositorio de datos, la lista de archivos o directorios correspondiente se actualiza con los nuevos metadatos. No se realiza ninguna acción con los objetos que se han eliminado del repositorio de datos.

Utilice los siguientes procedimientos para importar los cambios en los metadatos mediante la consola Amazon FSx y la CLI. Tenga en cuenta que puede utilizar una tarea de repositorio de datos para varias DRA.

Para importar cambios en los metadatos (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación, elija File systems y, a continuación, elija su sistema de archivos Lustre.
3. Elija la pestaña Data repository.
4. En el panel Data repository associations, elija las asociaciones de repositorios de datos para las que desea crear la tarea de importación.
5. En el menú Actions, elija Import task. Esta opción no está disponible si el sistema de archivos no está vinculado a un repositorio de datos. Aparece la página de Create import data repository task.




6. (Opcional) Especifique hasta 32 directorios o archivos para importar desde los buckets de S3 vinculados proporcionando las rutas a dichos directorios o archivos en Data repository paths to import.

> **Note**
>
> Si la ruta que proporciona no es válida, la tarea devuelve un error.

7. (Opcional) Elija Enable en el Completion report para generar un informe de finalización de la tarea una vez finalizada la tarea. Un task completion report proporciona detalles sobre los archivos procesados por la tarea que cumplen con el alcance indicado en el Report scope. Para especificar la ubicación en la que Amazon FSx entregará el informe, introduzca una ruta relativa en un repositorio de datos de S3 vinculado para la Report path.
8. Seleccione Crear.

Una notificación en la parte superior de la página de File systems muestra la tarea que acaba de crear en curso.

Para ver el estado y los detalles de la tarea, desplácese hacia abajo hasta el panel Data Repository Tasks de la pestaña Data Repository del sistema de archivos. El orden predeterminado muestra la tarea más reciente en la parte superior de la lista.

Para ver un resumen de la tarea en esta página, elija el Task ID de la tarea que acaba de crear. Aparece la página de Summary de la tarea.

Para importar cambios en los metadatos (CLI)

- Utilice el comando `create-data-repository-task` de la CLI para importar los cambios de metadatos en su sistema de archivos FSx para Lustre. La operación de API correspondiente es `CreateDataRepositoryTask`.

  ```
  $ aws fsx create-data-repository-task \
      --file-system-id fs-0123456789abcdef0 \
      --type IMPORT_METADATA_FROM_REPOSITORY \
      --paths s3://bucketname1/dir1/path1 \
      --report Enabled=true,Path=s3://bucketname1/dir1/
  path1,Format=REPORT_CSV_20191124,Scope=FAILED_FILES_ONLY
  ```

  Después de crear correctamente la tarea de repositorio de datos, Amazon FSx devuelve la descripción de la tarea en formato JSON.

Después de crear la tarea para importar metadatos del repositorio de datos vinculado, puede comprobar el estado de la tarea de importación del repositorio de datos. Para obtener más información sobre cómo ver las tareas del repositorio de datos, consulte Acceder a las tareas del repositorio de datos.

## Precargar los archivos en el sistema de archivos

Amazon FSx copia los datos del repositorio de datos de Amazon S3 cuando se accede a un archivo por primera vez. Gracias a este enfoque, la lectura o escritura inicial en un archivo tiene una pequeña latencia. Si su aplicación es sensible a esta latencia y sabe a qué archivos o directorios debe acceder, si lo desea, puede precargar el contenido de archivos o directorios individuales. Para ello, use el siguiente comando `hsm_restore`, como se indica a continuación.

Puede utilizar el comando `hsm_action` (emitido con la utilidad de usuario `lfs`) para comprobar que el contenido del archivo ha terminado de cargarse en el sistema de archivos. Un valor devuelto de `NOOP` indica que el archivo se ha cargado correctamente. Ejecute los siguientes comandos desde una instancia de procesamiento con el sistema de archivos montado. Sustituya *`path/to/file`* por la ruta del archivo que está precargando en el sistema de archivos.

```
sudo lfs hsm_restore path/to/file
sudo lfs hsm_action path/to/file
```

Puede precargar todo el sistema de archivos o todo un directorio del sistema de archivos mediante los siguientes comandos. (El ampersand final hace que un comando se ejecute como proceso en segundo plano). Si solicita la precarga de varios archivos simultáneamente, Amazon FSx carga sus archivos desde su repositorio de datos de Amazon S3 en paralelo. Si un archivo ya se ha cargado en el sistema de archivos, el comando `hsm_restore` no lo vuelve a cargar.

```
nohup find local/directory -type f -print0 | xargs -0 -n 1 sudo lfs hsm_restore &
```

> **Note**
>
> Si el bucket de S3 vinculado es más grande que el sistema de archivos, debería poder importar todos los metadatos de los archivos a su sistema de archivos. Sin embargo, solo puede cargar la cantidad de datos de archivos reales que quepa en el espacio de almacenamiento restante del sistema de archivos. Recibirá un mensaje de error si intenta acceder a los datos de los archivos cuando ya no quede espacio de almacenamiento en el sistema de archivos. Si esto ocurre, puede aumentar la cantidad de capacidad de almacenamiento según sea necesario. Para más información, consulte Administración de la capacidad de almacenamiento.

## Exportación de los cambios al repositorio de datos

Puede exportar cambios en los datos y cambios en los metadatos POSIX desde su sistema de archivos FSx para Lustre a un repositorio de datos enlazados. Los metadatos POSIX asociados incluyen la propiedad, los permisos y las marcas de tiempo.

Para exportar los cambios del sistema de archivos, utilice uno de los siguientes métodos.

- Configure el sistema de archivos para que exporte automáticamente los archivos nuevos, modificados o eliminados al repositorio de datos vinculado. Para más información, consulte Exporte automáticamente las actualizaciones a su bucket de S3.
- Utilice una tarea de repositorio de datos de exportación bajo demanda. Para obtener más información, consulte Uso de las tareas del repositorio de datos para exportar los cambios

Las tareas automáticas de exportación y exportación del repositorio de datos no se pueden ejecutar al mismo tiempo.

> **Important**
>
> La exportación automática no sincronizará las siguientes operaciones de metadatos del sistema de archivos con S3 si los objetos correspondientes están almacenados en S3 Glacier Flexible Retrieval:
>
> - chmod
> - chown
> - rename

Al activar la exportación automática para una asociación de repositorios de datos, el sistema de archivos exporta automáticamente los cambios en los datos y los metadatos de los archivos a medida que se crean, modifican o eliminan los archivos. Al exportar archivos o directorios mediante una tarea de exportación de repositorios de datos, el sistema de archivos solo exporta los archivos de datos y los metadatos que se crearon o modificaron desde la última exportación.

Tanto las tareas de exportación automática como las de exportación del repositorio de datos exportan metadatos POSIX. Para más información, consulte Soporte de metadatos POSIX para repositorios de datos.

> **Important**
>
> - Para garantizar que FSx para Lustre pueda exportar sus datos a su bucket de S3, debe almacenarlos en un formato compatible con UTF-8.
> - Las claves de objeto de S3 tienen una longitud máxima de 1024 bytes. FSx para Lustre no exportará archivos cuya clave de objeto S3 correspondiente supere los 1024 bytes.

> **Note**
>
> Todos los objetos creados mediante las tareas automáticas de exportación y exportación del repositorio de datos se escriben con la clase de almacenamiento S3 Standard.

Temas



## Exporte automáticamente las actualizaciones a su bucket de S3

Puede configurar su sistema de archivos FSx para Lustre para que actualice automáticamente el contenido de un bucket de S3 vinculado a medida que se añaden, modifican o eliminan archivos en el sistema de archivos. FSx para Lustre crea, actualiza o elimina el objeto en S3, en función del cambio en el sistema de archivos.

> **Note**
>
> La exportación automática no está disponible en FSx para sistemas de archivos `Scratch 1` o sistemas de archivos Lustre 2.10.

Puede exportar a un repositorio de datos que esté en la misma Región de AWS que el sistema de archivos o en una Región de AWS distinta.

Puede configurar la exportación automática al crear la asociación de repositorios de datos y actualizar la configuración de exportación automática en cualquier momento mediante la consola de administración de FSx, la AWS CLI y la API de AWS.

> **Note**
>
> Puede configurar tanto la exportación automática como la importación automática en la misma asociación de repositorios de datos. En este tema se describe únicamente la característica de exportación automática.

**Important**

- Si se modifica un archivo en el sistema de archivos con todas las políticas de exportación automática activadas y la importación automática desactivada, el contenido de ese archivo siempre se exporta al objeto correspondiente en S3. Si ya existe un objeto en la ubicación de destino, se sobrescribe.
- Si se modifica un archivo tanto en el sistema de archivos como en S3, con todas las políticas de importación y exportación automáticas activadas, el otro podría sobrescribir el archivo del sistema de archivos o el objeto de S3. No se garantiza que una edición posterior en una ubicación sobrescriba una edición anterior en otra ubicación. Si modifica el mismo archivo tanto en el sistema de archivos como en el bucket de S3, debe garantizar la coordinación a nivel de la aplicación para evitar conflictos. FSx para Lustre no evita escrituras conflictivas en varias ubicaciones.

La política de exportación especifica cómo desea que FSx para Lustre actualice el bucket de S3 vinculado a medida que cambia el contenido del sistema de archivos. Una asociación de repositorios de datos puede tener una de las siguientes políticas de exportación automática:

- New: FSx para Lustre actualiza automáticamente el repositorio de datos de S3 solo cuando se crea un nuevo archivo, directorio o enlace simbólico en el sistema de archivos.
- Changed: FSx para Lustre actualiza automáticamente el repositorio de datos de S3 solo cuando se modifica un archivo existente en el sistema de archivos. En el caso de los cambios en el contenido de los archivos, el archivo debe cerrarse antes de propagarse al repositorio de S3. Los cambios en los metadatos (cambio de nombre, propiedad, permisos y marcas de tiempo) se propagan al finalizar la operación. Al cambiar el nombre de los cambios (incluidos los movimientos), se elimina el objeto de S3 existente (renombrado previamente) y se crea un nuevo objeto de S3 con el nuevo nombre.
- Deleted: FSx para Lustre actualiza automáticamente el repositorio de datos de S3 solo cuando se elimina un archivo, directorio o enlace simbólico del sistema de archivos.
- Any combination of New, Changed, and Deleted: FSx para Lustre actualiza automáticamente el repositorio de datos de S3 cuando cualquiera de las acciones especificadas se produce en el sistema de archivos. Por ejemplo, puede especificar que el repositorio de S3 se actualice cuando se añada un archivo (New) o se elimine (Deleted) del sistema de archivos, pero no cuando se cambie un archivo.

- No policy configured: FSx para Lustre no actualiza automáticamente el repositorio de datos de S3 cuando se añaden, modifican o eliminan archivos del sistema de archivos. Si no configura una política de exportación, la exportación automática está deshabilitada. Aún puede exportar los cambios manualmente mediante una tarea de exportación de repositorio de datos, tal y como se describe en Uso de las tareas del repositorio de datos para exportar los cambios.

Para la mayoría de los casos de uso, se recomienda configurar una política de exportación de New, Changed y Deleted. Esta política garantiza que todas las actualizaciones realizadas en el sistema de archivos se exporten automáticamente al repositorio de datos de S3 vinculado.

Le recomendamos que active el registro en CloudWatch los registros para registrar la información sobre cualquier archivo o directorio que no se pueda exportar automáticamente. Las advertencias y los errores del registro contienen información sobre el motivo del error. Para más información, consulte Registros de eventos del repositorio de datos.

## Actualización de la configuración de exportación

Puede establecer la configuración de exportación de un sistema de archivos a un bucket de S3 vinculado al crear la asociación de repositorios de datos. Para más información, consulte Crear un enlace a un bucket de S3.

También puede actualizar la configuración de exportación en cualquier momento, incluida la política de exportación. Para más información, consulte Actualización de la configuración de asociación de repositorios de datos.

## Monitorización de la exportación automática

Puedes supervisar las asociaciones de repositorios de datos habilitadas para la exportación automática mediante un conjunto de métricas publicadas en Amazon CloudWatch. La métrica `AgeOfOldestQueuedMessage` representa la antigüedad de la actualización más antigua realizada en el sistema de archivos y que aún no se ha exportado a S3. Si `AgeOfOldestQueuedMessage` es mayor que cero durante un período prolongado, se recomienda reducir temporalmente el número de cambios (en particular, los cambios de nombre de los directorios) que se están realizando activamente en el sistema de archivos hasta que se reduzca la cola de mensajes. Para más información, consulte Métricas de AutoImport y AutoExport.

> **Important**
>
> Al eliminar una asociación de repositorios de datos o un sistema de archivos con la exportación automática habilitada, primero debe asegurarse de que `AgeOfOldestQueuedMessage` es cero, lo que significa que no hay cambios que aún no se hayan exportado. Si `AgeOfOldestQueuedMessage` es mayor que cero al eliminar la asociación de repositorios de datos o el sistema de archivos, los cambios que aún no se hayan exportado no llegarán al bucket de S3 vinculado. Para evitarlo, espere a que `AgeOfOldestQueuedMessage` llegue a cero antes de eliminar la asociación de repositorios de datos o el sistema de archivos.

## Uso de las tareas del repositorio de datos para exportar los cambios

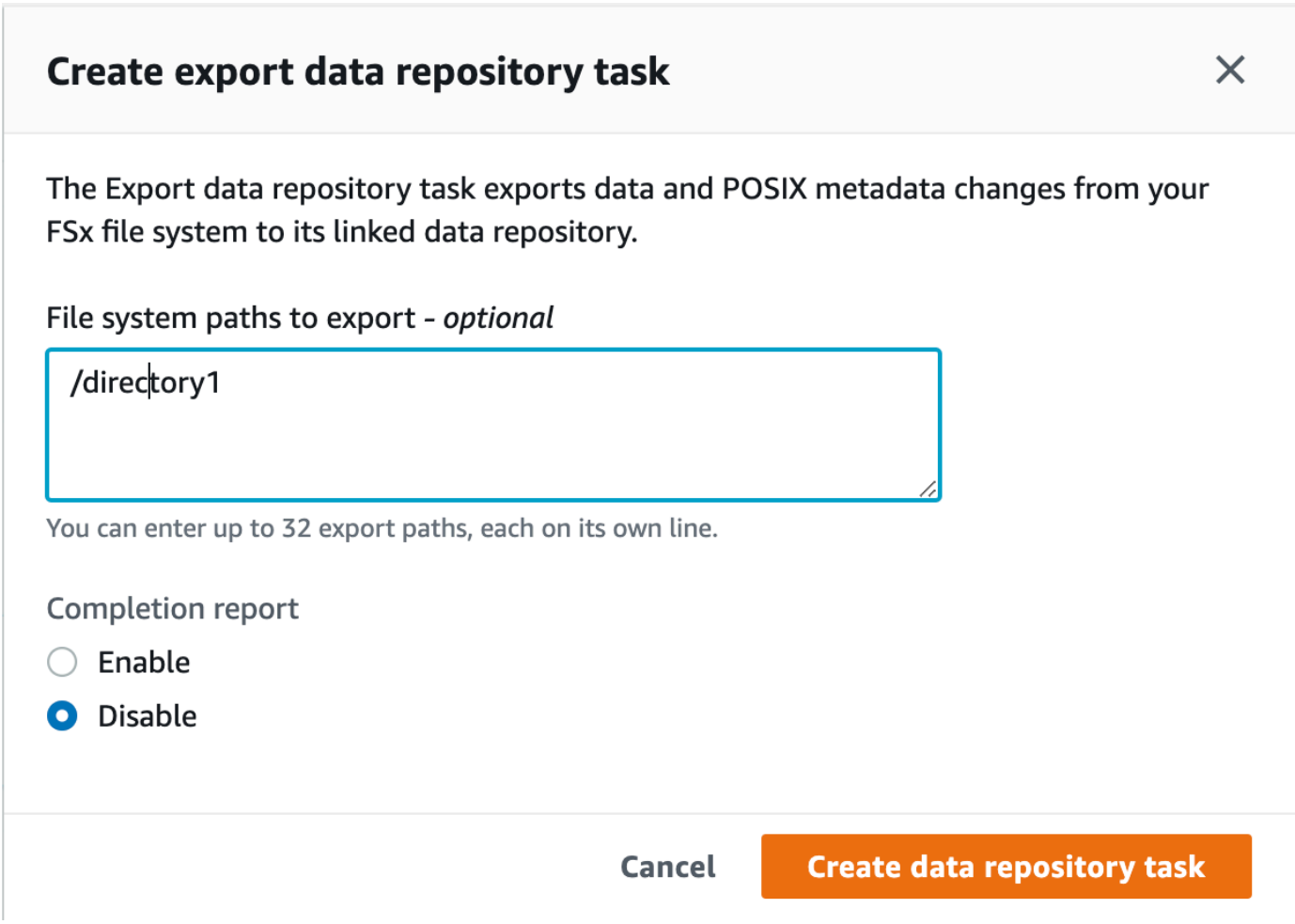
La tarea de exportación del repositorio de datos exporta los archivos nuevos o modificados en el sistema de archivos. Crea un objeto nuevo en S3 para cualquier archivo nuevo del sistema de archivos. Para cualquier archivo que se haya modificado en el sistema de archivos o cuyos metadatos se hayan modificado, el objeto correspondiente de S3 se sustituye por un objeto nuevo con los nuevos datos y metadatos. No se realiza ninguna acción en relación con los archivos que se han eliminado del sistema de archivos.

> **Note**
>
> Tenga en cuenta las siguientes consideraciones al utilizar las tareas de exportación de repositorios de datos:
>
> - No se admite el uso de caracteres comodín para incluir o excluir archivos para la exportación.
> - Al realizar operaciones `mv`, el archivo de destino después de moverlo se exportará a S3 aunque no se haya producido ningún cambio en el UID, el GID, el permiso o el contenido.

Utilice los siguientes procedimientos para exportar los cambios de datos y metadatos del sistema de archivos a buckets de S3 vinculados mediante la consola Amazon FSx y la CLI. Tenga en cuenta que puede utilizar una tarea de repositorio de datos para varias DRA.

Para exportar cambios (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación, elija File systems y, a continuación, elija su sistema de archivos Lustre.
3. Elija la pestaña Data repository.
4. En el panel Data repository associations, elija la asociación de repositorios de datos para la que desea crear la tarea de exportación.
5. Para Actions, elija Export. Esta opción no está disponible si el sistema de archivos no está vinculado a un repositorio de datos en S3. Aparece el cuadro de diálogo de Create export data repository task.




6. (Opcional) Especifique hasta 32 directorios o archivos para exportar desde su sistema de archivos Amazon FSx proporcionando las rutas a esos directorios o archivos en File system paths to export. Las rutas que proporcione deben estar en relación con el punto de montaje del sistema de archivos. Si el punto de montaje es `/mnt/fsx` y `/mnt/fsx/path1` es un directorio

o un archivo del sistema de archivos que desea exportar, la ruta que debe proporcionarse es `path1`.

> **Note**
>
> Si la ruta que proporciona no es válida, la tarea devuelve un error.

7. (Opcional) Elija Enable en el Completion report para generar un informe de finalización de la tarea una vez finalizada la tarea. Un task completion report proporciona detalles sobre los archivos procesados por la tarea que cumplen con el alcance indicado en el Report scope. Para especificar la ubicación en la que Amazon FSx entregará el informe, introduzca una ruta relativa en un repositorio de datos de S3 vinculado para la Report path.
8. Seleccione Crear.

   Una notificación en la parte superior de la página de File systems muestra la tarea que acaba de crear en curso.

Para ver el estado y los detalles de la tarea, desplácese hacia abajo hasta el panel Data Repository Tasks de la pestaña Data Repository del sistema de archivos. El orden predeterminado muestra la tarea más reciente en la parte superior de la lista.

Para ver un resumen de la tarea en esta página, elija el Task ID de la tarea que acaba de crear. Aparece la página de Summary de la tarea.

Para exportar cambios (CLI)

- Utilice el comando `create-data-repository-task` de la CLI para exportar datos y cambios de metadatos en su sistema de archivos FSx para Lustre. La operación de API correspondiente es `CreateDataRepositoryTask`.

```
$ aws fsx create-data-repository-task \
    --file-system-id fs-0123456789abcdef0 \
    --type EXPORT_TO_REPOSITORY \
    --paths path1,path2/file1 \
    --report Enabled=true
```

  Después de crear correctamente la tarea de repositorio de datos, Amazon FSx devuelve la descripción de la tarea en formato JSON, como se muestra en el siguiente ejemplo.

```
{
    "Task": {
        "TaskId": "task-123f8cd8e330c1321",
        "Type": "EXPORT_TO_REPOSITORY",
        "Lifecycle": "PENDING",
        "FileSystemId": "fs-0123456789abcdef0",
        "Paths": ["path1", "path2/file1"],
        "Report": {
            "Path":"s3://dataset-01/reports",
            "Format":"REPORT_CSV_20191124",
            "Enabled":true,
            "Scope":"FAILED_FILES_ONLY"
        },
        "CreationTime": "1545070680.120",
        "ClientRequestToken": "10192019-drt-12",
        "ResourceARN": "arn:aws:fsx:us-
east-1:123456789012:task:task-123f8cd8e330c1321"
    }
}
```

Después de crear la tarea para exportar datos al repositorio de datos vinculado, puede comprobar el estado de la tarea de exportación de datos. Para obtener más información sobre cómo ver las tareas del repositorio de datos, consulte Acceder a las tareas del repositorio de datos.

## Exportación de archivos mediante comandos de HSM

> **Note**
>
> Para exportar los cambios en los datos y metadatos del sistema de archivos FSx para Lustre a un repositorio de datos duradero en Amazon S3, utilice la característica de exportación automática que se describe en Exporte automáticamente las actualizaciones a su bucket de S3. También puede utilizar las tareas de exportación de repositorios de datos, que se describen en Uso de las tareas del repositorio de datos para exportar los cambios.

Para exportar un archivo individual a su repositorio de datos y comprobar que el archivo se ha exportado correctamente a su repositorio de datos, puede ejecutar los comandos que se muestran a continuación. Un valor devuelto de `states: (0x00000009) exists archived` indica que el archivo se ha exportado correctamente.

```
sudo lfs hsm_archive path/to/export/file
sudo lfs hsm_state path/to/export/file
```

> **Note**
>
> Debe ejecutar los comandos de HSM (como `hsm_archive`) como usuario raíz o mediante `sudo`.

Para exportar todo el sistema de archivos o un directorio completo del sistema de archivos, ejecute los siguientes comandos. Si exporta varios archivos simultáneamente, Amazon FSx para Lustre exporta los archivos a su repositorio de datos de Amazon S3 en paralelo.

```
nohup find local/directory -type f -print0 | xargs -0 -n 1 sudo lfs hsm_archive &
```

Para determinar si la exportación se ha completado, ejecute el siguiente comando.

```
find path/to/export/file -type f -print0 | xargs -0 -n 1 -P 8 sudo lfs hsm_state | awk
 '!/\<archived\>/ || /\<dirty\>/' | wc -l
```

Si el comando se devuelve y no quedan archivos, la exportación se ha completado.

## Tareas de repositorio de datos

Al usar las tareas de importación y exportación de repositorios de datos, puede administrar la transferencia de datos y metadatos entre su sistema de archivos de FSx para Lustre y cualquiera de sus repositorios de datos duraderos en Amazon S3.

Las tareas de repositorio de datos optimizan las transferencias de datos y metadatos entre el sistema de archivos de FSx para Lustre y un repositorio de datos en S3. Una forma de que hagan esto es mediante el seguimiento de los cambios entre el sistema de archivos de Amazon FSx y su repositorio de datos vinculado. También lo hacen mediante el uso de técnicas de transferencia paralela para transferir datos a velocidades de hasta cientos de Gb/s. Puede crear y ver las tareas del repositorio de datos mediante la consola de Amazon FSx AWS CLI, la API Amazon FSx y la API de Amazon FSx.

Las tareas de repositorio de datos mantienen los metadatos de la interfaz portátil del sistema operativo (POSIX) del sistema de archivos, incluidos la propiedad, los permisos y las marcas de

tiempo. Como las tareas mantienen estos metadatos, puede implementar y mantener controles de acceso entre el sistema de archivos de FSx para Lustre y sus repositorios de datos vinculados.

Puede utilizar una tarea de liberación de repositorios de datos para liberar espacio en el sistema de archivos para nuevos archivos mediante la liberación de archivos exportados a Amazon S3. El contenido del archivo liberado se elimina, pero los metadatos del archivo liberado permanecen en el sistema de archivos. Los usuarios y las aplicaciones pueden seguir accediendo a un archivo liberado volviendo a leer el archivo. Cuando el usuario o la aplicación lee el archivo liberado, FSx para Lustre recupera de forma transparente el contenido del archivo de Amazon S3.

## Tipos de tareas de repositorio de datos

Existen tres tipos de tareas de repositorio de datos:

- Las tareas Export (Exportar) repositorio de datos exportan desde su sistema de archivos Lustre a un bucket S3 vinculado.
- Las tareas Import (Importar) repositorio de datos importan desde un bucket S3 vinculado a su sistema de archivos Lustre.
- Las tareas Release (Liberar) repositorio de datos liberan archivos exportados a un bucket S3 vinculado desde su sistema de archivos Lustre.

Para obtener más información, consulte Creación de una tarea de repositorio de datos.

Temas

- Comprender el estado y los detalles de una tarea
- Uso de tareas de repositorio de datos
- Trabajar con informes de finalización de tareas
- Resolución de fallos en las tareas del repositorio de datos

## Comprender el estado y los detalles de una tarea

Una tarea de repositorio de datos puede tener uno de los siguientes estados:

- PENDING indica que Amazon FSx no ha iniciado la tarea.
- EXECUTING indica que Amazon FSx está procesando la tarea.

- FAILED indica que Amazon FSx no procesó correctamente la tarea. Por ejemplo, puede haber archivos que la tarea no haya podido procesar. Los detalles de la tarea proporcionan más información sobre el fallo. Para obtener más información sobre las tareas fallidas, consulte Resolución de fallos en las tareas del repositorio de datos.
- SUCCEEDED indica que Amazon FSx completó la tarea con éxito.
- CANCELED indica que la tarea se canceló y no se completó.
- CANCELING indica que Amazon FSx está cancelando la tarea.

Después de crear una tarea, puede ver la siguiente información detallada de una tarea de repositorio de datos mediante la consola, la CLI o la API de Amazon FSx:

- El tipo de tarea:
  - `EXPORT_TO_REPOSITORY` indica una tarea de exportación.
  - `IMPORT_METADATA_FROM_REPOSITORY` indica una tarea de importación.
  - `RELEASE_DATA_FROM_FILESYSTEM` indica una tarea de liberación.
- El sistema de archivos en el que se ejecutó la tarea.
- La hora de creación de la tarea.
- El estado de la tarea.
- El número total de archivos que procesó la tarea.
- El número total de archivos que la tarea procesó correctamente.
- El número total de archivos que la tarea no pudo procesar. Este valor es mayor que cero cuando el estado de la tarea es FAILED. La información detallada sobre los archivos que fallaron está disponible en un informe de finalización de tarea. Para obtener más información, consulte Trabajar con informes de finalización de tareas.
- La hora en que comenzó la tarea.
- La hora en que se actualizó por última vez el estado de la tarea. El estado de la tarea se actualiza cada 30 segundos.

Para obtener más información sobre el acceso a las tareas de repositorio de datos existentes, consulte Acceder a las tareas del repositorio de datos.

# Uso de tareas de repositorio de datos

Puede crear, duplicar, ver los detalles y cancelar las tareas del repositorio de datos mediante la consola, la CLI o la API de Amazon FSx.

Temas



## Creación de una tarea de repositorio de datos

Puede crear una tarea de repositorio de datos mediante la consola, la CLI o la API de Amazon FSx. Después de crear una tarea, puede ver el progreso y el estado de la tarea mediante la consola, la CLI o la API.

Puede crear tres tipos de tareas de repositorio de datos:

- La tarea Export (Exportar) repositorio de datos exporta desde su sistema de archivos Lustre a un bucket S3 vinculado. Para obtener más información, consulte Uso de las tareas del repositorio de datos para exportar los cambios.
- La tarea Import (Importar) repositorio de datos importa desde un bucket S3 vinculado a su sistema de archivos Lustre. Para obtener más información, consulte Uso de las tareas del repositorio de datos para importar los cambios.
- La tarea Release (Liberar) repositorio de datos libera los archivos de su sistema de archivos Lustre que se hayan exportado a un bucket S3 vinculado. Para obtener más información, consulte Utilizar las tareas del repositorio de datos para liberar archivos.

## Duplicación de una tarea

Puede duplicar una tarea de repositorio de datos existente en la consola de Amazon FSx. Cuando duplica una tarea, se muestra una copia exacta de la tarea existente en la página Crear tarea de repositorio de datos de importación o Crear tarea de repositorio de datos de exportación. Puede realizar cambios en las rutas para exportar o importar, según sea necesario, antes de crear y ejecutar la nueva tarea.

> **Note**
>
> Una solicitud para ejecutar una tarea duplicada fallará si ya se está ejecutando una copia exacta de esa tarea. Una copia exacta de una tarea que ya se está ejecutando contiene la misma ruta o rutas del sistema de archivos en el caso de una tarea de exportación o las mismas rutas del repositorio de datos en el caso de una tarea de importación.

Puede duplicar una tarea desde la vista de detalles de la tarea, el panel Tareas del repositorio de datos en la pestaña Repositorio de datos para el sistema de archivos o desde la página Tareas del repositorio de datos.

Para duplicar una tarea existente

1. Elija una tarea en el panel Tareas del repositorio de datos en la pestaña Repositorio de datos para el sistema de archivos.
2. Elija Duplicate task (Duplicar tarea). Según el tipo de tarea que elija, aparecerá la página Crear tarea de repositorio de datos de importación o Crear tarea de repositorio de datos de exportación. Todos los ajustes de la nueva tarea son idénticos a los de la tarea que está duplicando.
3. Cambie o añada las rutas desde las que quiera importar o a las que desea exportar.
4. Seleccione Crear.

## Acceder a las tareas del repositorio de datos

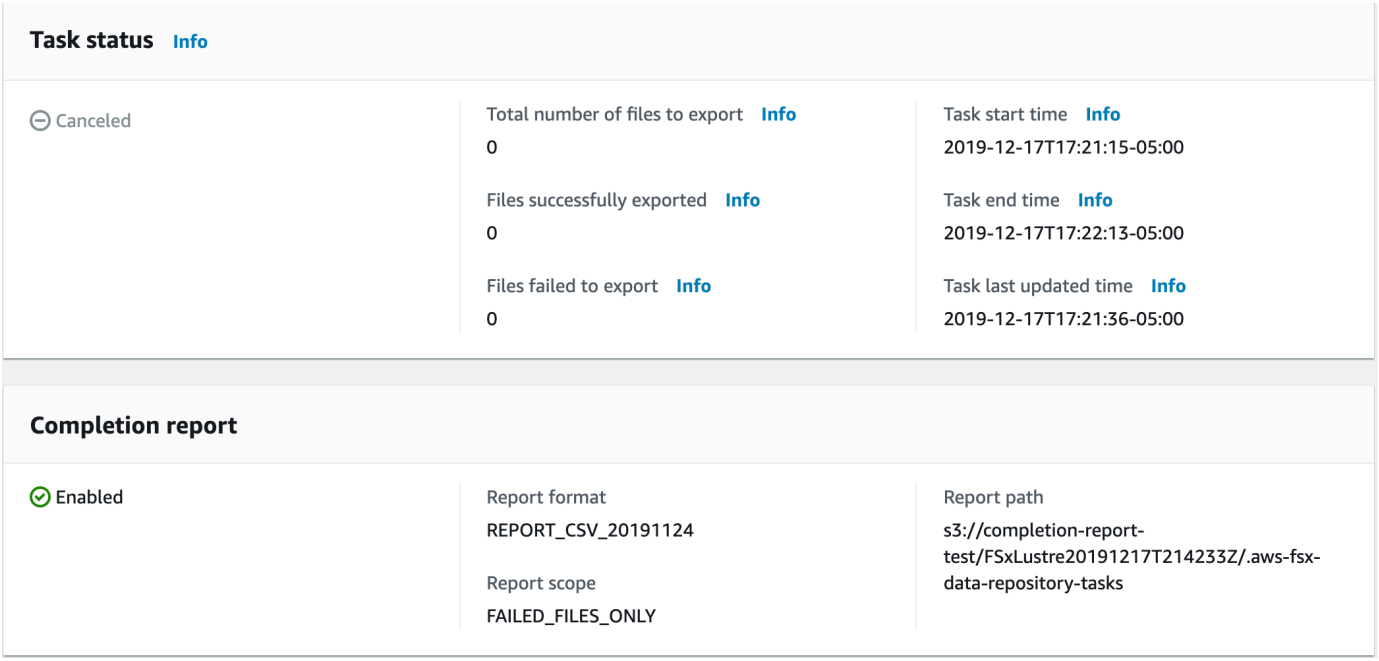
Después de crear una tarea de repositorio de datos, puede acceder a la tarea y a todas las tareas existentes en su cuenta mediante la consola, la CLI y la API de Amazon FSx. Amazon FSx proporciona la siguiente información detallada sobre las tareas:

- Todas las tareas existentes.
- Todas las tareas de un sistema de archivos específico.
- Todas las tareas de una asociación de repositorios de datos específica.
- Todas las tareas con un estado de ciclo de vida específico. Para obtener más información sobre los valores de estado del ciclo de vida de las tareas, consulte Comprender el estado y los detalles de una tarea.

Puede acceder a todas las tareas de repositorio de datos existentes en su cuenta mediante la consola, CLI o API de Amazon FSx, tal y como se describe a continuación.

Para ver las tareas del repositorio de datos y los detalles de las tareas (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación, elija Tareas del repositorio de datos (Lustre). Aparece la página de Tareas del repositorio de datos con las tareas existentes.
3. Para ver los detalles de una tarea, elija el ID de la tarea o el Nombre de la tarea en la página de Tareas del repositorio de datos. Aparece la página de detalles de la tarea.




Para recuperar las tareas del repositorio de datos y los detalles de las tareas (CLI)

Con el comando CLI `describe-data-repository-tasks` de Amazon FSx, podrá ver todas las tareas del repositorio de datos y sus detalles en su cuenta. `DescribeDataRepositoryTasks` es el comando de API equivalente.

- Utilice el siguiente comando para ver todos los objetos de tarea de repositorio de datos de su cuenta.

```
aws fsx describe-data-repository-tasks
```

  Si el comando tiene éxito, Amazon FSx devuelve la respuesta en formato JSON.

```
{
    "DataRepositoryTasks": [
        {
            "Lifecycle": "EXECUTING",
            "Paths": [],
            "Report": {
                "Path":"s3://dataset-01/reports",
                "Format":"REPORT_CSV_20191124",
                "Enabled":true,
                "Scope":"FAILED_FILES_ONLY"
            },
            "StartTime": 1591863862.288,
            "EndTime": ,
            "Type": "EXPORT_TO_REPOSITORY",
            "Tags": [],
            "TaskId": "task-0123456789abcdef3",
            "Status": {
                "SucceededCount": 4255,
                "TotalCount": 4200,
                "FailedCount": 55,
                "LastUpdatedTime": 1571863875.289
            },
            "FileSystemId": "fs-0123456789a7",
            "CreationTime": 1571863850.075,
            "ResourceARN": "arn:aws:fsx:us-east-1:1234567890:task/
task-0123456789abcdef3"
        },
        {
            "Lifecycle": "FAILED",
            "Paths": [],
            "Report": {
                "Enabled": false,
            },
            "StartTime": 1571863862.288,
            "EndTime": 1571863905.292,
            "Type": "EXPORT_TO_REPOSITORY",
            "Tags": [],
            "TaskId": "task-0123456789abcdef1",
            "Status": {
                "SucceededCount": 1153,
                "TotalCount": 1156,
                "FailedCount": 3,
                "LastUpdatedTime": 1571863875.289
```

```
            },
            "FileSystemId": "fs-0123456789abcdef0",
            "CreationTime": 1571863850.075,
            "ResourceARN": "arn:aws:fsx:us-east-1:1234567890:task/
task-0123456789abcdef1"
        },
        {
            "Lifecycle": "SUCCEEDED",
            "Paths": [],
            "Report": {
                "Path":"s3://dataset-04/reports",
                "Format":"REPORT_CSV_20191124",
                "Enabled":true,
                "Scope":"FAILED_FILES_ONLY"
            },
            "StartTime": 1571863862.288,
            "EndTime": 1571863905.292,
            "Type": "EXPORT_TO_REPOSITORY",
            "Tags": [],
            "TaskId": "task-04299453935122318",
            "Status": {
                "SucceededCount": 258,
                "TotalCount": 258,
                "FailedCount": 0,
                "LastUpdatedTime": 1771848950.012,
            },
            "FileSystemId": "fs-0123456789abcdef0",
            "CreationTime": 1771848950.012,
            "ResourceARN": "arn:aws:fsx:us-east-1:1234567890:task/
task-0123456789abcdef0"
        }
    ]
}
```

### Visualización de las tareas por sistema de archivos

Puede ver todas las tareas de un sistema de archivos específico mediante la consola, la CLI o la API de Amazon FSx, tal y como se describe a continuación.

Para ver las tareas por sistema de archivos (consola)

1. En el panel de navegación, elija File systems (Sistema de archivos). Aparece la página File system (Sistema de archivos).
2. Seleccione el sistema de archivos para el que desea ver las tareas del repositorio de datos. Aparecerá la página de detalles del sistema de archivos.
3. En la página de detalles del sistema de archivos, seleccione la pestaña Repositorio de datos. Todas las tareas de este sistema de archivos aparecen en el panel de Tareas del repositorio de datos.

Para recuperar tareas por sistema de archivos (CLI)

- Utilice el siguiente comando para ver todas las tareas del repositorio de datos del sistema de archivos `fs-0123456789abcdef0`.

```
aws fsx describe-data-repository-tasks \
    --filters Name=file-system-id,Values=fs-0123456789abcdef0
```

Si el comando tiene éxito, Amazon FSx devuelve la respuesta en formato JSON.

```
{
    "DataRepositoryTasks": [
        {
            "Lifecycle": "FAILED",
            "Paths": [],
            "Report": {
                "Path":"s3://dataset-04/reports",
                "Format":"REPORT_CSV_20191124",
                "Enabled":true,
                "Scope":"FAILED_FILES_ONLY"
            },
            "StartTime": 1571863862.288,
            "EndTime": 1571863905.292,
            "Type": "EXPORT_TO_REPOSITORY",
            "Tags": [],
            "TaskId": "task-0123456789abcdef1",
            "Status": {
                "SucceededCount": 1153,
                "TotalCount": 1156,
                "FailedCount": 3,
```

```
                "LastUpdatedTime": 1571863875.289
            },
            "FileSystemId": "fs-0123456789abcdef0",
            "CreationTime": 1571863850.075,
            "ResourceARN": "arn:aws:fsx:us-east-1:1234567890:task/
task-0123456789abcdef1"
        },
        {
            "Lifecycle": "SUCCEEDED",
            "Paths": [],
            "Report": {
                "Enabled": false,
            },
            "StartTime": 1571863862.288,
            "EndTime": 1571863905.292,
            "Type": "EXPORT_TO_REPOSITORY",
            "Tags": [],
            "TaskId": "task-0123456789abcdef0",
            "Status": {
                "SucceededCount": 258,
                "TotalCount": 258,
                "FailedCount": 0,
                "LastUpdatedTime": 1771848950.012,
            },
            "FileSystemId": "fs-0123456789abcdef0",
            "CreationTime": 1771848950.012,
            "ResourceARN": "arn:aws:fsx:us-east-1:1234567890:task/
task-0123456789abcdef0"
        }
    ]
}
```

## Cancelar una tarea de repositorio de datos

Puede cancelar una tarea de repositorio de datos mientras se encuentra en estado PENDIENTE o EN EJECUCIÓN. Cuando cancela una tarea, ocurre lo siguiente:

- Amazon FSx no procesa ningún archivo que esté en la cola para ser procesado.
- Amazon FSx continúa procesando cualquier archivo que esté actualmente en proceso.
- Amazon FSx no revierte ningún archivo que la tarea ya haya procesado.

Para cancelar una tarea de repositorio de datos (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Haga clic en el sistema de archivos para el que desee cancelar una tarea de repositorio de datos.
3. Abra la pestaña Repositorio de datos y desplácese hacia abajo para ver el panel Tareas del repositorio de datos.
4. Seleccione ID de tarea o Nombre de tarea para la tarea que quiere cancelar.
5. Seleccione Cancelar tarea para cancelar la tarea.
6. Introduzca el ID de la tarea para confirmar la solicitud de cancelación.

Para cancelar una tarea de repositorio de datos (consola)

Utilice el comando CLI `cancel-data-repository-task` de Amazon FSx para cancelar una tarea. `CancelDataRepositoryTask` es el comando de API equivalente.

- Utilice el siguiente comando para cancelar una tarea de repositorio de datos.

```
aws fsx cancel-data-repository-task \
    --task-id task-0123456789abcdef0
```

Si el comando tiene éxito, Amazon FSx devuelve la respuesta en formato JSON.

```
{
    "Status": "CANCELING",
    "TaskId": "task-0123456789abcdef0"
}
```

## Trabajar con informes de finalización de tareas

Un informe de finalización de tarea proporciona detalles sobre los resultados de una tarea de repositorio de datos de exportación, importación o liberación. El informe incluye los resultados de los archivos procesados por la tarea que coinciden con el alcance del informe. Puede especificar si se va a generar un informe para una tarea mediante el parámetro `Enabled`.

Amazon FSx entrega el informe al repositorio de datos enlazados del sistema de archivos en Amazon S3, utilizando la ruta que especificó al habilitar el informe para una tarea. El nombre de

archivo del informe es `report.csv` para las tareas de importación y `failures.csv` para las tareas de exportación o liberación.

El formato del informe es un archivo de valores separados por comas (CSV) que tiene tres campos: `FilePath`, `FileStatus` y `ErrorCode`.

Los informes se codifican con el formato RFC-4180 de la siguiente manera:

- Las rutas que comiencen con cualquiera de los siguientes caracteres aparecen entre comillas simples: `@ + - =`
- Las cadenas que contienen al menos uno de los caracteres siguientes van entre comillas dobles: `" ,`
- Todas las comillas dobles se escapan con una comilla doble adicional.

A continuación se muestran algunos ejemplos de codificación de informes:

- `@filename.txt` se convertirá en `"""@filename.txt"""`
- `+filename.txt` se convertirá en `"""+filename.txt"""`
- `file,name.txt` se convertirá en `"file,name.txt"`
- `file"name.txt` se convertirá en `"file""name.txt"`

Para obtener más información sobre la codificación RFC-4180, consulte Formato común RFC-4180 y tipo MIME para archivos de valores separados por comas [CSV] en el sitio web del IETF.

El siguiente es un ejemplo de la información proporcionada en un informe de finalización de tareas que incluye solo los archivos con errores.

```
myRestrictedFile,failed,S3AccessDenied
dir1/myLargeFile,failed,FileSizeTooLarge
dir2/anotherLargeFile,failed,FileSizeTooLarge
```

Para obtener más información sobre los fallos de las tareas y cómo resolverlos, consulte Resolución de fallos en las tareas del repositorio de datos.

## Resolución de fallos en las tareas del repositorio de datos

Puede activar el registro en CloudWatch Logs para registrar información sobre cualquier error que se haya producido al importar o exportar archivos mediante las tareas del repositorio de datos. Para

obtener información sobre CloudWatch los registros de eventos de Logs, consulteRegistros de eventos del repositorio de datos.

Cuando se produce un error en una tarea de repositorio de datos, puede encontrar el número de archivos que Amazon FSx no ha podido procesar en Error al exportar archivos en la página Estado de la tarea de la consola. O bien, puede usar la CLI o la API y ver la propiedad de la tarea `Status: FailedCount`. Para obtener información sobre cómo acceder a esta información, consulte Acceder a las tareas del repositorio de datos.

Para las tareas de repositorio de datos, Amazon FSx también proporciona, de forma opcional, información sobre los archivos y directorios específicos en los que se produjo un error en un informe de finalización. El informe de finalización de la tarea contiene la ruta del archivo o directorio del sistema de archivos de Lustre en el que se produjo el error, su estado y el motivo del error. Para obtener más información, consulte Trabajar con informes de finalización de tareas.

Una tarea de repositorio de datos puede fallar por varios motivos, incluidos los que se enumeran a continuación.

| Código de error | Explicación |
| --- | --- |
| `FileSizeTooLarge` | El tamaño máximo de objeto que admite Amazon S3 es de 5 TiB. |
| `InternalError` | Se ha producido un error en el sistema de archivos de Amazon FSx durante una tarea de importación, exportación o liberación. Por lo general, este código de error significa que el sistema de archivos de Amazon FSx en el que se ejecutó la tarea fallida se encuentra en un estado de ciclo de vida FAILED. Cuando esto ocurre, es posible que los archivos afectados no se puedan recuperar debido a la pérdida de datos. De lo contrario, puede utilizar los comandos de gestión de almacenamiento jerárquico (HSM) para exportar los archivos y directorios al repositorio de datos de S3. Para obtener más información, consulte Exportación de archivos mediante comandos de HSM. |

| Código de error | Explicación |
| --- | --- |
| `OperationNotPermitted` | Amazon FSx no ha podido liberar el archivo porque no se ha exportado a un bucket de S3 vinculado. Debe utilizar las tareas automátic as de exportación o exportación del repositorio de datos para asegurarse de que sus archivos se exporten primero al bucket de Amazon S3 vinculado. |
| `PathSizeTooLong` | La ruta de exportación es demasiado larga. La longitud máxima de la clave de objeto que admite S3 es de 1024 caracteres. |
| `ResourceBusy` | Amazon FSx no pudo exportar o liberar el archivo porque estaba siendo modificado por otro cliente del sistema de archivos. Puede volver a intentarlo una DataRepositoryTask vez que el flujo de trabajo haya terminado de escribir en el archivo. |

| Código de error | Explicación |
| --- | --- |
| `S3AccessDenied` | Se denegó el acceso a Amazon S3 para una tarea de exportación o importación de un repositorio de datos.<br><br>Para las tareas de exportación, el sistema de archivos de Amazon FSx debe tener permiso para realizar la operación `S3:PutObject` para exportar a un repositorio de datos vinculados en S3. Este permiso se concede en el rol vinculado al servicio `AWSServiceRoleForFSxS3Access_` *`fs-0123456789abcdef0`* . Para obtener más información, consulte Uso de roles vinculados a servicios para Amazon FSx.<br><br>Para las tareas de exportación, debido a que la tarea de exportación requiere que los datos fluyan fuera de la VPC de un sistema de archivos, este error puede producirse si el repositorio de destino tiene una política de bucket que contenga una de las claves de condición globales de IAM `aws:SourceVpc` o `aws:SourceVpce` .<br><br>Para las tareas de importación, el sistema de archivos Amazon FSx debe tener permiso para realizar las operaciones `S3:HeadObject` y `S3:GetObject` para importar desde un repositorio de datos enlazados en S3.<br><br>Para las tareas de importación, si su bucket de S3 usa el cifrado del lado del servidor con claves administradas por el cliente almacenadas en AWS Key Management Service (SSE-KMS), debe seguir las configuraciones de políticas que se indican en. Trabajo con |

| Código de error | Explicación |
| --- | --- |
| | buckets de Amazon S3 cifrados del lado del servidor<br><br>Si su bucket de S3 contiene objetos cargados desde una cuenta de bucket de S3 Cuenta de AWS distinta a la de su sistema de archivos, puede asegurarse de que las tareas del repositorio de datos puedan modificar los metadatos de S3 o sobrescribir los objetos de S3, independientemente de la cuenta en la que se hayan cargado. Le recomendamos que habilite la característica de la propiedad de objetos de S3 en el bucket de S3. Esta función le permite apropiarse de los objetos nuevos que otros Cuentas de AWS cargan en su bucket, ya que obliga a las cargas a proporcio nar la ACL predeterminada`-/-acl bucket-owner-full-control` . Para habilitar la propiedad de objetos de S3, elija la opción que prefiera el propietario del bucket en su bucket de S3. Para obtener más información, consulte Control de la propiedad de objetos cargados mediante la propiedad de objetos de S3 en la Guía del usuario de Amazon S3. |
| `S3Error` | Amazon FSx detectó un error relacionado con S3 que no era `S3AccessDenied` . |
| `S3FileDeleted` | Amazon FSx no pudo exportar un archivo de enlace duro porque el archivo de origen no existe en el repositorio de datos. |

| Código de error | Explicación |
| --- | --- |
| `S3ObjectInUnsupportedTier` | Amazon FSx ha importado correctamente un objeto sin enlace simbólico desde una clase de almacenamiento S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. El `FileStatus` será `succeeded with warning` en el informe de finalización de la tarea. La advertencia indica que, para recuperar los datos, primero debe restaurar el objeto S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive y luego utilizar un comando `hsm_restore` para importar el objeto. |
| `S3ObjectNotFound` | Amazon FSx no pudo importar o exportar el archivo porque no existe en el repositorio de datos. |
| `S3ObjectPathNotPosixCompliant` | El objeto Amazon S3 existe, pero no se puede importar porque no es un objeto compatible con POSIX. Para obtener información acerca de los metadatos POSIX soportados, consulte Soporte de metadatos POSIX para repositorios de datos. |
| `S3ObjectUpdateInProgressFromFileRename` | Amazon FSx no pudo liberar el archivo porque la exportación automática está procesando un cambio de nombre del archivo. El proceso de cambio de nombre de la exportación automática debe finalizar antes de poder liberar el archivo. |

| Código de error | Explicación |
| --- | --- |
| `S3SymlinkInUnsupportedTier` | Amazon FSx no pudo importar un objeto de enlace simbólico porque se encuentra en una clase de almacenamiento de Amazon S3 que no se admite, como la clase de almacenamiento S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. El `FileStatus` será `failed` en el informe de finalización de la tarea. |
| `SourceObjectDeletedBeforeReleasing` | Amazon FSx no pudo liberar el archivo del sistema de archivos porque el archivo fue eliminado del repositorio de datos antes de que pudiera ser liberado. |

## Liberación de archivos

Las tareas de repositorio de datos liberan los datos de los archivos de su sistema de archivos FSx for Lustre para liberar espacio para nuevos archivos. Al liberar un archivo, se retiene la lista de archivos y los metadatos, pero se elimina la copia local del contenido de ese archivo. Si un usuario o una aplicación accede a un archivo publicado, los datos se vuelven a cargar de forma automática y transparente en el sistema de archivos desde el bucket de Amazon S3 vinculado.

> **Note**
>
> Las tareas de repositorio de datos de versiones no están disponibles en los sistemas de archivos FSx for Lustre 2.10.

Los parámetros Rutas de publicación del sistema de archivos y Duración mínima desde el último acceso determinan qué archivos se publicarán.

- Rutas del sistema de archivos que se van a liberar: especifica la ruta desde la que se publicarán los archivos.
- Duración mínima desde el último acceso: especifica la duración, en días, para que se publique cualquier archivo al que no se haya accedido durante ese tiempo. El tiempo transcurrido desde la última vez que se accedió a un archivo se calcula tomando la diferencia entre la hora de

creación de la tarea de publicación y la última vez que se accedió a un archivo (el valor máximo es `atimemtime`, `yctime`).

Los archivos solo se publicarán a lo largo de la ruta del archivo si se han exportado a S3 y tienen una duración desde el último acceso superior a la duración mínima desde el último acceso. Si se establece una duración mínima de `0` días desde el último acceso, se liberarán los archivos independientemente de la duración que hayan tenido desde el último acceso.

> **Note**
>
> No se admite el uso de caracteres comodín para incluir o excluir archivos para su publicación.

Las tareas de publicación del repositorio de datos solo liberarán los datos de los archivos que ya se hayan exportado a un repositorio de datos de S3 vinculado. Puede exportar datos a S3 mediante la función de exportación automática, una tarea de exportación de un repositorio de datos o los comandos de HSM. Para comprobar que un archivo se ha exportado a su repositorio de datos, puede ejecutar el siguiente comando. Un valor devuelto de `states: (0x00000009) exists archived` indica que el archivo se ha exportado correctamente.

```
sudo lfs hsm_state path/to/export/file
```

> **Note**
>
> Debe ejecutar el comando HSM como usuario root o utilizando`sudo`.

Para publicar datos de archivos a intervalos regulares, puede programar una tarea de repositorio de datos de publicación periódica mediante Amazon EventBridge Scheduler. Para obtener más información, consulte Introducción a EventBridge Scheduler en la Guía del usuario de Amazon EventBridge Scheduler.

Temas

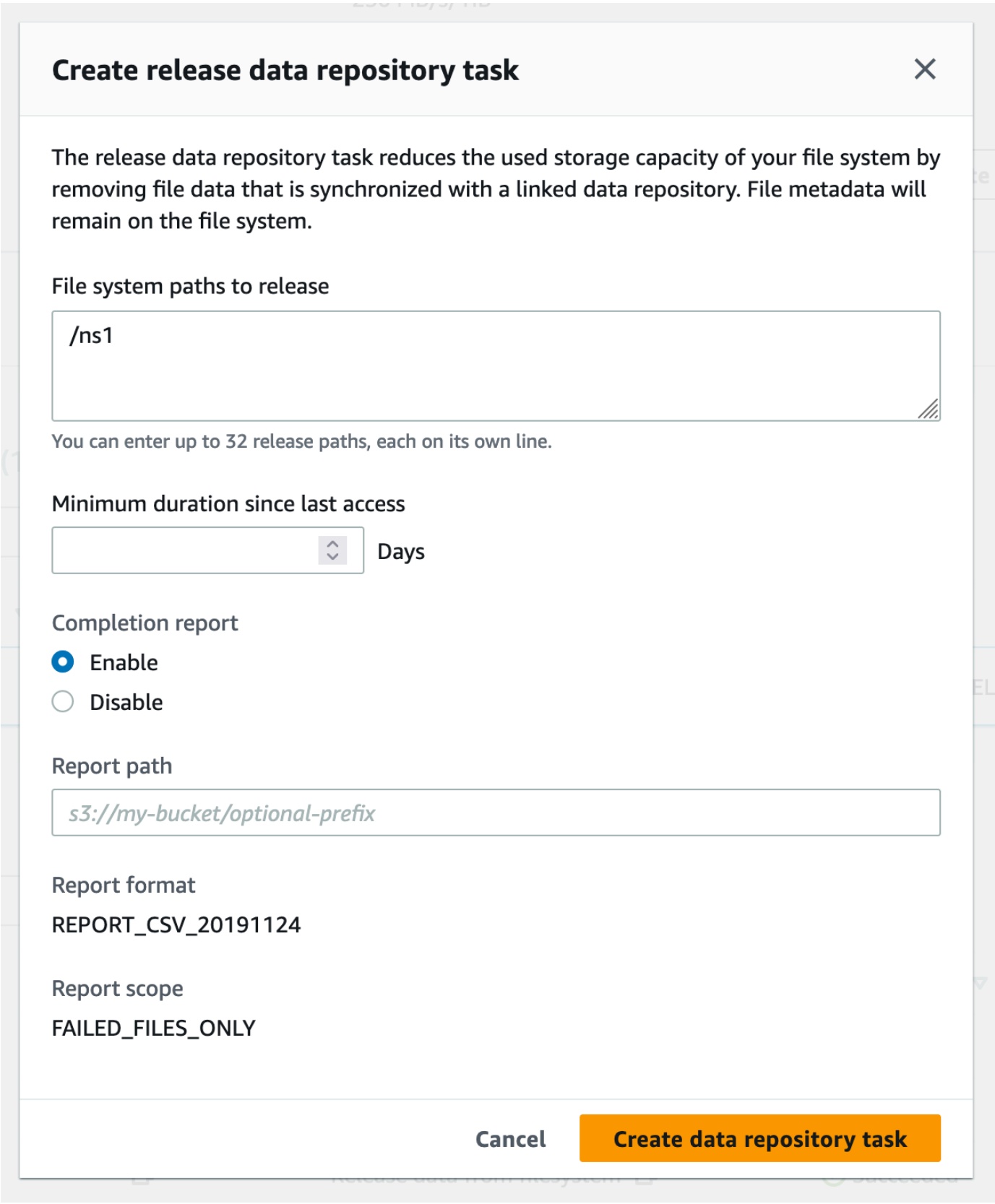
- Utilizar las tareas del repositorio de datos para liberar archivos

# Utilizar las tareas del repositorio de datos para liberar archivos

Utilice los siguientes procedimientos para crear tareas que liberen archivos del sistema de archivos mediante la consola Amazon FSx y la CLI. Al liberar un archivo, se retiene la lista de archivos y los metadatos, pero se elimina la copia local del contenido de ese archivo.

Para liberar archivos (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación izquierdo, elija File systems, a continuación, elija su sistema de archivos Lustre.
3. Elija la pestaña Data repository.
4. En el panel Data repository associations, elija la asociación de repositorios de datos para la que desea crear la tarea de liberación.
5. En Actions, elija Create read replica. Esta opción solo está disponible si el sistema de archivos está vinculado a un repositorio de datos en S3. Aparece el cuadro de diálogo de Create release data repository task.


Create release data repository task
The release data repository task reduces the used storage capacity of your file system by removing file data that is synchronized with a linked data repository. File metadata will remain on the file system.
File system paths to release
/ns1
You can enter up to 32 release paths, each on its own line.
Minimum duration since last access
Days
Completion report
Enable
Disable
Report path
s3://my-bucket/optional-prefix
Report format
REPORT_CSV_20191124
Report scope
FAILED_FILES_ONLY
Cancel
Create data repository task

6. En File system paths to release, especifique hasta 32 directorios o archivos que se van a liberar del sistema de archivos de Amazon FSx proporcionando las rutas a esos directorios o archivos. Las rutas que proporcione deben estar relacionadas con el punto de montaje del sistema de archivos. Por ejemplo, si el punto de montaje es `/mnt/fsx` y `/mnt/fsx/path1` es un archivo del sistema de archivos que desea liberar, la ruta que debe proporcionarse es `path1`. Para liberar todos los archivos del sistema de archivos, especifique una barra diagonal (/) como ruta.

   > **Note**
   >
   > Si la ruta que proporciona no es válida, la tarea devuelve un error.

7. En Minimum duration since last access, especifique la duración, en días, de modo que se libere cualquier archivo al que no se haya accedido durante ese período. La hora del último acceso se calcula utilizando el valor máximo de `atime`, `mtime`, y `ctime`. Se liberarán los archivos con un período de duración del último acceso superior a la duración mínima desde el último acceso (en relación con la hora de creación de la tarea). No se liberarán los archivos con un período de duración del último acceso inferior a este número de días, aunque estén en el campo File system paths to release. Indique una duración de `0` días para liberar los archivos independientemente de la duración desde el último acceso.
8. (Opcional) En Completion report, elija Enable para generar un informe de finalización de tareas que proporcione detalles sobre los archivos que cumplen el alcance indicado en el Report scope. Para especificar una ubicación para que Amazon FSx entregue el informe, introduzca una ruta relativa en el repositorio de datos de S3 vinculado del sistema de archivos para la Report path.
9. Elija Create data repository task.

   Una notificación en la parte superior de la página de File systems muestra la tarea que acaba de crear en curso.

Para ver el estado y los detalles de la tarea, en la pestaña Data Repository, desplácese hacia abajo hasta Data Repository Tasks. El orden predeterminado muestra la tarea más reciente en la parte superior de la lista.

Para ver un resumen de la tarea en esta página, elija el Task ID de la tarea que acaba de crear.

Para liberar archivos (CLI)

- Utilice el comando `create-data-repository-task` de la CLI para crear una tarea que libere archivos en el sistema de archivos FSx para Lustre. La operación de API correspondiente es `CreateDataRepositoryTask`.

  Establezca los siguientes parámetros:

  - Establezca `--file-system-id` como el ID del sistema de archivos del que está liberando archivos.
  - Establezca `--paths` en las rutas del sistema de archivos desde las que se liberarán los datos. Si se especifica un directorio, se liberan los archivos del directorio. Si se especifica una ruta de archivo, solo se libera ese archivo. Para liberar todos los archivos del sistema de archivos que se han exportado a un bucket de S3 vinculado, especifique una barra diagonal (/) para la ruta.
  - Establezca `--type` en `RELEASE_DATA_FROM_FILESYSTEM`.
  - Configure las opciones `--release-configuration DurationSinceLastAccess` de la siguiente manera:
    - `Unit`: se establece en `DAYS`.
    - `Value`: Especifique un número entero que represente la duración, en días, de modo que se libere cualquier archivo al que no se haya accedido durante ese período. Los archivos a los que se haya accedido durante un período inferior a este número de días no se liberarán, aunque estén incluidos en el parámetro `--paths`. Indique una duración de `0` días para liberar los archivos independientemente de la duración desde el último acceso.

  Este comando de ejemplo especifica que los archivos que se hayan exportado a un bucket de S3 vinculado y que cumplan los criterios `--release-configuration` se liberarán de los directorios de las rutas especificadas.

```
$ aws fsx create-data-repository-task \
    --file-system-id fs-0123456789abcdef0 \
    --type RELEASE_DATA_FROM_FILESYSTEM \
    --paths path1,path2/file1 \
    --release-configuration '{"DurationSinceLastAccess":
{"Unit":"DAYS","Value":10}}' \
    --report Enabled=false
```

Después de crear correctamente la tarea de repositorio de datos, Amazon FSx devuelve la descripción de la tarea en formato JSON.

Después de crear la tarea para liberar los archivos, puede comprobar el estado de la tarea. Para obtener más información sobre cómo ver las tareas del repositorio de datos, consulte Acceder a las tareas del repositorio de datos.

## Uso de Amazon FSx con sus datos en las instalaciones

Puede usar FSx para Lustre para procesar sus datos en las instalaciones con instancias de computación en la nube. FSx para Lustre admite el acceso AWS Direct Connect a través de una VPN, lo que le permite montar sus sistemas de archivos desde clientes en las instalaciones.

Para utilizar FSx para Lustre con sus datos en las instalaciones

1. Cree un sistema de archivos. Para más información, consulte Cree su sistema de archivos FSx for Lustre en el ejercicio de introducción.
2. Monte el sistema de archivos desde clientes en las instalaciones. Para más información, consulte Montaje de sistemas de archivos de Amazon FSx en las instalaciones o desde una VPC de Amazon interconectada.
3. Copie los datos que desea procesar en su sistema de archivos de FSx para Lustre.
4. Ejecute su carga de trabajo de procesamiento intensivo en instancias Amazon EC2 en la nube montando su sistema de archivos.
5. Al terminar, copie los resultados finales de su sistema de archivos a su ubicación de datos en las instalaciones y elimine su sistema de archivos FSx para Lustre.

## Registros de eventos del repositorio de datos

Puede activar el registro en CloudWatch Logs para registrar información sobre cualquier error que se haya producido al importar o exportar archivos mediante las tareas de importación automática, exportación automática y repositorio de datos. Para obtener más información, consulte Iniciar sesión con Amazon CloudWatch Logs.

> **Note**
>
> Cuando se produce un error en una tarea de repositorio de datos, Amazon FSx también escribe la información del error en el informe de finalización de la tarea. Para obtener más información acerca de los errores en los informes de finalización, consulte Resolución de fallos en las tareas del repositorio de datos.

Las tareas de importación automática, exportación automática y repositorio de datos pueden fallar por varios motivos, incluidos los que se indican a continuación. Para obtener información acerca de la visualización de estos registros, consulte Visualización de registros.

Importación de eventos

| Código de error | Nivel de registro | Mensajes de registro | Causa raíz | Código de error al finalizar el informe |
|---|---|---|---|---|
| `S3ImportListObjectError` | ERROR | *No se pudieron enumerar los objetos de S3 en el bucket de S3 bucket_name con el prefijo*. | Amazon FSx no pudo enumerar los objetos de S3 en el bucket de S3. Esto puede ocurrir si la política del bucket de S3 no proporciona suficientes permisos a Amazon FSx. | N/A |
| `S3ImportUnsupportedTierWarning` | WARN | Se ha producido un error al importar un objeto de S3 con la clave | Amazon FSx no pudo importar un objeto de S3 porque se encuentra en | `S3ObjectInUnsupportedTier` |

| Código de error | Nivel de registro | Mensajes de registro | Causa raíz | Código de error al finalizar el informe |
|---|---|---|---|---|
| | | *key_value* en el bucket de S3 *bucket_name* debido a un objeto de S3 en un nivel no admitido *S3_tier_name* . | una clase de almacenamiento de Amazon S3 que no se admite, como la clase de almacenamiento S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. | |

| Código de error | Nivel de registro | Mensajes de registro | Causa raíz | Código de error al finalizar el informe |
|---|---|---|---|---|
| `S3ImportSymlinkInUnsupportedTierWarning` | WARN | Se ha producido un error al importar un objeto de S3 con la clave *`key_value`* en el bucket de S3 *`bucket_name`* debido a un objeto de enlace simbólico S3 en un nivel no admitido *`S3_tier_name`* . | Amazon FSx no pudo importar un objeto de enlace simbólico porque se encuentra en una clase de almacenamiento de Amazon S3 que no se admite, como la clase de almacenamiento S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. | `S3SymlinkInUnsupportedTier` |

| Código de error | Nivel de registro | Mensajes de registro | Causa raíz | Código de error al finalizar el informe |
|---|---|---|---|---|
| `S3ImportAccessDenied` | ERROR | No se pudo importar el objeto de S3 con la clave *`key_value`* en el bucket de S3 *`bucket_name`* porque se denegó el acceso al objeto de S3. | Se denegó el acceso a Amazon S3 para una tarea de exportación e importación de un repositorio de datos.<br><br>Para las tareas de importación, el sistema de archivos Amazon FSx debe tener permiso para realizar las operaciones `s3:HeadObject` y `s3:GetObject` para importar desde un repositorio de datos enlazados en S3.<br><br>Para las tareas de importación, si su bucket de S3 utiliza cifrado del lado | `S3AccessDenied` |

| Código de error | Nivel de registro | Mensajes de registro | Causa raíz | Código de error al finalizar el informe |
|---|---|---|---|---|
| | | | del servidor con claves administradas por el cliente almacenadas en AWS Key Managemen t Service (SSE-KMS) , debe seguir las configura ciones de política que se indican en Trabajo con buckets de Amazon S3 cifrados del lado del servidor. | |

| Código de error | Nivel de registro | Mensajes de registro | Causa raíz | Código de error al finalizar el informe |
|---|---|---|---|---|
| `S3ImportDeleteAccessDenied` | ERROR | No se pudo eliminar el archivo local para el objeto de S3 con la clave *`key_value`* en el bucket de S3 *`bucket_name`* porque se denegó el acceso al objeto de S3. | Se denegó el acceso a un objeto de S3 a la importación automática. | N/A |

| Código de error | Nivel de registro | Mensajes de registro | Causa raíz | Código de error al finalizar el informe |
|---|---|---|---|---|
| `S3ImportObjectPathNotPosixCompliant` | ERROR | No se pudo importar el objeto de S3 con la clave *`key_value`* en el bucket de S3 *`bucket_name`* porque el objeto de S3 no es compatible con POSIX. | El objeto Amazon S3 existe, pero no se puede importar porque no es un objeto compatible con POSIX. Para obtener información acerca de los metadatos POSIX soportados, consulte Soporte de metadatos POSIX para repositorios de datos. | `S3ObjectPathNotPosixCompliant` |

| Código de error | Nivel de registro | Mensajes de registro | Causa raíz | Código de error al finalizar el informe |
|---|---|---|---|---|
| `S3ImportObjectTypeMismatch` | ERROR | No se pudo importar el objeto S3 con la clave *`key_value`* en el bucket de S3 *`bucket_name`* porque ya se ha importado un objeto de S3 con el mismo nombre en el sistema de archivos. | El objeto de S3 que se está importando es de un tipo diferente (archivo o directorio) al de un objeto existente con el mismo nombre en el sistema de archivos. | `S3ObjectTypeMismatch` |
| `S3ImportDirectoryMetadataUpdateError` | ERROR | No se pudieron actualizar los metadatos del directorio local debido a un error interno. | No se pudieron importar los metadatos de directorio debido a un error interno. | N/A |

| Código de error | Nivel de registro | Mensajes de registro | Causa raíz | Código de error al finalizar el informe |
|---|---|---|---|---|
| `S3ImportObjectDeleted` | ERROR | No se pudo importar el objeto de S3 con la clave *`key_value`* porque no se encontró en el bucket de S3 *`bucket_name`* . | Amazon FSx no pudo importar los metadatos de los archivos porque el objeto correspondiente no existe en el repositorio de datos. | `S3FileDeleted` |
| `S3ImportBucketDoesNotExist` | ERROR | No se pudo importar el objeto de S3 con la clave *`key_value`* en el bucket de S3 *`bucket_name`* porque el bucket no existe. | Amazon FSx no puede importar automáticamente un objeto de S3 al sistema de archivos porque el bucket de S3 ya no existe. | N/A |

| Código de error | Nivel de registro | Mensajes de registro | Causa raíz | Código de error al finalizar el informe |
|---|---|---|---|---|
| `S3ImportDeleteBucketDoesNotExist` | ERROR | No se pudo eliminar el archivo local para el objeto de S3 con la clave *`key_value`* en el bucket de S3 *`bucket_name`* porque el bucket no existe. | Amazon FSx no puede eliminar un archivo vinculado a un objeto de S3 en el sistema de archivos porque el bucket de S3 ya no existe. | N/A |
| `S3ImportDirectoryCreateError` | ERROR | No se pudo crear el directorio local debido a un error interno. | Amazon FSx no pudo importar automáticamente la creación de un directorio en el sistema de archivos debido a un error interno. | N/A |

| Código de error | Nivel de registro | Mensajes de registro | Causa raíz | Código de error al finalizar el informe |
|---|---|---|---|---|
| `NoDiskSpace` | ERROR | No se pudo importar el objeto S3 con la clave *`key_value`* en el bucket de S3 *`bucket_name`* porque el sistema de archivos está lleno. | El sistema de archivos se quedó sin espacio en disco en el servidor de metadatos mientras se creaba el archivo o directorio. | N/A |

Exportación de eventos

| Código de error | Nivel de registro | Mensajes de registro | Causa raíz | Código de error al finalizar el informe |
|---|---|---|---|---|
| `S3ExportInternalError` | ERROR | No se pudo exportar el objeto de S3 con la clave *`key_value en el`* bucket de S3 *`bucket_name`* debido a un error interno. | El objeto no se exportó debido a un error interno. | `INTERNAL_ERROR` |
| `S3ExportAccessDenied` | ERROR | No se pudo exportar el archivo porque se denegó | Se denegó el acceso a Amazon S3 para una tarea de | `S3AccessDenied` |

| Código de error | Nivel de registro | Mensajes de registro | Causa raíz | Código de error al finalizar el informe |
|---|---|---|---|---|
| | | el acceso al objeto de S3 con la clave *key_value* en el bucket de S3 *bucket_name* . | exportación de un repositorio de datos.<br><br>Para las tareas de exportación, el sistema de archivos de Amazon FSx debe tener permiso para realizar la operación `s3:PutObject` para exportar a un repositorio de datos vinculados en S3. Este permiso se concede en el rol vinculado al servicio `AWSServiceRoleForFSxS3Access_` *fs-0123456789abcdef0* . Para obtener más información, consulte Uso de roles vinculados | |

| Código de error | Nivel de registro | Mensajes de registro | Causa raíz | Código de error al finalizar el informe |
|---|---|---|---|---|
| | | | a servicios para Amazon FSx.<br><br>Como la tarea de exportación requiere que los datos fluyan fuera de la VPC de un sistema de archivos, este error puede producirse si el repositorio de destino tiene una política de bucket que contenga una de las claves de condición globales de IAM `aws:SourceVpc` o `aws:SourceVpce`.<br><br>Si su bucket de S3 contiene objetos cargados desde una Cuenta de AWS diferente a la de su cuenta de bucket de | |

| Código de error | Nivel de registro | Mensajes de registro | Causa raíz | Código de error al finalizar el informe |
|---|---|---|---|---|
| | | | S3 vinculada al sistema de archivos, puede asegurarse de que sus tareas de repositorio de datos puedan modificar los metadatos de S3 o sobrescribir objetos de S3 independientemente de la cuenta que los haya cargado. Le recomendamos que habilite la característica de la propiedad de objetos de S3 en el bucket de S3. Esta característica le permite tomar posesión de los nuevos objetos que otras Cuentas de AWS suben en el bucket, al forzar las subidas para proporcionar la ACL `--acl` | |

| Código de error | Nivel de registro | Mensajes de registro | Causa raíz | Código de error al finalizar el informe |
|---|---|---|---|---|
| | | | `bucket-owner-full-control` predefinida. Para habilitar la propiedad de objetos de S3, elija la opción que prefiera el propietario del bucket en su bucket de S3. Para obtener más información, consulte Control de la propiedad de objetos cargados mediante la propiedad de objetos de S3 en la Guía del usuario de Amazon S3. | |

| Código de error | Nivel de registro | Mensajes de registro | Causa raíz | Código de error al finalizar el informe |
|---|---|---|---|---|
| `S3ExportPathSizeTooLong` | ERROR | No se pudo exportar el archivo porque el tamaño de la ruta del archivo local supera la longitud máxima de clave de objeto admitida por S3. | La ruta de exportación es demasiado larga. La longitud máxima de la clave de objeto que admite S3 es de 1024 caracteres. | `PathSizeTooLong` |
| `S3ExportFileSizeTooLarge` | ERROR | No se pudo exportar el archivo porque su tamaño supera el tamaño máximo admitido para los objetos de S3. | El tamaño máximo de objeto que admite Amazon S3 es de 5 TiB. | `FileSizeTooLarge` |

| Código de error | Nivel de registro | Mensajes de registro | Causa raíz | Código de error al finalizar el informe |
|---|---|---|---|---|
| `S3ExportKMSKeyNotFound` | ERROR | No se pudo exportar el archivo del objeto de S3 con la clave *`key_value`* en el bucket de S3 *`bucket_name`* porque no se encontró la clave de KMS del bucket. | Amazon FSx no pudo exportar el archivo porque AWS KMS key no se pudo encontrar. Asegúrese de utilizar una clave que esté en la misma Región de AWS que el bucket de S3. Para obtener más información sobre la creación de claves KMS, consulte Creating keys (Creación de claves) en la Guía para desarrolladores de AWS Key Management Service. | `N/A` |

| Código de error | Nivel de registro | Mensajes de registro | Causa raíz | Código de error al finalizar el informe |
|---|---|---|---|---|
| `S3ExportResourceBusy` | ERROR | No se pudo exportar el archivo porque lo está utilizando otro proceso. | Amazon FSx no pudo exportar el archivo porque lo estaba modificando otro cliente del sistema de archivos. Puede volver a intentar la tarea cuando el flujo de trabajo haya terminado de escribirse en el archivo. | `ResourceBusy` |
| `S3ExportLocalObjectReleaseWithoutS3Source` | WARN | Exportación omitida: el archivo local está en estado liberado y no se ha encontrado un objeto de S3 vinculado con la clave *`key_value`* en el bucket *`bucket_name`* . | Amazon FSx no pudo exportar el archivo porque estaba publicado en el sistema de archivos. | N/A |

| Código de error | Nivel de registro | Mensajes de registro | Causa raíz | Código de error al finalizar el informe |
|---|---|---|---|---|
| `S3ExportLocalObjectNotMatchDra` | WARN | Exportación omitida: el archivo local no pertenece a una ruta de sistema de archivos vinculada a un repositorio de datos. | Amazon FSx no pudo exportar porque el objeto no pertenece a una ruta del sistema de archivos vinculada a un repositorio de datos. | N/A |
| `InternalAutoExportError` | ERROR | La exportación automática detectó un error interno al exportar un objeto del sistema de archivos | La exportación ha fallado debido a un error interno (a nivel de autoexportación o de lustre). | N/A |
| `S3CompletionReportUploadFailure` | ERROR | No se pudo cargar el informe de finalización de la tarea del repositorio de datos en *`bucket_name`* | Amazon FSx no ha podido cargar el informe de finalización. | N/A |

| Código de error | Nivel de registro | Mensajes de registro | Causa raíz | Código de error al finalizar el informe |
|---|---|---|---|---|
| `S3CompletionReportValidateFailure` | ERROR | No se pudo cargar el informe de finalización de la tarea del repositorio de datos en el bucket *`bucket_name`* porque la ruta del informe de finalización, *`report_path`*, no pertenece a un repositorio de datos asociado a este sistema de archivos | Amazon FSx no pudo cargar el informe de finalización porque la ruta S3 proporcionada por el cliente no pertenece a un repositorio de datos vinculado. | N/A |

# Trabajar con tipos de implementación antiguos

Esta sección se aplica a los sistemas de archivos con tipo de implementación Scratch 1, y también a los sistemas de archivos con tipos de implementación `Scratch 2` o `Persistent 1` que no utilizan asociaciones de repositorios de datos.

Temas

- Vincular su sistema de archivos a un bucket de Amazon S3
- Importar automáticamente actualizaciones desde un bucket de S3

# Vincular su sistema de archivos a un bucket de Amazon S3

Al crear un sistema de archivos de Amazon FSx para Lustre, puede vincularlo a un repositorio de datos duraderos en Amazon S3. Antes de crear su sistema de archivos, asegúrese de que ya haya creado el bucket de Amazon S3 al que va a realizar el enlace. En el asistente Crear sistema de archivos, se establecen las siguientes propiedades de configuración del repositorio de datos en el panel opcional Importar/Exportar repositorio de datos.

- Elija cómo mantiene actualizados Amazon FSx las descripciones de archivos y directorios a medida que agrega o modifica objetos en el bucket de S3 después de crear el sistema de archivos. Para obtener más información, consulte Importar automáticamente actualizaciones desde un bucket de S3.
- Importar bucket:: ingrese el nombre del bucket de S3 que está utilizando para el repositorio vinculado.
- Prefijo de importación: introduzca un prefijo de importación opcional si desea importar solo algunos listados de datos de archivos y directorios de su bucket de S3 a su sistema de archivos. El prefijo de importación define desde qué lugar del bucket de S3 se van a importar los datos.
- Prefijo de exportación: define dónde exporta Amazon FSx el contenido de su sistema de archivos a su bucket de S3 vinculado.

Puede tener una asignación 1:1 en la que Amazon FSx exporte datos desde su sistema de archivos FSx para Lustre a los mismos directorios del bucket de S3 desde el que se importaron. Para tener una asignación 1:1, especifique una ruta de exportación al bucket de S3 sin prefijos cuando cree su sistema de archivos.

- Al crear un sistema de archivos mediante la consola, elija la opción Exportar prefijo > El prefijo que especifique y deje el campo del prefijo en blanco.
- Al crear un sistema de archivos usando la CLI o la API AWS, especifique la ruta de exportación como el nombre del bucket de S3 sin prefijos adicionales, por ejemplo, `ExportPath=s3://lustre-export-test-bucket/`.

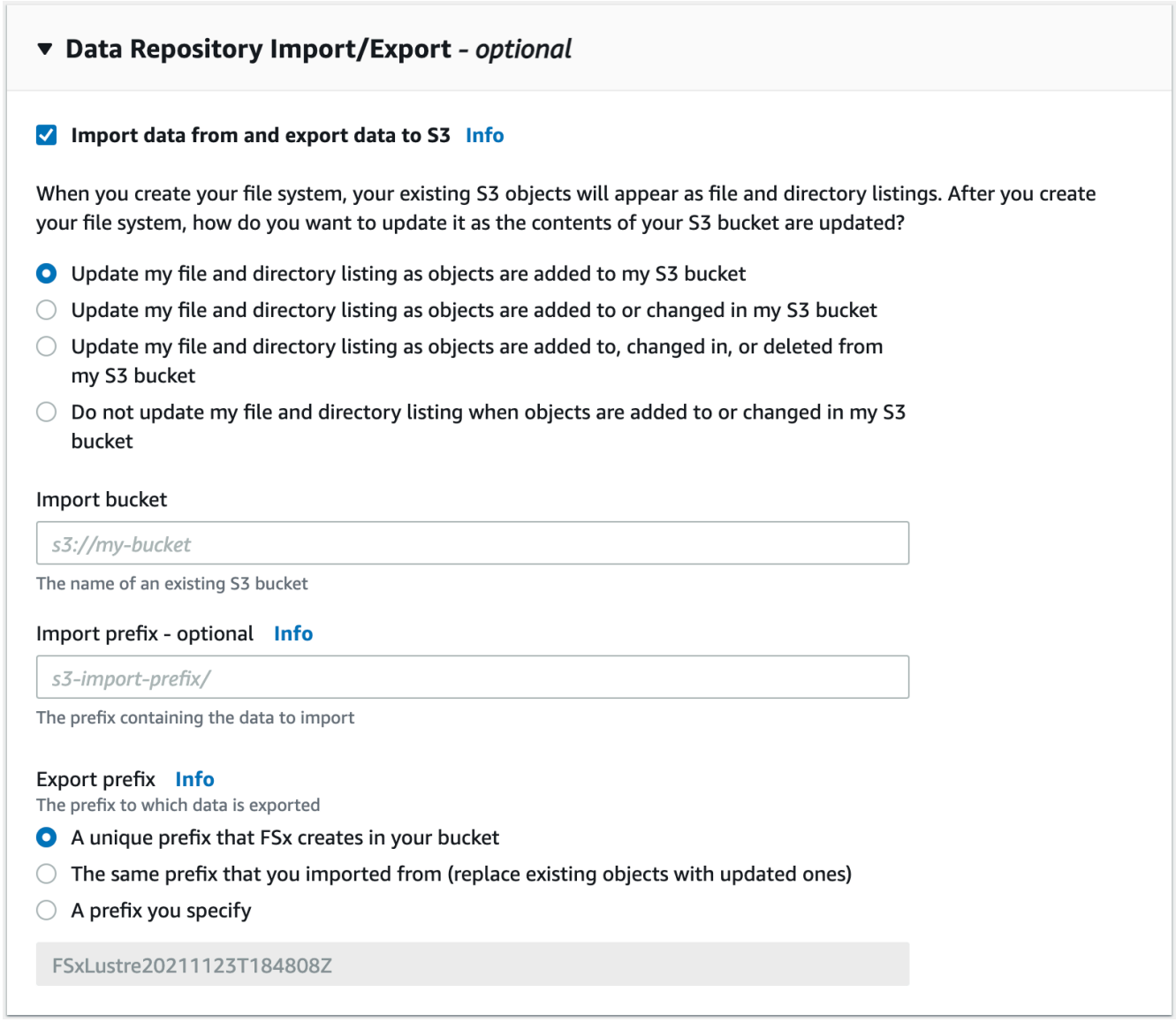
Utilizando este método, puede incluir un prefijo de importación cuando especifique la ruta de importación, y no afecta a una asignación 1:1 para las exportaciones.

## Creación de sistemas de archivos vinculados a un bucket de S3

Los siguientes procedimientos lo guiarán por el proceso de creación de un sistema de archivos Amazon FSx vinculado a un bucket de S3 mediante la consola de administración AWS y la interfaz de la línea de comandos AWS (AWSCLI).

Console

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel, elija Crear sistema de archivos.
3. Para el tipo de sistema de archivos, elija FSx para Lustre y seleccione Siguiente.
4. Proporcione la información necesaria para las secciones Información del sistema de archivos y Red y seguridad. Para obtener más información, consulte Cree su sistema de archivos FSx for Lustre.
5. Utilice el panel de Importación/Exportación de repositorios de datos para configurar un repositorio de datos vinculados en Amazon S3. Seleccione Importar datos y exportar datos a S3 para ampliar la sección Importación/Exportación del repositorio de datos y configurar los ajustes del repositorio de datos.




6. Elige cómo Amazon FSx mantiene actualizado el listado de archivos y directorios a medida que agrega o modificas objetos en el bucket de S3. Al crear el sistema de archivos, los objetos de S3 existentes aparecen como descripciones de archivos y directorios.

   - Actualizar mi lista de archivos y directorios a medida que se agregan objetos a mi bucket de S3: (predeterminado) Amazon FSx actualiza automáticamente las descripciones de archivos y directorios de cualquier objeto nuevo agregado al bucket de S3 vinculado que no exista actualmente en el sistema de archivos FSx. Amazon FSx no actualiza los listados de objetos que hayan cambiado en el bucket de S3. Amazon FSx no elimina los listados de objetos que se eliminan en el bucket de S3.

> **Note**
>
> La configuración predeterminada de las preferencias de importación para importar datos de un bucket de S3 vinculado mediante la CLI y la API es `NONE`. La configuración predeterminada de las preferencias de importación al utilizar la consola es actualizar Lustre a medida que se agregan nuevos objetos al bucket de S3.

- Actualizar mi listado de archivos y directorios a medida que se agregan o modifican objetos en mi bucket de S3: Amazon FSx actualiza automáticamente los listados de archivos y directorios de cualquier objeto nuevo agregado al bucket de S3 y de cualquier objeto existente que se cambie en el bucket de S3 después de elegir esta opción. Amazon FSx no elimina los listados de objetos que se eliminan en el bucket de S3.
- Actualizar mi lista de archivos y directorios a medida que se agregan, modifican o eliminan objetos de mi bucket de S3: Amazon FSx actualiza automáticamente los listados de archivos y directorios de cualquier objeto nuevo agregado al bucket de S3, de cualquier objeto existente que se cambie en el bucket de S3 y de cualquier objeto existente que se elimine en el bucket de S3 después de elegir esta opción.
- No actualizar mi archivo y directamente listado al agregar, cambiar o eliminar objetos de mi bucket de S3: Amazon FSx solo actualiza los listados de archivos y directorios del bucket de S3 vinculado cuando se crea el sistema de archivos. FSx no actualiza los listados de archivos y directorios para los objetos nuevos, modificados o eliminados después de elegir esta opción.

7. Introduzca un prefijo de importación opcional si desea importar solo algunos de los listados de archivos y directorios de datos de su bucket de S3 en el sistema de archivos. El prefijo de importación define desde qué lugar del bucket de S3 se van a importar los datos. Para obtener más información, consulte Importe automáticamente actualizaciones desde un bucket de S3.
8. Elija una de las opciones de Prefijo de exportación disponibles:

   - Un prefijo único que Amazon FSx crea en su bucket: elija esta opción para exportar objetos nuevos y modificados utilizando un prefijo generado por FSx para Lustre. El resultado es similar al siguiente: `/FSxLustre`*`file-system-creation- timestamp`*. La marca temporal está en formato UTC. Por ejemplo `FSxLustre20181105T222312Z`.

- El mismo prefijo del que importó (sustituya los objetos existentes por los actualizados): seleccione esta opción para reemplazar los objetos existentes por otros actualizados.
- Un prefijo que especifique: elija esta opción para conservar los datos importados y exportar los objetos nuevos y modificados con el prefijo que especifique. Para lograr una asignación 1:1 al exportar datos a su bucket de S3, elija esta opción y deje en blanco el campo de prefijo. FSx exportará los datos a los mismos directorios desde los que se importaron.

9. (Opcional) Establezca las Preferencias de mantenimiento o utilice los valores predeterminados del sistema.
10. Elija Siguiente y revise la configuración. Realice los cambios necesarios.
11. Seleccione Crear sistema de archivos.

AWS CLI

El siguiente ejemplo crea un sistema de archivos Amazon FSx vinculado al `lustre-export-test-bucket`, con una preferencia de importación que importa cualquier archivo nuevo, modificado o eliminado del repositorio de datos vinculado una vez creado el sistema de archivos.

> **Note**
>
> La configuración predeterminada de las preferencias de importación para importar datos de un bucket de S3 vinculado mediante la CLI y la API es `NONE`, que es diferente del comportamiento predeterminado cuando se utiliza la consola.

Para crear un sistema de archivos FSx para Lustre, utilice el comando CLI `create-file-system` de Amazon FSx, como se muestra a continuación. La operación de API correspondiente es `CreateFileSystem`.

```
$ aws fsx create-file-system \
--client-request-token CRT1234 \
--file-system-type LUSTRE \
--file-system-type-version 2.10 \
--lustre-configuration
AutoImportPolicy=NEW_CHANGED_DELETED,DeploymentType=SCRATCH_1,ImportPath=s
3://lustre-export-test-bucket/,ExportPath=s3://lustre-export-test-bucket/export,
PerUnitStorageThroughput=50 \
--storage-capacity 2400 \
--subnet-ids subnet-123456 \
```

```
--tags Key=Name,Value=Lustre-TEST-1 \
--region us-east-2
```

Después de crear correctamente el sistema de archivos, Amazon FSx devuelve la descripción del sistema de archivos como JSON, tal y como se muestra en el siguiente ejemplo.

```
{
    "FileSystems": [
        {
            "OwnerId": "owner-id-string",
            "CreationTime": 1549310341.483,
            "FileSystemId": "fs-0123456789abcdef0",
            "FileSystemType": "LUSTRE",
            "FileSystemTypeVersion": "2.10",
            "Lifecycle": "CREATING",
            "StorageCapacity": 2400,
            "VpcId": "vpc-123456",
            "SubnetIds": [
                "subnet-123456"
            ],
            "NetworkInterfaceIds": [
                "eni-039fcf55123456789"
            ],
            "DNSName": "fs-0123456789abcdef0.fsx.us-east-2.amazonaws.com",
            "ResourceARN": "arn:aws:fsx:us-east-2:123456:file-system/
fs-0123456789abcdef0",
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "Lustre-TEST-1"
                }
            ],
            "LustreConfiguration": {
                "DeploymentType": "PERSISTENT_1",
                "DataRepositoryConfiguration": {
                    "AutoImportPolicy": "NEW_CHANGED_DELETED",
                    "Lifecycle": "UPDATING",
                    "ImportPath": "s3://lustre-export-test-bucket/",
                    "ExportPath": "s3://lustre-export-test-bucket/export",
                    "ImportedFileChunkSize": 1024
                },
                "PerUnitStorageThroughput": 50
            }
```

```
        }
    ]
}
```

## Visualización de la ruta de exportación de un sistema de archivos

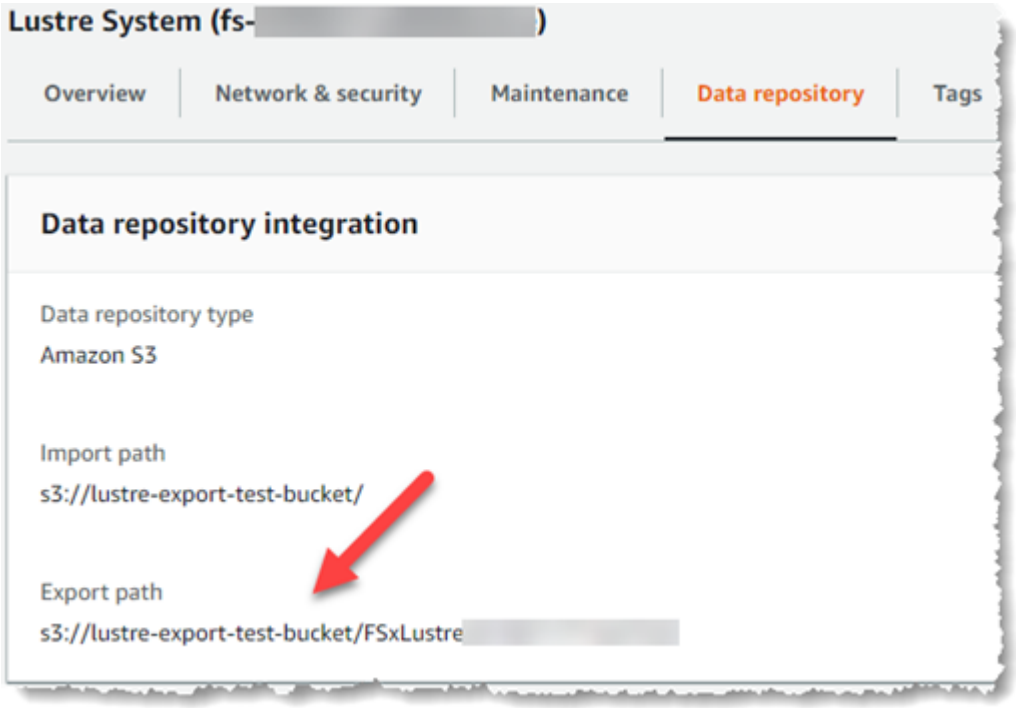
Puede ver la ruta de exportación de un sistema de archivos mediante la consola FSx para Lustre, la CLI AWS y la API.

Console

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/
2. Elija Nombre del sistema de archivos o ID del sistema de archivos para el sistema de archivos FSx para Lustre para el que desea ver la ruta de exportación.

   Aparecerá la página de detalles del sistema de archivos correspondiente.
3. Elija la pestaña Repositorio de datos.

   Aparece el panel de Integración del repositorio de datos que muestra las rutas de importación y exportación.



CLI

Para determinar la ruta de exportación del sistema de archivos, utilice el comando CLI describe-file-systemsAWS.

```
aws fsx describe-file-systems
```

Busque la propiedad `ExportPath` en `LustreConfiguration` en la respuesta.

```
{
    "OwnerId": "111122223333",
    "CreationTime": 1563382847.014,
    "FileSystemId": "",
    "FileSystemType": "LUSTRE",
    "Lifecycle": "AVAILABLE",
    "StorageCapacity": 2400,
    "VpcId": "vpc-6296a00a",
    "SubnetIds": [
        "subnet-1111111"
    ],
    "NetworkInterfaceIds": [
        "eni-0c288d5b8cc06c82d",
        "eni-0f38b702442c6918c"
    ],
    "DNSName": "fs-0123456789abcdef0.fsx.us-east-2.amazonaws.com",
    "ResourceARN": "arn:aws:fsx:us-east-2:267731178466:file-system/
fs-0123456789abcdef0",
    "Tags": [
        {
          "Key": "Name",
          "Value": "Lustre System"
        }
    ],
 "LustreConfiguration": {
    "DeploymentType": "SCRATCH_1",
    "DataRepositoryConfiguration": {
    "AutoImportPolicy": " NEW_CHANGED_DELETED",
    "Lifecycle": "AVAILABLE",
    "ImportPath": "s3://lustre-export-test-bucket/",
    "ExportPath": "s3://lustre-export-test-bucket/FSxLustre20190717T164753Z",
    "ImportedFileChunkSize": 1024
    }
  },
```

```
  "PerUnitStorageThroughput": 50,
  "WeeklyMaintenanceStartTime": "6:09:30"
}
```

### Estado del ciclo de vida del repositorio de datos

El estado del ciclo de vida del repositorio de datos proporciona información de estado sobre el repositorio de datos vinculado del sistema de archivos. Un repositorio de datos puede tener los siguientes estados de ciclo de vida.

- En creación: Amazon FSx está creando la configuración del repositorio de datos entre el sistema de archivos y el repositorio de datos vinculados. El repositorio de datos no está disponible.
- Disponible: El repositorio de datos está disponible para su uso.
- Actualizando: La configuración del repositorio de datos está siendo objeto de una actualización iniciada por el cliente que podría afectar a su disponibilidad.
- Mal configurado: Amazon FSx no puede importar automáticamente actualizaciones del bucket de S3 hasta que se corrija la configuración del repositorio de datos. Para obtener más información, consulte Resolución de problemas de un bucket de S3 vinculado mal configurado.

Puede ver el estado del ciclo de vida del repositorio de datos vinculados de un sistema de archivos mediante la consola de Amazon FSx, la interfaz de la línea de comandos AWS y la API de Amazon FSx. En la consola de Amazon FSx, puede acceder al estado del ciclo de vida del repositorio de datos en el panel Integración del repositorio de datos de la pestaña Repositorio de datos para el sistema de archivos. La propiedad `Lifecycle` se encuentra en el objeto `DataRepositoryConfiguration` en la respuesta a un comando de CLI `describe-file-systems` (la acción de API equivalente es `DescribeFileSystems`).

## Importar automáticamente actualizaciones desde un bucket de S3

De forma predeterminada, al crear un nuevo sistema de archivos, Amazon FSx importa los metadatos del archivo (el nombre, la propiedad, la marca de tiempo y los permisos) de los objetos del bucket de S3 vinculado al crear el sistema de archivos. Puede configurar su sistema de archivos FSx para Lustre para que importe automáticamente los metadatos de los objetos que se agreguen, modifiquen o eliminen de su bucket S3 tras la creación del sistema de archivos. FSx para Lustre actualiza el listado de archivos y directorios de un objeto modificado después de la creación de la misma manera que importa metadatos de archivos en la creación del sistema de archivos.

Cuando Amazon FSx actualiza la lista de archivos y directorios de un objeto modificado, si el objeto modificado del bucket de S3 ya no contiene sus metadatos, Amazon FSx mantiene los valores de metadatos actuales del archivo, en lugar de utilizar los permisos predeterminados.

> **Note**
>
> Los ajustes de importación están disponibles en FSx para los sistemas de archivos Lustre creados después de las 15:00 EDT del 23 de julio de 2020.

Puede establecer las preferencias de importación al crear un nuevo sistema de archivos y actualizar la configuración en los sistemas de archivos existentes mediante la consola de administración de FSx, la CLI AWS y la API AWS. Al crear el sistema de archivos, los objetos de S3 existentes aparecen como descripciones de archivos y directorios. Después de crear su sistema de archivos, ¿cómo desea actualizarlo a medida que se actualiza el contenido de su bucket de S3? Un sistema de archivos puede tener una de las siguientes preferencias de importación:

> **Note**
>
> El sistema de archivos FSx para Lustre y su bucket S3 vinculado deben estar ubicados en la misma Región AWS para importar automáticamente las actualizaciones.

- Actualizar mi lista de archivos y directorios a medida que se agregan objetos a mi bucket de S3: (predeterminado) Amazon FSx actualiza automáticamente las descripciones de archivos y directorios de cualquier objeto nuevo agregado al bucket de S3 vinculado que no exista actualmente en el sistema de archivos FSx. Amazon FSx no actualiza los listados de objetos que hayan cambiado en el bucket de S3. Amazon FSx no elimina los listados de objetos que se eliminan en el bucket de S3.

  > **Note**
  >
  > La configuración predeterminada de las preferencias de importación para importar datos de un bucket de S3 vinculado mediante la CLI y la API es `NONE`. La configuración predeterminada de las preferencias de importación al utilizar la consola es actualizar Lustre a medida que se agregan nuevos objetos al bucket de S3.

- Actualizar mi listado de archivos y directorios a medida que se agregan o modifican objetos en mi bucket de S3: Amazon FSx actualiza automáticamente los listados de archivos y directorios de cualquier objeto nuevo agregado al bucket de S3 y de cualquier objeto existente que se cambie en el bucket de S3 después de elegir esta opción. Amazon FSx no elimina los listados de objetos que se eliminan en el bucket de S3.
- Actualizar mi lista de archivos y directorios a medida que se agregan, modifican o eliminan objetos de mi bucket de S3: Amazon FSx actualiza automáticamente los listados de archivos y directorios de cualquier objeto nuevo agregado al bucket de S3, de cualquier objeto existente que se cambie en el bucket de S3 y de cualquier objeto existente que se elimine en el bucket de S3 después de elegir esta opción.
- No actualizar mi archivo y directamente listado al agregar, cambiar o eliminar objetos de mi bucket de S3: Amazon FSx solo actualiza los listados de archivos y directorios del bucket de S3 vinculado cuando se crea el sistema de archivos. FSx no actualiza los listados de archivos y directorios para los objetos nuevos, modificados o eliminados después de elegir esta opción.

Al configurar las preferencias de importación para actualizar los listados de archivos y directorios de su sistema de archivos en función de los cambios en el bucket de S3 vinculado, Amazon FSx crea una configuración de notificación de eventos en el bucket de S3 vinculado llamada `FSx`. No modifique ni elimine la configuración de notificación de eventos `FSx` en el bucket de S3, ya que esto impide la importación automática de listados de archivos y directorios nuevos o modificados a su sistema de archivos.

Cuando Amazon FSx actualiza un listado de archivos que ha cambiado en el bucket de S3 vinculado, sobrescribe el archivo local con la versión actualizada, incluso si el archivo está bloqueado por escritura. Del mismo modo, cuando Amazon FSx actualiza un listado de archivos cuando se ha eliminado el objeto correspondiente en el bucket de S3 vinculado, elimina el archivo local, incluso si el archivo está bloqueado por escritura.

Amazon FSx hará todo lo posible por actualizar su sistema de archivos. Amazon FSx no puede actualizar el sistema de archivos con cambios en las siguientes situaciones:

- Cuando Amazon FSx no tiene permiso para abrir el objeto S3 modificado o nuevo.
- Cuando se elimina o modifica la configuración de notificación de eventos `FSx` en el bucket S3 vinculado.

Cualquiera de estas condiciones provoca que el estado del ciclo de vida del repositorio de datos se convierta en Mal configurado. Para obtener más información, consulte Estado del ciclo de vida del repositorio de datos.

### Requisitos previos

Se requieren las siguientes condiciones para que Amazon FSx importe automáticamente los archivos nuevos, modificados o eliminados del bucket de S3 vinculado:

- El sistema de archivos y su bucket S3 vinculado deben estar ubicados en la misma Región AWS.
- El bucket S3 no tiene un estado de ciclo de vida mal configurado. Para obtener más información, consulte Estado del ciclo de vida del repositorio de datos.
- Su cuenta debe tener los permisos necesarios para configurar y recibir notificaciones de eventos en el bucket de S3 vinculado.

### Tipos de cambios de archivos compatibles

Amazon FSx admite la importación de los siguientes cambios en archivos y carpetas que se produzcan en el bucket de S3 vinculado:

- Cambios en el contenido de los archivos
- Cambios en los metadatos de archivos o carpetas
- Cambios en el destino o los metadatos del enlace simbólico

### Actualización de las preferencias de importación

Puede configurar las preferencias de importación de un sistema de archivos al crear un nuevo sistema de archivos. Para obtener más información, consulte Vincular su sistema de archivos a un bucket de S3.

También puede actualizar las preferencias de importación de un sistema de archivos después de crearlo mediante la consola de administración AWS, la CLI AWS y la API de Amazon FSx, como se muestra en el siguiente procedimiento.

Console

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.

2. En el panel, elija Sistemas de archivos.
3. Seleccione el sistema de archivos que desee gestionar para ver los detalles del sistema de archivos.
4. Elija Repositorio de datos para ver la configuración del repositorio de datos. Puede modificar las preferencias de importación si el estado del ciclo de vida es DISPONIBLE o MAL CONFIGURADO. Para obtener más información, consulte Estado del ciclo de vida del repositorio de datos.
5. Seleccione Acciones y, a continuación, elija Actualizar preferencias de importación para mostrar el cuadro de diálogo Actualizar preferencias de importación.
6. Seleccione la nueva configuración y, a continuación, elija Actualizar para realizar el cambio.

CLI

Para actualizar las preferencias de importación, utilice el comando CLI `update-file-system`. La operación de API correspondiente es `UpdateFileSystem`.

Después de actualizar correctamente el sistema de archivos `AutoImportPolicy`, Amazon FSx devuelve la descripción del sistema de archivos actualizado como JSON, como se muestra aquí:


```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            "CreationTime": 1549310341.483,
            "FileSystemId": "fs-0123456789abcdef0",
            "FileSystemType": "LUSTRE",
            "Lifecycle": "UPDATING",
            "StorageCapacity": 2400,
            "VpcId": "vpc-123456",
            "SubnetIds": [
                "subnet-123456"
            ],
            "NetworkInterfaceIds": [
                "eni-039fcf55123456789"
            ],
            "DNSName": "fs-0123456789abcdef0.fsx.us-east-2.amazonaws.com",
            "ResourceARN": "arn:aws:fsx:us-east-2:123456:file-system/
fs-0123456789abcdef0",
            "Tags": [
                {
```

```
                    "Key": "Name",
                    "Value": "Lustre-TEST-1"
                }
            ],
            "LustreConfiguration": {
                "DeploymentType": "SCRATCH_1",
                "DataRepositoryConfiguration": {
                    "AutoImportPolicy": "NEW_CHANGED_DELETED",
                    "Lifecycle": "UPDATING",
                    "ImportPath": "s3://lustre-export-test-bucket/",
                    "ExportPath": "s3://lustre-export-test-bucket/export",
                    "ImportedFileChunkSize": 1024
                }
                "PerUnitStorageThroughput": 50,
                "WeeklyMaintenanceStartTime": "2:04:30"
            }
        }
    ]
}
```

# Rendimiento de Amazon FSx para Lustre

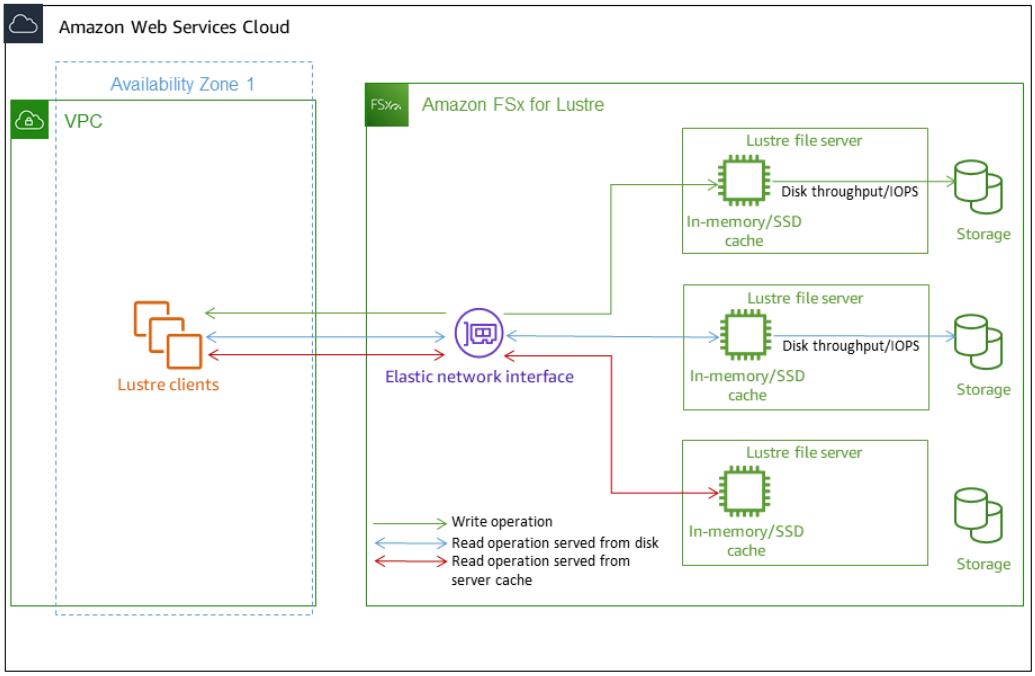
Amazon FSx para Lustre, basado en Lustre, el popular sistema de archivos de alto rendimiento, proporciona un rendimiento de escalado horizontal que aumenta linealmente con el tamaño del sistema de archivos. Los sistemas de archivos de Lustre se escalan horizontalmente en varios servidores de archivos y discos. Este escalado proporciona a cada cliente acceso directo a los datos almacenados en cada disco para eliminar muchos de los cuellos de botella presentes en los sistemas de archivos tradicionales. Amazon FSx para Lustre se basa en la arquitectura escalable de Lustre para soportar altos niveles de rendimiento en un gran número de clientes.

Temas



## Cómo funcionan los sistemas de archivos de FSx para Lustre

Cada sistema de archivos de FSx para Lustre consta de los servidores de archivos con los que se comunican los clientes y un conjunto de discos conectados a cada servidor de archivos que almacenan sus datos. Cada servidor de archivos emplea un caché en memoria rápido para mejorar el rendimiento de los datos a los que se accede con más frecuencia. Los sistemas de archivos basados en HDD también se pueden aprovisionar con una caché de lectura basada en SSD para mejorar aún más el rendimiento de los datos a los que se accede con más frecuencia. Cuando un cliente accede a los datos almacenados en la caché en memoria o SSD, el servidor de archivos no necesita leerlos del disco, lo que reduce la latencia y aumenta el rendimiento total que se puede obtener. El siguiente diagrama ilustra las rutas de una operación de escritura, una operación de lectura servida desde el disco y una operación de lectura servida desde la caché en memoria o SSD.




Cuando se leen datos almacenados en la caché en memoria o SSD del servidor de archivos, el rendimiento del sistema de archivos viene determinado por el rendimiento de la red. Cuando se escriben datos en el sistema de archivos, o cuando se leen datos que no están almacenados en la caché en memoria, el rendimiento del sistema de archivos viene determinado por el menor entre el rendimiento de la red y el rendimiento del disco.

Cuando aprovisiona un sistema de archivos Lustre HDD con una caché SSD, Amazon FSx crea una caché SSD con un tamaño automático del 20 % de la capacidad de almacenamiento HDD del sistema de archivos. De este modo, se consiguen latencias inferiores al milisegundo y mayores IOPS para los archivos a los que se accede con frecuencia.

## Rendimiento agregado del sistema de archivos

El rendimiento que soporta un sistema de archivos de FSx para Lustre es proporcional a su capacidad de almacenamiento. Los sistemas de archivos de Amazon FSx para Lustre escalan a cientos de GBps de rendimiento y millones de IOPS. Amazon FSx para Lustre también soporta el acceso simultáneo al mismo archivo o directorio desde miles de instancias de computación. Este acceso permite la comprobación rápida de datos desde la memoria de la aplicación al almacenamiento, que es una técnica común en la computación de alto rendimiento (HPC). Puede

aumentar la cantidad de almacenamiento y la capacidad de rendimiento según sea necesario en cualquier momento después de crear el sistema de archivos. Para obtener más información, consulte Administración de la capacidad de almacenamiento.

FSx para sistemas de archivos Lustre proporciona un rendimiento de lectura en ráfaga utilizando un mecanismo de crédito de E/S de red para asignar ancho de banda de la red basado en la utilización media del ancho de banda. Los sistemas de archivos acumulan créditos cuando el uso de su ancho de banda de la red está por debajo de sus límites de referencia, y pueden utilizar estos créditos cuando realizan transferencias de datos de red.

Las siguientes tablas muestran el rendimiento para el que están diseñadas las opciones de implementación de FSx para Lustre.

Rendimiento del sistema de archivos para opciones de almacenamiento SSD

| Tipo de implementación | Rendimiento de red (MB/s/TiB de almacenamiento aprovisionado) | | IOPS de red (IOPS/TiB de almacenamiento aprovisionado) | Almacenamiento en caché (GiB de RAM/TiB de almacenamiento aprovisionado) | Latencias de disco por operación de archivo (milisegundos, P50) | Rendimiento del disco (MBps/TiB de almacenamiento o caché SSD aprovisionada) | |
|---|---|---|---|---|---|---|---|
| | Referencia | Ráfaga | | | | Referencia | Ráfagas |
| SCRATCH_2 | 200 | 1300 | Base de decenas de miles<br>Ráfaga de cientos de miles | 6.7 | Metadatos: sub-ms<br>Datos: sub-ms | 200 (lectura)<br>100 (escritura) | - |
| PERSISTENT-125 | 320 | 1300 | | 3.4 | | 125 | 500 |
| PERSISTENT-250 | 640 | 1300 | | 6.8 | | 250 | 500 |
| PERSISTENT-500 | 1300 | - | | 13.7 | | 500 | - |
| PERSISTENT-1000 | 2600 | - | | 27.3 | | 1000 | - |

Rendimiento del sistema de archivos para opciones de almacenamiento HDD

| Tipo de implementación | Rendimiento de la red (MB/s/TiB de almacenamiento o caché SSD aprovisionada) | | IOPS de red (IOPS/TiB de almacenamiento aprovisionado) | Almacenamiento en caché (GiB de RAM/TiB de almacenamiento aprovisionado) | Latencias de disco por operación de archivo (milisegundos, P50) | Rendimiento del disco (MBps/TiB de almacenamiento o caché SSD aprovisionada) | |
|---|---|---|---|---|---|---|---|
| | Referencia | Ráfaga | | | | Referencia | Ráfagas |
| PERSISTENT-12 | | | | | | | |
| Almacenamiento en HDD | 40 | 375* | Base de decenas de miles<br>Ráfaga de cientos de miles | 0.4 memory | Metadatos: sub-ms<br>Datos: ms de un dígito | 12 | 80 (lectura)<br>50 (escritura) |
| Caché de lectura SSD | 200 | 1,900 | | Caché SSD 200 | Datos: sub-ms | 200 | - |
| PERSISTENT-40 | | | | | | | |
| Almacenamiento en HDD | 150 | 1,300* | Base de decenas de miles<br>Ráfaga de cientos de miles | 1.5 | Metadatos: sub-ms<br>Datos: ms de un dígito | 40 | 250 (lectura)<br>150 (escritura) |
| Caché de lectura SSD | 750 | 6500 | | 200 SSD cache | Datos: sub-ms | 200 | - |

Rendimiento del sistema de archivos para opciones de almacenamiento SSD de generaciones anteriores

| Tipo de implementación | Rendimiento de la red (MB/s por TiB de almacenamiento aprovisionado) | | IOPS de red (IOPS por TiB de almacenamiento aprovisionado) | Almacenamiento en caché (GiB por TiB de almacenamiento aprovisionado) | Latencias de disco por operación de archivo (milisegundos, P50) | Rendimiento del disco (MB/s por TiB de almacenamiento o caché SSD aprovisionada) | |
|---|---|---|---|---|---|---|---|
| | Referencia | Ráfaga | | | | Referencia | Ráfagas |
| PERSISTENT-50 | 250 | 1,300* | Base de decenas de miles | 2.2 RAM | Metadatos: sub-ms | 50 | 240 |
| PERSISTENT-100 | 500 | 1,300* | | 4.4 RAM | Datos: sub-ms | 100 | 240 |
| PERSISTENT-200 | 750 | 1,300* | Ráfaga de cientos de miles | 8.8 RAM | | 200 | 240 |

> **Note**
>
> *Los sistemas de archivos persistentes de las siguientes Regiones de AWS proporcionan una ráfaga de red de hasta 530 MB/s por TiB de almacenamiento: África (Ciudad del Cabo), Asia-Pacífico (Hong Kong), Asia-Pacífico (Osaka), Asia-Pacífico (Singapur), Canadá (centro), Europa (Fráncfort), Europa (Londres), Europa (Milán), Europa (Estocolmo), Medio Oriente (Baréin), América del Sur (São Paulo), China y Oeste de EE. UU. (Los Ángeles).

> **Note**
>
> La opción de implementación de FSx para Lustre SCRATCH_1 se diseñó para admitir 200 MB/s/TiB.

## Ejemplo: rendimiento de referencia y de ráfaga agregado

El siguiente ejemplo ilustra cómo la capacidad de almacenamiento y el rendimiento del disco afectan al rendimiento del sistema de archivos.

Un sistema de archivos persistente con una capacidad de almacenamiento de 4,8 TiB y 50 MB/s por TiB de rendimiento por unidad de almacenamiento proporciona un rendimiento de disco de referencia agregado de 240 MB/s y un rendimiento de disco en ráfaga de 1,152 GB/s.

Independientemente del tamaño del sistema de archivos, Amazon FSx para Lustre proporciona latencias constantes de menos de un milisegundo para las operaciones de archivos.

# Disposición de almacenamiento del sistema de archivos

Todos los datos de los archivos de Lustre se almacenan en volúmenes de almacenamiento llamado destinos de almacenamiento de objetos (OST). Todos los metadatos de archivos (incluidos nombres de archivos, marcas de tiempo, permisos, etc.) se almacenan en volúmenes de almacenamiento llamados destinos de metadatos (MDT). Los sistemas de archivos de Amazon FSx para Lustre se componen de un único MDT y varios OST. Cada OST tiene un tamaño aproximado de 1 a 2 TiB, según el tipo de implementación del sistema de archivos. Amazon FSx para Lustre distribuye sus datos de archivos entre los OST que componen su sistema de archivos para equilibrar la capacidad de almacenamiento con el rendimiento y la carga de IOPS.

Para ver el uso de almacenamiento de los MDT y OST que componen su sistema de archivos, ejecute el siguiente comando desde un cliente que tenga montado el sistema de archivos.

```
lfs df -h mount/path
```

El resultado de este comando tendrá un aspecto similar al siguiente.

Example

```
UUID                       bytes        Used   Available Use% Mounted on
mountname-MDT0000_UUID      68.7G        5.4M       68.7G   0% /fsx[MDT:0]
mountname-OST0000_UUID       1.1T        4.5M        1.1T   0% /fsx[OST:0]
mountname-OST0001_UUID       1.1T        4.5M        1.1T   0% /fsx[OST:1]

filesystem_summary:          2.2T        9.0M        2.2T   0% /fsx
```

# Fragmentación de datos en su sistema de archivos

Puede optimizar el rendimiento de su sistema de archivos con la fragmentación de archivos. Amazon FSx para Lustre distribuye automáticamente los archivos entre los OST para garantizar que los datos se sirven desde todos los servidores de almacenamiento. Puede aplicar el mismo concepto a nivel de archivo configurando cómo se distribuyen los archivos a través de múltiples OST.

Fragmentación significa que los archivos pueden ser divididos en múltiples trozos que son almacenados en diferentes OST. Cuando un archivo se divide en varios OST, las peticiones de lectura o escritura en el archivo se reparten entre esos OST, aumentando el rendimiento agregado o IOPS que sus aplicaciones pueden manejar a través de él.

Los siguientes son los diseños predeterminados de los sistemas de archivos de Amazon FSx para Lustre.

- Para los sistemas de archivos creados antes del 18 de diciembre de 2020, el diseño predeterminado especifica el número de franjas de 1. Esto significa que, a menos que se especifique un diseño diferente, cada archivo creado en Amazon FSx para Lustre con las herramientas estándar de Linux se almacena en un único disco.
- Para los sistemas de archivos creados después del 18 de diciembre de 2020, el diseño predeterminado es un diseño de archivos progresivo en el que los archivos de menos de 1 GB de

tamaño se almacenan en una franja, y a los archivos de mayor tamaño se les asigna un número de fragmento de 5.

- Para los sistemas de archivos creados después del 25 de agosto de 2023, la disposición por defecto es una disposición de archivos progresiva de 4 componentes que se explica en Disposición progresiva de archivos.
- Para todos los sistemas de archivos, independientemente de su fecha de creación, los archivos importados de Amazon S3 no utilizan el diseño predeterminado, sino que utilizan el diseño del parámetro `ImportedFileChunkSize` del sistema de archivos. Los archivos importados en S3 con un tamaño superior al `ImportedFileChunkSize` se almacenarán en varios OST con un número de franjas de `(FileSize / ImportedFileChunksize) + 1`. El valor predeterminado de `ImportedFileChunkSize` es 1 GiB.

Puede ver la configuración de diseño de un archivo o directorio mediante el comando `lfs getstripe`.

```
lfs getstripe path/to/filename
```

Este comando indica el número de franjas, el tamaño y el desfase de fragmentos de un archivo. El número de franjas indica el número de OST en las que se divide el archivo. El tamaño de franja es la cantidad de datos continuos que se almacenan en un OST. El desplazamiento de franja es el índice del primer OST sobre el que se divide el archivo.

## Modificar la configuración de franjas

Los parámetros de diseño de un archivo se establecen cuando se crea el archivo por primera vez. Utilice el comando `lfs setstripe` para crear un nuevo archivo vacío con una disposición específica.

```
lfs setstripe filename --stripe-count number_of_OSTs
```

El comando `lfs setstripe` afecta a la disposición de un nuevo archivo. Úselo para especificar la disposición de un archivo antes de crearlo. También puede definir una disposición para un directorio. Una vez establecida en un directorio, esa disposición se aplica a cada nuevo archivo añadido a ese directorio, pero no a los archivos existentes. Cualquier nuevo subdirectorio que cree también hereda la nueva disposición, que se aplica a los nuevos archivos o directorios que se creen dentro de ese subdirectorio.

Para modificar la disposición de un archivo existente, utilice el comando `lfs migrate`. Este comando copia el archivo según sea necesario para distribuir su contenido de acuerdo con la disposición que especifique en el comando. Por ejemplo, los archivos anexados o cuyo tamaño ha aumentado no cambian el número de franjas, por lo que hay que migrarlos para cambiar el diseño del archivo. Alternativamente, puede crear un nuevo archivo utilizando el comando `lfs setstripe` para especificar su distribución, copiar el contenido original en el nuevo archivo y cambiar el nombre del nuevo archivo para reemplazar el archivo original.

Puede haber casos en los que la configuración de la presentación por defecto no sea óptima para su carga de trabajo. Por ejemplo, un sistema de archivos con decenas de OST y una gran cantidad de archivos de varios gigabytes puede obtener un rendimiento superior al dividir los archivos en secciones superiores al valor de recuento de franjas predeterminado de cinco OST. La creación de archivos de gran tamaño con un número reducido de franjas puede provocar cuellos de botella en el rendimiento de E/S y también provocar que las OST se llenen. En este caso, puede crear un directorio con un mayor número de franjas para estos archivos.

Es importante configurar un diseño de franjas para archivos grandes (especialmente para archivos de más de un gigabyte de tamaño) por las siguientes razones:

- Mejora el rendimiento al permitir que varios OST y sus servidores asociados contribuyan con IOPS, ancho de banda de la red y recursos de CPU al leer y escribir archivos de gran tamaño.
- Reduce la probabilidad de que un pequeño subconjunto de OST se convierta en puntos calientes que limiten el rendimiento general de la carga de trabajo.
- Evita que un solo archivo grande llene un OST, lo que podría provocar errores de llenado del disco.

No existe una única configuración de distribución óptima para todos los casos de uso. Para obtener una guía detallada sobre la distribución de archivos, consulte Administración de la distribución de archivos (fragmentación) y del espacio libre en la documentación de Lustre.org. A continuación, se ofrecen unas directrices generales:

- El diseño de franjas es más importante para los archivos de gran tamaño, especialmente para los casos de uso en los que los archivos suelen tener un tamaño de cientos de megabytes o más. Por este motivo, el diseño predeterminado de un nuevo sistema de archivos asigna un recuento de franjas de cinco a los archivos de más de 1 GiB de tamaño.
- El recuento de franjas es el parámetro de diseño que se debe ajustar para los sistemas que admiten archivos de gran tamaño. El recuento de franjas especifica el número de volúmenes OST

que pueden contener fragmentos de un archivo segmentado. Por ejemplo, con un número de franjas de 2 y un tamaño de franja de 1 MiB, Lustre escribe fragmentos alternativos de 1 MiB de un archivo en cada una de las dos OST.

- El número efectivo de franjas es el menor entre el número real de volúmenes OST y el valor del recuento de franjas que especifique. Puede utilizar el valor especial del recuento de franjas de `-1` para indicar que las franjas deben colocarse en todos los volúmenes OST.
- Establecer un número de franjas grande para archivos pequeños no es óptimo, ya que, para algunas operaciones, Lustre requiere un recorrido de ida y vuelta en red a todos los OST de la maquetación, incluso si el archivo es demasiado pequeño para ocupar espacio en todos los volúmenes OST.
- Puede configurar una disposición progresiva de archivos (PFL) que permita que la disposición de un archivo cambie con el tamaño. Una configuración PFL puede simplificar la gestión de un sistema de archivos que tenga una combinación de archivos grandes y pequeños sin tener que establecer explícitamente una configuración para cada archivo. Para obtener más información, consulte Disposición progresiva de archivos.
- El tamaño predeterminado de la banda es de 1 MiB. Definir un desfase de franjas puede resultar útil en circunstancias especiales, pero en general es mejor dejarlo sin especificar y utilizar el valor predeterminado.

## Disposición progresiva de archivos

Puede especificar una configuración de diseño de archivos progresivo (PFL) para un directorio con el fin de especificar diferentes configuraciones de franjas para archivos pequeños y grandes antes de rellenarlo. Por ejemplo, puede establecer una PFL en el directorio de nivel superior antes de que se escriba cualquier dato en un nuevo sistema de archivos.

Para especificar una configuración de PFL, utilice el comando `lfs setstripe` con las opciones `-E` para especificar los componentes de disposición para archivos de diferentes tamaños, como el siguiente comando:

```
lfs setstripe -E 100M -c 1 -E 10G -c 8 -E 100G -c 16 -E -1 -c 32 /mountname/directory
```

Este comando establece cuatro componentes de disposición:

- El primer componente (`-E 100M -c 1`) indica un valor de recuento de franjas de 1 para archivos de un tamaño máximo de 100 MiB.

- El segundo componente (`-E 10G -c 8`) indica un recuento de franjas de 8 para archivos de hasta 10 GiB de tamaño.
- El tercer componente (`-E 100G -c 16`) indica un recuento de franjas de 16 para archivos de hasta 100 GiB de tamaño.
- El cuarto componente (`-E -1 -c 32`) indica un recuento de franjas de 32 para archivos de más de 100 GiB.

> **Important**
>
> Si se agregan datos a un archivo creado con una configuración PFL, se rellenarán todos sus componentes de diseño. Por ejemplo, con el comando de 4 componentes mostrado arriba, si crea un archivo de 1 MiB y luego agrega datos al final del archivo, el diseño del archivo se expandirá para tener un conteo de franjas de -1, es decir, todos los OST en el sistema. Esto no significa que se escribirán datos en cada OST, pero una operación como la lectura de la longitud del fichero enviará una petición en paralelo a cada OST, añadiendo una carga de red significativa al sistema de archivos.
>
> Por lo tanto, tenga cuidado de limitar el número de franjas para cualquier archivo de longitud pequeña o mediana al que posteriormente se le puedan agregar datos. Dado que los archivos de registro suelen crecer al añadirse nuevos registros, Amazon FSx para Lustre asigna un recuento de franjas predeterminado de 1 a cualquier archivo creado en modo de adición, independientemente de la configuración de franjas predeterminada especificada por su directorio principal.

La configuración de PFL predeterminada para los sistemas de archivos en Amazon FSx para Lustre creados después del 25 de agosto de 2023 se establece con este comando:

```
lfs setstripe -E 100M -c 1 -E 10G -c 8 -E 100G -c 16 -E -1 -c 32 /mountname
```

Los clientes con cargas de trabajo que tienen un acceso altamente concurrente en archivos medianos y grandes probablemente se beneficien de una disposición con más franjas en tamaños más pequeños y franjas en todos los OST para los archivos más grandes, como se muestra en la disposición de ejemplo de cuatro componentes.

# Supervisión del rendimiento y uso

Cada minuto, Amazon FSx for Lustre envía métricas de uso de cada disco (MDT y OST) a Amazon. CloudWatch

Para ver los detalles de uso agregados del sistema de archivos, puede consultar la estadística Suma de cada métrica. Por ejemplo, la suma de la estadística `DataReadBytes` indica el rendimiento total de lectura observado por todos los OST de un sistema de archivos. Del mismo modo, la suma de la estadística `FreeDataStorageCapacity` indica la capacidad total de almacenamiento disponible para los datos de los archivos en el sistema de archivos.

Para obtener más información sobre la supervisión del rendimiento del sistema de archivos, consulte Supervisión de Amazon FSx para Lustre.

# Consejos de rendimiento

Cuando utilice Amazon FSx para Lustre, tenga en cuenta los siguientes consejos de rendimiento. Para conocer los límites de servicio, consulte Cuotas.

- Tamaño medio de E/S: dado que Amazon FSx para Lustre es un sistema de archivos de red, cada operación de archivo pasa por un viaje de ida y vuelta entre el cliente y Amazon FSx para Lustre, incurriendo en una pequeña sobrecarga de latencia. Debido a esta latencia por operación, el desempeño global suele aumentar a la par que el tamaño medio de E/S, porque el costo se amortiza con la mayor cantidad de datos.
- Modelo de solicitud: Al activar las escrituras asíncronas en el sistema de archivos, las operaciones de escritura pendientes se almacenan en el búfer de memoria en la instancia de Amazon EC2 antes de escribirse en Amazon FSx para Lustre de forma asíncrona. Las escrituras asíncronas suelen tener latencias menores. Cuando se realizan escrituras asíncronas, el kernel utiliza memoria adicional para el almacenamiento en caché. Un sistema de archivos que haya habilitado las escrituras síncronas emite solicitudes síncronas a Amazon FSx para Lustre. Cada operación realizará un recorrido de ida y vuelta entre el cliente y Amazon FSx para Lustre.

> **Note**
>
> El modelo de solicitud elegido tiene contrapartidas en la coherencia (si utiliza varias instancias de Amazon EC2) y en la velocidad.

- Instancias de Amazon EC2: las aplicaciones que realizan un gran número de operaciones de lectura y escritura probablemente necesitan más memoria o capacidad de computación que las aplicaciones que no. Cuando lance sus instancias de Amazon EC2 para su carga de trabajo de cómputo intensivo, elija los tipos de instancia que tengan la cantidad de estos recursos que su aplicación necesita. Las características de desempeño de los sistemas de archivos de Amazon FSx para Lustre no dependen del uso de instancias optimizadas para Amazon EBS.
- Ajuste recomendado de las instancias de cliente para obtener un rendimiento óptimo

  1. Para todos los tipos y tamaños de instancias de cliente, recomendamos aplicar los siguientes ajustes:

     ```
     sudo lctl set_param osc.*.max_dirty_mb=64
     ```

  2. Para tipos de instancia de cliente con memoria de más de 64 GiB, recomendamos aplicar el siguiente ajuste:

     ```
     lctl set_param ldlm.namespaces.*.lru_max_age=600000
     ```

  3. Para tipos de instancia de cliente con más de 64 núcleos vCPU, recomendamos aplicar el siguiente ajuste:

     ```
     echo "options ptlrpc ptlrpcd_per_cpt_max=32" >> /etc/modprobe.d/modprobe.conf
     echo "options ksocklnd credits=2560" >> /etc/modprobe.d/modprobe.conf

     # reload all kernel modules to apply the above two settings
     sudo reboot
     ```

     Una vez montado el cliente, es necesario aplicar el siguiente ajuste:

     ```
     sudo lctl set_param osc.*OST*.max_rpcs_in_flight=32
     sudo lctl set_param mdc.*.max_rpcs_in_flight=64
     sudo lctl set_param mdc.*.max_mod_rpcs_in_flight=50
     ```

  Tenga en cuenta que se sabe que `lctl set_param` no persiste durante el reinicio. Dado que estos parámetros no pueden establecerse permanentemente desde el lado del cliente, se recomienda implementar una tarea cron de arranque para establecer la configuración con los ajustes recomendados.

- Equilibrio de la carga de trabajo entre los OST: en algunos casos, la carga de trabajo no impulsa el rendimiento total que puede ofrecer el sistema de archivos (200 MB/s por TiB de almacenamiento).

Si es así, puedes usar CloudWatch las métricas para solucionar problemas si el rendimiento se ve afectado por un desequilibrio en los patrones de E/S de la carga de trabajo. Para identificar si esta es la causa, consulte la CloudWatch métrica Maximum de Amazon FSx for Lustre.

En algunos casos, esta estadística muestra una carga igual o superior a 240 MBps de rendimiento (la capacidad de rendimiento de un único disco de 1,2 TiB de Amazon FSx para Lustre). En estos casos, la carga de trabajo no se distribuye uniformemente entre los discos. Si este es el caso, puede usar el comando `lfs setstripe` para modificar la división de archivos a los que su carga de trabajo accede con más frecuencia. Para obtener un rendimiento óptimo, distribuya los archivos con requisitos de alto rendimiento en todos los OST que componen su sistema de archivos.

Si los archivos se importan de un repositorio de datos, puede adoptar otro enfoque para distribuir los archivos de alto rendimiento de manera uniforme en todos los OST. Para ello, puede modificar el parámetro `ImportedFileChunkSize` al crear su próximo sistema de archivos Amazon FSx para Lustre.

Por ejemplo, supongamos que su carga de trabajo utiliza un sistema de archivos de 7,0 TiB (que se compone de 6 OST de 1,17 TiB) y necesita impulsar un rendimiento alto a través de archivos de 2,4 GiB. En este caso, puede establecer el valor `ImportedFileChunkSize` en `(2.4 GiB / 6 OSTs) = 400 MiB` para que los archivos se distribuyan uniformemente entre los OST del sistema de archivos.

# Acceso a sistemas de archivo

Con Amazon FSx, puede transferir sus cargas de trabajo con un uso intensivo de cómputo desde las instalaciones a la nube de Amazon Web Services importando datos a través de una VPN. AWS Direct Connect Puede acceder a su sistema de archivos Amazon FSx en las instalaciones, copiar los datos en su sistema de archivos según sea necesario y ejecutar cargas de trabajo de procesamiento de datos intensivo en instancias en la nube.

En la siguiente sección, puede aprender a acceder a su sistema de archivos Amazon FSx para Lustre en una instancia Linux. Además, puede encontrar información acerca de cómo utilizar el archivo `fstab` para volver a montar automáticamente el sistema de archivos después de los reinicios del sistema.

Antes de poder montar un sistema de archivos, debe crear, configurar y lanzar los recursos de AWS relacionados. Para obtener instrucciones detalladas, consulte Introducción a Amazon FSx para Lustre. A continuación, puede instalar y configurar el cliente Lustre en su instancia de procesamiento.

Temas



## Compatibilidad entre el sistema de archivos de Lustre y el núcleo del cliente

Recomendamos encarecidamente utilizar la versión Lustre para su sistema de archivos FSx for Lustre, que sea compatible con las versiones del núcleo de Linux de sus instancias cliente.

## Clientes de Amazon Linux

| Sistema operativo | Versión del sistema operativo | Versión mínima del kernel | Versión máxima del kernel | Versión del sistema de archivos | | |
|---|---|---|---|---|---|---|
| | | | | 2.10 | 2.12 | 2.15 |
| Amazon Linux 2023 | 6.1 | 6.1.79-99.167 | 6,1,79-99,167 + | no | sí | sí |
| Amazon Linux 2 | 5,10 | 5.10.144-127,601 | 5,10,144-127,601+ | yes | sí | sí |
| | | | <5.10.144-127.601 | yes | sí | no |
| | 5.4 | 5.4.214-120,368 | 5,4,214-120,368+ | yes | sí | sí |
| | | | 5.4.214-120.368 | yes | sí | no |
| | 4,14 | 4.14.294-220,533 | 4,14294-220,533+ | yes | sí | sí |
| | | | <4.14.294-220.533 | yes | sí | no |

## Clientes de Ubuntu

| Sistema operativo | Versión del sistema operativo | Versión mínima del kernel | Versión máxima del kernel | Versión del sistema de archivos | | |
|---|---|---|---|---|---|---|
| | | | | 2.10 | 2.12 | 2.15 |

| Sistema operativo | Versión del sistema operativo | Versión mínima del kernel | Versión máxima del kernel | Versión del sistema de archivos | | |
|---|---|---|---|---|---|---|
| Ubuntu | 22 | 6.2.0.1017.17~22.04 | 6.2.0. * | no | sí | sí |
| | | 5.15.0-1015-aws | 5.15.0-1031-aws | yes | sí | sí |
| | 20 | 5.15.0-1015-aws | 5.15.0+ | yes | sí | sí |
| | | 5.4.0-1011-aws | 5.13.0-1031-aws | yes | sí | no |

## Clientes RHEL/CentOS/Rocky Linux

| Sistema operativo | Versión del sistema operativo | Arquitectura | Versión mínima del kernel | Versión máxima del kernel | Versión del sistema de archivos | | |
|---|---|---|---|---|---|---|---|
| | | | | | 2.10 | 2.12 | 2.15 |
| RHEL/CentOS/Rocky Lin | 9.3 | Arm + x86 | 5.14.0-362.18.1 | 5.14.0-362.18.1 | no | sí | sí |
| | 9.0 | Arm + x86 | 5,14,0-70.13,1 | 5,14,0-770,30,1 | no | sí | sí |
| | 8.9 | Arm + x86 | 4.18.0-513* | 4,180-513* | yes | sí | sí |

| Sistema operativo | Versión del sistema operativo | Arquitectura | Versión mínima del kernel | Versión máxima del kernel | Versión del sistema de archivos | | |
|---|---|---|---|---|---|---|---|
| | 8.8 | Arm + x86 | 4.18.0-477* | 4.18.0-477* | yes | sí | sí |
| | 8.7 | Arm + x86 | 4.18.0-425* | 4.18.0-425* | yes | sí | sí |
| | 8.6 | Arm + x86 | 4.18.0-372* | 4.18.0-372* | yes | sí | sí |
| | 8.5 | Arm + x86 | 4.18.0-348* | 4.18.0-348* | yes | sí | sí |
| | 8.4 | Arm + x86 | 4.18.0-305* | 4.18.0-305* | yes | sí | sí |
| RHEL/ CentOS | 8.3 | Arm + x86 | 4.18.0-240* | 4.18.0-240* | yes | sí | no |
| | 8.2 | Arm + x86 | 4.18.0-193* | 4.18.0-193* | yes | sí | no |
| | 7.9 | x86 | 3.10.0-1160* | 3.10.0-1160* | yes | sí | sí |
| | 7.8 | x86 | 3.10.0-1127* | 3.10.0-1127* | yes | sí | no |
| | 7.7 | x86 | 3.10.0-1062* | 3.10.0-1062* | yes | sí | no |
| CentOS | 7.9 | Arm | 4.18.0-193* | 4.18.0-193* | yes | sí | sí |

| Sistema operativo | Versión del sistema operativo | Arquitectura | Versión mínima del kernel | Versión máxima del kernel | Versión del sistema de archivos | | |
|---|---|---|---|---|---|---|---|
| | 7.8 | Arm | 4.18.0-147* | 4.18.0-147* | yes | sí | sí |

# Instalación del cliente Lustre

Para montar su sistema de archivos Amazon FSx para Lustre desde una instancia de Linux, instale primero el cliente Lustre de código abierto. A continuación, dependiendo de la versión de su sistema operativo, utilice uno de los siguientes procedimientos. Para obtener información sobre el soporte del núcleo, consulteCompatibilidad entre el sistema de archivos de Lustre y el núcleo del cliente.

Si su instancia de computación no está ejecutando el kernel Linux especificado en las instrucciones de instalación, y no puede cambiar el kernel, puede construir su propio cliente Lustre. Para obtener más información, consulte Compilación de Lustre en Lustre Wiki.

## Amazon Linux

Para instalar el cliente Lustre en Amazon Linux 2023

1. Abra un terminal en su cliente de Linux.
2. Determine qué kernel se está ejecutando actualmente en su instancia de procesamiento mediante la ejecución del siguiente comando.

   ```
   uname -r
   ```

3. Revise la respuesta del sistema y compárela con los siguientes requisitos mínimos del núcleo para instalar el cliente Lustre en Amazon Linux 2023:

   - Requisito mínimo del kernel 6.1:6.1.79-99.167.amzn2023

   Si su instancia EC2 cumple con los requisitos mínimos del núcleo, continúe con el paso e instale el cliente lustre.

Si el comando devuelve un resultado inferior al requisito mínimo del kernel, actualice el kernel y reinicie su instancia de Amazon EC2 ejecutando el siguiente comando.

```
sudo dnf -y update kernel && sudo reboot
```

Compruebe que el kernel se haya actualizado usando el comando uname -r.

4. Descargue e instale el cliente Lustre con el siguiente comando.

```
sudo dnf install -y lustre-client
```

Para instalar el cliente Lustre en Amazon Linux 2

1. Abra un terminal en su cliente de Linux.
2. Determine qué kernel se está ejecutando actualmente en su instancia de procesamiento mediante la ejecución del siguiente comando.

```
uname -r
```

3. Revise la respuesta del sistema y compárela con los siguientes requisitos mínimos del núcleo para instalar el cliente Lustre en Amazon Linux 2:

   - Requisito mínimo de kernel 5.10 - 5.10.144-127.601.amzn2
   - Requisito mínimo de kernel 5.4 - 5.4.214-120.368.amzn2
   - Requisito mínimo de kernel 4.14 - 4.14.294-220.533.amzn2

   Si su instancia EC2 cumple con los requisitos mínimos del núcleo, continúe con el paso e instale el cliente lustre.

   Si el comando devuelve un resultado inferior al requisito mínimo del kernel, actualice el kernel y reinicie su instancia de Amazon EC2 ejecutando el siguiente comando.

```
sudo yum -y update kernel && sudo reboot
```

   Compruebe que el kernel se haya actualizado usando el comando uname -r.

4. Descargue e instale el cliente Lustre con el siguiente comando.

```
sudo amazon-linux-extras install -y lustre
```

Si no puede actualizar el kernel al requisito mínimo de kernel, puede instalar el cliente heredado 2.10 con el siguiente comando.

```
sudo amazon-linux-extras install -y lustre2.10
```

Para instalar el cliente Lustre en Amazon Linux

1. Abra un terminal en su cliente de Linux.
2. Determine qué kernel se está ejecutando actualmente en su instancia de procesamiento mediante la ejecución del siguiente comando. El cliente Lustre requiere un kernel de Amazon Linux `4.14, version 104` o superior.

   ```
   uname -r
   ```
3. Realice una de las acciones siguientes:

   - Si el comando devuelve `4.14.104-78.84.amzn1.x86_64` o una versión superior a 4.14, descargue e instale el cliente Lustre utilizando el siguiente comando.

     ```
     sudo yum install -y lustre-client
     ```
   - Si el comando devuelve un resultado inferior a `4.14.104-78.84.amzn1.x86_64`, actualice el kernel y reinicie su instancia de Amazon EC2 ejecutando el siguiente comando.

     ```
     sudo yum -y update kernel && sudo reboot
     ```

     Compruebe que el kernel se haya actualizado usando el comando uname -r. Luego, descargue e instale el cliente Lustre como se ha descrito anteriormente.

## CentOS, Rocky Linux y Red Hat

Para instalar el cliente Lustre en Centos, Red Hat y Rocky Linux 9.0 o 9.3

Puede instalar y actualizar los paquetes del cliente Lustre compatibles con Red Hat Enterprise Linux (RHEL), Rocky Linux y CentOS desde el repositorio de paquetes yum del cliente Lustre de Amazon

FSx. Estos paquetes están firmados para ayudar a garantizar que no han sido manipulados antes o durante la descarga. La instalación del repositorio falla si no instala la clave pública correspondiente en su sistema.

Para agregar el repositorio de paquetes yum del cliente Amazon FSx Lustre

1. Abra un terminal en su cliente de Linux.
2. Instala la clave pública de Amazon FSx rpm utilizando el siguiente comando.

```
curl https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-rpm-public-key.asc -o /tmp/fsx-rpm-public-key.asc
```

3. Importe la clave utilizando el siguiente comando.

```
sudo rpm --import /tmp/fsx-rpm-public-key.asc
```

4. Añada el repositorio y actualice el administrador de paquetes con el siguiente comando.

```
sudo curl https://fsx-lustre-client-repo.s3.amazonaws.com/el/9/fsx-lustre-client.repo -o /etc/yum.repos.d/aws-fsx.repo
```

Para configurar el repositorio yum del cliente Lustre de Amazon FSx

El repositorio de paquetes yum del cliente Amazon FSx Lustre está configurado de forma predeterminada para instalar el cliente Lustre que es compatible con la versión del núcleo que se incluyó inicialmente con las versiones más recientes compatibles de CentOS, Rocky Linux y RHEL 9. Para instalar un cliente Lustre que sea compatible con la versión del kernel que está utilizando, puede editar el archivo de configuración del repositorio.

Esta sección describe cómo determinar qué kernel está ejecutando, si necesita editar la configuración del repositorio, y cómo editar el archivo de configuración.

1. Determine qué kernel se está ejecutando actualmente en su instancia de procesamiento mediante la ejecución del siguiente comando.

```
uname -r
```

2. Realice una de las acciones siguientes:

- Si el comando devuelve `5.14.0-362*`, no necesita modificar la configuración del repositorio. Continúe con el procedimiento Para instalar el cliente Lustre.
- Si el comando vuelve a `5.14.0-70*` aparecer, debe editar la configuración del repositorio para que apunte al cliente Lustre de las versiones CentOS, Rocky Linux y RHEL 9.0.

3. Edite el archivo de configuración del repositorio para que apunte a una versión específica de RHEL utilizando el siguiente comando. *`specific_RHEL_version`*Sustitúyala por la versión de RHEL que necesites usar.

```
sudo sed -i 's#9#specific_RHEL_version#' /etc/yum.repos.d/aws-fsx.repo
```

   Por ejemplo, para apuntar a la versión 9.0, *`specific_RHEL_version`* sustitúyala por `9.0` en el comando, como en el siguiente ejemplo.

```
sudo sed -i 's#9#9.0#' /etc/yum.repos.d/aws-fsx.repo
```

4. Utilice el siguiente comando para borrar la caché yum.

```
sudo yum clean all
```

Para instalar el cliente de Lustre

- Instale los paquetes desde el repositorio utilizando el siguiente comando.

```
sudo yum install -y kmod-lustre-client lustre-client
```

Información adicional (Centos, Rocky Linux y Red Hat 9.0 y versiones posteriores)

Los comandos anteriores instalan los dos paquetes necesarios para montar e interactuar con su sistema de archivos Amazon FSx. El repositorio incluye paquetes Lustre adicionales, como un paquete que contiene el código fuente y paquetes que contienen pruebas, y puede instalarlos opcionalmente. Para listar todos los paquetes disponibles en el repositorio, utilice el siguiente comando.

```
yum --disablerepo="*" --enablerepo="aws-fsx" list available
```

Para descargar el rpm fuente, que contiene un tarball del código fuente upstream y el conjunto de parches que hemos aplicado, utilice el siguiente comando.

```
sudo yumdownloader --source kmod-lustre-client
```

Al ejecutar yum update, se instala una versión más reciente del módulo si está disponible y se sustituye la versión existente. Para evitar que la versión instalada actualmente se elimine en la actualización, añada una línea como la siguiente a su archivo `/etc/yum.conf`.

```
installonlypkgs=kernel, kernel-PAE, installonlypkg(kernel), installonlypkg(kernel-
module),
              installonlypkg(vm), multiversion(kernel), kmod-lustre-client
```

Esta lista incluye los paquetes de solo instalación por defecto, especificados en la página man `yum.conf` y en el paquete `kmod-lustre-client`.

Para instalar el cliente Lustre en Centos y Red Hat 8.2—8.9 o en Rocky Linux 8.4—8.9

Puede instalar y actualizar los paquetes del cliente Lustre compatibles con Red Hat Enterprise Linux (RHEL), Rocky Linux y CentOS desde el repositorio de paquetes yum del cliente Lustre de Amazon FSx. Estos paquetes están firmados para ayudar a garantizar que no han sido manipulados antes o durante la descarga. La instalación del repositorio falla si no instala la clave pública correspondiente en su sistema.

Para agregar el repositorio de paquetes yum del cliente Amazon FSx Lustre

1. Abra un terminal en su cliente de Linux.
2. Instala la clave pública de Amazon FSx rpm utilizando el siguiente comando.

   ```
   curl https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-rpm-public-
   key.asc -o /tmp/fsx-rpm-public-key.asc
   ```
3. Importe la clave utilizando el siguiente comando.

   ```
   sudo rpm --import /tmp/fsx-rpm-public-key.asc
   ```
4. Añada el repositorio y actualice el administrador de paquetes con el siguiente comando.

   ```
   sudo curl https://fsx-lustre-client-repo.s3.amazonaws.com/el/8/fsx-lustre-
   client.repo -o /etc/yum.repos.d/aws-fsx.repo
   ```

Para configurar el repositorio yum del cliente Lustre de Amazon FSx

El repositorio de paquetes yum del cliente Lustre de Amazon FSx está configurado por defecto para instalar el cliente Lustre que es compatible con la versión del kernel que se envió inicialmente con la última versión soportada de CentOS, Rocky Linux y RHEL 8. Para instalar un cliente Lustre que sea compatible con la versión del kernel que está utilizando, puede editar el archivo de configuración del repositorio.

Esta sección describe cómo determinar qué kernel está ejecutando, si necesita editar la configuración del repositorio, y cómo editar el archivo de configuración.

1. Determine qué kernel se está ejecutando actualmente en su instancia de procesamiento mediante la ejecución del siguiente comando.

   ```
   uname -r
   ```

2. Realice una de las acciones siguientes:

   - Si el comando devuelve `4.18.0-513*`, no necesita modificar la configuración del repositorio. Continúe con el procedimiento Para instalar el cliente Lustre.
   - Si el comando vuelve a `4.18.0-477*` aparecer, debe editar la configuración del repositorio para que apunte al cliente Lustre de las versiones CentOS, Rocky Linux y RHEL 8.8.
   - Si el comando devuelve `4.18.0-425*`, debe editar la configuración del repositorio para que apunte al cliente Lustre para la versión CentOS, Rocky Linux y RHEL 8.7.
   - Si el comando devuelve `4.18.0-372*`, debe editar la configuración del repositorio para que apunte al cliente Lustre para la versión CentOS, Rocky Linux y RHEL 8.6.
   - Si el comando devuelve `4.18.0-348*`, debe editar la configuración del repositorio para que apunte al cliente Lustre para la versión CentOS, Rocky Linux y RHEL 8.5.
   - Si el comando devuelve `4.18.0-305*`, debe editar la configuración del repositorio para que apunte al cliente Lustre para la versión CentOS, Rocky Linux y RHEL 8.4.
   - Si el comando devuelve `4.18.0-240*`, debe editar la configuración del repositorio para que apunte al cliente Lustre para la versión CentOS, Rocky Linux y RHEL 8.3.
   - Si el comando devuelve `4.18.0-193*`, debe editar la configuración del repositorio para que apunte al cliente Lustre para la versión CentOS, Rocky Linux y RHEL 8.2.

3. Edite el archivo de configuración del repositorio para que apunte a una versión específica de RHEL utilizando el siguiente comando.

```
sudo sed -i 's#8#specific_RHEL_version#' /etc/yum.repos.d/aws-fsx.repo
```

Por ejemplo, para apuntar a la versión 8.8, sustitúyala por `8.8` en el *`specific_RHEL_version`* comando.

```
sudo sed -i 's#8#8.8#' /etc/yum.repos.d/aws-fsx.repo
```

4. Utilice el siguiente comando para borrar la caché yum.

```
sudo yum clean all
```

Para instalar el cliente de Lustre

- Instale los paquetes desde el repositorio utilizando el siguiente comando.

```
sudo yum install -y kmod-lustre-client lustre-client
```

Información adicional (CentOS, Rocky Linux y Red Hat 8.2 y posterior)

Los comandos anteriores instalan los dos paquetes necesarios para montar e interactuar con su sistema de archivos Amazon FSx. El repositorio incluye paquetes Lustre adicionales, como un paquete que contiene el código fuente y paquetes que contienen pruebas, y puede instalarlos opcionalmente. Para listar todos los paquetes disponibles en el repositorio, utilice el siguiente comando.

```
yum --disablerepo="*" --enablerepo="aws-fsx" list available
```

Para descargar el rpm fuente, que contiene un tarball del código fuente upstream y el conjunto de parches que hemos aplicado, utilice el siguiente comando.

```
sudo yumdownloader --source kmod-lustre-client
```

Al ejecutar yum update, se instala una versión más reciente del módulo si está disponible y se sustituye la versión existente. Para evitar que la versión instalada actualmente se elimine en la actualización, añada una línea como la siguiente a su archivo `/etc/yum.conf`.

```
installonlypkgs=kernel, kernel-PAE, installonlypkg(kernel), installonlypkg(kernel-
module),
              installonlypkg(vm), multiversion(kernel), kmod-lustre-client
```

Esta lista incluye los paquetes de solo instalación por defecto, especificados en la página man `yum.conf` y en el paquete `kmod-lustre-client`.

Para instalar el cliente Lustre en CentOS y Red Hat 7.7, 7.8 o 7.9 (instancias x86_64)

Puede instalar y actualizar los paquetes del cliente Lustre compatibles con Red Hat Enterprise Linux (RHEL) y CentOS desde el repositorio de paquetes yum del cliente Lustre de Amazon FSx. Estos paquetes están firmados para ayudar a garantizar que no hayan sido manipulados antes o durante la descarga. La instalación del repositorio falla si no instala la clave pública correspondiente en su sistema.

Para agregar el repositorio de paquetes yum del cliente Amazon FSx Lustre

1. Abra un terminal en su cliente de Linux.
2. Instala la clave pública de Amazon FSx rpm utilizando el siguiente comando.

   ```
   curl https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-rpm-public-
   key.asc -o /tmp/fsx-rpm-public-key.asc
   ```

3. Importe la clave utilizando el siguiente comando.

   ```
   sudo rpm --import /tmp/fsx-rpm-public-key.asc
   ```

4. Añada el repositorio y actualice el administrador de paquetes con el siguiente comando.

   ```
   sudo curl https://fsx-lustre-client-repo.s3.amazonaws.com/el/7/fsx-lustre-
   client.repo -o /etc/yum.repos.d/aws-fsx.repo
   ```

Para configurar el repositorio yum del cliente Lustre de Amazon FSx

El repositorio de paquetes yum del cliente Lustre de Amazon FSx está configurado por defecto para instalar el cliente Lustre que es compatible con la versión del kernel que se envió inicialmente con la última versión compatible de CentOS y RHEL 7. Para instalar un cliente Lustre que sea compatible con la versión del kernel que está utilizando, puede editar el archivo de configuración del repositorio.

Esta sección describe cómo determinar qué kernel está ejecutando, si necesita editar la configuración del repositorio, y cómo editar el archivo de configuración.

1. Determine qué kernel se está ejecutando actualmente en su instancia de procesamiento mediante la ejecución del siguiente comando.

   ```
   uname -r
   ```

2. Realice una de las acciones siguientes:

   - Si el comando devuelve `3.10.0-1160*`, no necesita modificar la configuración del repositorio. Continúe con el procedimiento Para instalar el cliente Lustre.
   - Si el comando devuelve `3.10.0-1127*`, debe editar la configuración del repositorio para que apunte al cliente Lustre para la versión CentOS, Rocky Linux y RHEL 7.8.
   - Si el comando devuelve `3.10.0-1062*`, debe editar la configuración del repositorio para que apunte al cliente Lustre para la versión CentOS, Rocky Linux y RHEL 7.7.

3. Edite el archivo de configuración del repositorio para que apunte a una versión específica de RHEL utilizando el siguiente comando.

   ```
   sudo sed -i 's#7#specific_RHEL_version#' /etc/yum.repos.d/aws-fsx.repo
   ```

   Para señalar a la versión 7.8, sustituya *`specific_RHEL_version`* con `7.8` en el comando.

   ```
   sudo sed -i 's#7#7.8#' /etc/yum.repos.d/aws-fsx.repo
   ```

   Para señalar a la versión 7.7, sustituya *`specific_RHEL_version`* con `7.7` en el comando.

   ```
   sudo sed -i 's#7#7.7#' /etc/yum.repos.d/aws-fsx.repo
   ```

4. Utilice el siguiente comando para borrar la caché yum.

   ```
   sudo yum clean all
   ```

Para instalar el cliente de Lustre

- Instale los paquetes del cliente Lustre desde el repositorio utilizando el siguiente comando.

```
sudo yum install -y kmod-lustre-client lustre-client
```

Información adicional (CentOS, Rocky Linux y Red Hat 7.7 y posterior)

Los comandos anteriores instalan los dos paquetes necesarios para montar e interactuar con su sistema de archivos Amazon FSx. El repositorio incluye paquetes Lustre adicionales, como un paquete que contiene el código fuente y paquetes que contienen pruebas, y puede instalarlos opcionalmente. Para listar todos los paquetes disponibles en el repositorio, utilice el siguiente comando.

```
yum --disablerepo="*" --enablerepo="aws-fsx" list available
```

Para descargar el rpm fuente, que contiene un tarball del código fuente upstream y el conjunto de parches que hemos aplicado, utilice el siguiente comando.

```
 sudo yumdownloader --source kmod-lustre-client
```

Cuando ejecute yum update, se instalará una versión más reciente del módulo si está disponible, y se sustituirá la versión existente. Para evitar que la versión instalada actualmente se elimine en la actualización, añada una línea como la siguiente a su archivo `/etc/yum.conf`.

```
installonlypkgs=kernel, kernel-big-mem, kernel-enterprise, kernel-smp,
              kernel-debug, kernel-unsupported, kernel-source, kernel-devel, kernel-
PAE,
              kernel-PAE-debug, kmod-lustre-client
```

Esta lista incluye los paquetes de solo instalación por defecto, especificados en la página man `yum.conf` y en el paquete `kmod-lustre-client`.

Para instalar el cliente Lustre en Centos 7.8 o 7.9 (instancias basadas en AWS ARM con tecnología Graviton)

Puede instalar y actualizar paquetes de cliente Lustre desde el repositorio de paquetes yum de cliente Lustre de Amazon FSx que son compatibles con CentOS 7 para instancias EC2 basadas en Arm AWS y alimentadas por Graviton. Estos paquetes están firmados para ayudar a garantizar que no hayan sido manipulados antes o durante la descarga. La instalación del repositorio falla si no instala la clave pública correspondiente en su sistema.

Para agregar el repositorio de paquetes yum del cliente Amazon FSx Lustre

1. Abra un terminal en su cliente de Linux.
2. Instala la clave pública de Amazon FSx rpm utilizando el siguiente comando.

```
curl https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-rpm-public-key.asc -o /tmp/fsx-rpm-public-key.asc
```

```
curl https://fsx-lustre-client-repo-public-keys.s3.amazonaws.cn/fsx-rpm-public-key.asc -o /tmp/fsx-rpm-public-key.asc
```

3. Importe la clave utilizando el siguiente comando.

```
sudo rpm --import /tmp/fsx-rpm-public-key.asc
```

4. Añada el repositorio y actualice el administrador de paquetes con el siguiente comando.

```
sudo curl https://fsx-lustre-client-repo.s3.amazonaws.com/centos/7/fsx-lustre-client.repo -o /etc/yum.repos.d/aws-fsx.repo
```

Para configurar el repositorio yum del cliente Lustre de Amazon FSx

El repositorio de paquetes yum del cliente Lustre de Amazon FSx está configurado por defecto para instalar el cliente Lustre que es compatible con la versión del kernel que se envió inicialmente con la última versión compatible de CentOS 7. Para instalar un cliente Lustre que sea compatible con la versión del kernel que está utilizando, puede editar el archivo de configuración del repositorio.

Esta sección describe cómo determinar qué kernel está ejecutando, si necesita editar la configuración del repositorio, y cómo editar el archivo de configuración.

1. Determine qué kernel se está ejecutando actualmente en su instancia de procesamiento mediante la ejecución del siguiente comando.

```
uname -r
```

2. Realice una de las acciones siguientes:

   - Si el comando devuelve `4.18.0-193*`, no necesita modificar la configuración del repositorio. Continúe con el procedimiento Para instalar el cliente Lustre.

- Si el comando devuelve `4.18.0-147*`, debe editar la configuración del repositorio para que apunte al cliente Lustre para la versión CentOS 7.8.

3. Edite el archivo de configuración del repositorio para apuntar a la versión CentOS 7.8 mediante el siguiente comando.

```
sudo sed -i 's#7#7.8#' /etc/yum.repos.d/aws-fsx.repo
```

4. Utilice el siguiente comando para borrar la caché yum.

```
sudo yum clean all
```

Para instalar el cliente de Lustre

- Instale los paquetes desde el repositorio utilizando el siguiente comando.

```
sudo yum install -y kmod-lustre-client lustre-client
```

Información adicional (CentOS 7.8 o 7.9 para instancias EC2 basadas en ARM y alimentadas por AWS Graviton)

Los comandos anteriores instalan los dos paquetes necesarios para montar e interactuar con su sistema de archivos Amazon FSx. El repositorio incluye paquetes Lustre adicionales, como un paquete que contiene el código fuente y paquetes que contienen pruebas, y puede instalarlos opcionalmente. Para listar todos los paquetes disponibles en el repositorio, utilice el siguiente comando.

```
yum --disablerepo="*" --enablerepo="aws-fsx" list available
```

Para descargar el rpm fuente, que contiene un tarball del código fuente upstream y el conjunto de parches que hemos aplicado, utilice el siguiente comando.

```
 sudo yumdownloader --source kmod-lustre-client
```

Cuando ejecute yum update, se instalará una versión más reciente del módulo si está disponible, y se sustituirá la versión existente. Para evitar que la versión instalada actualmente se elimine en la actualización, añada una línea como la siguiente a su archivo `/etc/yum.conf`.

```
installonlypkgs=kernel, kernel-big-mem, kernel-enterprise, kernel-smp,
              kernel-debug, kernel-unsupported, kernel-source, kernel-devel, kernel-
PAE,
              kernel-PAE-debug, kmod-lustre-client
```

Esta lista incluye los paquetes de solo instalación por defecto, especificados en la página man `yum.conf` y en el paquete `kmod-lustre-client`.

## Ubuntu

Para instalar el cliente Lustre en Ubuntu 22.04

Puede obtener paquetes Lustre del repositorio Ubuntu 22.04 Amazon FSx. Para validar que el contenido del repositorio no haya sido manipulado antes o durante la descarga, se aplica una firma GNU Privacy Guard (GPG) a los metadatos del repositorio. La instalación del repositorio falla a menos que tenga la clave GPG pública correcta instalada en su sistema.

1. Abra un terminal en su cliente de Linux.
2. Siga estos pasos para añadir el repositorio de Amazon FSx Ubuntu:

   a. Si no ha registrado previamente un repositorio de Amazon FSx Ubuntu en su instancia cliente, descargue e instale la clave pública necesaria. Use el siguiente comando.

   ```
   wget -O - https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-
   ubuntu-public-key.asc | gpg --dearmor | sudo tee /usr/share/keyrings/fsx-
   ubuntu-public-key.gpg >/dev/null
   ```

   b. Agregue el repositorio de paquetes de Amazon FSx a su administrador de paquetes local mediante el siguiente comando.

   ```
   sudo bash -c 'echo "deb [signed-by=/usr/share/keyrings/fsx-ubuntu-public-
   key.gpg] https://fsx-lustre-client-repo.s3.amazonaws.com/ubuntu jammy main" > /
   etc/apt/sources.list.d/fsxlustreclientrepo.list && apt-get update'
   ```

3. Determine qué kernel se está ejecutando actualmente en su instancia de cliente y actualícelo según sea necesario. El cliente Lustre en Ubuntu 22.04 requiere kernel `5.15.0-1015-aws` o posterior tanto para instancias EC2 basadas en x86 como para instancias EC2 basadas en Arm y equipadas con procesadores Graviton AWS .

   a. Ejecute el siguiente comando para determinar qué kernel se está ejecutando.

```
uname -r
```

b. Ejecute el siguiente comando para actualizar a la última versión de Ubuntu kernel y Lustre y reinicie.

```
sudo apt install -y linux-aws lustre-client-modules-aws && sudo reboot
```

Si la versión de su kernel es superior a `5.15.0-1015-aws` tanto para las instancias EC2 basadas en x86 como para las instancias EC2 basadas en Graviton, y no desea actualizar a la última versión del kernel, puede instalar Lustre para el kernel actual con el siguiente comando.

```
sudo apt install -y lustre-client-modules-$(uname -r)
```

Se instalarán los dos paquetes Lustre necesarios para montar e interactuar con su sistema de archivos de FSx para Lustre. Opcionalmente puede instalar paquetes adicionales relacionados como un paquete que contiene el código fuente y paquetes que contienen pruebas que se incluyen en el repositorio.

c. Liste todos los paquetes disponibles en el repositorio utilizando el siguiente comando.

```
sudo apt-cache search ^lustre
```

d. (Opcional) Si desea que la actualización del sistema también actualice siempre los módulos de cliente Lustre, asegúrese de que el paquete `lustre-client-modules-aws` esté instalado mediante el siguiente comando.

```
sudo apt install -y lustre-client-modules-aws
```

> **Note**
>
> Si obtiene un error `Module Not Found`, consulte Para solucionar errores de módulos faltantes.

Para instalar el cliente Lustre en Ubuntu 20.04

Los clientes Lustre 2.12 son compatibles con Ubuntu 20.04 con kernel 5.15.0-1015-aws o posterior. Los clientes Lustre 2.10 son compatibles con Ubuntu 20.04 con el núcleo 5.4.0-1011-aws o posterior en las instancias EC2 basadas en x86 y con el kernel 5.4.0-1015-aws o posterior en las instancias EC2 basadas en ARM con procesadores Graviton. AWS

Puede obtener paquetes Lustre del repositorio Ubuntu 20.04 Amazon FSx. Para validar que el contenido del repositorio no haya sido manipulado antes o durante la descarga, se aplica una firma GNU Privacy Guard (GPG) a los metadatos del repositorio. La instalación del repositorio falla a menos que tenga la clave GPG pública correcta instalada en su sistema.

1. Abra un terminal en su cliente de Linux.
2. Siga estos pasos para añadir el repositorio de Amazon FSx Ubuntu:

   a. Si no ha registrado previamente un repositorio de Amazon FSx Ubuntu en su instancia cliente, descargue e instale la clave pública necesaria. Use el siguiente comando.

   ```
   wget -O - https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-ubuntu-public-key.asc | gpg --dearmor | sudo tee /usr/share/keyrings/fsx-ubuntu-public-key.gpg >/dev/null
   ```

   b. Agregue el repositorio de paquetes de Amazon FSx a su administrador de paquetes local mediante el siguiente comando.

   ```
   sudo bash -c 'echo "deb [signed-by=/usr/share/keyrings/fsx-ubuntu-public-key.gpg] https://fsx-lustre-client-repo.s3.amazonaws.com/ubuntu focal main" > /etc/apt/sources.list.d/fsxlustreclientrepo.list && apt-get update'
   ```

3. Determine qué kernel se está ejecutando actualmente en su instancia de cliente y actualícelo según sea necesario.

   a. Ejecute el siguiente comando para determinar qué kernel se está ejecutando.

   ```
   uname -r
   ```

   b. Ejecute el siguiente comando para actualizar a la última versión de Ubuntu kernel y Lustre y reinicie.

   ```
   sudo apt install -y linux-aws lustre-client-modules-aws && sudo reboot
   ```

Si la versión de su kernel es superior a `5.4.0-1011-aws` para las instancias EC2 basadas en x86, o superior a `5.4.0-1015-aws` para las instancias EC2 basadas en Graviton, y no desea actualizar a la última versión del kernel, puede instalar Lustre para el kernel actual con el siguiente comando.

```
sudo apt install -y lustre-client-modules-$(uname -r)
```

Se instalarán los dos paquetes Lustre necesarios para montar e interactuar con su sistema de archivos de FSx para Lustre. Opcionalmente puede instalar paquetes adicionales relacionados como un paquete que contiene el código fuente y paquetes que contienen pruebas que se incluyen en el repositorio.

c. Liste todos los paquetes disponibles en el repositorio utilizando el siguiente comando.

```
sudo apt-cache search ^lustre
```

d. (Opcional) Si desea que la actualización del sistema también actualice siempre los módulos de cliente Lustre, asegúrese de que el paquete `lustre-client-modules-aws` esté instalado mediante el siguiente comando.

```
sudo apt install -y lustre-client-modules-aws
```

> **Note**
>
> Si obtiene un error `Module Not Found`, consulte Para solucionar errores de módulos faltantes.

Para instalar el cliente Lustre en Ubuntu 18.04

> **Note**
>
> La última versión soportada del kernel de Ubuntu 18 es `5.4.0.1103.aws`.

Puede obtener paquetes Lustre del repositorio Ubuntu 18.04 Amazon FSx. Para validar que el contenido del repositorio no haya sido manipulado antes o durante la descarga, se aplica una firma

GNU Privacy Guard (GPG) a los metadatos del repositorio. La instalación del repositorio falla a menos que tenga la clave GPG pública correcta instalada en su sistema.

1. Abra un terminal en su cliente de Linux.
2. Siga estos pasos para añadir el repositorio de Amazon FSx Ubuntu:

   a. Si no ha registrado previamente un repositorio de Amazon FSx Ubuntu en su instancia cliente, descargue e instale la clave pública necesaria. Use el siguiente comando.

   ```
   wget -O - https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-ubuntu-public-key.asc | gpg --dearmor | sudo tee /usr/share/keyrings/fsx-ubuntu-public-key.gpg >/dev/null
   ```

   b. Agregue el repositorio de paquetes de Amazon FSx a su administrador de paquetes local mediante el siguiente comando.

   ```
   sudo bash -c 'echo "deb [signed-by=/usr/share/keyrings/fsx-ubuntu-public-key.gpg] https://fsx-lustre-client-repo.s3.amazonaws.com/ubuntu bionic main" > /etc/apt/sources.list.d/fsxlustreclientrepo.list && apt-get update'
   ```

3. Determine qué kernel se está ejecutando actualmente en su instancia de cliente y actualícelo según sea necesario. El cliente Lustre de Ubuntu 18.04 requiere el kernel o una versión posterior para las instancias EC2 basadas en x86 y un kernel `4.15.0-1054-aws` o posterior para las instancias EC2 basadas en ARM con procesadores Graviton. `5.3.0-1023-aws` AWS

   a. Ejecute el siguiente comando para determinar qué kernel se está ejecutando.

   ```
   uname -r
   ```

   b. Ejecute el siguiente comando para actualizar a la última versión de Ubuntu kernel y Lustre y reinicie.

   ```
   sudo apt install -y linux-aws lustre-client-modules-aws && sudo reboot
   ```

   Si la versión de su kernel es superior a `4.15.0-1054-aws` para las instancias EC2 basadas en x86, o superior a `5.3.0-1023-aws` para las instancias EC2 basadas en Graviton, y no desea actualizar a la última versión del kernel, puede instalar Lustre para el kernel actual con el siguiente comando.

```
sudo apt install -y lustre-client-modules-$(uname -r)
```

Se instalarán los dos paquetes Lustre necesarios para montar e interactuar con su sistema de archivos de FSx para Lustre. Opcionalmente, puede instalar paquetes relacionados adicionales, como un paquete que contiene el código fuente y paquetes que contienen pruebas que se incluyen en el repositorio.

c. Liste todos los paquetes disponibles en el repositorio utilizando el siguiente comando.

```
sudo apt-cache search ^lustre
```

d. (Opcional) Si desea que la actualización del sistema también actualice siempre los módulos de cliente Lustre, asegúrese de que el paquete `lustre-client-modules-aws` esté instalado mediante el siguiente comando.

```
sudo apt install -y lustre-client-modules-aws
```

> **Note**
>
> Si obtiene un error `Module Not Found`, consulte Para solucionar errores de módulos faltantes.

Para solucionar errores de módulos faltantes

Si obtiene un error `Module Not Found` durante la instalación en cualquier versión de Ubuntu, haga lo siguiente

Cambie su kernel a la anterior versión soportada. Enumere todas las versiones disponibles del paquete e instale el núcleo correspondiente. lustre-client-modules Para ello, utilice el siguiente comando.

```
sudo apt-cache search lustre-client-modules
```

Por ejemplo, si la última versión que se incluye en el repositorio es `lustre-client-modules-5.4.0-1011-aws`, haga lo siguiente:

1. Instale el kernel para el que se creó este paquete utilizando los siguientes comandos.

```
sudo apt-get install -y linux-image-5.4.0-1011-aws
```

```
sudo sed -i 's/GRUB_DEFAULT=.\+/GRUB\_DEFAULT="Advanced options for Ubuntu>Ubuntu,
 with Linux 5.4.0-1011-aws"/' /etc/default/grub
```

```
sudo update-grub
```

2. Reinicie su instancia utilizando el siguiente comando.

```
sudo reboot
```

3. Instale el cliente Lustre utilizando el siguiente comando.

```
sudo apt-get install -y lustre-client-modules-$(uname -r)
```

## SUSE Linux

Para instalar el cliente Lustre en SUSE Linux 12 SP3, SP4 o SP5

Para instalar el cliente Lustre en SUSE Linux 12 SP3

1. Abra un terminal en su cliente de Linux.
2. Instala la clave pública de Amazon FSx rpm utilizando el siguiente comando.

```
sudo wget https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-sles-
public-key.asc
```

3. Importe la clave utilizando el siguiente comando.

```
sudo rpm --import fsx-sles-public-key.asc
```

4. Añada el repositorio para el cliente Lustre utilizando el siguiente comando.

```
sudo wget https://fsx-lustre-client-repo.s3.amazonaws.com/suse/sles-12/SLES-12/fsx-
lustre-client.repo
```

5. Descargue e instale el cliente Lustre con los siguientes comandos.

```
sudo zypper ar --gpgcheck-strict fsx-lustre-client.repo
sudo sed -i 's#SLES-12#SP3#' /etc/zypp/repos.d/aws-fsx.repo
sudo zypper refresh
sudo zypper in lustre-client
```

Para instalar el cliente Lustre en SUSE Linux 12 SP4

1. Abra un terminal en su cliente de Linux.
2. Instala la clave pública de Amazon FSx rpm utilizando el siguiente comando.

```
sudo wget https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-sles-
public-key.asc
```

3. Importe la clave utilizando el siguiente comando.

```
sudo rpm --import fsx-sles-public-key.asc
```

4. Añada el repositorio para el cliente Lustre utilizando el siguiente comando.

```
sudo wget https://fsx-lustre-client-repo.s3.amazonaws.com/suse/sles-12/SLES-12/fsx-
lustre-client.repo
```

5. Realice una de las acciones siguientes:

   - Si instaló SP4 directamente, descargue e instale el cliente Lustre con los siguientes comandos.

     ```
     sudo zypper ar --gpgcheck-strict fsx-lustre-client.repo
     sudo sed -i 's#SLES-12#SP4#' /etc/zypp/repos.d/aws-fsx.repo
     sudo zypper refresh
     sudo zypper in lustre-client
     ```

   - Si migró de SP3 a SP4 y anteriormente agregó el repositorio de Amazon FSx para SP3, descargue e instale el cliente Lustre con los siguientes comandos.

     ```
     sudo zypper ar --gpgcheck-strict fsx-lustre-client.repo
     sudo sed -i 's#SP3#SP4#' /etc/zypp/repos.d/aws-fsx.repo
     sudo zypper ref
     sudo zypper up --force-resolution lustre-client-kmp-default
     ```

Para instalar el cliente Lustre en SUSE Linux 12 SP5

1. Abra un terminal en su cliente de Linux.
2. Instala la clave pública de Amazon FSx rpm utilizando el siguiente comando.

```
sudo wget https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-sles-public-key.asc
```

3. Importe la clave utilizando el siguiente comando.

```
sudo rpm --import fsx-sles-public-key.asc
```

4. Añada el repositorio para el cliente Lustre utilizando el siguiente comando.

```
sudo wget https://fsx-lustre-client-repo.s3.amazonaws.com/suse/sles-12/SLES-12/fsx-lustre-client.repo
```

5. Realice una de las acciones siguientes:

   - Si instaló SP5 directamente, descargue e instale el cliente Lustre con los siguientes comandos.

   ```
   sudo zypper ar --gpgcheck-strict fsx-lustre-client.repo
   sudo zypper refresh
   sudo zypper in lustre-client
   ```

   - Si migró de SP4 a SP5 y anteriormente agregó el repositorio de Amazon FSx para SP4, descargue e instale el cliente Lustre con los siguientes comandos.

   ```
   sudo sed -i 's#SP4#SLES-12' /etc/zypp/repos.d/aws-fsx.repo
   sudo zypper ref
   sudo zypper up --force-resolution lustre-client-kmp-default
   ```

> **Note**
>
> Es posible que tenga que reiniciar la instancia de procesamiento para que el cliente finalice la instalación.

# Montaje desde una instancia de Amazon Elastic Compute Cloud

Puede montar su sistema de archivos desde una instancia de Amazon EC2.

Para montar el sistema de archivos desde Amazon EC2

1. Conecte con la instancia de Amazon EC2.
2. Cree un directorio en su sistema de archivos de FSx para Lustre para el punto de montaje con el siguiente comando.

   ```
   $ sudo mkdir -p /fsx
   ```

3. Monte el sistema de archivos de Amazon FSx para Lustre en el directorio que ha creado. Utilice el siguiente comando y sustituya los siguientes elementos:

   - Reemplace *`file_system_dns_name`* con el nombre DNS real del sistema de archivos.
   - Reemplace *`mountname`* con el nombre de montaje del sistema de archivos. Este nombre de montaje es devuelto en la respuesta de la operación API `CreateFileSystem`. También se devuelve en la respuesta al describe-file-systems AWS CLI comando y en la operación de la DescribeFileSystemsAPI.

   ```
   sudo mount -t lustre -o relatime,flock file_system_dns_name@tcp:/mountname /fsx
   ```

   Este comando monta el sistema de archivos con dos opciones: `-o relatime` y `flock`:

   - `relatime` – Si bien la opción `atime` mantiene los datos `atime` (tiempos de acceso al inodo) cada vez que se accede a un archivo, la opción `relatime` también mantiene los datos `atime`, pero no para cada vez que se accede a un archivo. Con la opción `relatime` habilitada, los datos `atime` se escriben en el disco solo si el archivo se ha modificado desde que los datos `atime` se actualizaron por última vez (`mtime`), o si se accedió al archivo por última vez hace más de un cierto tiempo (6 horas por defecto). El uso de la opción `relatime` o `atime` optimizará los procesos de liberación de archivos.

     > **Note**
     >
     > Si su carga de trabajo requiere una precisión exacta del tiempo de acceso, puede montar con la opción de montaje `atime`. Sin embargo, hacerlo puede afectar al

rendimiento de la carga de trabajo al aumentar el tráfico de red necesario para mantener valores de tiempo de acceso precisos.
Si su carga de trabajo no requiere tiempo de acceso a metadatos, el uso de la opción de montaje `noatime` para desactivar las actualizaciones del tiempo de acceso puede proporcionar una ganancia de rendimiento. Tenga en cuenta que los procesos centrados `atime` como la liberación de archivos o la liberación de la validez de los datos serán imprecisos en su liberación.

- `flock` – Permite el bloqueo de archivos para su sistema de archivos. Si no quiere activar el bloqueo de archivos, utilice el comando `mount` sin `flock`.

4. Compruebe que el comando de montaje se haya realizado correctamente listando el contenido del directorio en el que ha montado el sistema de archivos, /mnt/fsx mediante el siguiente comando.

```
$ ls /fsx
import-path  lustre
$
```

También puede utilizar el comando `df`, a continuación.

```
$ df
Filesystem                     1K-blocks    Used  Available Use% Mounted on
devtmpfs                         1001808       0    1001808   0% /dev
tmpfs                            1019760       0    1019760   0% /dev/shm
tmpfs                            1019760     392    1019368   1% /run
tmpfs                            1019760       0    1019760   0% /sys/fs/cgroup
/dev/xvda1                       8376300 1263180    7113120  16% /
123.456.789.0@tcp:/mountname 3547698816   13824 3547678848   1% /fsx
tmpfs                             203956       0     203956   0% /run/user/1000
```

Los resultados muestran el sistema de archivos Amazon FSx montado en /fsx.

# Montaje de Amazon Elastic Container Service

Puede acceder a su sistema de archivos de FSx para Lustre desde un contenedor de Docker de Amazon Elastic Container Service (Amazon ECS) en una instancia de Amazon EC2. Puede hacerlo utilizando cualquiera de las siguientes opciones:

1. Montando su sistema de archivos de FSx para Lustre desde la instancia de Amazon EC2 que aloja sus tareas de Amazon ECS y exportando este punto de montaje a sus contenedores.
2. Montando el sistema de archivos directamente en el contenedor de tareas.

Para obtener más información sobre Amazon ECS, consulte ¿Qué es Amazon Elastic Container Service? en la Guía para desarrolladores de Amazon Elastic Container Service.

Recomendamos utilizar la opción 1 (Montaje desde una instancia de Amazon EC2 que aloja tareas de Amazon ECS) porque proporciona un mejor uso de los recursos, especialmente si inicia muchos contenedores (más de cinco) en la misma instancia EC2 o si sus tareas son de corta duración (menos de 5 minutos).

Utilice la opción 2 (Montaje desde un contenedor de Docker), si no puede configurar la instancia EC2, o si su aplicación requiere la flexibilidad del contenedor.

> **Note**
>
> No se admite el montaje de FSx for Lustre en AWS un tipo de lanzamiento de Fargate.

Las siguientes secciones describen los procedimientos de cada una de las opciones para montar su sistema de archivos de FSx para Lustre desde un contenedor Amazon ECS.

Temas

- Montaje desde una instancia de Amazon EC2 que aloja tareas de Amazon ECS
- Montaje desde un contenedor de Docker

## Montaje desde una instancia de Amazon EC2 que aloja tareas de Amazon ECS

Este procedimiento muestra cómo puede configurar una instancia de Amazon ECS en EC2 para montar localmente su sistema de archivos de FSx para Lustre. El procedimiento utiliza las propiedades del contenedor `volumes` y `mountPoints` para compartir el recurso y hacer que este sistema de archivos sea accesible para las tareas que se ejecutan localmente. Para obtener más información, consulte Lanzamiento de una instancia de contenedor de Amazon ECS en la Guía del desarrollador de Amazon Elastic Container Service.

Este procedimiento es para una AMI de Amazon Linux 2 optimizada para Amazon ECS. Si utiliza otra distribución de Linux, consulte Instalación del cliente Lustre.

Para montar su sistema de archivos desde Amazon ECS en una instancia EC2

1. Al lanzar instancias de Amazon ECS, ya sea manualmente o utilizando un grupo de escalado automático, añada las líneas del siguiente ejemplo de código al final del campo Datos de usuario. Reemplace los siguientes elementos en el ejemplo:

   - Reemplace *file_system_dns_name* con el nombre DNS real del sistema de archivos.
   - Reemplace *mountname* con el nombre de montaje del sistema de archivos.
   - Reemplace *mountpoint* por el punto de montaje del sistema de archivos, que deberá crear.

   ```
   #!/bin/bash

   ...<existing user data>...

   fsx_dnsname=file_system_dns_name
   fsx_mountname=mountname
   fsx_mountpoint=mountpoint
   amazon-linux-extras install -y lustre
   mkdir -p "$fsx_mountpoint"
   mount -t lustre ${fsx_dnsname}@tcp:/${fsx_mountname} ${fsx_mountpoint} -o
    relatime,flock
   ```

2. Al crear sus tareas de Amazon ECS, añada las siguientes propiedades de contenedor `volumes` y `mountPoints` en la definición JSON. Reemplace *mountpoint* con el punto de montaje del sistema de archivos (como `/mnt/fsx`).

   ```
   {
       "volumes": [
              {
                     "host": {
                          "sourcePath": "mountpoint"
                     },
                     "name": "Lustre"
              }
       ],
       "mountPoints": [
              {
   ```

```
                "containerPath": "mountpoint",
                "sourceVolume": "Lustre"
            }
    ],
}
```

## Montaje desde un contenedor de Docker

El siguiente procedimiento muestra cómo puede configurar un contenedor de tareas de Amazon ECS para instalar el paquete `lustre-client` y montar en él su sistema de archivos de FSx para Lustre. El procedimiento utiliza una imagen de Docker de Amazon Linux (`amazonlinux`), pero un enfoque similar puede funcionar para otras distribuciones.

Para montar el sistema de archivos desde un contenedor de Docker

1. En su contenedor de Docker, instale el paquete `lustre-client` y monte su sistema de archivos de FSx para Lustre con la propiedad `command`. Reemplace los siguientes elementos en el ejemplo:

   - Reemplace *`file_system_dns_name`* con el nombre DNS real del sistema de archivos.
   - Reemplace *`mountname`* con el nombre de montaje del sistema de archivos.
   - Reemplace *`mountpoint`* con el punto de montaje del sistema de archivos.

   ```
   "command": [
     "/bin/sh -c \"amazon-linux-extras install -y lustre; mount -t
    lustre file_system_dns_name@tcp:/mountname mountpoint -o relatime,flock;\""
   ],
   ```

2. Agregue la capacidad `SYS_ADMIN` a su contenedor para autorizarlo a montar su sistema de archivos de FSx para Lustre, utilizando la propiedad `linuxParameters`.

   ```
   "linuxParameters": {
     "capabilities": {
         "add": [
           "SYS_ADMIN"
         ]
      }
   }
   ```

# Montaje de sistemas de archivos de Amazon FSx en las instalaciones o desde una VPC de Amazon interconectada

Puede acceder a su sistema de archivos Amazon FSx de dos maneras. Una es desde las instancias de Amazon EC2 ubicadas en una VPC de Amazon que está interconectada a la VPC del sistema de archivos. La otra proviene de clientes locales que están conectados a la VPC de su sistema de archivos AWS Direct Connect mediante una VPN.

Conecte la VPC del cliente y la VPC de su sistema de archivos Amazon FSx mediante una conexión de emparejamiento de VPC o una puerta de enlace de tránsito de VPC. Cuando utiliza una conexión de emparejamiento de VPC o una puerta de enlace de tránsito de VPC para conectar las VPC, las instancias de Amazon EC2 que se encuentran en una VPC pueden acceder a los sistemas de archivos de Amazon FSx de otra VPC, incluso si las VPC pertenecen a cuentas diferentes.

Antes de utilizar el siguiente procedimiento, debe configurar una conexión de emparejamiento de VPC o una puerta de enlace de tránsito de VPC.

Una puerta de enlace de tránsito es un hub de tránsito de red que puede utilizar para interconectar sus VPC y redes en las instalaciones. Para obtener más información acerca del uso de puertas de enlace de tránsito de VPC, consulte Introducción a las puertas de enlace de tránsito en la Guía de puertas de enlace de tránsito de Amazon VPC.

Una conexión de emparejamiento de VPC es una conexión de red entre dos instancias de VPC. Este tipo de conexión permite enrutar el tráfico entre ellas mediante direcciones de protocolo de Internet versión 4 (IPv4) o de protocolo de Internet versión 6 (IPv6) privadas. Puede usar el emparejamiento de VPC para conectar VPC dentro de la misma AWS región o entre regiones. AWS Para obtener más información sobre la conexión de emparejamiento de las VPC, consulte ¿Qué es una conexión de emparejamiento de VPC? en la Guía de conexión de emparejamiento de VPC de Amazon.

Puede montar su sistema de archivos desde fuera de su VPC utilizando la dirección IP de su interfaz de red principal. La interfaz de red principal es la primera interfaz de red que se devuelve al ejecutar el comando. `aws fsx describe-file-systems` AWS CLI También puede obtener esta dirección IP desde la consola de administración de Amazon Web Services.

La siguiente tabla ilustra los requisitos de dirección IP para acceder a los sistemas de archivos de Amazon FSx utilizando un cliente que está fuera de la VPC del sistema de archivos.

| Para clientes ubicados en... | Acceso a los sistemas de archivos creados antes del 17 de diciembre de 2020 | Acceso a los sistemas de archivos creados a partir del 17 de diciembre de 2020 |
|---|---|---|
| Emparejamiento de VPC utilizando el emparejamiento de VPC o AWS Transit Gateway | Los clientes con direcciones IP dentro un rango de direcciones IP privadas de acuerdo con la norma RFC 1918:<br>• 10.0.0.0/8<br>• 172.16.0.0/12<br>• 192.168.0.0/16 | ✓ |
| Redes interconectadas que utilizan AWS Direct Connect o AWS VPN | | ✓ |

Si necesita acceder al sistema de archivos Amazon FSx creado antes del 17 de diciembre de 2020, con un intervalo de direcciones IP no privadas, puede crear un nuevo sistema de archivos restaurando una copia de seguridad del sistema de archivos. Para obtener más información, consulte Trabajo con copias de seguridad.

Para recuperar la dirección IP de la interfaz de red primaria de un sistema de archivos

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación, elija Sistema de archivos.
3. Seleccione el sistema de archivos en el panel.
4. En la página de detalles del sistema de archivos, seleccione Red y seguridad.
5. En Interfaz de red, seleccione el ID de su interfaz de red elástica primaria. Al hacerlo, accederá a la consola de Amazon EC2.
6. En la pestaña Detalles, busque la Primary private IPv4 IP. Esta es la dirección IP de su interfaz de red principal.

> **Note**
>
> No puede utilizar la resolución de nombres del sistema de nombres de dominio (DNS) al montar un sistema de archivos de Amazon FSx desde fuera de la VPC a la que está asociado.

# Montaje automático de su sistema de archivos Amazon FSx

Puede actualizar el archivo `/etc/fstab` de su instancia de Amazon EC2 después de conectarse a la instancia por primera vez para que monte su sistema de archivos de Amazon FSx cada vez que se reinicie.

## Cómo usar /etc/fstab para montar FSx para Lustre automáticamente

Para montar automáticamente el directorio del sistema de archivos de Amazon FSx cuando se reinicie la instancia de Amazon EC2, puede utilizar el archivo `fstab`. El archivo `fstab` contiene información sobre los sistemas de archivos. El comando `mount -a`, que se ejecuta durante el startup de la instancia, monta los sistemas de archivos enumerados en el archivo `fstab`.

> **Note**
>
> Antes de que pueda actualizar el archivo `/etc/fstab` de su instancia EC2, asegúrese de que ya ha creado su sistema de archivos Amazon FSx. Para obtener más información, consulte Cree su sistema de archivos FSx for Lustre en el Ejercicio de introducción.

Para actualizar el archivo /etc/fstab en la instancia EC2

1. Conéctese a la instancia EC2 y abra el archivo `/etc/fstab` en un editor.
2. Añada la línea siguiente al archivo `/etc/fstab`.

   Monte el sistema de archivos de Amazon FSx para Lustre en el directorio que ha creado. Utilice el siguiente comando y sustituya lo siguiente:

   - Sustitúyalo *`/fsx`* por el directorio en el que desea montar el sistema de archivos de Amazon FSx.
   - Reemplace *`file_system_dns_name`* con el nombre DNS real del sistema de archivos.

- Reemplace *mountname* con el nombre de montaje del sistema de archivos. Este nombre de montaje es devuelto en la respuesta de la operación API `CreateFileSystem`. También se devuelve en la respuesta al describe-file-systems AWS CLI comando y en la operación de la `DescribeFileSystems` API.

```
file_system_dns_name@tcp:/mountname /fsx lustre defaults,relatime,flock,_netdev,x-systemd.automount,x-systemd.requires=network.service 0 0
```

> **Warning**
>
> Use la opción `_netdev`, empleada para identificar los sistemas de archivos de red, cuando monte su sistema de archivos automáticamente. Si falta `_netdev`, la instancia EC2 puede dejar de responder. Este resultado se debe a que los sistemas de archivos de red se deben inicializar después de que la instancia de procesamiento inicia sus redes. Para obtener más información, consulte Se produce un error de montaje automático y la instancia no responde.

3. Guarde los cambios en el archivo.

La instancia EC2 está configurada ahora para montar el sistema de archivos de Amazon FSx cuando se reinicia.

> **Note**
>
> En algunos casos, es posible que su instancia de Amazon EC2 deba iniciarse independientemente del estado de su sistema de archivos de Amazon FSx montado. En estos casos, agregue la opción `nofail` a la entrada de su sistema de archivos en el archivo `/etc/fstab`.

Los campos de la línea de código que ha agregado al archivo `/etc/fstab` hacen lo siguiente.

| Campo | Descripción |
| --- | --- |
| *file_system_dns_name* @tcp:/ | El nombre DNS de su sistema de archivos Amazon FSx, que identifica el sistema de archivos. Puedes obtener este nombre desde la consola o mediante programación desde el SDK AWS CLI o desde un AWS SDK. |
| *mountname* | El nombre de montaje para el sistema de archivos. Puede obtener este nombre de la consola o mediante programación mediante el describe-file-systems comando o la AWS API o el SDK AWS CLI mediante la operación. DescribeFileSystems |
| */fsx* | El punto de montaje para el sistema de archivos de Amazon FSx en su instancia EC2. |
| `lustre` | El tipo de sistema de archivos, Amazon FSx. |
| `mount options` | Opciones de montaje para el sistema de archivos, presentadas como una lista separada por comas de las siguientes opciones:<br>• `defaults` – Este valor indica al sistema operativo que utilice las opciones de montaje por defecto. Puede listar las opciones de montaje por defecto después de que el sistema de archivos haya sido montado viendo la salida del comando `mount`.<br>• `relatime` – Esta opción mantiene los datos `atime` (tiempos de acceso al inodo), pero no para cada vez que se accede a un archivo. Con esta opción activada, `atime` los datos se escriben en el disco solo si el archivo ha sido modificado desde que los datos `atime` se actualizaron por última vez (`mtime`), o si se accedió al archivo por última vez hace más de un cierto tiempo (un día por defecto). Si desea desactivar las actualizaciones del tiempo de acceso al inodo, utilice la opción de montaje `noatime`.<br>• `flock` – monta tu sistema de archivos con el bloqueo de archivos activado. Si no quiere activar el bloqueo de archivos, utilice la opción de `noflock` montaje en su lugar.<br>• `_netdev` – el valor indica al sistema operativo que el sistema de archivos reside en un dispositivo que requiere acceso a la red. Esta |

| Campo | Descripción |
| --- | --- |
| | opción impide que la instancia monte el sistema de archivos hasta que se haya habilitado la red en el cliente. |
| `x-systemd.automount,x-systemd.requires=network.service` | Estas opciones garantizan que el montador automático no se ejecute hasta que la conectividad de red esté en línea.<br><br>**Note**<br>Para Ubuntu 22.04, utilice la opción `x-systemd.requires=systemd-networkd-wait-online.service` en lugar de la opción `x-systemd.requires=network.service` . |
| `0` | Un valor que indica si el sistema de archivos debe ser respaldado por dump. Para Amazon FSx, este valor debería ser `0`. |
| `0` | Valor que indica el orden en el que `fsck` comprueba los sistemas de ficheros en el arranque. Para sistemas de archivos de Amazon FSx, este valor debe ser `0` para indicar que `fsck` no se debe ejecutar durante el startup. |

## Montaje de conjuntos de archivos específicos

Al usar la característica de conjuntos de archivos de Lustre, puede montar solo un subconjunto del espacio de nombres del sistema de archivos, que se denomina conjunto de archivos. Para montar un conjunto de archivos del sistema de archivos, en el cliente se especifica la ruta del subdirectorio después del nombre del sistema de archivos. El montaje de un conjunto de archivos (también llamado montaje de subdirectorio) limita la visibilidad del espacio de nombres del sistema de archivos en un cliente específico.

Ejemplo: monte un conjunto de archivos Lustre

1. Asuma que tiene un sistema de archivos de FSx para Lustre con los siguientes directorios:

```
team1/dataset1/
```

```
team2/dataset2/
```

2. Solo debe montar el conjunto de archivos `team1/dataset1`, haciendo solo esta parte del sistema de archivos visible localmente en el cliente. Utilice el siguiente comando y sustituya los siguientes elementos:

   - Reemplace *`file_system_dns_name`* con el nombre DNS real del sistema de archivos.
   - Reemplace *`mountname`* con el nombre de montaje del sistema de archivos. Este nombre de montaje es devuelto en la respuesta de la operación API `CreateFileSystem`. También se devuelve en la respuesta del describe-file-systems AWS CLI comando y en la operación de la DescribeFileSystemsAPI.

```
mount -t lustre file_system_dns_name@tcp:/mountname/team1/dataset1 /fsx
```

Cuando utilice la característica del conjunto de archivos Lustre, tenga en cuenta lo siguiente:

- No hay restricciones que impidan a un cliente volver a montar el sistema de archivos utilizando un conjunto de archivos diferente, o ningún conjunto de archivos.
- Al utilizar un conjunto de archivos, es posible que algunos comandos administrativos de Lustre que requieren acceso al directorio `.lustre/` no funcionen, como el comando `lfs fid2path`.
- Si tiene previsto montar varios subdirectorios del mismo sistema de archivos en el mismo host, tenga en cuenta que esto consume más recursos que un único punto de montaje, y podría ser más eficiente montar el directorio raíz del sistema de archivos solo una vez.

Para obtener más información sobre la característica de conjunto de archivos de Lustre, consulte el Manual de operaciones de Lustre en el sitio web de documentación de Lustre..

## Desmontaje de sistemas de archivos

Antes de eliminar un sistema de archivos, le recomendamos que lo desmonte de todas las instancias de Amazon EC2 a las que esté conectado. Puede desmontar un sistema de archivos en su instancia de Amazon EC2 ejecutando el comando `umount` de la propia instancia. No puede desmontar un sistema de archivos Amazon FSx a través del, AWS CLI AWS Management Console el o a través de ninguno de los AWS SDK. Para desmontar un sistema de archivos de Amazon FSx conectado

a una instancia de Amazon EC2 que ejecuta Linux, utilice el comando `umount` como se muestra a continuación:

```
umount /mnt/fsx
```

Le recomendamos que no especifique las demás opciones `umount`. Evite la configuración de otras opciones `umount` que sean diferentes de los valores predeterminados.

Puede comprobar que el sistema de archivos de Amazon FSx se haya desmontado ejecutando el comando `df`. Este comando muestra las estadísticas de uso del disco de los sistemas de archivos actualmente montados en la instancia de Amazon EC2 basada en Linux. Si el sistema de archivos de Amazon FSx que desea desmontar no aparece en la salida del comando `df`, esto significa que el sistema de archivos está desmontado.

Example – Identifica el estado de montaje de un sistema de archivos de Amazon FSx y desmóntalo

```
$ df -T
Filesystem Type 1K-blocks Used Available Use% Mounted on
file-system-id.fsx.aws-region.amazonaws.com@tcp:/mountname /fsx 3547708416 61440
 3547622400 1% /fsx
      /dev/sda1 ext4 8123812 1138920 6884644 15% /
```

```
$ umount /fsx
```

```
$ df -T
```

```
Filesystem Type 1K-blocks Used Available Use% Mounted on
/dev/sda1 ext4 8123812 1138920 6884644 15% /
```

# Trabajar con instancias de spot de Amazon EC2

FSx para Lustre se puede utilizar con instancias de spot EC2 para reducir significativamente los costos de Amazon EC2. Una instancia de spot es una instancia EC2 sin utilizar que está disponible por un precio inferior al precio bajo demanda. Amazon EC2 puede interrumpir su instancia de spot si la demanda de instancias de spot supera el precio máximo, si la oferta de instancias de spot aumenta o si la oferta de instancias de spot disminuye.

Cuando Amazon EC2 interrumpe una instancia de spot, proporciona un aviso de interrupción de instancia de spot, que envía a la instancia una advertencia dos minutos antes de que Amazon EC2 la interrumpa. Para obtener más información, consulte Instancias de spot en la Guía del usuario de Amazon EC2 para instancias de Linux.

Para garantizar que los sistemas de archivos de Amazon FSx no se vean afectados por las interrupciones de instancias de spot de EC2, recomendamos desmontar los sistemas de archivos de Amazon FSx antes de finalizar o hibernar las instancias de spot de EC2. Para obtener más información, consulte Desmontaje de sistemas de archivos.

## Cómo manejar las interrupciones de las instancias de spot de Amazon EC2

FSx para Lustre es un sistema de archivos distribuido donde las instancias de servidor y cliente cooperan para proporcionar un sistema de archivos fiable y de alto rendimiento. Mantienen un estado distribuido y coherente entre las instancias cliente y servidor. Los servidores FSx para Lustre delegan permisos de acceso temporal a los clientes mientras están activamente realizando E/S y almacenando en caché datos del sistema de archivos. Se espera que los clientes respondan en un corto período de tiempo cuando los servidores les soliciten revocar sus permisos de acceso temporal. Para proteger el sistema de archivos de los clientes que se comportan mal, los servidores pueden desalojar a los clientes de Lustre que no respondan después de unos minutos. Para evitar tener que esperar varios minutos a que un cliente que no responde responda a la solicitud del servidor, es importante desmontar limpiamente los clientes Lustre, especialmente antes de terminar las instancias de spot de EC2.

La instancia de spot de EC2 envía avisos de terminación con 2 minutos de antelación antes de cerrar una instancia. Le recomendamos que automatice el proceso de desmontar limpiamente los clientes Lustre antes de terminar las instancias de spot de EC2.

Example – Script para desmontar limpiamente las instancias de spot EC2 terminadas

Este script de ejemplo elimina de forma limpia la terminación de instancias de spot de EC2 haciendo lo siguiente:

- Vigila los avisos de terminación de Spot.
- Cuando recibe un aviso de terminación:
  - Detiene las aplicaciones que estén accediendo al sistema de archivos.
  - Desmonta el sistema de archivos antes de finalizar la instancia.

Puede adaptar el script como necesite, especialmente para cerrar su aplicación de manera adecuada. Para obtener más información sobre las mejores prácticas para manejar las interrupciones de instancias de spot, consulte Prácticas recomendadas para manejar las interrupciones de instancias de spot de EC2.

```
#!/bin/bash

# TODO: Specify below the FSx mount point you are using
*FSXPATH=/fsx*

cd /

TOKEN=$(curl -s -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600")
if [ "$?" -ne 0 ]; then
    echo "Error running 'curl' command" >&2
    exit 1
fi

# Periodically check for termination
while sleep 5
do

    HTTP_CODE=$(curl -H "X-aws-ec2-metadata-token: $TOKEN" -s -w %{http_code} -o /dev/
null http://169.254.169.254/latest/meta-data/instance-action)

    if [[ "$HTTP_CODE" -eq 401 ]] ; then
        # Refreshing Authentication Token
        TOKEN=$(curl -s -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 30")
        continue
    elif [[ "$HTTP_CODE" -ne 200 ]] ; then
        # If the return code is not 200, the instance is not going to be interrupted
        continue
    fi

    echo "Instance is getting terminated. Clean and unmount '$FSXPATH' ..."
    curl -H "X-aws-ec2-metadata-token: $TOKEN" -s http://169.254.169.254/latest/meta-
data/instance-action
    echo

    # Gracefully stop applications accessing the filesystem
    #
```

```
    # TODO*: Replace with the proper command to stop your application if possible*

    # Kill every process still accessing Lustre filesystem
    echo "Kill every process still accessing Lustre filesystem..."
    fuser -kMm -TERM "${FSXPATH}"; sleep 2
    fuser -kMm -KILL "${FSXPATH}"; sleep 2

    # Unmount FSx For Lustre filesystem
    if ! umount -c "${FSXPATH}"; then
        echo "Error unmouting '$FSXPATH'. Processes accessing it:" >&2
        lsof "${FSXPATH}"

        echo "Retrying..."
        continue
    fi

    # Start a graceful shutdown of the host
    shutdown now

done
```

# Administración de sistemas de archivos

FSx para Lustre proporciona un conjunto de características que simplifican el rendimiento de las tareas administrativas. Estas incluyen la capacidad de realizar point-in-time copias de seguridad, administrar las cuotas de almacenamiento del sistema de archivos, administrar la capacidad de almacenamiento y rendimiento, administrar la compresión de datos y establecer períodos de mantenimiento para realizar parches de software rutinarios del sistema.

Puede administrar sus sistemas de archivos FSx for Lustre mediante la consola de administración de Amazon FSx AWS Command Line Interface ,AWS CLI(), la API de Amazon FSx o los SDK. AWS

Temas



## Trabajo con copias de seguridad

Con Amazon FSx para Lustre, puede realizar copias de seguridad automáticas diarias e iniciadas por el usuario de sistemas de archivos persistentes que no estén vinculados a un repositorio de datos duradero de Amazon S3. Las copias de seguridad de Amazon FSx son file-system-consistent incrementales y de larga duración. Para garantizar una alta durabilidad, Amazon FSx para Lustre almacena las copias de seguridad en Amazon Simple Storage Service (Amazon S3) con una durabilidad del 99,999999999 % (11 9 unidades).

Las copias de seguridad del sistema de archivos de FSx para Lustre son copias de seguridad incrementales basadas en bloques, independientemente de que se generen mediante la característica de copia de seguridad diaria automática o la función de copia de seguridad iniciada

por el usuario. Esto significa que, cuando realiza una copia de seguridad, Amazon FSx compara los datos de su sistema de archivos con la copia de seguridad anterior a nivel de bloque. A continuación, Amazon FSx almacena una copia de todos los cambios a nivel de bloque en la nueva copia de seguridad. Los datos a nivel de bloque que permanecen inalterados desde la copia de seguridad anterior no se almacenan en la nueva copia de seguridad. La duración del proceso de copia de seguridad depende de la cantidad de datos que hayan cambiado desde que se realizó la última copia de seguridad y es independiente de la capacidad de almacenamiento del sistema de archivos. La siguiente lista muestra los tiempos de copia de seguridad en diferentes circunstancias:

- La copia de seguridad inicial de un sistema de archivos completamente nuevo con muy pocos datos tarda unos minutos en completarse.
- La copia de seguridad inicial de un sistema de archivos completamente nuevo, realizada después de cargar TB de datos, tarda horas en completarse.
- Una segunda copia de seguridad del sistema de archivos con TB de datos y con cambios mínimos en los datos a nivel de bloque (relativamente pocas creaciones o modificaciones) tarda unos segundos en completarse.
- Una tercera copia de seguridad del mismo sistema de archivos después de añadir y modificar una gran cantidad de datos tarda horas en completarse.

Cuando se elimina una copia de seguridad, solo se borran los datos que son únicos de dicha copia de seguridad. Cada copia de seguridad de FSx for Lustre contiene toda la información necesaria para crear un nuevo sistema de archivos a partir de la copia de seguridad y point-in-time restaurar de forma eficaz una instantánea del sistema de archivos.

Crear copias de seguridad periódicas para el sistema de archivos es una práctica recomendada que complementa la replicación que Amazon FSx para Lustre realiza en el sistema de archivos. Las copias de seguridad de Amazon FSx ayudan a satisfacer sus necesidades de cumplimiento y retención de copias de seguridad. Trabajar con copias de seguridad de Amazon FSx para Lustre es fácil, ya sea para crear copias de seguridad, copiar una copia de seguridad, restaurar un sistema de archivos a partir de una copia de seguridad o eliminar una copia de seguridad.

Los sistemas de archivos temporales no son compatibles con las copias de seguridad, ya que estos sistemas de archivos están diseñados para almacenamiento temporal y procesamiento de datos de corto plazo. Las copias de seguridad no se admiten en los sistemas de archivos vinculados a un bucket de Amazon S3 porque el bucket de S3 sirve como repositorio de datos principal y el sistema de archivos de Lustre no contiene necesariamente el conjunto de datos completo en un momento dado.

Temas



## Soporte de copias de seguridad en FSx para Lustre

Las copias de seguridad solo son compatibles con los sistemas de archivos persistentes FSx para Lustre que no están vinculados a un repositorio de datos de Amazon S3.

Amazon FSx no es compatible con las copias de seguridad en sistemas de archivos temporales, ya que estos sistemas están diseñados para el almacenamiento temporal y el procesamiento de datos de corto plazo. Amazon FSx no es compatible con las copias de seguridad en sistemas de archivos vinculados a un bucket de Amazon S3 porque el bucket de S3 sirve como repositorio de datos principal y el sistema de archivos no contiene necesariamente el conjunto de datos completo en un momento dado. Para obtener más información, consulte Opciones de implementación del sistema de archivos y Uso de repositorios de datos.

## Trabajo con copias de seguridad diarias automáticas

Amazon FSx para Lustre puede realizar una copia de seguridad diaria automática de su sistema de archivos. Estas copias de seguridad diarias automáticas se producen durante el período de copias de seguridad diarias que se estableció al crear el sistema de archivos. Durante la ventana de copia de seguridad automática, las E/S de almacenamiento pueden quedar suspendidas brevemente mientras se inicializa el proceso de copia de seguridad (normalmente durante unos pocos segundos). Al elegir la ventana de copia de seguridad diaria, le recomendamos que elija una hora del día que sea conveniente. Lo ideal es que esta hora esté fuera del horario normal de funcionamiento de las aplicaciones que utilizan el sistema de archivos.

Las copias de seguridad diarias automáticas se guardan durante un período de tiempo determinado, conocido como período de retención. Puede asignar al período de retención de copia de seguridad

un valor de entre 0 días y 90 días. Si se establece el período de retención en 0 (cero) días, se desactivan las copias de seguridad diarias automáticas. El periodo de retención predeterminado para las copias de seguridad diarias automáticas es de 0 días. Las copias de seguridad diarias automáticas se eliminan cuando se elimina el sistema de archivos.

> **Note**
>
> Si se establece el período de retención en 0 días, nunca se realizará una copia de seguridad automática del sistema de archivos. Le recomendamos encarecidamente que utilice copias de seguridad diarias automáticas para los sistemas de archivos que tengan algún nivel de funcionalidad crítica asociado.

Puede usar la AWS CLI o uno de los AWS SDK para cambiar la ventana de copias de seguridad y el período de retención de las copias de seguridad de sus sistemas de archivos. Utilice la operación API `UpdateFileSystem` o el comando CLI `update-file-system`.

## Trabajo con copias de seguridad iniciadas por el usuario

Amazon FSx para Lustre le permite realizar copias de seguridad manuales de sus sistemas de archivos en cualquier momento. Puede hacerlo mediante la consola Amazon FSx para Lustre, la API o la AWS Command Line Interface (CLI). Las copias de seguridad de los sistemas de archivos de Amazon FSx iniciadas por los usuarios nunca caducan y están disponibles durante el tiempo que desee conservarlas. Las copias de seguridad iniciadas por los usuarios se conservan incluso después de eliminar el sistema de archivos del que se hizo la copia de seguridad. Puede eliminar las copias de seguridad iniciadas por el usuario únicamente mediante la consola, la API o la CLI de Amazon FSx para Lustre, y Amazon FSx nunca las elimina automáticamente. Para obtener más información, consulte Eliminación de copias de seguridad.

### Crear copias de seguridad iniciadas por el usuario

El siguiente procedimiento le explica cómo crear una copia de seguridad iniciada por el usuario en la consola Amazon FSx para un sistema de archivos existente.

Para crear una copia de seguridad del sistema de archivos iniciada por el usuario

1. Abra la consola de Amazon FSx para Lustre en https://console.aws.amazon.com/fsx/.
2. En el panel de la consola, elija el nombre del sistema de archivos del que desea hacer una copia de seguridad.

3. En Actions, elija Create backup.
4. En el cuadro de diálogo Create backup que se abre, proporciona un nombre para la copia de seguridad. Los nombres de las copias de seguridad pueden tener un máximo de 256 caracteres Unicode, incluidas letras, espacios en blanco, números y caracteres especiales . + - = _ : /
5. Elija Create backup.

Ya ha creado la copia de seguridad de su sistema de archivos. Para encontrar una tabla de todas sus copias de seguridad en la consola Amazon FSx para Lustre, seleccione Backups en el panel de navegación de la izquierda. Puede buscar el nombre que le dio a su copia de seguridad y la tabla filtra para mostrar solo los resultados coincidentes.

Cuando crea una copia de seguridad iniciada por el usuario como se describe en este procedimiento, tiene el tipo `USER_INITIATED` y el estado Creating, mientras que Amazon FSx crea la copia de seguridad. El estado cambia a Transferring mientras la copia de seguridad se transfiere a Amazon S3, hasta que esté completamente disponible.

## Uso de AWS Backup con Amazon FSx

AWS Backup es una forma sencilla y rentable de proteger sus datos realizando copias de seguridad de sus sistemas de archivos de Amazon FSx. AWS Backup es un servicio de copias de seguridad unificado diseñado para simplificar la creación, migración, restauración y eliminación de copias de seguridad, y que proporciona funciones de informes y auditorías mejoradas. AWS Backup le permite desarrollar fácilmente una estrategia de copias de seguridad centralizada para fines jurídicos, reglamentarios y de conformidad. AWS Backup también simplifica la protección de sus volúmenes de almacenamiento, bases de datos y sistemas de archivos de AWS al proporcionar una ubicación central en la que puede hacer lo siguiente:

- Configurar y auditar los recursos de AWS en los que desea realizar una copia de seguridad.
- Automatizar la programación de copias de seguridad.
- Establecer políticas de retención.
- Copiar las copias de seguridad entre regiones de AWS y cuentas de AWS.
- Monitorizar toda la actividad reciente de copias de seguridad y restauración.

AWS Backup utiliza la funcionalidad de copia de seguridad integrada de Amazon FSx. Las copias de seguridad realizadas desde la consola de AWS Backup tienen el mismo nivel de coherencia y rendimiento del sistema de archivos y las mismas opciones de restauración que las copias de

seguridad que se realizan a través de la consola de Amazon FSx. Si utiliza AWS Backup para administrar estas copias de seguridad, obtiene funcionalidades adicionales, como opciones de retención ilimitadas y la posibilidad de crear copias de seguridad programadas con una frecuencia de hasta una hora. Además, AWS Backup retiene las copias de seguridad incluso después de eliminar el sistema de archivos de origen. Esto protege contra la eliminación accidental o malintencionada.

Las copias de seguridad realizadas por AWS Backup se consideran copias de seguridad iniciadas por el usuario y se incluyen en la cuota de copias de seguridad iniciadas por el usuario de Amazon FSx. Puede ver y restaurar las copias de seguridad realizadas por AWS Backup en la consola, la CLI y la API de Amazon FSx. Las copias de seguridad creadas por AWS Backup tienen el tipo de copia de seguridad `AWS_BACKUP`. Sin embargo, no puede eliminar las copias de seguridad realizadas por AWS Backup en la consola, la CLI ni la API de Amazon FSx. Para obtener más información sobre cómo utilizar AWS Backup para realizar copias de seguridad de sus sistemas de archivos de Amazon FSx, consulte Trabajar con sistemas de archivos de Amazon FSx en la Guía para desarrolladores de AWS Backup.

## Copiar copias de seguridad

Puede usar Amazon FSx para copiar manualmente las copias de seguridad de la misma cuenta de AWS a otra región de AWS (copias entre regiones) o dentro de la misma región de AWS (copias dentro de la misma región). Solo puede realizar copias entre regiones dentro de la misma partición de AWS. Puede crear copias de seguridad iniciadas por el usuario mediante la consola, la AWS CLI o la API de Amazon FSx. Cuando crea una copia de seguridad iniciada por el usuario, tiene el tipo`USER_INITIATED`.

También puede utilizar AWS Backup para copiar copias de seguridad entre regiones de AWS y cuentas de AWS. AWS Backup es un servicio de administración de copias de seguridad totalmente gestionado que proporciona una interfaz central para los planes de copia de seguridad basados en políticas. Con la gestión entre cuentas, puede utilizar automáticamente políticas de copia de seguridad para aplicar planes de copia de seguridad en las cuentas de su organización.

Las copias de seguridad entre regiones son particularmente valiosas para la recuperación de desastres entre regiones. Las copias de seguridad se toman y se copian en otra región de AWS para que, en caso de que se produzca un desastre en la región de AWS principal, poder restaurarlas a partir de las copias de seguridad y recuperar rápidamente la disponibilidad en la otra región de AWS. También puede utilizar copias de seguridad para clonar el conjunto de datos de archivos en otra región de AWS o dentro de la misma región de AWS. Puede realizar copias de seguridad dentro de la misma cuenta de AWS (entre regiones o dentro de una región) mediante la consola Amazon FSx,

la AWS CLI o la API de Amazon FSx para Lustre. También puede utilizar AWS Backup para realizar copias de seguridad, a pedido o en función de políticas.

Las copias de seguridad multicuenta son valiosas para cumplir con los requisitos de cumplimiento normativo que se requieren para copiar copias de seguridad en una cuenta aislada. También proporcionan un nivel adicional de protección de datos para evitar la eliminación accidental o malintencionada de las copias de seguridad, la pérdida de credenciales o el peligro de las claves AWS KMS. Las copias de seguridad multicuenta permiten realizar copias de seguridad agrupadas (copiar copias de seguridad de varias cuentas principales a una cuenta de copia de seguridad aislada) y distribuidas (copiar copias de seguridad de una cuenta principal a varias cuentas de copias de seguridad aisladas).

Puede realizar copias de seguridad multicuenta utilizando AWS Backup con el soporte AWS Organizations. Los límites de cuenta para las copias entre cuentas están definidos por las políticas AWS Organizations. Para obtener más información sobre cómo AWS Backup realiza copias de seguridad entre cuentas, consulte Cómo crear copias de seguridad de Cuentas de AWS en la Guía para desarrolladores de AWS Backup.

## Limitaciones de las copias de seguridad

A continuación se indican algunas limitaciones al copiar copias de seguridad:

- Las copias de seguridad interregionales solo se admiten entre dos regiones comercialesRegiones de AWS, entre las regiones de China (Pekín) y China (Ningxia), y entre las regiones (EE. UU. Este) y AWS GovCloud AWS GovCloud (EE. UU. oeste), pero no entre esos conjuntos de regiones.
- Las copias de seguridad entre regiones no son compatibles con las regiones registradas.
- Puede realizar copias de seguridad dentro de la región en cualquier región de AWS.
- La copia de seguridad de origen debe tener el estado de `AVAILABLE` antes de poder copiarla.
- No puede eliminar una copia de seguridad de origen si se está copiando. Es posible que transcurra un breve intervalo entre el momento en que la copia de seguridad de destino esté disponible y el momento en que se le permita eliminar la copia de seguridad de origen. Debe tener en cuenta este retraso si vuelve a intentar eliminar una copia de seguridad de origen.
- Puede tener hasta cinco solicitudes de copia de seguridad en curso en una única región de AWS destino por cuenta.

### Permisos para copias de seguridad entre regiones

Se utiliza una declaración de política de IAM para conceder permisos para realizar una operación de copia de seguridad. Para comunicarse con la región de origen de AWS para solicitar la copia de una copia de seguridad de base de datos entre regiones, el solicitante (rol de IAM o usuario de IAM) debe tener acceso a la copia de seguridad de origen y a la región AWS de origen.

La política se utiliza para conceder permisos a la acción `CopyBackup` para la operación de copia de seguridad. Las acciones se especifican en el campo `Action` de la política y el valor del recurso se especifica en el campo `Resource` de la política.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "fsx:CopyBackup",
            "Resource": "arn:aws:fsx:*:111122223333:backup/*"
        }
    ]
}
```

Para obtener más información general sobre las políticas de IAM, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.

### Copias completas e incrementales

Al copiar una copia de seguridad en una copia de seguridad distinta Región de AWS de la fuente, la primera copia es una copia de seguridad completa. Después de la primera copia de seguridad, todas las copias de seguridad posteriores a la misma región de destino dentro de la misma cuenta de AWS son incrementales, siempre que no haya eliminado todas las copias de seguridad previamente copiadas en esa región y haya utilizado la misma clave AWS KMS. Si no se cumplen ambas condiciones, la operación de copia da como resultado una copia de seguridad completa (no incremental).

## Copiar copias de seguridad dentro de la misma Cuenta de AWS

Puede copiar copias de seguridad de los sistemas de archivos FSx for Lustre mediante la CLI y AWS Management Console la API, tal y como se describe en los siguientes procedimientos.

Para copiar una copia de seguridad dentro de la misma cuenta (entre regiones o dentro de una región) mediante la consola

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación, elija Backups.
3. En la tabla Backups, elija la copia de seguridad que desee copiar y, a continuación, elija Copy backup.
4. En la sección Settings, realice lo siguiente:
   - En la lista Destination Region, elija una región AWS de destino en la que copiar la copia de seguridad. El destino puede estar en otra región de AWS (copia entre regiones) o dentro de la misma región de AWS (copia dentro de la región).
   - (Opcional) Seleccione Copy Tags para copiar las etiquetas de la copia de seguridad de origen a la copia de seguridad de destino. Si selecciona Copy Tags y también las añade en el paso 6, se fusionarán todas las etiquetas.
5. Para Encryption, elija la clave de cifrado AWS KMS para cifrar la copia de seguridad copiada.
6. Para Tags, introduzca una clave y un valor para añadir etiquetas a la copia de seguridad. Si añade etiquetas aquí y también seleccionó Copy Tags en el paso 4, todas las etiquetas se fusionarán.
7. Elija Copy backup.

   La copia de seguridad se copia dentro de la misma ubicación Cuenta de AWS que la seleccionada. Región de AWS

Para copiar una copia de seguridad dentro de la misma cuenta (entre regiones o dentro de una región) utilizando la CLI

- Use el comando `copy-backup` CLI o la operación de CopyBackupAPI para copiar una copia de seguridad en la misma AWS cuenta, ya sea en una AWS región o dentro de una AWS región.

  El siguiente comando copia una copia de seguridad con un identificador `backup-0abc123456789cba7` de la región `us-east-1`.

```
aws fsx copy-backup \
  --source-backup-id backup-0abc123456789cba7 \
  --source-region us-east-1
```

La respuesta muestra la descripción de la copia de seguridad copiada.

Puede ver sus copias de seguridad en la consola de Amazon FSx o mediante programación mediante el comando `describe-backups` CLI o la operación de API. DescribeBackups

## Restauración de copias de seguridad

Puede utilizar una copia de seguridad disponible para crear un nuevo sistema de archivos y restaurar de forma efectiva una point-in-time instantánea de otro sistema de archivos. Puede restaurar una copia de seguridad utilizando la consola, la AWS CLI, o uno de los AWS SDK. La restauración de una copia de seguridad en un nuevo sistema de archivos lleva el mismo tiempo que la creación de un nuevo sistema de archivos. Los datos restaurados a partir de la copia de seguridad se cargan de forma diferida en el sistema de archivos, durante el cual se experimentará una latencia ligeramente superior.

El siguiente procedimiento le explica cómo restaurar una copia de seguridad mediante la consola para crear un nuevo sistema de archivos.

> **Note**
>
> Solo puede restaurar la copia de seguridad en un sistema de archivos del mismo tipo de versión de Lustre, tipo de implementación, rendimiento por unidad de almacenamiento, capacidad de almacenamiento, tipo de compresión de datos y región de AWS que la original. Puede aumentar la capacidad de almacenamiento del sistema de archivos restaurado una vez que esté disponible. Para obtener más información, consulte Administración de la capacidad de almacenamiento.

Para restaurar un sistema de archivos a partir de una copia

1. Abra la consola de Amazon FSx para Lustre en https://console.aws.amazon.com/fsx/.
2. En el panel de la consola, elija Backups en el menú de la izquierda.
3. En la tabla Backups, elija la copia de seguridad que desee restaurar y, a continuación, elija Restore backup.

   Al hacerlo, se abrirá el asistente de creación del sistema de archivos. Este asistente es idéntico al asistente de creación de sistemas de archivos estándar, excepto en la configuración del

sistema de archivos (por ejemplo, el tipo de implementación y el rendimiento por unidad de almacenamiento). Sin embargo, puede cambiar la configuración de la VPC asociada y la configuración de la copia de seguridad.

4. Complete el asistente igual que cuando crea un nuevo sistema de archivos.
5. Elija Review and create.
6. Revise la configuración que eligió para el sistema de archivos Amazon FSx para Lustre y, a continuación, elija Create file system.

Ha realizado la restauración a partir de una copia de seguridad y ahora se está creando un nuevo sistema de archivos. Cuando su estado cambie a `AVAILABLE`, podrá utilizar el sistema de archivos con normalidad.

## Eliminación de copias de seguridad

Eliminar una copia de seguridad es una acción permanente e irrecuperable. También se eliminan todos los datos de una copia de seguridad eliminada. No elimine una copia de seguridad a menos que esté seguro de que no la necesitará de nuevo en el futuro. No puede eliminar las copias de seguridad realizadas por AWS Backup en la consola, la CLI ni la API de Amazon FSx.

Para eliminar una copia de seguridad

1. Abra la consola de Amazon FSx para Lustre en https://console.aws.amazon.com/fsx/.
2. En el panel de la consola, elija Backups en el menú de la izquierda.
3. En la tabla Backups, elija la copia de seguridad que desee eliminar y, a continuación, elija Delete backup.
4. En el cuadro de diálogo Delete backups que se abre, confirme que el ID de la copia de seguridad identifica la copia de seguridad que desea eliminar.
5. Confirme que la casilla de la copia de seguridad que desea eliminar está marcada.
6. Elija Delete backups.

La copia de seguridad y todos los datos incluidos se eliminarán ahora de forma permanente e irrecuperable.

# Cuotas de almacenamiento

Puede crear cuotas de almacenamiento para usuarios, grupos y proyectos en los sistemas de archivos de FSx para Lustre. Con las cuotas de almacenamiento, podrá limitar la cantidad de espacio en disco y el número de archivos que puede consumir un usuario, grupo o proyecto. Las cuotas de almacenamiento registran automáticamente el uso a nivel de usuario, grupo y proyecto para que pueda supervisar el consumo independientemente de si decide establecer límites de almacenamiento o no.

Amazon FSx impone cuotas e impide que los usuarios que las hayan superado escriban en el espacio de almacenamiento. Cuando los usuarios superan sus cuotas, deben eliminar suficientes archivos para quedar por debajo de los límites de cuota y poder escribir de nuevo en el sistema de archivos.

Temas



## Cumplimiento de cuotas

La aplicación de cuotas de usuario, grupo y proyecto se activa automáticamente en todos los sistemas de archivos de FSx para Lustre. No se puede deshabilitar la aplicación de cuotas.

## Tipos de cuotas

Los administradores del sistema con credenciales de usuario raíz de la AWS cuenta pueden crear los siguientes tipos de cuotas:

- Una cuota de usuario se aplica a un usuario individual. La cuota de un usuario específico puede ser diferente de las cuotas de otros usuarios.
- Una cuota de grupo se aplica a todos los usuarios que son miembros de un grupo específico.

- Una cuota de proyecto se aplica a todos los archivos o directorios asociados a un proyecto. Un proyecto puede incluir varios directorios o archivos individuales ubicados en diferentes directorios dentro de un sistema de archivos.

  > **Note**
  >
  > Las cuotas de proyecto solo se admiten en la versión 2.15 de Lustre en los sistemas de archivos FSx for Lustre.

- Una cuota de bloques limita la cantidad de espacio en disco que puede consumir un usuario, un grupo o un proyecto. El tamaño de almacenamiento se configura en kilobytes.
- Una cuota de inodos limita la cantidad de archivos o directorios que puede crear un usuario, un grupo o un proyecto. El número máximo de inodos se configura como un número entero.

> **Note**
>
> No se admiten las cuotas por defecto.

Si establece cuotas para un usuario concreto y un grupo, y el usuario es miembro de ese grupo, el uso de datos del usuario se aplica a ambas cuotas. También está limitado por ambas cuotas. Si se alcanza alguno de los límites de cuota, el usuario no podrá escribir en el sistema de archivos.

> **Note**
>
> Las cuotas establecidas para el usuario raíz no se aplican. Del mismo modo, escribir datos como usuario raíz usando el comando `sudo` evita la aplicación de la cuota.

## Límites de cuota y períodos de gracia

Amazon FSx aplica las cuotas de usuarios, grupos y proyectos como un límite estricto o flexible con un período de gracia configurable.

El límite estricto es el límite absoluto. Si los usuarios superan su límite estricto, se produce un error en la asignación de bloques o inodos y aparece el mensaje de que Se ha superado la cuota de disco. Los usuarios que hayan alcanzado su límite máximo de cuota deben eliminar suficientes archivos

o directorios como para superar el límite de cuota antes de poder volver a escribir en el sistema de archivos. Cuando se establece un período de gracia, los usuarios pueden superar el límite flexible dentro del período de gracia si están por debajo del límite estricto.

En el caso de los límites flexibles, se configura un período de gracia en segundos. El límite flexible debe ser menor que el límite estricto.

Puede establecer diferentes períodos de gracia para las cuotas de inodo y de bloque. También puede establecer diferentes períodos de gracia para una cuota de usuario, una cuota de grupo y una cuota de proyecto. Cuando las cuotas de usuario, grupo y proyecto tienen períodos de gracia diferentes, el límite flexible se transforma en límite estricto una vez transcurrido el período de gracia de cualquiera de estas cuotas.

Cuando los usuarios superan un límite flexible, Amazon FSx les permite seguir superando su cuota hasta que haya transcurrido el período de gracia o hasta que se alcance el límite estricto. Una vez finalizado el período de gracia, el límite flexible se convierte en límite estricto y los usuarios no pueden realizar ninguna otra operación de escritura hasta que su consumo de almacenamiento vuelva a ser inferior a los límites de cuota de bloques o de inodos definidos. Los usuarios no reciben ninguna notificación o advertencia cuando comienza el período de gracia.

## Cómo establecer y ver las cuotas

Las cuotas de almacenamiento se establecen mediante los comandos `lfs` del sistema de archivos de Lustre en su terminal Linux. El comando `lfs setquota` establece límites de cuota, y el comando `lfs quota` muestra información de cuota.

Para obtener más información sobre los comandos de cuota de Lustre, consulte el Manual de operaciones de Lustre en el Sitio web de documentación de Lustre.

### Establecer cuotas de usuario, grupo y proyecto

La sintaxis del comando `setquota` para establecer las cuotas de usuarios, grupos o proyectos es la siguiente.

```
lfs setquota {-u|--user|-g|--group|-p|--project} username|groupname|projectid
             [-b block_softlimit] [-B block_hardlimit]
             [-i inode_softlimit] [-I inode_hardlimit]
             /mount_point
```

Donde:

- `-u` o `--user` especifica un usuario para establecerle una cuota.
- `-g` o `--group` especifica un grupo para establecerle una cuota.
- `-p` o `--project` especifica un proyecto para establecerle una cuota.
- `-b` establece una cuota por bloques con un límite flexible. `-B` establece una cuota de bloques con un límite estricto. Tanto *`block_softlimit`* como *`block_hardlimit`* se expresan en kilobytes y el valor mínimo es 1024 KB.
- `-i` establece una cuota de inodos con un límite flexible. `-I` establece una cuota de inodos con un límite estricto. Tanto *`inode_softlimit`* como *`inode_hardlimit`* se expresan en número de inodos y el valor mínimo es de 1024 inodos.
- *`mount_point`* es el directorio en el que se montó el sistema de archivos.

Ejemplo de cuota de usuario: el siguiente comando establece un límite de 5000 KB de bloques flexibles, un límite de 8000 KB de bloques estrictos, un límite de 2000 inodos flexibles y un límite de 3000 inodos estrictos para `user1` en el sistema de archivos montado en `/mnt/fsx`.

```
sudo lfs setquota -u user1 -b 5000 -B 8000 -i 2000 -I 3000 /mnt/fsx
```

Ejemplo de cuota de grupo: el siguiente comando establece un límite de bloques estrictos de 100 000 KB para el grupo llamado `group1` en el sistema de archivos montado en `/mnt/fsx`.

```
sudo lfs setquota -g group1 -B 100000 /mnt/fsx
```

Ejemplo de cuota de proyecto: en primer lugar, asegúrese de haber utilizado el comando `project` para asociar los archivos y directorios deseados al proyecto. Por ejemplo, el siguiente comando asocia todos los archivos y subdirectorios del directorio `/mnt/fsxfs/dir1` al proyecto cuyo identificador de proyecto es `100`.

```
sudo lfs project -p 100 -r -s /mnt/fsxfs/dir1
```

Luego, utilice el comando `setquota` para establecer la cuota del proyecto. El siguiente comando establece un límite de bloques flexibles de 307 200 KB, un límite de bloques estrictos de 309 200 KB, un límite de inodos flexibles de 10 000 y un límite de inodos estrictos de 11 000 para el proyecto `250` en el sistema de archivos montado en `/mnt/fsx`.

```
sudo lfs setquota -p 250 -b 307200 -B 309200 -i 10000 -I 11000 /mnt/fsx
```

## Establecer períodos de gracia

El período de gracia predeterminado es de una semana. Puede ajustar el período de gracia predeterminado para los usuarios, grupos o proyectos mediante la siguiente sintaxis.

```
lfs setquota -t {-u|-g|-p}
             [-b block_grace]
             [-i inode_grace]
             /mount_point
```

Donde:

- `-t` indica que se establecerá un período de gracia.
- `-u` establece un período de gracia para todos los usuarios.
- `-g` establece un período de gracia para todos los grupos.
- `-p` establece un período de gracia para todos los proyectos.
- `-b` establece un período de gracia para las cuotas en bloque. `-i` establece un período de gracia para las cuotas de inodos. Tanto *`block_grace`* como *`inode_grace`* se expresan en segundos enteros o en el formato `XXwXXdXXhXXmXXs`.
- *`mount_point`* es el directorio en el que se montó el sistema de archivos.

El siguiente comando establece períodos de gracia de 1000 segundos para las cuotas de bloqueo de usuarios y de 1 semana y 4 días para las cuotas de inodos de usuarios.

```
sudo lfs setquota -t -u -b 1000 -i 1w4d /mnt/fsx
```

## Visualización de las cuotas

El comando `quota` muestra información sobre las cuotas de usuario, las cuotas de grupo, las cuotas de proyectos y los períodos de gracia.

| Ver comando de cuotas | Se muestra información de cuota |
| --- | --- |
| `lfs quota /`*`mount_point`* | Información general de cuota (uso y límites de disco) para el usuario que ejecuta el |

| Ver comando de cuotas | Se muestra información de cuota |
| --- | --- |
| | comando y el grupo primario del usuario. |
| `lfs quota -u username /mount_point` | Información general sobre las cuotas de un usuario específico. Los usuarios con credenciales de usuario root de la AWS cuenta pueden ejecutar este comando para cualquier usuario, pero los usuarios que no sean root no pueden ejecutar este comando para obtener información sobre las cuotas de otros usuarios. |
| `lfs quota -u username -v /mount_point` | Información general de cuotas para un usuario específico y estadísticas detalladas de cuotas para cada destino de almacenamiento de objetos (OST) y destino de metadatos (MDT). Los usuarios con credenciales de usuario raíz de la AWS cuenta pueden ejecutar este comando para cualquier usuario, pero los usuarios que no son root no pueden ejecutar este comando para obtener información sobre las cuotas de otros usuarios. |

| Ver comando de cuotas | Se muestra información de cuota |
| --- | --- |
| `lfs quota -g groupname /mount_point` | Información general sobre cuotas para un grupo específico. |
| `lfs quota -p projectid /mount_point` | Información general sobre cuotas para un proyecto específico. |
| `lfs quota -t -u /mount_point` | Tiempos de gracia de bloque e inodo para cuotas de usuario. |
| `lfs quota -t -g /mount_point` | Tiempos de gracia de bloque e inodo para cuotas de grupo. |
| `lfs quota -t -p /mount_point` | Tiempos de gracia de bloque e inodo para cuotas de proyecto. |

## Cuotas y buckets vinculados de Amazon S3

Puede vincular su sistema de archivos de FSx para Lustre a un repositorio de datos de Amazon S3. Para obtener más información, consulte Vincular su sistema de archivos a un bucket de S3.

Puede elegir opcionalmente una carpeta o prefijo específico dentro de un bucket S3 vinculado como ruta de importación a su sistema de archivos. Cuando se especifica una carpeta en Amazon S3 y se importa a su sistema de archivos desde S3, solo los datos de esa carpeta se aplican a la cuota. Los datos de todo el bucket no se tienen en cuenta para los límites de cuota.

Los metadatos de archivo de un bucket de S3 vinculado se importan a una carpeta con una estructura que coincide con la carpeta importada desde Amazon S3. Estos archivos cuentan para las cuotas de inodos de los usuarios y grupos propietarios de los archivos.

Cuando un usuario realiza una `hsm_restore` o carga diferida de un archivo, el tamaño completo del archivo cuenta para la cuota de bloque asociada al propietario del archivo. Por ejemplo, si el usuario

A carga de forma diferida un archivo que es propiedad del usuario B, la cantidad de almacenamiento y el uso de inodos se tienen en cuenta para la cuota del usuario B. Del mismo modo, cuando un usuario utiliza la API de Amazon FSx para liberar un archivo, los datos se liberan de las cuotas de bloque del usuario o grupo propietario del archivo.

Dado que las restauraciones HSM y la carga diferida se realizan con acceso raíz, eluden la aplicación de cuotas. Una vez importados, los datos se incluyen en el usuario o grupo en función de la propiedad establecida en S3, lo que puede hacer que los usuarios o grupos superen sus límites de bloques. Si esto ocurre, deberán liberar los archivos para poder volver a escribir en el sistema de archivos.

Del mismo modo, los sistemas de archivos con la importación automática habilitada crearán automáticamente nuevos inodos para los objetos añadidos a S3. Estos nuevos inodos se crean con acceso raíz y eluden la aplicación de cuotas mientras se crean. Estos nuevos inodos contarán para los usuarios y grupos, basándose en quién es el propietario del objeto en S3. Si esos usuarios y grupos exceden sus cuotas de inodos basándose en la actividad de importación automática, tendrán que eliminar archivos para liberar capacidad adicional y situarse por debajo de sus límites de cuota.

### Cuotas y restauración de copias de seguridad

Al restaurar una copia de seguridad, la configuración de cuotas del sistema de archivos original se implementa en el sistema de archivos restaurado. Por ejemplo, si se establecen cuotas en el sistema de archivos A, y se crea el sistema de archivos B a partir de una copia de seguridad del sistema de archivos A, se aplicarán las cuotas del sistema de archivos A en el sistema de archivos B.

## Administración de la capacidad de almacenamiento

Puede aumentar la capacidad de almacenamiento configurada en su sistema de archivos de FSx para Lustre si necesita almacenamiento y rendimiento adicionales. Como el rendimiento de un sistema de archivos de FSx para Lustre se amplía linealmente con la capacidad de almacenamiento, también se obtiene un aumento comparable en la capacidad de rendimiento. Para aumentar la capacidad de almacenamiento, puede utilizar la consola Amazon FSx, la AWS Command Line Interface (AWS CLI) o la API de Amazon FSx.

Cuando solicita una actualización de la capacidad de almacenamiento de su sistema de archivos, Amazon FSx añade automáticamente nuevos servidores de archivos de red y escala su servidor de metadatos. Mientras se escala la capacidad de almacenamiento, es posible que el sistema de archivos no esté disponible durante unos minutos. Las operaciones de archivo realizadas por los clientes mientras el sistema de archivos no está disponible se reintentarán de forma transparente

y finalmente tendrán éxito una vez completado el escalado de almacenamiento. Durante el tiempo en que el sistema de archivos no esté disponible, el estado del sistema de archivos se establece en `UPDATING`. Una vez completado el escalado del almacenamiento, el estado del sistema de archivos se establece en `AVAILABLE`.

A continuación, Amazon FSx ejecuta un proceso de optimización del almacenamiento que reequilibra de forma transparente los datos entre los servidores de archivos existentes y los recién añadidos. El reequilibrio se realiza en segundo plano sin afectar a la disponibilidad del sistema de archivos. Durante el reequilibrio, es posible que el rendimiento del sistema de archivos disminuya a medida que se consumen recursos para el movimiento de datos. En la mayoría de los sistemas de archivos, la optimización del almacenamiento tarda desde unas horas hasta unos días. Podrá acceder a su sistema de archivos y utilizarlo durante la fase de optimización.

Puede realizar un seguimiento del progreso de la optimización del almacenamiento en cualquier momento mediante la consola, la CLI y la API de Amazon FSx. Para obtener más información, consulte Supervisión de los aumentos de capacidad de almacenamiento.

Temas



## Consideraciones a la hora de aumentar la capacidad de almacenamiento

Estos son algunos aspectos importantes que se deben tener en cuenta al aumentar la capacidad de almacenamiento:

- Solo aumentar: solo puede aumentar la capacidad de almacenamiento de un sistema de archivos; no puede reducirla.
- Aumentar los incrementos: al aumentar la capacidad de almacenamiento, utilice los incrementos que aparecen en el cuadro de diálogo Aumentar la capacidad de almacenamiento.
- Tiempo entre aumentos: no puede realizar nuevos incrementos de la capacidad de almacenamiento en un sistema de archivos hasta 6 horas después de haber solicitado el último

aumento, o hasta que se haya completado el proceso de optimización del almacenamiento, lo que sea más largo.

- Capacidad de rendimiento: al aumentar la capacidad de almacenamiento, aumenta automáticamente la capacidad de rendimiento. En el caso de los sistemas de archivos HDD persistentes con caché SSD, la capacidad de almacenamiento en caché de lectura también se incrementa de forma similar para mantener una caché SSD con un tamaño equivalente al 20 por ciento de la capacidad de almacenamiento del HDD. Amazon FSx calcula los nuevos valores de las unidades de capacidad de almacenamiento y de capacidad de rendimiento y los muestra en el cuadro de diálogo Aumentar la capacidad de almacenamiento.

  > **Note**
  >
  > Puede modificar de forma independiente la capacidad de rendimiento de un sistema de archivos persistente basado en SSD sin tener que actualizar la capacidad de almacenamiento del sistema de archivos. Para obtener más información, consulte Administración de la capacidad de rendimiento.

- Tipo de implementación: puede aumentar la capacidad de almacenamiento de todos los tipos de implementación, excepto los sistemas de archivos Scratch 1. Si dispone de un sistema de archivos Scratch 1, puede crear uno nuevo con una mayor capacidad de almacenamiento.

## Cuándo aumentar la capacidad de almacenamiento

Aumente la capacidad de almacenamiento del sistema de archivos cuando se esté agotando la capacidad de almacenamiento libre. Utilice la `FreeStorageCapacity` CloudWatch métrica para supervisar la cantidad de almacenamiento libre disponible en el sistema de archivos. Puedes crear una CloudWatch alarma de Amazon en esta métrica y recibir una notificación cuando caiga por debajo de un umbral específico. Para obtener más información, consulte Supervisión con Amazon CloudWatch.

Puedes usar CloudWatch las métricas para monitorear los niveles de uso del rendimiento continuo de tu sistema de archivos. Si determina que su sistema de archivos necesita una mayor capacidad de rendimiento, puede utilizar la información de las métricas como ayuda para decidir en qué medida aumentar la capacidad de almacenamiento. Para obtener información acerca de cómo determinar el rendimiento actual de su sistema de archivos, consulte Cómo usar las métricas Amazon FSx para Lustre. Para obtener información sobre cómo la capacidad de almacenamiento afecta a la capacidad de rendimiento, consulte Rendimiento de Amazon FSx para Lustre.

También puede ver la capacidad de almacenamiento y el rendimiento total del sistema de archivos en el panel de Resumen de la página de detalles del sistema de archivos.

## Cómo se gestionan el escalado de almacenamiento concurrente y las solicitudes de copia de seguridad

Puede solicitar una copia de seguridad justo antes de que comience un flujo de trabajo de escalado de almacenamiento o mientras está en curso. La secuencia de cómo Amazon FSx gestiona las dos solicitudes es la siguiente:

- Si hay un flujo de trabajo de escalado de almacenamiento en curso (el estado del escalado del almacenamiento es `IN_PROGRESS` y el estado del sistema de archivos es `UPDATING`) y usted solicita una copia de seguridad, la solicitud de copia de seguridad se pone en cola. La tarea de copia de seguridad se inicia cuando el escalado del almacenamiento se encuentra en la fase de optimización del almacenamiento (el estado del escalado del almacenamiento es `UPDATED_OPTIMIZING` y el estado del sistema de archivos es `AVAILABLE`).
- Si la copia de seguridad está en curso (el estado de la copia de seguridad es `CREATING`) y solicita el escalado de almacenamiento, la solicitud de escalado de almacenamiento se pone en cola. El flujo de trabajo de escalado del almacenamiento se inicia cuando Amazon FSx transfiere la copia de seguridad a Amazon S3 (el estado de la copia de seguridad es `TRANSFERRING`).

Si hay una solicitud de escalado del almacenamiento pendiente y una solicitud de copia de seguridad del sistema de archivos también está pendiente, la tarea de copia de seguridad tiene mayor prioridad. La tarea de escalado del almacenamiento no comenzará hasta que finalice la tarea de copia de seguridad.

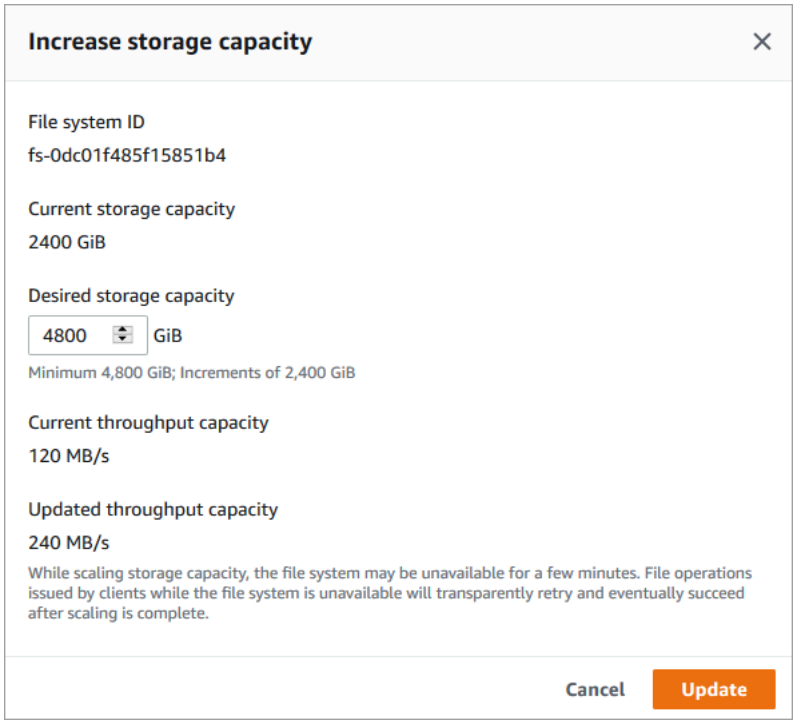
## Cómo aumentar la capacidad de almacenamiento

Puede aumentar la capacidad de almacenamiento de un sistema de archivos con la consola de Amazon FSx, la AWS CLI o la API de Amazon FSx.

Para aumentar la capacidad de almacenamiento de un sistema de archivos (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Vaya a Sistemas de archivos y elija el sistema de archivos de Lustre al que desee aumentarle la capacidad de almacenamiento.

3. En Acciones, seleccione Actualizar capacidad de almacenamiento. O bien, en el panel Resumen, seleccione Actualizar junto a Capacidad de almacenamiento del sistema de archivos para mostrar el cuadro de diálogo Aumentar capacidad de almacenamiento.




4. En Capacidad de almacenamiento deseada, indique una nueva capacidad de almacenamiento en GiB que sea mayor que la capacidad de almacenamiento actual del sistema de archivos:

   - Para un sistema de archivos SSD persistente o Scratch 2, este valor debe estar expresado en múltiplos de 2400 GiB.
   - Para sistemas de archivos HDD persistente, este valor debe estar expresado en múltiplos de 6000 GiB para sistemas de archivos de 12 MB/s/TiB y múltiplos de 1800 GiB para sistemas de archivos de 40 MB/s/TiB.

> **Note**
>
> No se puede aumentar la capacidad de almacenamiento de los sistemas de archivos Scratch 1.

5. Seleccione Actualizar para iniciar la actualización de la capacidad de almacenamiento.
6. Puede supervisar el progreso de la actualización en la página de información de los Sistemas de archivos, en la pestaña Actualizaciones.

Para aumentar la capacidad de almacenamiento de un sistema de archivos (CLI)

1. Para aumentar la capacidad de almacenamiento de un sistema de archivos FSx for Lustre, AWS CLI utilice el comando. update-file-system Establezca los siguientes parámetros:

   Establezca `--file-system-id` en el ID del sistema de archivos que va a actualizar.

   Establezca `--storage-capacity` en un valor entero que sea la cantidad, en GiB, del aumento de la capacidad de almacenamiento. Para un sistema de archivos SSD persistente o Scratch 2, este valor debe estar expresado en múltiplos de 2400. Para sistemas de archivos HDD persistente, este valor debe estar expresado en múltiplos de 6000 para sistemas de archivos de 12 MB/s/TiB y múltiplos de 1800 para sistemas de archivos de 40 MB/s/TiB. El nuevo valor objetivo debe ser mayor que la capacidad actual de almacenamiento del sistema de archivos.

   Este comando especifica un valor objetivo de capacidad de almacenamiento de 9600 GiB para un sistema de archivos SSD persistente o Scratch 2.

   ```
   $ aws fsx update-file-system \
       --file-system-id fs-0123456789abcdef0 \
       --storage-capacity 9600
   ```

2. Puede supervisar el progreso de la actualización mediante el AWS CLI comando. describe-file-systems Busque las `administrative-actions` en los resultados.

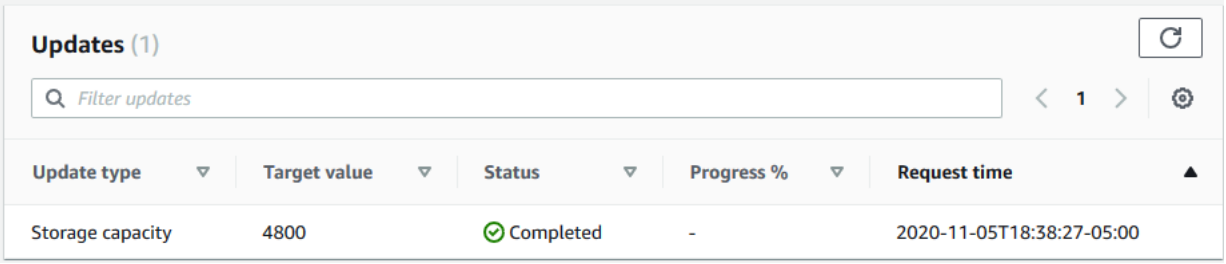
   Para obtener más información, consulte AdministrativeAction.

## Supervisión de los aumentos de capacidad de almacenamiento

Puede supervisar el progreso del aumento de capacidad de almacenamiento con la consola de Amazon FSx, la API o la AWS CLI.

Supervisión de los aumentos en la consola

En la pestaña Actualizaciones en la página de detalles del sistema de archivos, puede ver las 10 actualizaciones más recientes para cada tipo de actualización.




Puede ver la siguiente información:

Tipo de actualización

Los tipos admitidos son Capacidad de almacenamiento y Optimización del almacenamiento.

Valor de destino

El valor que desea alcanzar con la actualización de la capacidad de almacenamiento del sistema de archivos.

Status

Se actualiza el estado actual de la capacidad de almacenamiento. Los valores posibles son los siguientes:

- Pendiente: Amazon FSx recibió la solicitud de actualización, pero no comenzó a procesarla.
- En curso: Amazon FSx está procesando la solicitud de actualización.
- Actualizado; Optimizando: Amazon FSx aumentó la capacidad de almacenamiento del sistema de archivos. El proceso de optimización del almacenamiento ahora está reequilibrando los datos entre los servidores de archivos.
- Finalizado: el aumento de la capacidad de almacenamiento se completó correctamente.
- Error: no se pudo aumentar la capacidad de almacenamiento. Elija el signo de interrogación (?) para ver información sobre la causa de un error en la actualización del almacenamiento.

% de progreso

El progreso del proceso de optimización del almacenamiento se ve reflejado por el porcentaje completado.

Tiempo de solicitud

La hora en que Amazon FSx recibió la solicitud de acción de actualización.

La supervisión aumenta con la AWS CLI y la API

Puede ver y supervisar la capacidad de almacenamiento del sistema de archivos y aumentar las solicitudes mediante el describe-file-systemsAWS CLIcomando y la acción de la DescribeFileSystemsAPI. La matriz de `AdministrativeActions` enumera las 10 acciones de actualización más recientes para cada tipo de acción administrativa. Al aumentar la capacidad de almacenamiento de un sistema de archivos, se generan dos `AdministrativeActions`: una acción de `FILE_SYSTEM_UPDATE` y una de `STORAGE_OPTIMIZATION`.

En el siguiente ejemplo se muestra un extracto de la respuesta de un comando de la CLI describe-file-systems: El sistema de archivos tiene una capacidad de almacenamiento de 4800 GB y hay una acción administrativa pendiente para aumentar la capacidad de almacenamiento a 9600 GB.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 4800,
            "AdministrativeActions": [
                {
                     "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                     "RequestTime": 1581694764.757,
                     "Status": "PENDING",
                     "TargetFileSystemValues": {
                         "StorageCapacity": 9600
                     }
                },
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
                    "Status": "PENDING",
                }
            ]
```

Amazon FSx procesa primero la acción de `FILE_SYSTEM_UPDATE` y añade nuevos servidores de archivos al sistema de archivos. Cuando el sistema de archivos tiene disponible el nuevo almacenamiento, el estado de `FILE_SYSTEM_UPDATE` cambia a `UPDATED_OPTIMIZING`. La capacidad de almacenamiento muestra el nuevo valor mayor y Amazon FSx comienza a procesar la

acción administrativa de `STORAGE_OPTIMIZATION`. Esto se muestra en el siguiente extracto de la respuesta de un comando de CLI describe-file-systems.

La propiedad `ProgressPercent` muestra el avance del proceso de optimización del almacenamiento. Una vez que el proceso de optimización del almacenamiento finaliza correctamente, el estado de la acción de `FILE_SYSTEM_UPDATE` cambia a `COMPLETED`, y la acción de `STORAGE_OPTIMIZATION` deja de aparecer.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 9600,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "RequestTime": 1581694764.757,
                    "Status": "UPDATED_OPTIMIZING",
                    "TargetFileSystemValues": {
                        "StorageCapacity": 9600
                }
                },
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
                    "Status": "IN_PROGRESS",
                    "ProgressPercent": 50,
                }
            ]
```

Si se produce un error en el aumento de la capacidad de almacenamiento, el estado de la acción `FILE_SYSTEM_UPDATE` cambia a `FAILED`. La propiedad `FailureDetails` otorga información sobre el error, como se muestra en el siguiente ejemplo.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
```

```
            .
            .
            .
            "StorageCapacity": 4800,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "FailureDetails": {
                        "Message": "string"
                    },
                    "RequestTime": 1581694764.757,
                    "Status": "FAILED",
                    "TargetFileSystemValues":
                        "StorageCapacity": 9600
                }
            ]
```

# Administración de la capacidad de rendimiento

Todos los sistemas de archivos de FSx para Lustre tienen una capacidad de rendimiento que se configura al crear el sistema de archivos. El rendimiento de un sistema de archivos de FSx para Lustre se mide en megabytes por segundo. por tebibyte (MB/s/TiB). La capacidad de rendimiento es un factor que determina la velocidad en la que el servidor de archivos que aloja el sistema de archivos puede almacenar los datos de los archivos. Los niveles más altos de capacidad de rendimiento también vienen con niveles más altos de operaciones de E/S por segundo (IOPS) y más memoria para el almacenamiento en caché de los datos en el servidor de archivos. Para obtener más información, consulte Rendimiento de Amazon FSx para Lustre.

Puede modificar el nivel de rendimiento de un sistema de archivos persistente basado en SSD aumentando o disminuyendo el valor del rendimiento del sistema de archivos por unidad de almacenamiento. Los valores válidos dependen del tipo de implementación del sistema de archivos, como se indica a continuación:

- Para los tipos de implementación basados en SSD Persistent_1, los valores válidos son 50, 100 y 200 MB/s/TiB.
- Para los tipos de implementación basados en SSD Persistent_2, los valores válidos son 125, 250, 500 y 1000 MB/s/TiB.

Puede ver el valor actual del rendimiento del sistema de archivos por unidad de almacenamiento, como se indica a continuación:

- Uso de la consola: en el panel de Resumen de la página de información del sistema de archivos, el campo Rendimiento por unidad de almacenamiento muestra el valor actual.
- Uso de la CLI o la API: utilice el comando describe-file-systemsCLI o la operación de DescribeFileSystemsAPI y busque la `PerUnitStorageThroughput` propiedad.

Al modificar la capacidad de rendimiento del sistema de archivos, entre bastidores, Amazon FSx cambia los servidores de archivos del sistema de archivos. Su sistema de archivos no estará disponible durante unos minutos mientras se escala la capacidad de rendimiento. Se le facturará la nueva cantidad de capacidad de rendimiento una vez que el sistema de archivos lo tenga disponible.

Temas



## Consideraciones a la hora de actualizar la capacidad de rendimiento

Estos son algunos elementos importantes que se deben tener en cuenta al actualizar la capacidad de rendimiento:

- Aumentar o disminuir: puede aumentar o disminuir la capacidad de rendimiento de un sistema de archivos.
- Actualice los incrementos: al modificar la capacidad de rendimiento, utilice los incrementos que aparecen en el cuadro de diálogo Actualizar el nivel de rendimiento.
- Tiempo entre aumentos: no se pueden realizar más cambios de capacidad de rendimiento en un sistema de archivos hasta 6 horas después de la última petición, o hasta que el proceso de optimización de rendimiento haya finalizado, lo que dure más tiempo.
- Tipo de implementación: solo puede actualizar la capacidad de rendimiento de los tipos de implementación persistentes basados en SSD.

## Cuándo modificar la capacidad de rendimiento

Amazon FSx se integra con Amazon CloudWatch, lo que le permite supervisar los niveles de uso del rendimiento continuo de su sistema de archivos. El desempeño (rendimiento e IOPS) que puede utilizar su sistema de archivos depende de las características específicas de su carga de trabajo, además de la capacidad de rendimiento, y la capacidad y el tipo de almacenamiento del sistema de archivos. Para obtener información acerca de cómo determinar el rendimiento actual de su sistema de archivos, consulte Cómo usar las métricas Amazon FSx para Lustre. Para obtener información sobre CloudWatch las métricas, consulte. Supervisión con Amazon CloudWatch

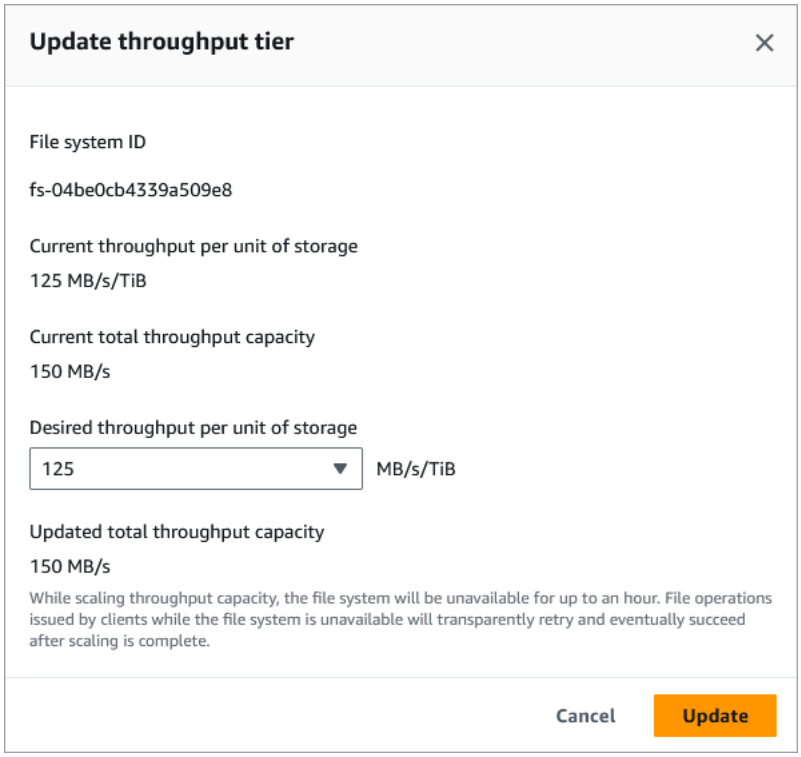
## Cómo modificar la capacidad de rendimiento

Puede modificar la capacidad de rendimiento de un sistema de archivos con la consola de Amazon FSx, AWS Command Line Interface (AWS CLI) o la API de Amazon FSx.

Para modificar la capacidad de rendimiento de un sistema de archivos (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Vaya a Sistemas de archivos y elija el sistema de archivos de FSx para Lustre para el que desee modificar la capacidad de rendimiento.
3. En Acciones, selecciona Actualizar nivel de rendimiento. O bien, en el panel Resumen, seleccione Actualizar junto a la capacidad de rendimiento del sistema de archivos.

   Aparece la ventana Actualizar el nivel de rendimiento.
4. Seleccione el nuevo valor para el rendimiento deseado por unidad de almacenamiento de la lista.




5. Seleccione Actualizar para iniciar la actualización de la capacidad de rendimiento.

> **Note**
>
> Su sistema de archivos puede experimentar un breve período de inactividad durante la actualización.

Para modificar la capacidad de rendimiento de un sistema de archivos (CLI)

- Para modificar la capacidad de rendimiento de un sistema de archivos, utilice el comando update-file-systemCLI (o la operación UpdateFileSystemAPI equivalente). Establezca los siguientes parámetros:
  - Establezca `--file-system-id` en el ID del sistema de archivos que va a actualizar.
  - Establezca `--lustre-configuration PerUnitStorageThroughput` a un valor de `50` `100`, o `200` MB/s/TiB para sistemas de archivo Persistent_1 SSD, o a un valor de `125`, `250`, `500`, o un sistema de archivo `1000` MB/s/TiB for Persistent_2 SSD.

  Este comando especifica que la capacidad de rendimiento se establezca en 1000 MB/s/TiB para el sistema de archivos.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration PerUnitStorageThroughput=1000
```

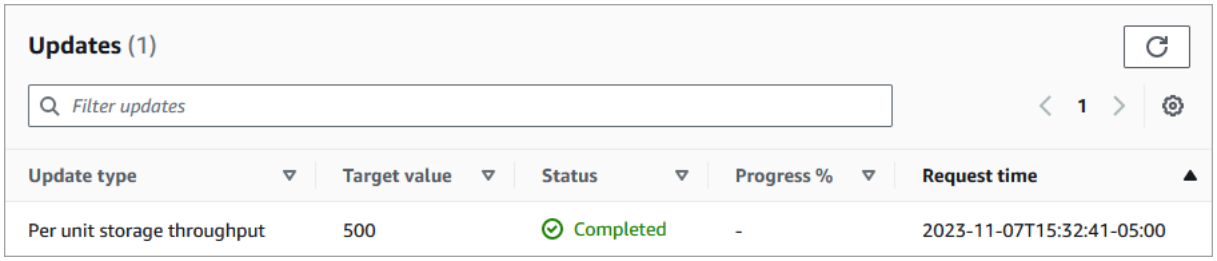
## Supervisión de los cambios en la capacidad de rendimiento

Puede supervisar el progreso de una modificación de la capacidad de rendimiento con la consola Amazon FSx, la API y la AWS CLI.

Supervisión de los cambios en la capacidad de rendimiento (consola)

Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.

- En la pestaña Actualizaciones de la página de detalles del sistema de archivos, puede ver las 10 acciones de actualización más recientes para cada tipo de acción de actualización.




  Para ver las acciones de actualización de la capacidad de rendimiento, puede consultar la siguiente información.

  Tipo de actualización

  El tipo admitido es el rendimiento de almacenamiento por unidad.

  Valor de destino

  El valor deseado para cambiar el rendimiento del sistema de archivos por unidad de almacenamiento.

  Status

  El estado actual de la actualización. Para las actualizaciones de capacidad de rendimiento, los valores posibles son los siguientes:

  - Pendiente: Amazon FSx recibió la solicitud de actualización, pero no comenzó a procesarla.

- En curso: Amazon FSx está procesando la solicitud de actualización.
- Actualizado; Optimización: Amazon FSx actualizó los recursos de E/S de red, CPU y memoria del sistema de archivos. El nuevo nivel de rendimiento de E/S de disco está disponible para las operaciones de escritura. En las operaciones de lectura, el rendimiento de E/S del disco se situará entre el nivel anterior y el nuevo hasta que el sistema de archivos deje de estar en este estado.
- Finalizado: la actualización de la capacidad de rendimiento se completó correctamente.
- Error: se produjo un error en la actualización de la capacidad de rendimiento. Elija el signo de interrogación (? ) para ver detalles sobre el motivo por el que se produjo un error en la actualización del rendimiento.

Tiempo de solicitud

La hora en que Amazon FSx recibió la solicitud de actualización.

Supervisión de las actualizaciones del sistema de archivos (CLI)

- Puede ver y supervisar las solicitudes de modificación de la capacidad de rendimiento del sistema de archivos mediante el comando describe-file-systemsCLI y la acción de la DescribeFileSystemsAPI. La matriz de `AdministrativeActions` enumera las 10 acciones de actualización más recientes para cada tipo de acción administrativa. Al modificar la capacidad de rendimiento de un sistema de archivos, se genera una acción administrativa de `FILE_SYSTEM_UPDATE`.

  En el siguiente ejemplo se muestra un extracto de la respuesta de un comando de la CLI `describe-file-systems`. El sistema de archivos tiene un rendimiento objetivo por unidad de almacenamiento de 500 MB/s/TiB.

```
.
.
.
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "LustreConfiguration": {
            "PerUnitStorageThroughput": 500
```

```
            }
          }
      }
]
```

Cuando Amazon FSx procesa la acción correctamente, el estado cambia a `COMPLETED`. La nueva capacidad de rendimiento está entonces disponible para el sistema de archivos y se muestra en la propiedad `PerUnitStorageThroughput`.

Si se produce un error en la modificación de la capacidad de rendimiento, el estado cambia a `FAILED`, y la propiedad `FailureDetails` brinda información sobre el error.

# Compresión de datos de Lustre

Puede utilizar la característica de compresión de datos de Lustre para ahorrar costos en sus sistemas de archivos y almacenamiento de copias de seguridad de alto rendimiento de Amazon FSx para Lustre. Cuando la compresión de datos está habilitada, Amazon FSx para Lustre comprime automáticamente los archivos recién escritos antes de escribirlos en el disco y los descomprime automáticamente cuando se leen.

La compresión de datos utiliza el algoritmo LZ4, que está optimizado para ofrecer altos niveles de compresión sin afectar negativamente al rendimiento del sistema de archivos. El LZ4 es un algoritmo de confianza de la comunidad de Lustre orientado al rendimiento que proporciona un equilibrio entre la velocidad de compresión y el tamaño del archivo comprimido. Habilitar la compresión de datos no suele tener un impacto apreciable en la latencia.

La compresión de datos reduce la cantidad de datos que se transfieren entre los servidores de archivos y el almacenamiento de Amazon FSx para Lustre. Si aún no utiliza formatos de archivo comprimidos, verá un aumento en la capacidad de rendimiento general del sistema de archivos al utilizar la compresión de datos. Los aumentos de la capacidad de rendimiento relacionados con la compresión de datos se limitarán una vez que se hayan saturado las tarjetas de interfaz de red front-end.

Por ejemplo, si su sistema de archivos es un tipo de implementación PERSISTENT-50 SSD, el rendimiento de la red tiene una base de 250 MB/s por TiB de almacenamiento. El rendimiento del disco tiene una base de 50 MB/s por TiB. Con la compresión de datos, el rendimiento del disco podría aumentar de 50 MB/s por TiB a un máximo de 250 MB/s por TiB, que es el límite de rendimiento de red de referencia. Para obtener más información sobre los límites de rendimiento

de la red y el disco, consulte las tablas de rendimiento del sistema de archivos en Rendimiento agregado del sistema de archivos. Para obtener más información sobre el rendimiento de la compresión de datos, consulte la publicación Gaste menos y aumente el rendimiento con la compresión de datos Amazon FSx para Lustre en el Blog sobre almacenamiento AWS.

Temas

- Administración de la compresión de datos
- Comprimir archivos escritos anteriormente
- Visualización del tamaño de los archivos
- Uso de métricas de CloudWatch

## Administración de la compresión de datos

Puede activar o desactivar la compresión de datos al crear un nuevo sistema de archivos Amazon FSx para Lustre. La compresión de datos está desactivada de forma predeterminada al crear un sistema de archivos Amazon FSx para Lustre desde la consola, AWS CLI o la API.

Para activar la compresión de datos al crear un sistema de archivos (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Siga el procedimiento para crear un nuevo sistema de archivos que se describe en Cree su sistema de archivos FSx for Lustre en la sección Primeros pasos.
3. En la sección de información del sistema de archivos, en el tipo de compresión de datos, elija LZ4.
4. Complete el asistente igual que cuando crea un nuevo sistema de archivos.
5. Elija Review and create (Revisar y crear).
6. Revise la configuración que eligió para el sistema de archivos Amazon FSx para Lustre y, a continuación, elija Create file system (Crear sistema de archivo).

Cuando el sistema de archivos esté disponible, se activará la compresión de datos.

Para activar la compresión de datos al crear un sistema de archivos (CLI)

- Para crear un sistema de archivos FSx para Lustre con la compresión de datos activada, utilice el comando CLI de Amazon FSx `create-file-system` con el parámetro

`DataCompressionType`, como se muestra a continuación. La operación de API correspondiente es CreateFileSystem.

```
$ aws fsx create-file-system \
      --client-request-token CRT1234 \
      --file-system-type LUSTRE \
      --file-system-type-version 2.12 \
      --lustre-configuration
 DeploymentType=PERSISTENT_1,PerUnitStorageThroughput=50,DataCompressionType=LZ4 \
      --storage-capacity 3600 \
      --subnet-ids subnet-123456 \
      --tags Key=Name,Value=Lustre-TEST-1 \
      --region us-east-2
```

Después de crear correctamente el sistema de archivos, Amazon FSx devuelve la descripción del sistema de archivos como JSON, tal y como se muestra en el siguiente ejemplo.

```
{

    "FileSystems": [
        {
            "OwnerId": "111122223333",
            "CreationTime": 1549310341.483,
            "FileSystemId": "fs-0123456789abcdef0",
            "FileSystemType": "LUSTRE",
            "FileSystemTypeVersion": "2.12",
            "Lifecycle": "CREATING",
            "StorageCapacity": 3600,
            "VpcId": "vpc-123456",
            "SubnetIds": [
                "subnet-123456"
            ],
            "NetworkInterfaceIds": [
                "eni-039fcf55123456789"
            ],
            "DNSName": "fs-0123456789abcdef0.fsx.us-east-2.amazonaws.com",
            "ResourceARN": "arn:aws:fsx:us-east-2:123456:file-system/
fs-0123456789abcdef0",
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "Lustre-TEST-1"
```

```
                }
            ],
            "LustreConfiguration": {
                "DeploymentType": "PERSISTENT_1",
                "DataCompressionType": "LZ4",
                "PerUnitStorageThroughput": 50
            }
        }
    ]
}
```

También puede cambiar la configuración de compresión de datos de sus sistemas de archivos existentes. Al activar la compresión de datos en un sistema de archivos existente, solo se comprimen los archivos recién escritos y no se comprimen los existentes. Para obtener más información, consulte Comprimir archivos escritos anteriormente.

Para actualizar la compresión de datos de un sistema de archivos existente (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Vaya a Sistemas de archivos y elija el sistema de archivos de Lustre para el cual desea administrar la compresión de datos.
3. En Acciones, elija Actualizar el tipo de compresión de datos.
4. En el cuadro de diálogo Actualizar el tipo de compresión de datos, seleccione LZ4 para activar la compresión de datos o NONE para desactivarla.
5. Elija Actualizar.
6. Puede supervisar el progreso de la actualización en la página de información de los Sistemas de archivos, en la pestaña Actualizaciones.

Para actualizar la compresión de datos de un sistema de archivos existente (CLI)

Para actualizar la configuración de compresión de datos de un sistema de archivos FSx para Lustre existente, utilice el comando AWS CLI update-file-system. Establezca los siguientes parámetros:

- Establezca `--file-system-id` en el ID del sistema de archivos que va a actualizar.
- Establezca `--lustre-configuration DataCompressionType` a `NONE` para desactivar la compresión de datos o `LZ4` para activar la compresión de datos con el algoritmo LZ4.

Este comando especifica que la compresión de datos se activa con el algoritmo LZ4.

```
$ aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration DataCompressionType=LZ4
```

### Configuración de la compresión de datos al crear un sistema de archivos a partir de una copia de seguridad

Puede utilizar una copia de seguridad disponible para crear un nuevo sistema de archivos Amazon FSx para Lustre. Al crear un nuevo sistema de archivos a partir de una copia de seguridad, no es necesario especificar el `DataCompressionType`; la configuración se aplicará utilizando la configuración `DataCompressionType` de la copia de seguridad. Si decide especificar el `DataCompressionType` al crear desde copia de seguridad, el valor debe coincidir con la configuración del `DataCompressionType` de la copia de seguridad.

Para ver la configuración de una copia de seguridad, selecciónela en la pestaña Copias de seguridad de la consola de Amazon FSx. Los detalles de la copia de seguridad aparecerán en la página Resumen de la copia de seguridad. También puedes ejecutar el comando `describe-backups` AWS CLI (la acción equivalente de la API es `DescribeBackups`).

## Comprimir archivos escritos anteriormente

Los archivos no se comprimen si se crearon cuando la compresión de datos estaba desactivada en el sistema de archivos Amazon FSx para Lustre. Activar la compresión de datos no comprimirá automáticamente los datos existentes sin comprimir.

Puede usar el comando `lfs_migrate` que se instala como parte de la instalación del cliente Lustre para comprimir los archivos existentes. Para ver un ejemplo, consulte Compresión FSXL disponible en GitHub.

## Visualización del tamaño de los archivos

Puede utilizar los siguientes comandos para ver los tamaños sin comprimir y comprimidos de sus archivos y directorios.

- du muestra los tamaños comprimidos.
- `du --apparent-size` muestra los tamaños sin comprimir.
- `ls -l` muestra los tamaños sin comprimir.

Los siguientes ejemplos muestran la salida de cada comando con el mismo archivo.

```
$ du -sh samplefile
272M samplefile
$ du -sh --apparent-size samplefile
1.0G samplefile
$ ls -lh samplefile
-rw-r--r-- 1 root root 1.0G May 10 21:16 samplefile
```

La opción `-h` es útil para estos comandos porque imprime los tamaños en un formato legible para las personas.

### Uso de métricas de CloudWatch

Puede utilizar las métricas de los Registros de Amazon CloudWatch para ver el uso del sistema de archivos. La métrica `LogicalDiskUsage` muestra el uso total del disco lógico (sin compresión) y la métrica `PhysicalDiskUsage` muestra el uso total del disco físico (con compresión). Estas dos métricas solo están disponibles si el sistema de archivos tiene habilitada la compresión de datos o si la tenía habilitada anteriormente.

Puede determinar la relación de compresión de su sistema de archivos dividiendo el `Sum` de la estadística `LogicalDiskUsage` entre el `Sum` de la estadística `PhysicalDiskUsage`. Para obtener información sobre el uso de las matemáticas métricas para calcular esta relación, consulte Matemáticas métricas: relación de compresión de datos.

Para obtener más información sobre la supervisión del rendimiento del sistema de archivos, consulte Supervisión de Amazon FSx para Lustre.

## Lustre root squash

Root squash es una característica administrativa que agrega una capa adicional de control de acceso a archivos sobre el actual control de acceso basado en red y los permisos de archivos POSIX. Utilizando la característica Root squash, puede restringir el acceso a nivel de raíz de los clientes que intentan acceder a su sistema de archivos FSx para Lustre como raíz.

Los permisos de usuario raíz son necesarios para realizar acciones administrativas, tales como la gestión de permisos en sistemas de archivos FSx para Lustre. Sin embargo, el acceso raíz proporciona acceso sin restricciones a los usuarios, permitiéndoles saltarse las comprobaciones

de permisos para acceder, modificar o borrar objetos del sistema de archivos. Con la característica root squash, puede evitar el acceso no autorizado o la eliminación de datos especificando un ID de usuario (UID) y un ID de grupo (GID) que no sean raíz para su sistema de archivos. Los usuarios raíz que accedan al sistema de archivos se convertirán automáticamente en el usuario/grupo especificado con menos privilegios y con permisos limitados establecidos por el administrador del almacenamiento.

La característica root squash también permite, de forma opcional, proporcionar una lista de clientes a los que no afecta la configuración de root squash. Estos clientes pueden acceder al sistema de archivos como raíz, con privilegios sin restricciones.

Temas



## Cómo funciona Root Squash

La característica root squash funciona reasignando el ID de usuario (UID) y el ID de grupo (GID) del usuario raíz a un UID y GID especificados por el administrador del sistema Lustre. La característica root squash también permite especificar, de forma opcional, un conjunto de clientes a los que no se aplica la reasignación de UID/GID.

Cuando se crea un nuevo sistema de archivos FSx para Lustre, root squash está deshabilitado de forma predeterminada. Para activar root squash, configure un UID y GID root squash para su sistema de archivos FSx para Lustre. Los valores UID y GID son números enteros que pueden oscilar entre `0` y `4294967294`:

- Un valor distinto de cero para UID y GID habilita el root squash. Los valores UID y GID pueden ser diferentes, pero cada uno debe ser un valor distinto de cero.
- Un valor de `0` (cero) para UID y GID indica raíz, y por lo tanto desactiva la característica root squash.

Durante la creación del sistema de archivos, puede utilizar la consola de Amazon FSx para proporcionar los valores UID y GID de root squash en la propiedad Root Squash, como se muestra en. Para habilitar root squash al crear un sistema de archivos (consola) También puede usar el `RootSquash` parámetro con la API AWS CLI o para proporcionar los valores de UID y GID, como se muestra en. Para habilitar la característica root squash al crear un sistema de archivos (CLI)

Opcionalmente, también puede especificar una lista de NID de clientes para los que no se aplique root squash. Un NID de cliente es un Identificador de Red Lustre utilizado para identificar de forma única a un cliente. Puede especificar el NID como una dirección única o como un rango de direcciones:

- Una dirección única se describe en el formato estándar Lustre NID especificando la dirección IP del cliente seguida del identificador de red Lustre (por ejemplo, `10.0.1.6@tcp`).
- Un rango de direcciones se describe utilizando un guion para separar el rango (por ejemplo, `10.0.[2-10].[1-255]@tcp`).
- Si no especifica ningún NID de cliente, no habrá excepciones al root squash.

Al crear o actualizar el sistema de archivos, puede utilizar la propiedad Exceptions to Root Squash de la consola de Amazon FSx para proporcionar la lista de los NID de los clientes. En la API AWS CLI o, utilice el `NoSquashNids` parámetro. Para obtener más información, consulte los procedimientos enAdministración de root squash.

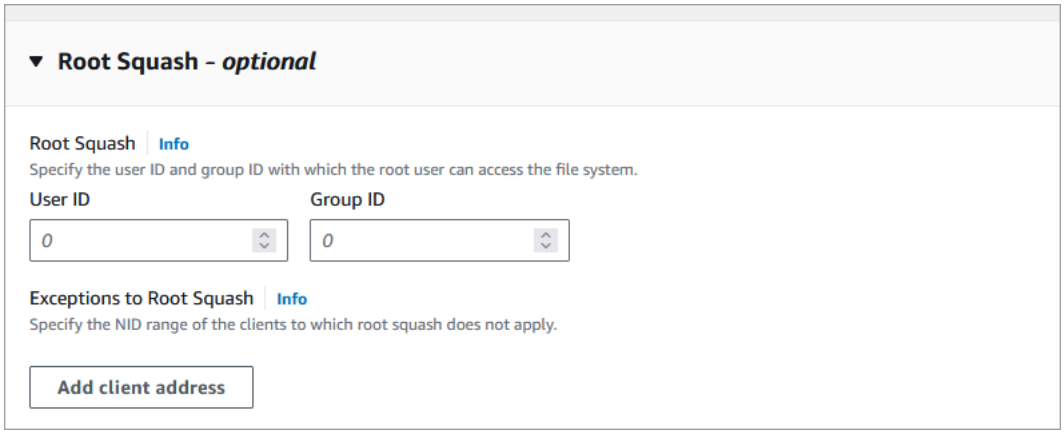
> **Note**
>
> Root Squash no es compatible con las copias de seguridad ni con las restauraciones. Para utilizar copias de seguridad y restauraciones, debe deshabilitar root squash configurando el `RootSquash` parámetro en `0:0` y el `NoSquashNids` parámetro en `[]` con la API AWS CLI o, o bien, seleccionando Disable en el cuadro de diálogo Update Root Squash Settings de la consola de Amazon FSx.

## Administración de root squash

Durante la creación del sistema de archivos, root squash está deshabilitado de forma predeterminada. Puede activar el root squash al crear un nuevo sistema de archivos Amazon FSx for Lustre desde la consola o API de Amazon FSxAWS CLI.

Para habilitar root squash al crear un sistema de archivos (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Siga el procedimiento para crear un nuevo sistema de archivos que se describe en Cree su sistema de archivos FSx for Lustre en la sección Primeros pasos.
3. Abre la sección Root Squash (opcional).




4. En el caso de Root Squash, proporcione los ID de usuario y grupo con los que el usuario root puede acceder al sistema de archivos. Puede especificar cualquier número entero en el rango de 1 —4294967294:

   1. En el campo ID de usuario, especifique el ID de usuario que utilizará el usuario raíz.
   2. En el caso del ID de grupo, especifique el ID de grupo que utilizará el usuario raíz.

5. (Opcional) Para las excepciones a Root Squash, haga lo siguiente:

   1. Seleccione Añadir dirección de cliente.
   2. En el campo Direcciones de los clientes, especifique la dirección IP de un cliente al que no se aplica root squash. Para obtener información sobre el formato de la dirección IP, consulteCómo funciona Root Squash.
   3. Repita el procedimiento según sea necesario para añadir más direcciones IP de clientes.

6. Complete el asistente igual que cuando crea un nuevo sistema de archivos.
7. Elija Review and create.
8. Revise la configuración que eligió para el sistema de archivos Amazon FSx para Lustre y, a continuación, elija Create file system.

Cuando el sistema de archivos está disponible, root squash está activado.

Para habilitar la característica root squash al crear un sistema de archivos (CLI)

- Para crear un sistema de archivos FSx para Lustre con root squash activado, utilice el comando CLI `create-file-system` de Amazon FSx con el parámetro el `RootSquashConfiguration`. La operación de API correspondiente es CreateFileSystem.

  En el parámetro `RootSquashConfiguration`, elija las siguientes opciones:

- `RootSquash`: Los valores UID:GID separados por dos puntos que especifican el ID de usuario y el ID de grupo que debe utilizar el usuario raíz. Puede especificar cualquier número entero en el rango de `0`-`4294967294` (0 es raíz) para cada ID (por ejemplo, `65534:65534`).
- `NoSquashNids`: Especifique los identificadores de red (NID) de Lustre de los clientes a los que no se aplicará la característica root squash. Para obtener información sobre el formato de NID del cliente, consulte Cómo funciona Root Squash.

En el siguiente ejemplo, se crea un sistema de archivos FSx para Lustre con root squash activado:

```
$ aws fsx create-file-system \
      --client-request-token CRT1234 \
      --file-system-type LUSTRE \
      --file-system-type-version 2.15 \
      --lustre-configuration
 "DeploymentType=PERSISTENT_2,PerUnitStorageThroughput=250,DataCompressionType=LZ4,
\
          RootSquashConfiguration={RootSquash="65534:65534",\
          NoSquashNids=["10.216.123.47@tcp", "10.216.12.176@tcp"]}" \
      --storage-capacity 2400 \
      --subnet-ids subnet-123456 \
      --tags Key=Name,Value=Lustre-TEST-1 \
      --region us-east-2
```

Después de crear correctamente el sistema de archivos, Amazon FSx devuelve la descripción del sistema de archivos como JSON, tal y como se muestra en el siguiente ejemplo.

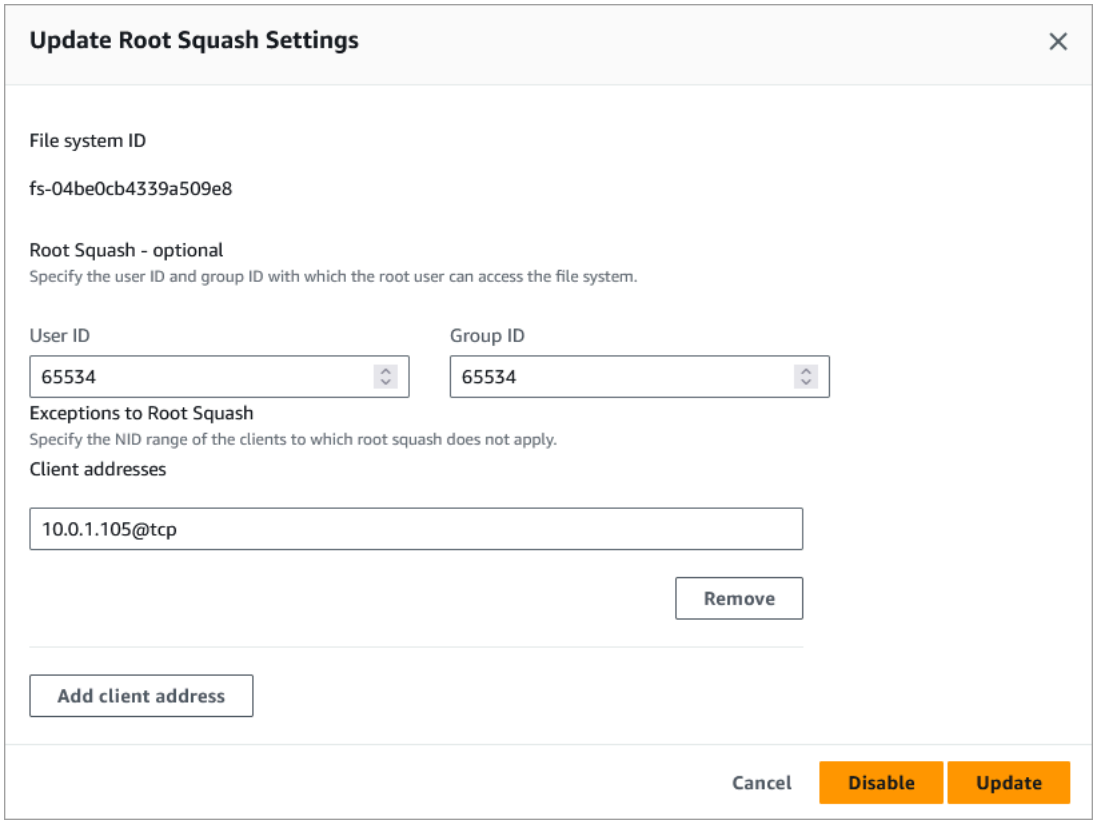
```
{

    "FileSystems": [
        {
            "OwnerId": "111122223333",
            "CreationTime": 1549310341.483,
            "FileSystemId": "fs-0123456789abcdef0",
            "FileSystemType": "LUSTRE",
            "FileSystemTypeVersion": "2.15",
            "Lifecycle": "CREATING",
            "StorageCapacity": 2400,
            "VpcId": "vpc-123456",
```

```
            "SubnetIds": [
                "subnet-123456"
            ],
            "NetworkInterfaceIds": [
                "eni-039fcf55123456789"
            ],
            "DNSName": "fs-0123456789abcdef0.fsx.us-east-2.amazonaws.com",
            "ResourceARN": "arn:aws:fsx:us-east-2:123456:file-system/
fs-0123456789abcdef0",
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "Lustre-TEST-1"
                }
            ],
            "LustreConfiguration": {
                "DeploymentType": "PERSISTENT_2",
                "DataCompressionType": "LZ4",
                "PerUnitStorageThroughput": 250,
                "RootSquashConfiguration": {
                    "RootSquash": "65534:65534",
                    "NoSquashNids": "10.216.123.47@tcp 10.216.29.176@tcp"
            }
        }
    ]
}
```

También puede actualizar la configuración de root squash de su sistema de archivos existente mediante la consola o API de Amazon FSx. AWS CLI Por ejemplo, puede cambiar los valores de UID y GID de root squash, añadir o eliminar los NID de cliente o deshabilitar root squash.

Para actualizar la configuración de root squash en un sistema de archivos existente (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Vaya a Sistemas de archivos y elija el sistema de archivos Lustre para el que quiere administrar root squash.
3. En Acciones, selecciona Actualizar calabacines. O bien, en el panel de resumen, seleccione Actualizar junto al campo Root Squash del sistema de archivos para que aparezca el cuadro de diálogo Actualizar la configuración de Root Squash.




4. En el caso de Root Squash, actualice los ID de usuario y grupo con los que el usuario root puede acceder al sistema de archivos. Puede especificar cualquier número entero en el rango de `0` —`4294967294`. Para deshabilitar el squash raíz, especifique `0` (cero) para ambos identificadores.

    1. En el campo ID de usuario, especifique el ID de usuario que utilizará el usuario root.
    2. En el caso del ID de grupo, especifique el ID de grupo que utilizará el usuario raíz.

5. Para ver las excepciones a Root Squash, haga lo siguiente:

    1. Elija Agregar dirección de cliente.
    2. En el campo Direcciones de los clientes, especifique la dirección IP de un cliente al que no se aplica root squash,
    3. Repita el procedimiento según sea necesario para añadir más direcciones IP de clientes.

6. Seleccione Actualizar.

> **Note**
>
> Si la función root squash está habilitada y desea deshabilitarla, elija Desactivar en lugar de realizar los pasos 4 a 6.

Puede supervisar el progreso de la actualización en la página de información de los Sistemas de archivos, en la pestaña Actualizaciones.

Para actualizar la configuración de root squash en un sistema de archivos (CLI) existente

Para actualizar la configuración de root squash de un sistema de archivos FSx for Lustre existente, AWS CLI utilice el comando. update-file-system La operación de API correspondiente es UpdateFileSystem.

Establezca los siguientes parámetros:

- Establezca `--file-system-id` en el ID del sistema de archivos que va a actualizar.
- Establezca las opciones `--lustre-configuration RootSquashConfiguration` de la siguiente manera:
  - `RootSquash`: Establezca los valores UID:GID separados por dos puntos que especifican el ID de usuario y el ID de grupo que debe utilizar el usuario raíz. Puede especificar cualquier número entero en el rango de `0`–`4294967294` (0 es raíz) para cada ID. Para deshabilitar root squash, especifique `0:0` para los valores de UID:GID.
  - `NoSquashNids`: Especifique los identificadores de red (NID) de Lustre de los clientes a los que no se aplicará la característica root squash. Use `[]` para eliminar todos los NID de cliente, lo que significa que no habrá excepciones para root squash.

Este comando especifica que root squash está habilitado usando `65534` como valor para el ID de usuario y el ID de grupo del usuario raíz.

```
$ aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration RootSquashConfiguration={RootSquash="65534:65534", \
          NoSquashNids=["10.216.123.47@tcp", "10.216.12.176@tcp"]}
```

Si el comando tiene éxito, Amazon FSx para Lustre devuelve la respuesta en formato JSON.

Puede ver la configuración de root squash de su sistema de archivos en el panel de resumen de la página de detalles del sistema de archivos de la consola Amazon FSx o en respuesta a un comando de `describe-file-systems`CLI (la acción de API equivalente es `DescribeFileSystems`).

## Estado del sistema de archivos FSx for Lustre

Puede ver el estado de un sistema de archivos de Amazon FSx mediante la consola de Amazon FSx, el AWS CLI comando o la operación de la describe-file-systemsAPI. DescribeFileSystems

| Estado del sistema de archivos | Descripción |
| --- | --- |
| DISPONIBLE | El sistema de archivos se encuentra en buen estado y está accesible y disponible para su uso. |
| EN CREACIÓN | Amazon FSx está creando un nuevo sistema de archivos. |
| ELIMINANDO | Amazon FSx está eliminando un sistema de archivos existente. |
| ACTUALIZANDO | El sistema de archivos está siendo objeto de una actualización iniciada por el cliente. |
| MAL CONFIGURADO | El sistema de archivos está mal configurado, pero es recuperable. |
| FALLA | Este estado puede significar cualquiera de los siguientes:<br>• El sistema de archivos ha generado un error y Amazon FSx no puede recuperarlo.<br>• Al crear un nuevo sistema de archivos, Amazon FSx no pudo crear el sistema de archivos. |

# Etiquetar los recursos de Amazon FSx

Para ayudarlo a administrar sus sistemas de archivos y otros recursos de Amazon FSx para Lustre, puede asignar sus propios metadatos a cada recurso en forma de etiquetas. Las etiquetas le permiten clasificar los recursos de AWS de diversas maneras, por ejemplo, según su finalidad, propietario o entorno. Esto es útil cuando tiene muchos recursos del mismo tipo: puede identificar rápidamente un recurso específico en función de las etiquetas que le haya asignado. En este tema se describe qué son las etiquetas y cómo crearlas.

Temas



## Conceptos básicos de etiquetas

Una etiqueta es una marca que se asigna a un recurso de AWS. Cada etiqueta está formada por una clave y un valor opcional, ambos definidos por el usuario.

Las etiquetas le permiten clasificar los recursos de AWS de diversas maneras, por ejemplo, según su finalidad, propietario o entorno. Por ejemplo, podría definir un conjunto de etiquetas para los sistemas de archivos Amazon FSx para Lustre de su cuenta que lo ayuden a realizar un seguimiento del propietario y el nivel de pila de cada instancia.

Recomendamos que idee un conjunto de claves de etiqueta que cumpla sus necesidades para cada tipo de recurso. Mediante el uso de un conjunto coherente de claves de etiquetas, podrá administrar los recursos más fácilmente. Puede buscar y filtrar los recursos en función de las etiquetas que agregue.

Las etiquetas no tienen ningún significado semántico para Amazon FSx, por lo que se interpretan estrictamente como cadenas de caracteres. Además, las etiquetas no se asignan a los recursos automáticamente. Puede editar las claves y los valores de las etiquetas y también puede eliminar etiquetas de un recurso en cualquier momento. Puede establecer el valor de una etiqueta como una cadena vacía, pero no puede asignarle un valor nulo. Si añade una etiqueta con la misma clave que una etiqueta existente en ese recurso, el nuevo valor sobrescribirá al antiguo. Si elimina un recurso, también se eliminará cualquier etiqueta asignada a dicho recurso.

Si utiliza la API de Amazon FSx para Lustre, la CLI AWS o un SDK AWS, puede usar la acción `TagResource` de la API para aplicar etiquetas a los recursos existentes. Además, algunas acciones de creación de recursos le permiten especificar etiquetas para un recurso al crear dicho recurso. Si no se pueden aplicar etiquetas durante la creación del recurso, el proceso de creación del recurso se revierte. Esto garantiza que los recursos se creen con etiquetas o, de lo contrario, no se creen y que ningún recurso se quede jamás sin etiquetar. Al etiquetar los recursos en el momento de su creación, se eliminar la necesidad de ejecutar scripts de etiquetado personalizados tras la creación del recurso. Para obtener más información acerca de cómo habilitar a los usuarios para etiquetar recursos al crearlos, consulte Conceder permisos para etiquetar recursos durante la creación.

## Cómo etiquetar los recursos

Puede etiquetar los recursos de Amazon FSx para Lustre que existen en la cuenta. Si utiliza la consola de Amazon FSx, puede aplicar etiquetas a los recursos mediante la pestaña Tags (Etiquetas) de la pantalla correspondiente al recurso. Al crear recursos, puede aplicar la clave de Name (Nombre) con un valor y puede aplicar las etiquetas que desee al crear un nuevo sistema de archivos. La consola puede organizar los recursos según la etiqueta de Name (Nombre), si bien dicha etiqueta no tiene significado semántico para el servicio de Amazon FSx para Lustre.

En sus políticas de IAM, puede aplicar permisos de nivel de recursos basados en etiquetas a las acciones de la API de Amazon FSx para Lustre que admitan el etiquetado durante la creación para implementar un control detallado de los usuarios y los grupos que pueden etiquetar recursos durante su creación. Sus recursos están debidamente protegidos frente a la creación — las etiquetas se aplican inmediatamente a los recursos, por lo que cualquier permiso de nivel de recursos basado en etiquetas que controle el uso de los recursos es efectivo inmediatamente. Se puede realizar un seguimiento y un registro más precisos de los recursos. Puede establecer el etiquetado obligatorio de los nuevos recursos y controlar qué claves y valores de etiquetas se usan en ellos.

También puede aplicar permisos de nivel de recursos para las acciones `TagResource` y `UntagResource` de la API de Amazon FSx para Lustre en las políticas de IAM para controlar qué claves y valores de etiquetas se usan en los recursos existentes.

Para obtener más información acerca del etiquetado de recursos para facturación, consulte Uso de etiquetas de asignación de costos en la Guía del usuario de AWS Billing.

## Restricciones de las etiquetas

Se aplican las siguientes restricciones básicas a las etiquetas:

- Número máximo de etiquetas por recurso: 50
- Para cada recurso, cada clave de etiqueta debe ser única y solo puede tener un valor.
- Longitud máxima de la clave: 128 caracteres Unicode en UTF-8
- Longitud máxima del valor: 256 caracteres Unicode en UTF-8
- Los caracteres permitidos para las etiquetas de Amazon FSx para Lustre son: letras, números y espacios representables en UTF-8, además de los siguientes caracteres: + - = . _ : / @.
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas.
- El prefijo `aws:` se reserva para uso de AWS. Si la etiqueta tiene una clave de etiqueta con este prefijo, no puede editar ni eliminar la clave o el valor de la etiqueta. Las etiquetas que tengan el prefijo `aws:` no cuentan para el límite de etiquetas por recurso.

No puede eliminar un recurso basándose únicamente en sus etiquetas; debe especificar el identificador del recurso. Por ejemplo, para eliminar un sistema de archivos etiquetado con una clave de etiqueta llamada `DeleteMe`, debe utilizar la acción `DeleteFileSystem` con el identificador de recurso del sistema de archivos, como fs-1234567890abcdef0.

Cuando etiqueta recursos públicos o compartidos, las etiquetas que asigne solo están disponibles para su Cuenta de AWS; ninguna otra Cuenta de AWS tendrá acceso a esas etiquetas. Para el control de acceso a recursos compartidos basado en etiquetas, cada Cuenta de AWS debe asignar su propio conjunto de etiquetas para controlar el acceso al recurso.

### Permisos y etiqueta

Para obtener más información sobre los permisos necesarios para etiquetar los recursos de Amazon FSx en el momento de la creación, consulte Conceder permisos para etiquetar recursos durante la creación. Para obtener más información sobre el uso de etiquetas para restringir el acceso a los recursos de Amazon FSx en las políticas de IAM, consulte Uso de etiquetas para controlar el acceso a los recursos de Amazon FSx .

## Períodos de mantenimiento de Amazon FSx para Lustre

Amazon FSx para Lustre realiza parches de software rutinarios para el software de Lustre que administra. El período de mantenimiento es su oportunidad de controlar el día y la hora de la semana en que se realizará la aplicación de los parches de software.

La aplicación de parches debería requerir solo una fracción del período de mantenimiento de 30 minutos. Durante estos pocos minutos, su sistema de archivos no estará disponible

temporalmente. El período de mantenimiento se selecciona durante la creación del sistema de ficheros. Si no tiene preferencia horaria, se le asigna un período predeterminado de 30 minutos.

FSx para Lustre le permite ajustar su ventana de mantenimiento según sea necesario para adaptarse a su carga de trabajo y sus requisitos operativos. Puede cambiar su período de mantenimiento con la frecuencia que necesite, siempre que se programe un período de mantenimiento al menos una vez cada 14 días. Si se publica un parche y no ha programado un período de mantenimiento en un plazo de 14 días, FSx para Lustre procederá al mantenimiento del sistema de archivos para garantizar su seguridad y fiabilidad.

Puede usar la consola de administración de Amazon FSx, AWS CLI, la API AWS o uno de los SDK AWS para cambiar el período de mantenimiento de sus sistemas de archivos.

Para cambiar el período de mantenimiento mediante la consola

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación, elija Sistema de archivos.
3. Elija el sistema de archivos para el que desea cambiar el período de mantenimiento. Aparecerá la página de detalles del sistema de archivos.
4. Seleccione la pestaña Mantenimiento. Aparece el panel de Configuración del período de mantenimiento.
5. Seleccione Editar e introduzca el nuevo día y hora en que desea que comience el período de mantenimiento.
6. Elija Guardar para guardar los cambios. La nueva hora de inicio del mantenimiento se muestra en el panel de Configuración.

Puede cambiar el período de mantenimiento del sistema de archivos mediante el comando CLI update-file-system. Ejecute el siguiente comando y sustituya el ID del sistema de archivos por el ID de su sistema de archivos y la fecha y la hora en las que desee iniciar el período.

```
aws fsx update-file-system --file-system-id fs-01234567890123456 --lustre-configuration
 WeeklyMaintenanceStartTime=1:01:30
```

## Eliminación de un sistema de archivos

Puede eliminar un sistema de archivos Amazon FSx for Lustre mediante la consola Amazon FSx, la API Amazon FSx y AWS CLI la API Amazon FSx. Antes de eliminar un sistema de archivos de FSx

para Lustre, debe desmontarlo de todas las instancias de Amazon EC2 conectadas. En los sistemas de archivos vinculados a S3, para garantizar que todos los datos se vuelvan a escribir en S3 antes de eliminar el sistema de archivos, puede controlar que la AgeOfOldestQueuedMessagemétrica sea cero (si utiliza la exportación automática) o ejecutar una tarea de exportación de datos en un repositorio de datos. Si tiene habilitada la exportación automática y desea utilizar una tarea de exportación de repositorios de datos, debe deshabilitar la exportación automática antes de ejecutar la tarea de exportación de repositorios de datos.

Para eliminar un sistema de archivos después de desmontarlo de cada instancia de Amazon EC2:

- Usando la consola: siga el procedimiento descrito en Eliminar recursos.
- Uso de la API o la CLI: utilice la operación DeleteFileSystemAPI o el comando delete-file-systemCLI.

# Migración a Amazon FSx para Lustre usando AWS DataSync

Se puede utilizar AWS DataSync para transferir datos entre sistemas de archivos de FSx para Lustre. DataSync es un servicio de transferencia de datos que simplifica, automatiza y acelera la transferencia y la replicación de datos entre sistemas de almacenamiento autogestionados y servicios de almacenamiento de AWS a través de Internet o AWS Direct Connect. DataSync puede transferir los datos de sistemas de archivos y también los metadatos, como la propiedad, las marcas temporales y los permisos de acceso.

## Cómo migrar archivos existentes a FSx para Lustre usando AWS DataSync

Puede utilizar DataSync con FSx para sistemas de archivos Lustre para realizar migraciones de datos puntuales, incorporar datos periódicamente para cargas de trabajo distribuidas, y programar la replicación para la protección y recuperación de datos. Para obtener información sobre escenarios de transferencia específicos, consulte ¿Dónde puedo transferir mis datos? en la Guía del usuario AWS DataSync.

### Requisitos previos

Para migrar datos a su configuración de FSx para Lustre, necesita un servidor y una red que cumplan con los requisitos de DataSync. Para obtener más información, consulte Requisitos para DataSync en la AWS DataSyncGuía del usuario.

- Ha creado un sistema de archivo FSx para Lustre de destino. Para obtener más información, consulte Cree su sistema de archivos FSx for Lustre.
- Los sistemas de archivos de origen y destino están conectados en la misma nube privada virtual (VPC). El sistema de archivos de origen puede estar ubicado en las instalaciones o en otra Amazon VPC, Cuenta de AWS o Región de AWS, pero debe estar en una red sincronizada con la del sistema de archivos de destino mediante Amazon VPC Peering, Transit Gateway, AWS Direct Connect o AWS VPN. Para obtener más información, consulte ¿Qué es una conexión de emparejamiento de VPC? en la Amazon VPC Peering Guide.

> **Note**
>
> DataSync solo puede transferir a través de Cuentas de AWS hacia FSx para Lustre o desde FSx para Lustre si la otra ubicación de transferencia es Amazon S3.

## Pasos básicos para migrar archivos mediante DataSync

La transferencia de archivos de un origen a un destino usando DataSync implica los siguientes pasos básicos:

- Descargue e implemente un agente en su entorno y actívelo (no es necesario si se realiza una transferencia entre Servicios de AWS).
- Cree y configure una ubicación de origen y destino.
- Cree una tarea.
- Ejecute la tarea para transferir archivos desde el origen al destino.

Para obtener más información, consulte los siguientes temas en la Guía del usuario de AWS DataSync:

- Transferencia entre almacenamiento en las instalaciones y AWS
- Configuración de transferencias AWS DataSync con Amazon FSx para Lustre en la Guía del usuario AWS DataSync.
- Implementación de su agente en Amazon EC2

# Supervisión de Amazon FSx para Lustre

Puede utilizar las siguientes herramientas de supervisión automatizadas para vigilar Amazon FSx para Lustre e informar cuando haya algún problema:

- Supervisión con Amazon CloudWatch: CloudWatch recopila y procesa datos sin procesar de Amazon FSx para Lustre en métricas legibles y casi en tiempo real. Puede crear una alarma de CloudWatch que envíe un mensaje de Amazon SNS cuando la alarma cambie de estado.
- Supervisión mediante el registro de Lustre: puede supervisar los eventos de registro habilitados para su sistema de archivos. El registro de Lustre escribe estos eventos en los Registros de Amazon CloudWatch.
- Supervisión de registros de AWS CloudTrail: comparta archivos de registro entre cuentas, supervise los archivos de registro de CloudTrail en tiempo real enviándolos a CloudWatch Logs, escriba aplicaciones de procesamiento de registros en Java y compruebe que los archivos de registro no hayan cambiado después de que CloudTrail los entregara.

Temas



## Supervisión con Amazon CloudWatch

Puede supervisar los sistemas de archivos mediante Amazon CloudWatch, que recopila y procesa datos sin procesar de Amazon FSx para Lustre en métricas legibles y casi en tiempo real. Estas estadísticas se retienen durante un período de 15 meses, de forma que pueda obtener acceso a información de historial y obtener una mejor perspectiva acerca del desempeño de su aplicación web o servicio. De forma predeterminada, los datos de las métricas de Amazon FSx para Lustre se envían automáticamente a CloudWatch en períodos de 1 minuto. Para obtener más información acerca de CloudWatch, consulte ¿Qué es Amazon CloudWatch? en la Guía del usuario de Amazon CloudWatch.

Las métricas de CloudWatch se presentan como bytes sin procesar. Los bytes no se redondean a un decimal o múltiple binario de la unidad.

# Métricas del sistema de archivos

FSx para Lustre publica las siguientes métricas en el espacio de nombres de `FSx` en CloudWatch. Para cada métrica, FSx para Lustre emite un punto de datos por disco por minuto. Para ver los detalles agregados del sistema de archivos, puede utilizar la estadística `Sum`. Tenga en cuenta que los servidores de archivos detrás de sus sistemas de archivos FSx para Lustre están repartidos en múltiples discos.

| Métrica | Descripción |
| --- | --- |
| `DataReadBytes` | El número de bytes para las operaciones de lectura del sistema de archivos.<br><br>La estadística `Sum` es el número total de bytes asociados a las operaciones de lectura durante el período. La estadística `Minimum` es el número mínimo de bytes asociados a las operaciones de lectura en un solo disco. La estadística `Maximum` es el número máximo de bytes asociados a las operaciones de lectura en el disco. La estadísti ca `Average` es el número medio de bytes asociados a las operacion es de lectura por disco. La estadística `SampleCount` es el número de discos.<br><br>Para calcular el rendimiento medio (bytes por segundo) de un período, divida la estadística `Sum` por el número de segundos del período.<br><br>Unidades:<br><br>• Bytes para `Sum`, `Minimum`, `Maximum` y `Average`.<br>• Recuento de `SampleCount` .<br><br>Estadísticas válidas: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCou nt` |
| `DataWriteBytes` | El número de bytes para las operaciones de escritura del sistema de archivos.<br><br>La estadística `Sum` es el número total de bytes asociados a las operaciones de escritura. La estadística `Minimum` es el número mínimo |

| Métrica | Descripción |
| --- | --- |
| | de bytes asociados a las operaciones de escritura en un solo disco. La estadística `Maximum` es el número máximo de bytes asociados a las operaciones de escritura en el disco. La estadística `Average` es el número medio de bytes asociados a las operaciones de escritura por disco. La estadística `SampleCount` es el número de discos.<br><br>Para calcular el rendimiento medio (bytes por segundo) de un período, divida la estadística `Sum` por el número de segundos del período.<br><br>Unidades:<br><br>• Bytes para `Sum`, `Minimum`, `Maximum` y `Average`.<br>• Recuento de `SampleCount` .<br><br>Estadísticas válidas: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount` |

| Métrica | Descripción |
| --- | --- |
| `DataReadOperations` | El número de operaciones de lectura.<br><br>La estadística `Sum` es el número total de operaciones de lectura. La estadística `Minimum` es el número mínimo de operaciones de lectura en un solo disco. La estadística `Maximum` es el número máximo de operaciones de lectura en el disco. La estadística `Average` es el número medio de operaciones de lectura por disco. La estadística `SampleCount` es el número de discos.<br><br>Para calcular el número medio de operaciones de lectura (operaciones por segundo) de un período, divida la estadística `Sum` por el número de segundos del período.<br><br>Unidades:<br><br>• Bytes para `Sum`, `Minimum`, `Maximum` y `Average`.<br>• Recuento de `SampleCount` .<br><br>Estadísticas válidas: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount` |

| Métrica | Descripción |
| --- | --- |
| `DataWriteOperations` | El número de operaciones de escritura.<br><br>La estadística `Sum` es el número total de operaciones de escritura. La estadística `Minimum` es el número mínimo de operaciones de escritura en un solo disco. La estadística `Maximum` es el número máximo de operaciones de escritura en el disco. La estadística `Average` es el número medio de operaciones de escritura por disco. La estadística `SampleCount` es el número de discos.<br><br>Para calcular el número medio de operaciones de escritura (operaciones por segundo) de un período, divida la estadística `Sum` por el número de segundos del período.<br><br>Unidades:<br><br>• Bytes para `Sum`, `Minimum`, `Maximum` y `Average`.<br>• Recuento de `SampleCount` .<br><br>Estadísticas válidas: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount` |

| Métrica | Descripción |
| --- | --- |
| `MetadataOperations` | El número de operaciones de metadatos.<br><br>La estadística `Sum` es el recuento de operaciones de metadatos. La estadística `Minimum` es el número mínimo de operaciones de metadatos por disco. La estadística `Maximum` es el número máximo de operaciones de metadatos por disco. La estadística `Average` es el número medio de operaciones de metadatos por disco. La estadística `SampleCount` es el número de discos.<br><br>Para calcular el valor medio de las operaciones de metadatos (operaciones por segundo) durante un período, divida la estadística `Sum` por el número de segundos del período.<br><br>Unidades:<br><br>• Recuento de `Sum`, `Minimum`, `Maximum`, `Average` y `SampleCount` .<br><br>Estadísticas válidas: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount` |

| Métrica | Descripción |
| --- | --- |
| FreeDataStorageCapacity | La cantidad de capacidad de almacenamiento disponible.<br><br>La estadística Sum es el número total de bytes disponibles en el sistema de archivos. La estadística Minimum es el número total de bytes disponibles en el disco más lleno. La estadística Maximum es el número total de bytes disponibles en el disco con la mayor cantidad de almacenamiento disponible restante. La estadística Average es el número medio de bytes disponibles por disco. La estadística SampleCount es el número de discos.<br><br>Unidades:<br><br>• Bytes para Sum, Minimum, Maximum.<br>• Recuento de SampleCount .<br><br>Estadísticas válidas: Sum, Minimum, Maximum, Average, SampleCount |
| LogicalDiskUsage | La cantidad de datos lógicos almacenados (sin comprimir).<br><br>La estadística Sum es el número total de bytes lógicos almacenados en el sistema de archivos. La estadística Minimum es el menor número de bytes lógicos almacenados en un disco del sistema de archivos. La estadística Maximum es el mayor número de bytes lógicos almacenados en un disco del sistema de archivos. La estadística Average es el número medio de bytes lógicos almacenados por disco. La estadística SampleCount es el número de discos.<br><br>Unidades:<br><br>• Bytes para Sum, Minimum, Maximum.<br>• Recuento de SampleCount .<br><br>Estadísticas válidas: Sum, Minimum, Maximum, Average, SampleCount |

| Métrica | Descripción |
| --- | --- |
| PhysicalDiskUsage | La cantidad de almacenamiento ocupada físicamente por los datos del sistema de archivos (comprimidos).<br><br>La estadística Sum es el número total de bytes ocupados en discos en el sistema de ficheros. La estadística Minimum es el número total de bytes ocupados en el disco más vacío. La estadística Maximum es el número total de bytes ocupados en el disco más lleno. La estadística Average es el número medio de bytes ocupados por disco. La estadística SampleCount es el número de discos.<br><br>Unidades:<br><br>• Bytes para Sum, Minimum, Maximum.<br>• Recuento de SampleCount .<br><br>Estadísticas válidas: Sum, Minimum, Maximum, Average, SampleCount |

## Métricas de AutoImport y AutoExport

FSx para Lustre publica las siguientes métricas AutoImport (importación automática) y AutoExport (exportación automática) en el espacio de nombres FSx en CloudWatch. Estas métricas utilizan dimensiones para permitir mediciones más granulares de sus datos. Todas las métricas AutoImport y AutoExport tienen las dimensiones FileSystemId y Publisher.

| Métrica | Descripción |
| --- | --- |
| AgeOfOldestQueuedMessage<br><br>Dimensión: AutoExport | La antigüedad, en segundos, del mensaje más antiguo en espera de ser exportado.<br><br>La estadística Average es la edad media del mensaje más antiguo en espera de ser exportado. La estadística Maximum es el número máximo de segundos que un mensaje ha permanecido en la cola de exportación. La estadística Minimum es el número máximo de segundos que un |

| Métrica | Descripción |
| --- | --- |
| | mensaje ha permanecido en la cola. Un valor de cero indica que no hay mensajes esperando a ser exportados.<br><br>Unidades: segundos<br><br>Estadísticas válidas: `Average`, `Minimum`, `Maximum` |
| `RepositoryRenameOperations`<br><br>Dimensión: `AutoExport` | El número de cambios de nombre procesados por el sistema de archivos en respuesta a un cambio de nombre de directorio mayor.<br><br>La estadística `Sum` es el número total de operaciones de cambio de nombre que se producen al cambiar el nombre de un directorio. La estadística `Average` es el número medio de operaciones de cambio de nombre del sistema de archivos. La estadística `Maximum` es el número máximo de operaciones de cambio de nombre asociadas a un cambio de nombre de directorio en el sistema de archivos. La estadística `Minimum` es el número mínimo de cambios de nombres asociados a un cambio de nombre de directorio en el sistema de archivos.<br><br>Unidades: recuento<br><br>Estadísticas válidas: `Sum`, `Minimum`, `Maximum`, `Average` |
| `AgeOfOldestQueuedMessage`<br><br>Dimensión: `AutoImport` | La antigüedad, en segundos, del mensaje más antiguo en espera de ser importado.<br><br>La estadística `Average` es la edad media del mensaje más antiguo en espera de ser importado. La estadística `Maximum` es el número máximo de segundos que un mensaje ha permanecido en la cola de importación. La estadística `Minimum` es el número mínimo de segundos que un mensaje ha permanecido en la cola de importación. Un valor de cero indica que no hay mensajes esperando a ser importados.<br><br>Unidades: segundos<br><br>Estadísticas válidas: `Average`, `Minimum`, `Maximum` |

# Amazon FSx para Lustre

Las métricas de Amazon FSx para Lustre utilizan el espacio de nombres `FSx` y proporcionan métricas para la dimensión, `FileSystemId`. El ID de un sistema de archivos se puede encontrar utilizando el comando `describe-file-systems` AWS CLI, y toma la forma de *`fs-01234567890123456`*.

Hay una dimensión adicional disponible, `Publisher`, en CloudWatch y AWS CLI para las métricas `AutoImport` y `AutoImport` para denotar qué servicio publicó las métricas.

## Cómo usar las métricas Amazon FSx para Lustre

Las métricas mostradas por Amazon FSx para Lustre proporcionan información que puede analizar de diferentes maneras. La siguiente lista muestra algunos usos frecuentes de las métricas. Se trata de sugerencias que puede usar como punto de partida y no de una lista completa.

| ¿Cómo puedo determinar... | Métricas relevantes (dimensión \| métrica) |
|---|---|
| el rendimiento de mi sistema de archivos? | SUM (DataReadBytes + DataWriteBytes) /Período (en segundos) |
| las IOPS de mi sistema de archivos? | IOPS totales = SUM (DataReadOperations + DataWriteOperations + MetadataOperations)/Período (en segundos) |
| la relación de compresión de datos de mi sistema de archivos? | SUM (LogicalDiskUsage) / SUM (PhysicalDiskUsage) |
| Si las actualizaciones de mi sistema de archivos se han sincronizado con mi bucket S3? | AutoExport \| AgeOfOldestQueuedMessage |
| Si las actualizaciones de mi bucket S3 se han sincronizado | AutoImport \| AgeOfOldestQueuedMessage |

| ¿Cómo puedo determinar... | Métricas relevantes (dimensión \| métrica) |
| --- | --- |
| con mi sistema de archivos? | |

## Matemáticas métricas: relación de compresión de datos

La calculadora de métricas le permiten consultar varias métricas de CloudWatch y usar expresiones matemáticas para crear nuevas series temporales basadas en estas métricas. Puede visualizar las series temporales resultantes en la consola de CloudWatch y agregarlas a los paneles. Para obtener más información sobre la matemática métrica, consulte Uso de la matemática métrica en la Guía del usuario de Amazon CloudWatch.

Esta expresión matemática métrica calcula la relación de compresión de datos de su sistema de archivos Amazon FSx para Lustre. Para calcular esta relación, primero obtenga la estadística de suma del uso total del disco lógico (sin compresión), que proporciona la métrica `LogicalDiskUsage`. A continuación, divídalo por la estadística de la suma del uso total del disco físico (con compresión), proporcionada por la métrica `PhysicalDiskUsage`.

Así que si su lógica es esta: suma de `LogicalDiskUsage` ÷ suma de `PhysicalDiskUsage`

A continuación, la información de las métricas de CloudWatch es la siguiente.

| ID | Métrica usable | Estadística | Período |
| --- | --- | --- | --- |
| m1 | `LogicalDiskUsage` | Sum | 1 minuto |
| m2 | `PhysicalDiskUsage` | Sum | 1 minuto |

Su ID de cálculo de métrica y expresión son los siguientes.

| ID | Expresión |
| --- | --- |
| e1 | `m1/m2` |

`e1` es la relación de compresión de datos.

## Acceso a métricas de CloudWatch

Puede ver las métricas de Amazon FSx para Lustre para CloudWatch de muchas maneras. Puede verlas a través de la consola de CloudWatch, o puede acceder a ellas mediante la CLI de CloudWatch o la API de CloudWatch. Los siguientes procedimientos le muestran cómo obtener acceso a las métricas a través de estas herramientas.

Para ver las métricas a través de la consola de CloudWatch

1. Abra la consola de CloudWatch.
2. En el panel de navegación, seleccione Métricas.
3. Seleccione el espacio de nombres FSx.
4. (Opcional) Para ver una métrica, escriba su nombre en el campo de búsqueda.
5. De manera opcional, para filtrar por dimensión, seleccione FileSystemId.

Para obtener acceso a las métricas desde la AWS CLI

- Utilice el comando `list-metrics` con el espacio de nombres de `--namespace "AWS/FSx"`. Para obtener más información, consulte Referencia de comandos de la AWS CLI.

Para obtener acceso a las métricas desde la API de CloudWatch

- Llame a `GetMetricStatistics`. Para obtener más información, consulte la Referencia de la API de Amazon CloudWatch.

## Creación de alarmas de CloudWatch para supervisar Amazon FSx para Lustre

Puede crear una alarma de CloudWatch que envíe un mensaje de Amazon SNS cuando la alarma cambia de estado. Una alarma vigila una única métrica durante el período especificado y realiza una o varias acciones en función del valor de la métrica relativo a un determinado umbral durante una serie de períodos de tiempo. La acción es una notificación que se envía a un tema de Amazon SNS o a una política de escalado automático.

Las alarmas invocan acciones únicamente para los cambios de estado prolongados. Las alarmas de CloudWatch no invocan acciones solo por tener un estado determinado. Es necesario que el estado haya cambiado y que se mantenga durante un número específico de períodos.

Los siguientes procedimientos describen cómo crear alarmas para Amazon FSx para Lustre.

Para establecer alarmas utilizando la consola de CloudWatch

1. Inicie sesión en la AWS Management Console y abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. Elija Crear alarma. Esto lanza el asistente de creación de alarmas.
3. Elija Métricas de FSx, y desplácese a través de las métricas de Amazon FSx para Lustre para ubicar la métrica en la que desea colocar una alarma. Para mostrar solo las métricas de Amazon FSx para Lustre en este cuadro de diálogo, busque el ID del sistema de archivos del sistema de archivos. Seleccione la métrica para crear una alarma y elija Siguiente.
4. En la sección Condiciones, elija las condiciones que desea para la alarma, y luego, Siguiente.

   > **Note**
   >
   > Es posible que las métricas no se publiquen durante el mantenimiento del sistema de archivos. Para evitar cualquier cambio innecesario y engañoso en el estado de las alarmas, y para configurarlas de manera que sean resistentes a los puntos de datos faltantes, consulte Configuración del modo en que las alarmas de CloudWatch tratan los datos faltantes en la Guía del usuario de Amazon CloudWatch.

5. Si desea que CloudWatch le envíe un correo electrónico cuando se alcance el estado de la alarma, para Siempre que esta alarma, elija El estado es ALARMA. En Enviar notificación a, elija un tema de SNS existente. Si elige Crear tema, puede definir el nombre y las direcciones de correo electrónico de una nueva lista de suscripción de correo electrónico. Esta lista se guarda y aparece en este cuadro para futuras alarmas.

   > **Note**
   >
   > Si utiliza Crear tema para crear un nuevo tema de Amazon SNS, verifique las direcciones de correo electrónico antes de enviarles notificaciones. Los correos electrónicos solo se envían cuando la alarma entra en estado de alarma. Si este cambio

en el estado de la alarma se produce antes de que se verifiquen las direcciones de correo electrónico, no recibirán ninguna notificación.

6. Previsualice la alarma que va a crear en el área Vista previa de alarma. Si aparece como se esperaba, seleccione Crear alarma.

Para configurar una alarma mediante la AWS CLI

- Llame a `put-metric-alarm`. Para obtener más información, consulte la referencia de comandos de la AWS CLI.

Para configurar una alarma mediante la API de CloudWatch

- Llame a `PutMetricAlarm`. Para obtener más información, consulte la Referencia de la API de Amazon CloudWatch.

## Iniciar sesión con Amazon CloudWatch Logs

FSx for Lustre permite registrar en Amazon Logs los eventos de error y advertencia de los repositorios de datos asociados a su sistema de archivos. CloudWatch

> **Note**
>
> El registro con Amazon CloudWatch Logs solo está disponible en Amazon FSx para los sistemas de archivos Lustre creados después de las 15:00 PST del 30 de noviembre de 2021.

Temas

## Información general de los registros

Si tiene repositorios de datos vinculados a su sistema de archivos FSx for Lustre, puede habilitar el registro de eventos del repositorio de datos en Amazon Logs. CloudWatch Los eventos de error y advertencia se pueden registrar a partir de las siguientes operaciones del repositorio de datos:

- Exportación automática
- Tareas de repositorio de datos

Para obtener más información sobre estas operaciones y sobre cómo vincular a los repositorios de datos, consulte Uso de repositorios de datos con Amazon FSx para Lustre.

Puede configurar los niveles de registro que registra Amazon FSx; es decir, si Amazon FSx va a registrar los eventos de error únicamente, solo los eventos de advertencia, o tanto los eventos de error como de advertencia. También puede desactivar el registro de eventos en cualquier momento.

> **Note**
>
> Le recomendamos encarecidamente que habilite los registros para los sistemas de archivos que tienen cualquier nivel de funcionalidad crítica asociada a ellos.

## Registro de destinos

Cuando el registro está activado, FSx for Lustre debe configurarse con un destino de CloudWatch Amazon Logs. El destino del registro de eventos es un grupo de CloudWatch registros de Amazon Logs y Amazon FSx crea un flujo de registro para su sistema de archivos dentro de este grupo de registros. CloudWatch Logs le permite almacenar, ver y buscar registros de eventos de auditoría en la CloudWatch consola de Amazon, ejecutar consultas en los CloudWatch registros mediante Logs Insights y activar CloudWatch alarmas o funciones Lambda.

El destino del registro se elige al crear el sistema de archivos de FSx para Lustre o, posteriormente, al actualizarlo. Para obtener más información, consulte Administración de registros.

De forma predeterminada, Amazon FSx creará y utilizará un grupo de CloudWatch registros predeterminado en su cuenta como destino del registro de eventos. Si desea utilizar un grupo de CloudWatch registros personalizado como destino del registro de eventos, estos son los requisitos para el nombre y la ubicación del destino del registro de eventos:

- El nombre del grupo de CloudWatch registros debe empezar por el `/aws/fsx/` prefijo.
- Si no tiene un grupo de CloudWatch registros existente al crear o actualizar un sistema de archivos en la consola, Amazon FSx for Lustre puede crear y usar un flujo de registros predeterminado CloudWatch en `/aws/fsx/lustre` el grupo de registros. El flujo de registro se creará con el formato `datarepo_file_system_id` (por ejemplo, `datarepo_fs-0123456789abcdef0`).
- Si no quiere usar el grupo de registros predeterminado, la interfaz de usuario de configuración le permite crear un grupo de CloudWatch registros al crear o actualizar su sistema de archivos en la consola.
- El grupo de CloudWatch registros de destino debe estar en la misma AWS partición y Cuenta de AWS como su sistema de archivos Amazon FSx for Lustre. Región de AWS

Puede cambiar el destino del registro de eventos en cualquier momento. Al hacerlo, los nuevos registros de eventos se envían solo al nuevo destino.

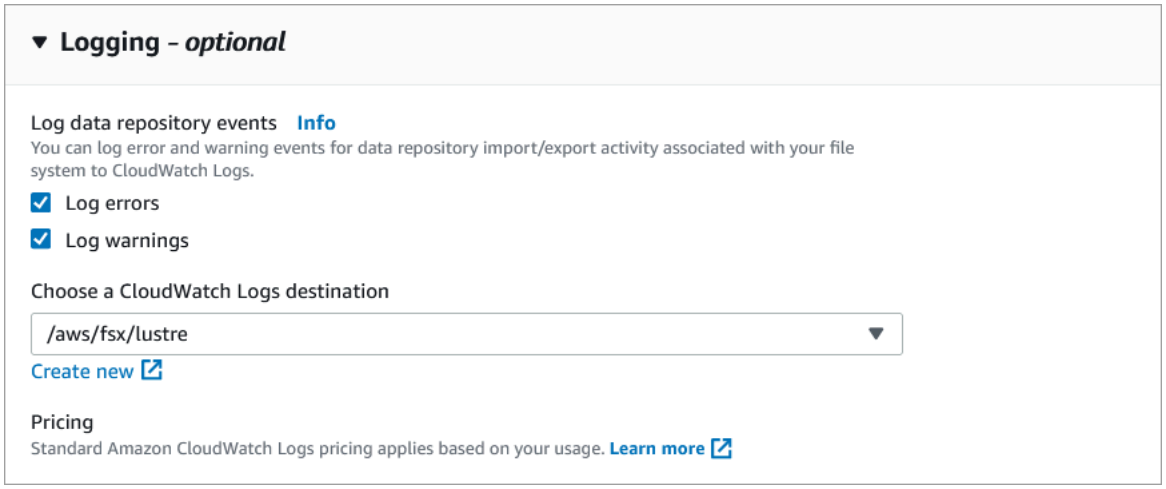
## Administración de registros

El destino del registro se elige al crear el sistema de archivos de FSx para Lustre o, posteriormente, al actualizarlo. El registro está activado de forma predeterminada al crear un sistema de archivos desde la consola Amazon FSx. Sin embargo, el registro está desactivado de forma predeterminada al crear un sistema de archivos con la API AWS CLI o con Amazon FSx.

En los sistemas de archivos existentes que tienen activado el registro, puede cambiar la configuración del registro de eventos, incluido el nivel de registro para el que se registrarán los eventos y el destino del registro. Puede realizar estas tareas mediante la consola de Amazon FSx o la API AWS CLI de Amazon FSx.

Para habilitar el registro al crear un sistema de archivos (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Siga el procedimiento para crear un nuevo sistema de archivos que se describe en Cree su sistema de archivos FSx for Lustre en la sección Primeros pasos.
3. Abra la sección Registro (opcional). El registro está habilitado de forma predeterminada.




4. Continúe con la siguiente sección del asistente de creación del sistema de archivos.

Cuando el sistema de archivos esté disponible, se habilitará el registro.

Para habilitar el registro al crear un sistema de archivos (CLI)

1. Al crear un nuevo sistema de archivos, utilice la `LogConfiguration` propiedad junto con la CreateFileSystemoperación para habilitar el registro en el nuevo sistema de archivos.

```
create-file-system --file-system-type LUSTRE \
    --storage-capacity 1200 --subnet-id subnet-08b31917a72b548a9  \
    --lustre-configuration "LogConfiguration={Level=WARN_ERROR, \
        Destination="arn:aws:logs:us-east-1:234567890123:log-group:/aws/fsx/
testEventLogging"}"
```

2. Cuando el sistema de archivos esté disponible, se habilitará la característica de registro.

Para cambiar la configuración de registro (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Vaya a Sistemas de archivos y elija el sistema de archivos de Lustre para el que desee gestionar el registro.
3. Elija la pestaña Monitorización.
4. En el panel de registro, seleccione Actualizar.
5. En el cuadro de diálogo Actualizar la configuración del registro, cambie los ajustes deseados.

a. Seleccione Registrar errores para registrar solo los eventos de error o Registrar advertencias para registrar solo los eventos de advertencia, o ambas opciones. El registro estará desactivado si no se selecciona nada.

b. Elija un destino de registro de CloudWatch registros existente o cree uno nuevo.

6. Seleccione Guardar.

Para cambiar la configuración de registro (CLI)

- Utilice el comando CLI `update-file-system` o la operación API equivalente CLI `UpdateFileSystem`.

```
update-file-system --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration "LogConfiguration={Level=WARN_ERROR, \
        Destination="arn:aws:logs:us-east-1:234567890123:log-group:/aws/fsx/
testEventLogging"}"
```

## Visualización de registros

Puede ver los registros una vez que Amazon FSx haya empezado a emitirlos. También puede ver los siguientes registros:

- Para ver los registros, ve a la CloudWatch consola de Amazon y elige el grupo de registros y el flujo de registros a los que se envían los registros de eventos. Para obtener más información, consulta Ver los datos de registro enviados a CloudWatch Logs en la Guía del usuario de Amazon CloudWatch Logs.
- Puede utilizar CloudWatch Logs Insights para buscar y analizar sus datos de registro de forma interactiva. Para obtener más información, consulte Análisis de datos de registro con CloudWatch Logs Insights, en la Guía del usuario de Amazon CloudWatch Logs.
- También puede exportar registros a Amazon S3. Para obtener más información, consulte Exportación de datos de registro a Amazon S3, en la Guía del usuario de Amazon CloudWatch Logs.

Para obtener más información sobre los motivos de los fallos, consulte Registros de eventos del repositorio de datos.

# Registro de llamadas a la API FSx para Lustre con AWS CloudTrail

Amazon FSx para Lustre se integra con AWS CloudTrail, un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un servicio de AWS en Amazon FSx para Lustre. CloudTrail captura todas las llamadas a la API para Amazon FSx para Lustre como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de Amazon FSx para Lustre y las llamadas desde el código a las operaciones de la API de Amazon FSx para Lustre.

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 FSx para Lustre. Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Historial de eventos. Mediante la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a Amazon FSx para Lustre. También puede identificar la dirección IP desde la que se realizó la solicitud, quién realizó la solicitud, cuándo se realizó y detalles adicionales.

Para obtener más información acerca de CloudTrail, consulte la Guía del usuario de AWS CloudTrail.

## Información de Amazon FSx para Lustre en CloudTrail

CloudTrail se habilita en su cuenta de AWS cuando la crea. Cuando se produce una actividad de la API en Amazon FSx para Lustre, dicha actividad se registra en un evento de CloudTrail junto con los eventos de los demás servicios de AWS en Historial de eventos. Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte Ver eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de los eventos de la cuenta de AWS, incluidos los eventos de Amazon FSx para Lustre, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De manera predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS. El seguimiento registra los eventos de todas las regiones de AWS en 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 obtener más información, consulte los siguientes temas en la Guía del usuario de AWS CloudTrail:

- 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 llamadas a la API de Amazon FSx para Lustre. Por ejemplo, las llamadas a las operaciones `CreateFileSystem` y `TagResource` generan entradas en los archivos de registro de CloudTrail.

Cada entrada de registro o evento contiene información acerca de quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario 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 obtener más información, consulte el Elemento userIdentity de CloudTrail en la Guía del usuario de AWS CloudTrail.

## Descripción de las entradas de archivos de registro de Amazon FSx para Lustre

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros a un bucket de Amazon S3 que usted especifique. Los archivos log de CloudTrail pueden contener una o varias entradas de log. 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.

El siguiente ejemplo muestra una entrada de registro de CloudTrail que muestra la operación `TagResource` cuando sea crea una etiqueta para un sistema de archivos desde la consola.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": “111122223333”,
        "arn": "arn:aws:sts::111122223333:root”,
```

```
        "accountId": “111122223333”,
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE”,
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T22:36:07Z"
            }
        }
    },
    "eventTime": "2018-11-14T22:36:07Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": “192.0.2.0”,
    "userAgent": “console.amazonaws.com”,
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789”
    },
    "responseElements": null,
    "requestID": “aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51”,
    "eventID": “bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p”,
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": “111122223333”
}
```

El siguiente ejemplo muestra una entrada de registro de CloudTrail que muestra la acción `UntagResource` cuando sea elimina una etiqueta para un sistema de archivos desde la consola.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": "111122223333",
        "arn": "arn:aws:sts::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
```

```
                "creationDate": "2018-11-14T23:40:54Z"
            }
        }
    },
    "eventTime": "2018-11-14T23:40:54Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "UntagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789"
    },
    "responseElements": null,
    "requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",
    "eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": "111122223333"
}
```

# Seguridad en FSx para Lustre

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la nube de Amazon Web Services. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información acerca de los programas de conformidad que se aplican a Amazon FSx para Lustre, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le permite comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Amazon FSx para Lustre. En los siguientes temas, se mostrará cómo configurar Amazon FSx para satisfacer sus objetivos de seguridad y conformidad. También puede aprender a utilizar otros servicios de Amazon que ayudan a monitorear y proteger los recursos de Amazon FSx para Lustre.

A continuación, encontrará una descripción de las consideraciones de seguridad para trabajar con Amazon FSx.

Temas

# Protección de datos en Amazon FSx para Lustre

El modelo de se aplica a protección de datos en Amazon FSx for Lustre. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los. 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 sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios 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 la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados 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 por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información 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 FSx u otro dispositivo Servicios de AWS mediante la consola, la API o AWS los AWS CLI SDK. 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



# Cifrado de datos en Amazon FSx para Lustre

Amazon FSx para Lustre admite dos formas de cifrado para sistemas de archivos, el cifrado de datos en reposo y cifrado de datos en tránsito. El cifrado de los datos en reposo se activa de forma automática al crear un sistema de archivos Amazon FSx. El cifrado de datos en tránsito se habilita automáticamente cuando accede a un sistema de archivos de Amazon FSx desde instancias de Amazon EC2 que admiten esta característica.

## Cuándo usar cifrado

Si su organización está sujeta a políticas reglamentarias o corporativas que requieren el cifrado de datos y metadatos en reposo, recomendamos crear un sistema de archivos cifrados y montar el sistema de archivos con el cifrado de datos en tránsito.

Para obtener más información sobre cómo crear un sistema de archivos cifrado en reposo mediante la consola, consulte Crear su sistema de archivos de Amazon FSx para Lustre.

Temas



## Cifrado de datos en reposo

El cifrado de los datos en reposo se habilita automáticamente al crear un sistema de archivos Amazon FSx for Lustre AWS Management Console a través de la AWS CLI API Amazon FSx o uno de los SDK o mediante programación. AWS Su organización podría necesitar el cifrado en reposo de todos los datos que cumplan una clasificación específica o que se asocien a una determinada aplicación, carga de trabajo o entorno. Si crea un sistema de archivos persistente, puede especificar la AWS KMS clave con la que se cifrarán los datos. Si crea un sistema de archivos Scratch, los datos se cifran usando claves gestionadas por Amazon FSx. Para obtener más información sobre cómo

crear un sistema de archivos cifrado en reposo mediante la consola, consulte Crear su sistema de archivos de Amazon FSx para Lustre.

> **Note**
>
> La infraestructura de administración de AWS claves utiliza algoritmos criptográficos aprobados por las Normas Federales de Procesamiento de Información (FIPS) 140-2. La infraestructura se adhiere a las recomendaciones del Instituto Nacional de Normas y Tecnología (NIST) 800-57.

Para obtener más información sobre cómo se usa FSx for AWS KMS Lustre, consulte. Cómo utiliza Amazon FSx for Lustre AWS KMS

Funcionamiento del cifrado en reposo

En un sistema de archivos cifrados, los datos y los metadatos se cifran automáticamente antes de escribirse en el sistema de archivos. Del mismo modo, cuando se leen los datos y metadatos, se descifran automáticamente antes de que se presenten a la aplicación. Estos procesos los administra Amazon FSx para Lustre de forma transparente, por lo que no tiene que modificar las aplicaciones.

Amazon FSx para Lustre utiliza el algoritmo de cifrado AES-256 estándar del sector para cifrar datos en reposo de sistemas de archivos. Para obtener más información, consulte los Conceptos básicos de la criptografía en la Guía del desarrollador AWS Key Management Service .

Cómo utiliza Amazon FSx for Lustre AWS KMS

Amazon FSx for Lustre cifra los datos automáticamente antes de escribirlos en el sistema de archivos y los descifra automáticamente a medida que se leen. Los datos se cifran mediante un cifrado de bloques XTS-AES-256. Todos los sistemas de archivos Scratch FSx for Lustre están cifrados en reposo con claves gestionadas por. AWS KMS Amazon FSx for Lustre se AWS KMS integra con la administración de claves. Las claves utilizadas para cifrar los sistemas de archivos Scratch en reposo son únicas por sistema de archivos y se destruyen una vez eliminado el sistema de archivos. En el caso de los sistemas de archivos persistentes, debe elegir la clave KMS utilizada para cifrar y descifrar los datos. Puede especificar qué clave se usará cuando se cree un sistema de archivos persistente. Puede habilitar, deshabilitar o revocar concesiones en esta clave de KMS. Esta clave de KMS puede ser de uno de los dos siguientes tipos:

- Clave administrada de AWS para Amazon FSx: es la clave de KMS predeterminada. No se le cobrará por crear ni almacenar una clave de KMS, pero sí por utilizarla. Para más información, consulte Precios de AWS Key Management Service.
- Clave administrada por el cliente: se trata de la clave de KMS más flexible, ya que puede configurar las políticas de claves y concesiones para varios usuarios o servicios. Para obtener más información sobre la creación de claves administradas por el cliente, consulte Creación de claves en la Guía para AWS Key Management Service desarrolladores.

Si utiliza una clave administrada por el cliente como clave de KMS para el cifrado y descifrado de datos de archivo, puede activar la rotación de claves. Cuando habilitas la rotación de claves, la rota AWS KMS automáticamente una vez al año. Además, una clave administrada por el cliente le permite elegir el momento en que desea deshabilitar, volver a habilitar, eliminar o revocar el acceso a su clave gestionada por el cliente en cualquier momento.

> **Important**
>
> Amazon FSx solo admite claves KMS de cifrado simétricas. No puede utilizar claves KMS asimétricas con Amazon FSx.

### Políticas clave de Amazon FSx para AWS KMS

Las políticas de claves son la forma principal de controlar el acceso a las claves KMS. Para obtener más información acerca de las políticas de claves, consulte Uso de las políticas de claves en AWS KMS en la Guía para desarrolladores de AWS Key Management Service .En la siguiente lista se describen todos los permisos relacionados con AWS KMS que Amazon FSx admite para sistemas de archivos cifrados en reposo:

- kms:Encrypt: (opcional) cifra texto no cifrado en texto cifrado. Este permiso está incluido en la política de claves predeterminada.
- kms: Decrypt: (obligatorio) descifra texto cifrado. El texto cifrado es texto no cifrado que se ha cifrado previamente. Este permiso está incluido en la política de claves predeterminada.
- kms: ReEncrypt — (Opcional) Cifra los datos del lado del servidor con una nueva clave de KMS, sin exponer el texto sin formato de los datos del lado del cliente. Los datos se descifran en primer lugar y luego se vuelven a cifrar. Este permiso está incluido en la política de claves predeterminada.

- kms: GenerateDataKeyWithoutPlaintext — (Obligatorio) Devuelve una clave de cifrado de datos cifrada con una clave KMS. Este permiso está incluido en la política de claves predeterminada en kms: GenerateDataKey *.
- kms: CreateGrant — (Obligatorio) Añade una concesión a una clave para especificar quién puede utilizarla y en qué condiciones. Las concesiones son mecanismos de permiso alternativo para las políticas de claves. Para obtener más información sobre las concesiones, consulte Uso de concesiones en la Guía para desarrolladores de AWS Key Management Service . Este permiso está incluido en la política de claves predeterminada.
- kms: DescribeKey — (Obligatorio) Proporciona información detallada sobre la clave KMS especificada. Este permiso está incluido en la política de claves predeterminada.
- kms: ListAliases — (opcional) Muestra todos los alias clave de la cuenta. Si utiliza la consola para crear un sistema de archivos cifrados, este permiso rellena la lista para seleccionar la clave de KMS. Le recomendamos que utilice este permiso para proporcionar la mejor experiencia de usuario. Este permiso está incluido en la política de claves predeterminada.

## Cifrado de datos en tránsito

Scratch 2 y los sistemas de archivos persistentes pueden cifrar automáticamente los datos en tránsito. En la siguiente tabla, si hay una marca de verificación en la celda para ese tipo de implementación Región de AWS, los datos se cifran en tránsito cuando se accede al sistema de archivos desde las instancias de Amazon EC2 que admiten el cifrado en tránsito y también para todas las comunicaciones entre los hosts del sistema de archivos. Para saber qué instancias EC2 soportan el cifrado en tránsito, consulte Cifrado en tránsito en la Guía del usuario de Amazon EC2 para instancias Linux.

El cifrado de datos en tránsito para sistemas de archivos temporales y persistentes está disponible a continuación. Regiones de AWS

| Región de AWS | Scratch_2 | Persistent_1 | Persistent_2 |
|---|---|---|---|
| US East (Ohio) | ✓ | ✓ | ✓ |
| Este de EE. UU. (Norte de Virginia) | ✓ | ✓ | ✓ |
| Oeste de EE. UU. (Oregón) | ✓ | ✓ | ✓ |

| Región de AWS | Scratch_2 | Persistent_1 | Persistent_2 |
|---|---|---|---|
| Oeste de EE. UU. (Norte de California)* | ✓ | ✓ | |
| Oeste de EE. UU. (Los Ángeles) | ✓ | ✓ | |
| AWS GovCloud (Este de EE. UU.) * | ✓ | ✓ | |
| AWS GovCloud (Estados Unidos-Oeste) | ✓ | ✓ | |
| Canadá (centro)* | ✓ | ✓ | ✓ |
| Europa (Irlanda) | ✓ | ✓ | ✓ |
| Europa (Milán) | ✓ | ✓ | |
| Europa (Fráncfort) | ✓ | ✓ | ✓ |
| Europa (París) | ✓ | ✓ | |
| Europa (Londres) | ✓ | ✓ | ✓ |
| Europa (Estocolmo)* | ✓ | ✓ | ✓ |
| Asia-Pacífico (Seúl) | ✓ | | ✓ |
| Asia-Pacífico (Singapur) | ✓ | ✓ | ✓ |
| Asia-Pacífico (Tokio)* | ✓ | ✓ | ✓ |
| Asia-Pacífico (Bombay)* | ✓ | ✓ | ✓ |
| Asia-Pacífico (Hong Kong)* | ✓ | ✓ | ✓ |
| Asia-Pacífico (Sídney)* | ✓ | ✓ | ✓ |
| Israel (Tel Aviv)* | | ✓ | |
| América del Sur (São Paulo)* | ✓ | ✓ | |

> **Note**
>
> * El cifrado de datos en tránsito está disponible para los sistemas de archivos creados después del 11 de abril de 2021.

# Privacidad del tráfico entre redes

Este tema describe cómo Amazon FSx protege las conexiones desde el servicio a otras ubicaciones.

## Tráfico entre Amazon FSx y clientes en las instalaciones

Dispone de dos opciones de conectividad entre su red privada y AWS:

- Una AWS Site-to-Site VPN conexión. Para obtener más información, consulte ¿Qué es AWS Site-to-Site VPN?
- Una AWS Direct Connect conexión. Para obtener más información, consulte ¿Qué es AWS Direct Connect?

Puede acceder a FSx for Lustre a través de la red para acceder AWS a las operaciones de API publicadas para realizar tareas administrativas y a los puertos de Lustre para interactuar con el sistema de archivos.

### Cifrar el tráfico de la API

Para acceder a las operaciones AWS de API publicadas, los clientes deben ser compatibles con Transport Layer Security (TLS) 1.2 o una versión posterior. Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3. Los clientes también deben admitir conjuntos de cifrado con confidencialidad directa total (PFS) tales como Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Diffie-Hellman Ephemeral (ECDHE). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos. Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puede utilizar AWS Security Token Service (STS) para generar credenciales de seguridad temporales para firmar solicitudes.

### Cifrado del tráfico de datos

El cifrado de los datos en tránsito se habilita desde las instancias EC2 compatibles que acceden a los sistemas de archivos desde dentro de Nube de AWS. Para obtener más información, consulte

Cifrado de datos en tránsito. FSx para Lustre no ofrece cifrado de forma nativa en tránsito entre clientes locales y sistemas de archivos.

# Administración de identidades y accesos para Amazon FSx para Lustre

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 quién puede autenticarse (iniciar sesión) y autorizarse (tener permisos) para utilizar los recursos de Amazon FSx. IAM es un servicio de Servicio de AWS que se puede utilizar sin cargo adicional.

Temas



## Público

La forma de utilizar AWS Identity and Access Management (IAM) difiere, dependiendo del trabajo que realice en Amazon FSx.

Usuario de servicio: si utiliza el servicio Amazon FSx para realizar su trabajo, el administrador proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Amazon FSx para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se gestiona el acceso puede ayudarlo a solicitar los permisos correctos a su administrador. Si no puede acceder a una característica de Amazon FSx, consulte Solución de problemas de acceso e identidad de Amazon FSx para Lustre.

Administrador de servicio: si está a cargo de los recursos de Amazon FSx en su empresa, probablemente tenga acceso completo a Amazon FSx. Es su trabajo determinar a qué características y recursos de Amazon FSx 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 sobre cómo su empresa puede utilizar IAM con Amazon FSx, consulte Cómo funciona Amazon FSx para Lustre 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 FSx. Para ver ejemplos de políticas basadas en identidad de Amazon FSx que puede utilizar en IAM, consulte Ejemplos de políticas basadas en identidad para Amazon FSx para Lustre.

## 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 de 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 usa las herramientas de AWS, debe firmar usted mismo las solicitudes. Para obtener más información sobre el método recomendado para la firma de 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 obtener 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 AWS

Cuando se crea una Cuenta de AWS, se comienza con una identidad de inicio de sesión que tiene acceso completo a todos los recursos y 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 email 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 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 obtener más información, consulte ¿Qué es el 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 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 Consolecambiando de roles. Puede asumir un rol llamando a una operación de 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 IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center.
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.

- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. 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 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.
- Acceso entre servicios: algunos 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 obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
  - Rol vinculado a servicios: un rol vinculado a servicios 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 de 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 de EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia asociado 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 obtener más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias de 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 las 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 añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con dicha política puede obtener información del rol de la AWS Management Console, la AWS CLI o la API de AWS.

### Políticas basadas en identidades

Las políticas basadas en identidades son documentos de políticas de permisos JSON que puede adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. 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 obtener 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 de 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 especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del Usuario de IAM.

- Políticas de control de 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 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 obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del Usuario de IAM.

### Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para obtener información sobre cómo AWS decide si permite 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 FSx para Lustre con IAM

Antes de utilizar IAM para administrar el acceso a Amazon FSx, conozca qué características de IAM están disponibles para su uso con Amazon FSx.

Características de IAM que puede utilizar con Amazon FSx para Lustre

| Característica de IAM | Soporte de Amazon FSx |
|---|---|
| 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) | Sí |
| Credenciales temporales | Sí |
| Sesiones de acceso directo (FAS) | Sí |
| Roles de servicio | No |
| Roles vinculados al servicio | Sí |

Para obtener una perspectiva general sobre cómo funcionan Amazon FSx 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 de Amazon FSx basadas en identidad

| | |
|---|---|
| Compatibilidad con las políticas basadas en identidades | Sí |

Las políticas basadas en identidades son documentos de políticas de permisos JSON que puede adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. 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 obtener 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 FSx

Para ver ejemplos de políticas basadas en identidad de Amazon FSx, consulte Ejemplos de políticas basadas en identidad para Amazon FSx para Lustre.

## Políticas basadas en recursos de Amazon FSx

| | |
|---|---|
| Compatibilidad con las políticas basadas en recursos | No |

## Acciones de políticas para Amazon FSx

| | |
|---|---|
| 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 permitir o denegar el acceso en una política. Las acciones de la política generalmente tienen el mismo nombre que la operación de API de 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 las acciones de Amazon FSx, consulte Acciones definidas por Amazon FSx para Lustre en la Referencia de autorizaciones de servicio.

Las acciones de políticas de Amazon FSx utilizan el siguiente prefijo antes de la acción:

```
fsx
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "fsx:action1",
      "fsx:action2"
         ]
```

Para ver ejemplos de políticas basadas en identidad de Amazon FSx, consulte Ejemplos de políticas basadas en identidad para Amazon FSx para Lustre.

## Recursos de políticas para Amazon FSx

| | |
|---|---|
| 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 tipos de recursos de Amazon FSx y sus ARN, consulte Tipos de recurso definidos por Amazon FSx para Lustre en la Referencia de autorizaciones de servicio. Para obtener información acerca de las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por Amazon FSx para Lustre.

Para ver ejemplos de políticas basadas en identidad de Amazon FSx, consulte Ejemplos de políticas basadas en identidad para Amazon FSx para Lustre.

## Claves de condición de políticas para Amazon FSx

| | |
|---|---|
| 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.

Para ver una lista de las claves de condición de Amazon FSx, consulte Claves de condición para Amazon FSx para Lustre en la Referencia de autorizaciones de servicio. Para obtener más

información sobre las acciones y los recursos con los que puede utilizar una clave de condición, consulte Acciones definidas por Amazon FSx para Lustre.

Para ver ejemplos de políticas basadas en identidad de Amazon FSx, consulte Ejemplos de políticas basadas en identidad para Amazon FSx para Lustre.

## Listas de control de acceso (ACL) de Amazon FSx

| | |
|---|---|
| Admite las ACL | No |

## Control de acceso basado en atributos (ABAC) con Amazon FSx

| | |
|---|---|
| Admite ABAC (etiquetas en las políticas) | Sí |

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.

Para obtener más información sobre el etiquetado de recursos de Amazon FSx, consulte Etiquetar los recursos de Amazon FSx.

Para consultar un ejemplo de política basada en la identidad para limitar el acceso a un recurso en función de las etiquetas de ese recurso, consulte Uso de etiquetas para controlar el acceso a los recursos de Amazon FSx .

## Uso de credenciales temporales con Amazon FSx

| | |
|---|---|
| Admite 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.

Utilice 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 obtener más información sobre el 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.

## Sesiones de acceso directo para Amazon FSx

| | |
|---|---|
| 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 FSx

| | |
|---|---|
| Compatible con roles de servicio | No |

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de Amazon FSx. Edite los roles de servicio solo cuando Amazon FSx proporcione orientación para hacerlo.

### Roles vinculados a servicios para Amazon FSx

| | |
|---|---|
| Admite roles vinculados a servicios | Sí |

Un rol vinculado a servicios 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 obtener más información sobre la creación y administración de roles vinculados a servicios de Amazon FSx, consulte Uso de roles vinculados a servicios para Amazon FSx.

## Ejemplos de políticas basadas en identidad para Amazon FSx para Lustre

De forma predeterminada, los usuarios y roles no tienen permiso para crear ni modificar los recursos de Amazon FSx. 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 añadir las políticas de IAM a roles, y los usuarios pueden asumirlos.

Para obtener información sobre cómo crear una política basada en identidad 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.

A fin de obtener más información sobre las acciones y los tipos de recursos definidos por Amazon FSx, incluido el formato de los ARN para cada tipo de recurso, consulte Acciones, recursos y claves de condición para Amazon FSx para Lustre en la Referencia de autorizaciones de servicio.

Temas

- Prácticas recomendadas sobre las políticas
- Uso de la consola de Amazon FSx
- Cómo permitir a los usuarios consultar sus propios permisos

## Prácticas recomendadas sobre las políticas

Las políticas basadas en identidad determinan si alguien puede crear, eliminar o acceder a los recursos de Amazon FSx 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 de 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 obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. xPara más información, consulte la política de validación del 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 obtener más información, consulte Configuración de acceso a una API protegida por MFA en la Guía del 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 FSx

Para acceder a la consola de Amazon FSx para Lustre, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle mostrar y consultar los detalles sobre los recursos de Amazon FSx 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 roles puedan seguir utilizando la consola de Amazon FSx, también asocie la política administrada por AWS a las entidades

`AmazonFSxConsoleReadOnlyAccess`. Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM.

Puede consultar esta `AmazonFSxConsoleReadOnlyAccess` y otras políticas de servicios administrados de Amazon FSx en AWS políticas gestionadas para Amazon FSx.

### 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": "*"
        }
```

```
    ]
}
```

# AWS políticas gestionadas para Amazon FSx

Una política AWS administrada es una política independiente creada y administrada por. AWS AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

## AmazonF SxServiceRolePolicy

Permite a Amazon FSx gestionar los AWS recursos en su nombre. Consulte Uso de roles vinculados a servicios para Amazon FSx para obtener más información.

## AWS política gestionada: AmazonF SxDeleteServiceLinkedRoleAccess

No puede asociar `AmazonFSxDeleteServiceLinkedRoleAccess` a sus entidades IAM. Esta política está vinculada a un servicio, y se utiliza únicamente con un rol vinculado a un servicio de dicho servicio. No puede adjuntar, separar, modificar ni eliminar esta política. Para obtener más información, consulte Uso de roles vinculados a servicios para Amazon FSx.

Esta política concede permisos administrativos que permiten a Amazon FSx eliminar su función vinculada a servicios para el acceso a Amazon S3, que solo utiliza Amazon FSx para Lustre.

Detalles de los permisos

Esta política incluye permisos que permiten `iam` a Amazon FSx ver, eliminar y ver el estado de eliminación del rol vinculado al servicio FSx para el acceso a Amazon S3.

Para ver los permisos de esta política, consulte AmazonF SxDeleteServiceLinkedRoleAccess en la Guía de referencia de políticas AWS administradas.

## AWS política gestionada: AmazonF SxFullAccess

Puede adjuntar AmazonF SxFullAccess a sus entidades de IAM. Amazon FSx también asocia esta política a un rol de servicio que permite a Amazon FSx realizar acciones en su nombre.

Proporciona acceso total a Amazon FSx y acceso a los servicios relacionados AWS .

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `fsx`: permite que las entidades principales tengan acceso completo para realizar todas las acciones de Amazon FSx, excepto `BypassSnaplockEnterpriseRetention`.
- `ds`— Permite a los directores ver información sobre los AWS Directory Service directorios.
- `ec2`
  - Permite a los directores crear etiquetas en las condiciones especificadas.
  - Proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una VPC.
- `iam`: permite que las entidades principales creen un rol vinculado al servicio Amazon FSx en nombre del usuario. Esto es necesario para que Amazon FSx pueda gestionar AWS los recursos en nombre del usuario.
- `logs`: permite que las entidades principales creen grupos de registros, registren flujos y escriban eventos en los flujos de registro. Esto es necesario para que los usuarios puedan supervisar el acceso al sistema de archivos de FSx for Windows File Server enviando los registros de acceso de auditoría CloudWatch a Logs.
- `firehose`— Permite a los directores escribir registros en una Amazon Data Firehose. Esto es necesario para que los usuarios puedan supervisar el acceso al sistema de archivos de FSx for Windows File Server enviando registros de acceso de auditoría a Firehose.

Para ver los permisos de esta política, consulte AmazonF SxFullAccess en la Guía de referencia de políticas AWS administradas.

## AWS política gestionada: AmazonF SxConsoleFullAccess

Puede adjuntar la política de `AmazonFSxConsoleFullAccess` a las identidades de IAM.

Esta política concede permisos administrativos que permiten el acceso total a Amazon FSx y a los AWS servicios relacionados a través del. AWS Management Console

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `fsx`: permite a las entidades principales realizar todas las acciones en la consola de administración de Amazon FSx, excepto `BypassSnaplockEnterpriseRetention`.
- `cloudwatch`— Permite a los directores ver CloudWatch las alarmas y las métricas en la consola de administración de Amazon FSx.
- `ds`— Permite a los directores enumerar información sobre un directorio. AWS Directory Service
- `ec2`
  - Permite a los directores crear etiquetas en las tablas de enrutamiento, enumerar las interfaces de red, las tablas de enrutamiento, los grupos de seguridad, las subredes y la VPC asociada a un sistema de archivos Amazon FSx.
  - Permite a los directores proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una VPC.
- `kms`— Permite a los directores enumerar los alias de las claves. AWS Key Management Service
- `s3`: permite que las entidades principales creen listas de algunos o todos los objetos de un bucket de Amazon S3 (hasta 1000).
- `iam`: concede permiso para crear un rol de IAM que permite a un servicio de Amazon FSx realizar acciones en su nombre.

Para ver los permisos de esta política, consulta AmazonF SxConsoleFullAccess en la Guía de referencia de políticas AWS gestionadas.

## AWS política gestionada: AmazonF SxConsoleReadOnlyAccess

Puede adjuntar la política de `AmazonFSxConsoleReadOnlyAccess` a las identidades de IAM.

Esta política concede permisos de solo lectura a Amazon FSx y los AWS servicios relacionados para que los usuarios puedan ver información sobre estos servicios en. AWS Management Console

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `fsx`: permite que las entidades principales vean información sobre los sistemas de archivos de Amazon FSx, incluidas todas las etiquetas, en la consola de administración de Amazon FSx.
- `cloudwatch`— Permite a los directores ver CloudWatch las alarmas y las métricas en la consola de administración de Amazon FSx.
- `ds`— Permite a los directores ver información sobre un AWS Directory Service directorio en la consola de administración de Amazon FSx.
- `ec2`
  - Permite a los directores ver las interfaces de red, los grupos de seguridad, las subredes y la VPC asociada a un sistema de archivos de Amazon FSx en la consola de administración de Amazon FSx.
  - Proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una VPC.
- `kms`— Permite a los directores ver los alias de AWS Key Management Service las claves en la consola de administración de Amazon FSx.
- `log`— Permite a los directores describir los grupos de CloudWatch registros de Amazon Logs asociados a la cuenta que realiza la solicitud. Esto es necesario para que las entidades principales puedan ver la configuración existente de auditoría de acceso a archivos para un sistema de archivos de FSx para Windows File Server.
- `firehose`— Permite a los directores describir los flujos de entrega de Amazon Data Firehose asociados a la cuenta que realiza la solicitud. Esto es necesario para que las entidades principales puedan ver la configuración existente de auditoría de acceso a archivos para un sistema de archivos de FSx para Windows File Server.

Para ver los permisos de esta política, consulte AmazonF SxConsoleReadOnlyAccess en la Guía de referencia de políticas AWS gestionadas.

## AWS política gestionada: AmazonF SxReadOnlyAccess

Puede adjuntar la política de `AmazonFSxReadOnlyAccess` a las identidades de IAM.

Esta política incluye los siguientes permisos.

- `fsx`: permite que las entidades principales vean información sobre los sistemas de archivos de Amazon FSx, incluidas todas las etiquetas, en la consola de administración de Amazon FSx.
- `ec2`— Proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una VPC.

Para ver los permisos de esta política, consulte AmazonF SxReadOnlyAccess en la Guía de referencia de políticas AWS administradas.

## Amazon FSx actualiza las políticas gestionadas AWS

Consulte los detalles sobre las actualizaciones de las políticas AWS gestionadas para Amazon FSx 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 la página Historial del documento de Amazon FSx.

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| AmazonF SxServiceRolePolicy: actualización de una política existente | Amazon FSx agregó un nuevo permiso `ec2:GetSecurityGroupsForVpc` que permite a los directores proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una VPC. | 9 de enero de 2024 |
| AmazonF SxReadOnlyAccess: actualización de una política existente | Amazon FSx agregó un nuevo permiso `ec2:GetSecurityGroupsForVpc` que permite a los directores proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una VPC. | 9 de enero de 2024 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| AmazonF SxConsole ReadOnlyAccess: actualización de una política existente | Amazon FSx agregó un nuevo permiso `ec2:GetSecurityGroupsForVpc` que permite a los directores proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una VPC. | 9 de enero de 2024 |
| AmazonF SxFullAccess: actualización de una política existente | Amazon FSx agregó un nuevo permiso `ec2:GetSecurityGroupsForVpc` que permite a los directores proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una VPC. | 9 de enero de 2024 |
| AmazonF SxConsole FullAccess: actualización de una política existente | Amazon FSx agregó un nuevo permiso `ec2:GetSecurityGroupsForVpc` que permite a los directores proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una VPC. | 9 de enero de 2024 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| AmazonF SxFullAccess: actualización de una política existente | Amazon FSx agregó un nuevo permiso para permitir a los usuarios realizar la replicación de datos entre regiones y cuentas de FSx para los sistemas de archivos OpenZFS. | 20 de diciembre de 2023 |
| AmazonF SxConsole FullAccess: actualización de una política existente | Amazon FSx agregó un nuevo permiso para permitir a los usuarios realizar la replicación de datos entre regiones y cuentas de FSx para los sistemas de archivos OpenZFS. | 20 de diciembre de 2023 |
| AmazonF SxFullAccess: actualización de una política existente | Amazon FSx agregó un nuevo permiso para permitir a los usuarios realizar la replicación bajo demanda de volúmenes de FSx para sistemas de archivos OpenZFS. | 26 de noviembre de 2023 |
| AmazonFSxConsoleFu llAccess: actualización de una política existente | Amazon FSx agregó un nuevo permiso para permitir a los usuarios realizar la replicación bajo demanda de volúmenes de FSx para sistemas de archivos OpenZFS. | 26 de noviembre de 2023 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| AmazonFSxFullAccess: actualización de una política existente | Amazon FSx ha añadido nuevos permisos para que los usuarios puedan ver, activar y desactivar el soporte de VPC compartido para FSx en los sistemas de archivos Multi-AZ de ONTAP. | 14 de noviembre de 2023 |
| AmazonF SxConsole FullAccess: actualización de una política existente | Amazon FSx ha añadido nuevos permisos para que los usuarios puedan ver, activar y desactivar el soporte de VPC compartido para FSx en los sistemas de archivos Multi-AZ de ONTAP. | 14 de noviembre de 2023 |
| AmazonF SxFullAccess: actualización de una política existente | Amazon FSx añadió nuevos permisos para que Amazon FSx pueda administrar las configuraciones de red de FSx de los sistemas de archivos OpenZFS Multi-AZ. | 9 de agosto de 2023 |
| AWS política gestionada: AmazonF SxServiceRolePolicy: actualización a una política existente | Amazon FSx modificó el `cloudwatch:PutMetricData` permiso existente para que Amazon FSx publique las CloudWatch métricas en el espacio de nombres. `AWS/FSx` | 24 de julio de 2023 |
| AmazonFSxFullAccess: actualización de una política existente | Amazon FSx actualizó la política para eliminar el permiso de `fsx:*` y añadir acciones específicas de `fsx`. | 13 de julio de 2023 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| AmazonF SxConsole FullAccess: actualización a una política existente | Amazon FSx actualizó la política para eliminar el permiso de `fsx:*` y añadir acciones específicas de `fsx`. | 13 de julio de 2023 |
| AmazonF SxConsole ReadOnlyAccess: actualiza ción a una política existente | Amazon FSx añadió nuevos permisos para que los usuarios puedan ver las métricas de rendimiento mejoradas y las acciones recomendadas de los sistemas de archivos de FSx para Windows File Server en la consola de Amazon FSx. | 21 de septiembre de 2022 |
| AmazonF SxConsole FullAccess: actualización a una política existente | Amazon FSx añadió nuevos permisos para que los usuarios puedan ver las métricas de rendimiento mejoradas y las acciones recomendadas de los sistemas de archivos de FSx para Windows File Server en la consola de Amazon FSx. | 21 de septiembre de 2022 |
| AmazonF SxReadOnlyAccess — Se inició la política de seguimiento | Esta política concede acceso de solo lectura a todos los recursos de Amazon FSx y a cualquier etiqueta asociada a ellos. | 4 de febrero de 2022 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| AmazonF SxDeleteServiceLinkedRoleAccess — Se inició la política de seguimiento | Esta política concede permisos administrativos que permiten que Amazon FSx elimine el rol vinculado a servicios para el acceso a Amazon S3. | 7 de enero de 2022 |
| AmazonF SxServiceRolePolicy: actualización a una política existente | Amazon FSx ha añadido nuevos permisos que permiten a Amazon FSx gestionar las configuraciones de red de Amazon FSx para los sistemas de archivos ONTAP. NetApp | 2 de septiembre de 2021 |
| AmazonFSxFullAccess: actualización de una política existente | Amazon FSx añadió nuevos permisos para que Amazon FSx cree etiquetas en las tablas de enrutamiento de EC2 para llamadas restringidas. | 2 de septiembre de 2021 |
| AmazonF SxConsoleFullAccess: actualización a una política existente | Amazon FSx ha añadido nuevos permisos para permitir a Amazon FSx crear Amazon FSx para los sistemas de archivos Multi-AZ de ONTAP. NetApp | 2 de septiembre de 2021 |
| AmazonF SxConsoleFullAccess: actualización de una política existente | Amazon FSx añadió nuevos permisos para que Amazon FSx cree etiquetas en las tablas de enrutamiento de EC2 para llamadas restringidas. | 2 de septiembre de 2021 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| AmazonF SxServiceRolePolicy: actualización a una política existente | Amazon FSx ha añadido nuevos permisos para permitir a Amazon FSx describir y escribir en las secuencias de registros. CloudWatch<br><br>Esto es necesario para que los usuarios puedan ver los registros de auditoría de acceso a los archivos de los sistemas de archivos FSx for Windows File Server CloudWatch mediante registros. | 8 de junio de 2021 |
| AmazonF SxServiceRolePolicy: actualización de una política existente | Amazon FSx ha añadido nuevos permisos para permitir a Amazon FSx describir y escribir en las transmisiones de entrega de Amazon Data Firehose.<br><br>Esto es necesario para que los usuarios puedan ver los registros de auditoría de acceso a los archivos de un sistema de archivos FSx for Windows File Server mediante Amazon Data Firehose. | 8 de junio de 2021 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| AmazonF SxFullAccess: actualización a una política existente | Amazon FSx agregó nuevos permisos para permitir a los directores describir y crear grupos de CloudWatch registros, flujos de registro y escribir eventos en flujos de registro.<br><br>Esto es necesario para que los directores puedan ver los registros de auditoría de acceso a los archivos de los sistemas CloudWatch de archivos FSx for Windows File Server mediante registros. | 8 de junio de 2021 |
| AmazonF SxFullAccess: actualización de una política existente | Amazon FSx ha añadido nuevos permisos para permitir a los directores describir y escribir registros en una Amazon Data Firehose.<br><br>Esto es necesario para que los usuarios puedan ver los registros de auditoría de acceso a los archivos de un sistema de archivos FSx for Windows File Server mediante Amazon Data Firehose. | 8 de junio de 2021 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| AmazonF SxConsole FullAccess: actualización a una política existente | Amazon FSx ha añadido nuevos permisos para que los directores puedan describir los grupos de CloudWatch registros de Amazon Logs asociados a la cuenta que realiza la solicitud.<br><br>Esto es necesario para que los directores puedan elegir un grupo de CloudWatch registros existente al configura r la auditoría de acceso a los archivos para un sistema de archivos FSx for Windows File Server. | 8 de junio de 2021 |
| AmazonF SxConsole FullAccess: actualización a una política existente | Amazon FSx ha añadido nuevos permisos para que los directores puedan describir las transmisiones de entrega de Amazon Data Firehose asociadas a la cuenta que realiza la solicitud.<br><br>Esto es necesario para que los directores puedan elegir un flujo de entrega de Firehose existente al configurar la auditoría de acceso a los archivos para un sistema de archivos FSx for Windows File Server. | 8 de junio de 2021 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| AmazonF SxConsole ReadOnlyAccess: actualización a una política existente | Amazon FSx ha añadido nuevos permisos para que los directores puedan describir los grupos de CloudWatch registros de Amazon Logs asociados a la cuenta que realiza la solicitud.<br><br>Esto es necesario para que las entidades principales puedan ver la configuración existente de auditoría de acceso a archivos para un sistema de archivos de FSx para Windows File Server. | 8 de junio de 2021 |
| AmazonF SxConsole ReadOnlyAccess: actualización de una política existente | Amazon FSx ha añadido nuevos permisos para que los directores puedan describir las transmisiones de entrega de Amazon Data Firehose asociadas a la cuenta que realiza la solicitud.<br><br>Esto es necesario para que las entidades principales puedan ver la configuración existente de auditoría de acceso a archivos para un sistema de archivos de FSx para Windows File Server. | 8 de junio de 2021 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Amazon FSx inició un seguimiento de los cambios | Amazon FSx comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas. | 8 de junio de 2021 |

## Solución de problemas de acceso e identidad de Amazon FSx para Lustre

Utilice la siguiente información para diagnosticar y solucionar los problemas habituales que pueden surgir cuando se trabaja con Amazon FSx e IAM.

Temas

- No tengo autorización para realizar una acción en Amazon FSx
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir a personas externas a mi Cuenta de AWS el acceso a mis recursos de Amazon FSx

### No tengo autorización para realizar una acción en Amazon FSx

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `fsx:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fsx:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `fsx:`*`GetWidget`*.

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.

## No estoy autorizado a realizar tareas como: PassRole

Si recibe un error que indica que no tiene autorización para llevar a cabo la acción `iam:PassRole`, las políticas se deben actualizar para permitirle pasar un rol a Amazon FSx.

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 FSx. 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 FSx

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 FSx admite estas características, consulte Cómo funciona Amazon FSx para Lustre con IAM.
- Para obtener información sobre 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 tus 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 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.

## Uso de etiquetas con Amazon FSx

Puede utilizar etiquetas para controlar el acceso a los recursos de Amazon FSx e implementar el control de acceso basado en atributos (ABAC). Para aplicar etiquetas a los recursos de Amazon FSx durante la creación, los usuarios deben tener determinados permisos IAM AWS Identity and Access Management.

### Conceder permisos para etiquetar recursos durante la creación

Con algunas acciones del API de creación de recursos de Amazon FSx para Lustre, puede especificar etiquetas al crear el recurso. Puede utilizar estas etiquetas de recursos para implementar el control de acceso basado en atributos (ABAC). Para obtener más información, consulte ¿Qué es ABAC para AWS? en la Guía del usuario de IAM.

Para que los usuarios puedan etiquetar recursos durante su creación, deben tener permiso para utilizar la acción que crea el recurso, como `fsx:CreateFileSystem`. Si se especifican etiquetas en la acción de creación de recursos, IAM realiza una autorización adicional en la acción `fsx:TagResource` para verificar que los usuarios tengan permisos para crear etiquetas. Por lo tanto, los usuarios también deben tener permisos explícitos para usar la acción `fsx:TagResource`.

La siguiente directiva de ejemplo permite a los usuarios crear sistemas de archivos y aplicarles etiquetas durante la creación en una Cuenta de AWS determinada.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateFileSystem",
```

```
            "fsx:TagResource"
         ],
         "Resource": [
            "arn:aws:fsx:region:account-id:file-system/*"
         ]
      }
   ]
}
```

De la misma manera, la siguiente política permite que los usuarios creen copias de seguridad en un sistema de archivos específico, y apliquen cualquier etiqueta a la copia de seguridad durante la creación de la copia de seguridad.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateBackup"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/file-system-id*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:backup/*"
    }
  ]
}
```

La acción `fsx:TagResource` solo se evalúa si se aplican etiquetas durante la acción de creación de recursos. Por lo tanto, un usuario que tenga permisos para crear un recurso (suponiendo que no existan condiciones de etiquetado) no necesita permiso para utilizar la acción `fsx:TagResource` si no se especifica ninguna etiqueta en la solicitud. Sin embargo, si el usuario intenta crear un recurso con etiquetas, la solicitud dará un error si el usuario no tiene permisos para utilizar la acción `fsx:TagResource`.

Para obtener más información acerca del etiquetado de recursos de Amazon FSx, consulte Etiquetar los recursos de Amazon FSx. Para obtener más información sobre el uso de etiquetas para controlar

el acceso a los recursos de Amazon FSx para Lustre, consulte Uso de etiquetas para controlar el acceso a los recursos de Amazon FSx .

## Uso de etiquetas para controlar el acceso a los recursos de Amazon FSx

Para controlar el acceso a los recursos y las acciones de Amazon FSx, puede utilizar políticas de (IAM) basadas en etiquetas. Puede proporcionar este control de dos maneras:

- Puede controlar el acceso a los recursos de Amazon FSx basándose en las etiquetas de dichos recursos.
- Puede controlar qué etiquetas se pueden pasar en una condición de solicitud IAM.

Para obtener más información sobre el uso de etiquetas para controlar el acceso a los recursos de AWS, consulte Control del acceso mediante el uso de etiquetas en la Guía del usuario de IAM. Para obtener más información acerca del etiquetado de recursos de Amazon FSx en la creación, consulte Conceder permisos para etiquetar recursos durante la creación. Para obtener más información acerca del etiquetado de recursos, consulte Etiquetar los recursos de Amazon FSx.

Control del acceso a un recurso en función de las etiquetas

Para controlar qué acciones puede realizar un usuario o rol en un recurso de Amazon FSx, puede utilizar etiquetas en el recurso. Por ejemplo, es posible que desee permitir o denegar acciones de la API específicas en un recurso del sistema de archivos en función del par clave-valor de la etiqueta del recurso.

Example Política de ejemplo: crear un sistema de archivos al proporcionar una etiqueta específica

Esta política permite que el usuario cree un sistema de archivos solo cuando lo etiqueta con un par clave-valor específico, en este ejemplo, `key=Department, value=Finance`.

```
{
    "Effect": "Allow",
    "Action": [
        "fsx:CreateFileSystem",
        "fsx:TagResource"
    ],
    "Resource": "arn:aws:fsx:region:account-id:file-system/*",
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/Department": "Finance"
```

```
        }
    }
}
```

Example Política de ejemplo: crear copias de seguridad únicamente de los sistemas de archivos con una etiqueta específica

Esta política permite que los usuarios creen copias de seguridad únicamente de los sistemas de archivos que estén etiquetados con el par clave-valor `key=Department, value=Finance`, y la copia de seguridad se creará con la etiqueta `Deparment=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }

    ]
}
```

Example Política de ejemplo: crear un sistema de archivos con una etiqueta específica a partir de copias de seguridad que tengan una etiqueta específica

Esta política permite que los usuarios creen sistemas de archivos que tengan la etiqueta `Department=Finance` únicamente a partir de copias de seguridad etiquetadas con `Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateFileSystemFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateFileSystemFromBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example Política de ejemplo: eliminar los sistemas de archivos con etiquetas específicas

Esta política permite que un usuario elimine únicamente los sistemas de archivos que estén etiquetados con `Department=Finance`. Si crea una copia de seguridad final, debe etiquetarla con

`Department=Finance`. Para los sistemas de archivos Lustre, los usuarios necesitan el privilegio `fsx:CreateBackup` para crear la copia de seguridad final.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteFileSystem"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example Ejemplo de política: crear tareas de repositorio de datos en sistemas de archivos con una etiqueta específica

Esta política permite a los usuarios crear tareas de repositorio de datos etiquetadas con `Department=Finance`, y solo en sistemas de archivos etiquetados con `Department=Finance`.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateDataRepositoryTask"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateDataRepositoryTask",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:task/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

## Uso de roles vinculados a servicios para Amazon FSx

Amazon FSx utiliza funciones vinculadas a AWS Identity and Access Management servicios (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que se encuentra vinculado directamente a Amazon FSx. Amazon FSx predefine las funciones vinculadas al servicio e incluyen todos los permisos que el servicio necesita para llamar a otros AWS servicios en su nombre.

Un rol vinculado al servicio simplifica la configuración de Amazon FSx, porque ya no tendrá que agregar manualmente los permisos requeridos. Amazon FSx define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo Amazon FSx puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. De esta forma, se protegen los recursos de Amazon FSx, ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Para obtener información sobre otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Roles vinculados a servicios. Seleccione una opción Sí con un enlace para ver la documentación sobre el rol vinculado al servicio en cuestión.

## Permisos de roles vinculados a servicios para Amazon FSx

Amazon FSx utiliza dos funciones vinculadas a servicios denominadas `AWSServiceRoleForAmazonFSx` y `AWSServiceRoleForFSxS3Access_`*`fs-01234567890`* que realizan determinadas acciones en su cuenta. Algunos ejemplos de estas acciones son la creación de interfaces de red elásticas para sus sistemas de archivos en su VPC y el acceso a su repositorio de datos en un bucket de Amazon S3. Para `AWSServiceRoleForFSxS3Access_`*`fs-01234567890`*, este rol vinculado a un servicio se crea para cada sistema de archivos Amazon FSx para Lustre que cree y que esté vinculado a un bucket de S3.

AWSServiceRoleForAmazonFSx detalles de permisos

`AWSServiceRoleForAmazonFSx`En efecto, la política de permisos de roles permite a Amazon FSx realizar las siguientes acciones administrativas en nombre del usuario en todos los recursos aplicables AWS :

Para ver las actualizaciones de esta política, consulte AmazonF SxServiceRolePolicy

> **Note**
>
> Lo AWSServiceRoleForAmazonFSx utilizan todos los tipos de sistemas de archivos de Amazon FSx; algunos de los permisos enumerados no se aplican a FSx for Lustre.

- `ds`— Permite a Amazon FSx ver, autorizar y desautorizar las aplicaciones de su directorio. AWS Directory Service
- `ec2`: permite a Amazon FSx realizar lo siguiente:
  - Ver, crear y desasociar las interfaces de red asociadas a un sistema de archivos Amazon FSx.
  - Ver una o varias direcciones IP elásticas asociadas a un sistema de archivos de Amazon FSx.

  - Ver las VPC de Amazon, los grupos de seguridad y las subredes asociadas a un sistema de archivos de Amazon FSx.
  - Proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una VPC.
  - Cree un permiso para que un usuario AWS autorizado realice determinadas operaciones en una interfaz de red.
- `cloudwatch`— Permite a Amazon FSx publicar puntos de datos métricos en el espacio de nombres CloudWatch AWS /FSx.
- `route53`: permite que Amazon FSx asocie una Amazon VPC con una zona alojada privada.
- `logs`— Permite a Amazon FSx describir y escribir en los flujos de registro de CloudWatch Logs. Esto permite a los usuarios enviar los registros de auditoría de acceso a los archivos de un sistema de archivos FSx for Windows File Server a CloudWatch una secuencia de registros.
- `firehose`— Permite a Amazon FSx describir y escribir en las transmisiones de entrega de Amazon Data Firehose. Esto permite a los usuarios publicar los registros de auditoría de acceso a los archivos de un sistema de archivos FSx for Windows File Server en una transmisión de entrega de Amazon Data Firehose.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateFileSystem",
            "Effect": "Allow",
            "Action": [
                "ds:AuthorizeApplication",
                "ds:GetAuthorizedApplicationDetails",
                "ds:UnauthorizeApplication",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAddresses",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVPCs",
                "ec2:DisassociateAddress",
```

```
                "ec2:GetSecurityGroupsForVpc",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PutMetrics",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/FSx"
                }
            }
        },

        {
            "Sid": "TagResourceNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "AmazonFSx.FileSystemId"
                }
            }
        },
        {
            "Sid": "ManageNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
```

```
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
                }
            }
        },
        {
            "Sid": "ManageRouteTable",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
                }
            }
        },
        {
            "Sid": "PutCloudWatchLogs",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/fsx/*"
        },
        {
            "Sid": "ManageAuditLogs",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
```

```
                "firehose:PutRecord",
                "firehose:PutRecordBatch"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
        }
    ]
}
```

Todas las actualizaciones de esta política están detalladas en Amazon FSx actualiza las políticas gestionadas AWS.

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

AWSServiceRoleForFSxS3Access detalles de permisos

En efecto`AWSServiceRoleForFSxS3Access_`*`file-system-id`*, la política de permisos de funciones permite a Amazon FSx realizar las siguientes acciones en un bucket de Amazon S3 que aloja el repositorio de datos de un sistema de archivos Amazon FSx for Lustre.

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:Get*`
- `s3:List*`
- `s3:PutBucketNotification`
- `s3:PutObject`

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

## Creación de un rol vinculado a un servicio para Amazon FSx

No necesita crear manualmente un rol vinculado a servicios. Al crear un sistema de archivos en la AWS Management Console AWS CLI, la o la AWS API, Amazon FSx crea automáticamente el rol vinculado al servicio.

> **Important**
>
> Este rol vinculado a servicios puede aparecer en su cuenta si se ha completado una acción en otro servicio que utilice las características compatibles con este rol. Para obtener más información, consulte Un nuevo rol ha aparecido en mi cuenta de IAM.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al crear un sistema de archivos, Amazon FSx vuelve a crear el rol vinculado al servicio por usted.

## Edición de un rol vinculado a servicios para Amazon FSx

Amazon FSx no le permite editar estas funciones vinculadas a servicios. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

## Eliminación de un rol vinculado a un servicio para Amazon FSx

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Sin embargo, debe eliminar todos los sistemas de archivo y copias de seguridad para poder eliminar el rol vinculado al servicio de forma manual.

> **Note**
>
> Si el servicio de Amazon FSx utiliza el rol al intentar eliminar los recursos, se podría generar un error en la eliminación. En tal caso, espere unos minutos e intente de nuevo la operación.

Cómo eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM, la CLI de IAM o la API de IAM para eliminar el rol vinculado a servicios AWSServiceRoleForAmazonFSx. Para más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

### Regiones admitidas para los roles vinculados al servicio de Amazon FSx

Amazon FSx admite el uso de roles vinculados al servicio en todas las regiones en las que se encuentra disponible el servicio. Para obtener más información, consulte Regiones y puntos de conexión de AWS.

## Control de acceso al sistema de archivos con Amazon VPC

Se puede acceder a un sistema de archivos de Amazon FSx a través de una interfaz de red elástica que reside en la nube privada virtual (VPC) basada en el servicio Amazon VPC que asocie a su sistema de archivos. El acceso al sistema de archivos Amazon FSx se realiza a través de su nombre DNS, que se asigna a la interfaz de red del sistema de archivos. Solo los recursos dentro de la VPC asociada, o una VPC interconectada, pueden obtener acceso a la interfaz de red de su sistema de archivos. Para obtener más información, consulte ¿Qué es Amazon VPC? en la Guía del usuario de Amazon VPC.

> **Warning**
>
> No debe modificar ni eliminar la interfaz de red elástica de Amazon FSx. Si se modifica o elimina la interfaz de red, se puede provocar una pérdida permanente de la conexión entre la VPC y el sistema de archivos.

### Grupos de seguridad de Amazon VPC

Para controlar aún más el tráfico de red que pasa por la interfaz de red de su sistema de archivos dentro de su VPC, utilice grupos de seguridad para limitar el acceso a sus sistemas de archivos. Un grupo de seguridad actúa como un firewall virtual para controlar el tráfico de sus recursos asociados. En este caso, el recurso asociado es la interfaz de red de su sistema de archivos. También utiliza grupos de seguridad de VPC para controlar el tráfico de red de sus clientes de Lustre.

#### Controlar el acceso mediante reglas de entrada y salida

Para utilizar un grupo de seguridad para controlar el acceso a su sistema de archivos Amazon FSx y clientes Lustre, añada las reglas de entrada para controlar el tráfico entrante y las reglas de salida para controlar el tráfico saliente de su sistema de archivos y clientes Lustre. Asegúrese de que dispone de las reglas de tráfico de red adecuadas en su grupo de seguridad para asignar el recurso

compartido de archivos de su sistema de archivos de Amazon FSx a una carpeta de su instancia de computación compatible.

Para obtener más información sobre las reglas del grupo de seguridad, consulte las Reglas del grupo de seguridad en la Guía del usuario de Amazon EC2 para instancias de Linux.

Para crear un grupo de seguridad para su sistema de archivos Amazon FSx

1. Abra la consola Amazon EC2 en https://console.aws.amazon.com/ec2.
2. En el panel de navegación, elija Grupos de seguridad.
3. Elija Crear grupo de seguridad.
4. Especifique un nombre y una descripción para el grupo de seguridad.
5. Para la VPC, elija la VPC asociada a su sistema de archivos Amazon FSx para crear el grupo de seguridad dentro de esa VPC.
6. Para crear el grupo de seguridad, haga clic en Crear.

A continuación, añada reglas de entrada al grupo de seguridad que acaba de crear para permitir el tráfico Lustre entre sus servidores de archivos FSx para Lustre.

Para agregar reglas de entrada a su grupo de seguridad

1. Seleccione el grupo de seguridad que acaba de crear si aún no está seleccionado. En Acciones, elija Editar reglas de entrada.
2. Agregue las siguientes reglas de entrada.

| Tipo | Protocolo | Rango de puertos | Origen | Descripción |
|---|---|---|---|---|
| Regla TCP personalizada | TCP | 988 | Elija Personalizado e introduzca el ID del grupo de seguridad que acaba de crear | Permite el tráfico de Lustre entre FSx para los servidores de archivos de Lustre |
| Regla TCP personalizada | TCP | 988 | Elija Personalizar e introduzca | Permite el tráfico de Lustre |

| Tipo | Protocolo | Rango de puertos | Origen | Descripción |
|---|---|---|---|---|
| | | | los ID de grupo de seguridad de los grupos de seguridad asociados a los clientes de Lustre | entre servidores de archivos FSx para Lustre y clientes Lustre |
| Regla TCP personalizada | TCP | 1018-1023 | Elija Personalizado e introduzca el ID del grupo de seguridad que acaba de crear | Permite el tráfico de Lustre entre FSx para los servidores de archivos de Lustre |
| Regla TCP personalizada | TCP | 1018-1023 | Elija Personalizar e introduzca los ID de grupo de seguridad de los grupos de seguridad asociados a los clientes de Lustre | Permite el tráfico de Lustre entre servidores de archivos FSx para Lustre y clientes Lustre |

3. Seleccione Guardar para guardar y aplicar las nuevas reglas de entrada.

De forma predeterminada, las reglas del grupo de seguridad permiten todo el tráfico saliente (Todos, 0.0.0.0/0). Si su grupo de seguridad no permite todo el tráfico saliente, agregue las siguientes reglas salientes a su grupo de seguridad. Estas reglas permiten el tráfico entre servidores de archivos FSx para Lustre y clientes Lustre, y entre servidores de archivos Lustre.

Para agregar reglas de salida a su grupo de seguridad

1. Elija el mismo grupo de seguridad al que acaba de añadir las reglas de entrada. En Acciones, elija Editar reglas de salida.
2. Agregue las siguientes reglas de salida.

| Tipo | Protocolo | Rango de puertos | Origen | Descripción |
|---|---|---|---|---|
| Regla TCP personalizada | TCP | 988 | Elija Personalizado e introduzca el ID del grupo de seguridad que acaba de crear | Permite el tráfico de Lustre entre FSx para los servidores de archivos de Lustre |
| Regla TCP personalizada | TCP | 988 | Elija Personalizar e introduzca los ID de grupo de seguridad del grupo de seguridad asociado a los clientes de Lustre | Permite el tráfico de Lustre entre servidores de archivos FSx para Lustre y clientes Lustre |
| Regla TCP personalizada | TCP | 1018-1023 | Elija Personalizado e introduzca el ID del grupo de seguridad que acaba de crear | Permite el tráfico de Lustre entre FSx para los servidores de archivos de Lustre |
| Regla TCP personalizada | TCP | 1018-1023 | Elija Personalizar e introduzca los ID de grupo de seguridad | Permite el tráfico de Lustre entre servidores de archivos |

| Tipo | Protocolo | Rango de puertos | Origen | Descripción |
|---|---|---|---|---|
| | | | de los grupos de seguridad asociados a los clientes de Lustre | FSx para Lustre y clientes Lustre |

3. Seleccione Guardar para guardar y aplicar las nuevas reglas de salida.

Asociar el grupo de seguridad a su sistema de archivos de Amazon FSx

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel de control de la consola, elija su sistema de archivos para ver sus detalles.
3. En la pestaña Red y seguridad, elija los identificadores de interfaz de red de su sistema de archivos (por ejemplo, `ENI-0123456789012345`6). De este modo, se redirigirá a la consola de Amazon EC2.
4. Elija cada ID de interfaz de red. Cada acción abre una instancia nueva de la consola de Amazon EC2 en el navegador. Para cada grupo de seguridad, seleccione Modificar grupos de seguridad para Acciones.
5. En el cuadro de diálogo Cambiar grupos de seguridad, elija los grupos de seguridad que desee utilizar y seleccione Guardar.

## Reglas del grupo de seguridad de VPC del cliente Lustre

Puede utilizar los grupos de seguridad de la VPC para controlar el acceso a sus clientes Lustre añadiendo reglas de entrada para controlar el tráfico entrante y reglas de salida para controlar el tráfico saliente de sus clientes Lustre. Asegúrese de tener las reglas de tráfico de red adecuadas en su grupo de seguridad para garantizar que el tráfico Lustre pueda fluir entre sus clientes Lustre y sus sistemas de archivos de Amazon FSx.

Agregue las siguientes reglas de entrada a los grupos de seguridad aplicados a sus clientes Lustre.

| Tipo | Protocolo | Rango de puertos | Origen | Descripción |
|---|---|---|---|---|
| Regla TCP personalizada | TCP | 988 | Elija Personalizado e introduzca los ID de los grupos de seguridad que se aplican a sus clientes Lustre | Permite el tráfico de Lustre entre los clientes de Lustre |
| Regla TCP personalizada | TCP | 988 | Elija Personalizado e introduzca los ID de los grupos de seguridad asociados a sus sistemas de archivo FSx para Lustre | Permite el tráfico de Lustre entre servidores de archivos FSx para Lustre y clientes Lustre |
| Regla TCP personalizada | TCP | 1018-1023 | Elija Personalizado e introduzca los ID de los grupos de seguridad que se aplican a sus clientes Lustre | Permite el tráfico de Lustre entre los clientes de Lustre |
| Regla TCP personalizada | TCP | 1018-1023 | Elija Personalizado e introduzca los ID de los grupos de seguridad asociados a sus sistemas de | Permite el tráfico de Lustre entre servidores de archivos FSx para Lustre y clientes Lustre |

| Tipo | Protocolo | Rango de puertos | Origen | Descripción |
|---|---|---|---|---|
| | | | archivo FSx para Lustre | |

Agregue las siguientes reglas de salida a los grupos de seguridad aplicados a sus clientes Lustre.

| Tipo | Protocolo | Rango de puertos | Origen | Descripción |
|---|---|---|---|---|
| Regla TCP personalizada | TCP | 988 | Elija Personalizado e introduzca los ID de los grupos de seguridad que se aplican a sus clientes Lustre | Permite el tráfico de Lustre entre los clientes de Lustre |
| Regla TCP personalizada | TCP | 988 | Elija Personalizado e introduzca los ID de los grupos de seguridad asociados a sus sistemas de archivo FSx para Lustre | Permite el tráfico de Lustre entre servidores de archivos FSx para Lustre y clientes Lustre |
| Regla TCP personalizada | TCP | 1018-1023 | Elija Personalizado e introduzca los ID de los grupos de seguridad que se aplican a sus clientes Lustre | Permite el tráfico de Lustre entre los clientes de Lustre |

| Tipo | Protocolo | Rango de puertos | Origen | Descripción |
|---|---|---|---|---|
| Regla TCP personalizada | TCP | 1018-1023 | Elija Personalizado e introduzca los ID de los grupos de seguridad asociados a sus sistemas de archivo FSx para Lustre | Permite el tráfico de Lustre entre servidores de archivos FSx para Lustre y clientes Lustre |

## ACL de la red de Amazon VPC

Otra opción para proteger el acceso al sistema de archivos de la VPC es establecer listas de control de acceso de la red (ACL de la red). Si bien las ACL de la red funcionan de forma separada de los grupos de seguridad, tienen funciones similares para añadir una capa de seguridad adicional a los recursos de la VPC. Para obtener más información sobre la implementación del control de acceso mediante ACL de red, consulte Controlar el tráfico hacia las subredes utilizando las ACL de red en la Guía del usuario de Amazon VPC.

## Validación de la conformidad de Amazon FSx para Lustre

Para saber si un Servicio de AWS está incluido en el ámbito de programas de conformidad específicos, consulte Servicios de AWS en el ámbito del programa de conformidad y elija el programa de conformidad que le interese. Para obtener información general, consulte Programas de conformidad de AWS.

Puede descargar los informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact.

Su responsabilidad de conformidad al utilizar servicios de AWS se determina en función de la sensibilidad de los datos, los objetivos de cumplimiento de su empresa y la legislación y los reglamentos correspondientes. AWS proporciona los siguientes recursos para ayudar con la conformidad:

- Guías de inicio rápido de seguridad y conformidad: estas guías de implementación tratan consideraciones sobre arquitectura y ofrecen pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- Architecting for HIPAA Security and Compliance on Amazon Web Services (Arquitectura para la seguridad y el cumplimiento de la HIPAA en Amazon Web Services): en este documento técnico, se describe cómo las empresas pueden utilizar AWS para crear aplicaciones aptas para HIPAA.

> **Note**
>
> No todos los Servicios de AWS son aptos para HIPAA. Para obtener más información, consulte la Referencia de servicios aptos para HIPAA.

- Recursos de conformidad de AWS: este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- AWSGuías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde la perspectiva del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad de Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Normas y Tecnología (NIST), el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de recursos con reglas en la Guía para desarrolladores de AWS Config: el servicio AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub: este servicio de AWS proporciona una visión completa de su estado de seguridad en 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.
- AWS Audit Manager: este Servicio de AWS le ayuda a auditar continuamente el uso de AWS con el fin de simplificar la forma en que administra el riesgo y la conformidad con las normativas y los estándares del sector.

# Amazon FSx para Lustre y Puntos de conexión de VPC de interfaz (AWS PrivateLink)

Puede mejorar la postura de seguridad de su VPC configurando Amazon FSx para que utilice un punto de conexión de VPC de interfaz. Los puntos de conexión de la interfaz cuentan con AWS PrivateLink, una tecnología que permite acceder de forma privada a las API de Amazon FSx sin necesidad de contar con una puerta de enlace de Internet, un dispositivo NAT, una conexión VPN o una conexión de AWS Direct Connect. Las instancias de la VPC no necesitan direcciones IP públicas para comunicarse con las API de Amazon FSx. El tráfico entre la VPC y Amazon FSx no sale de la red AWS.

Cada punto de conexión de VPC de la interfaz está representado por una o más interfaces de red elásticas en las subredes. Una interfaz de red proporciona una dirección IP privada que sirve como punto de entrada del tráfico dirigido a la API de Amazon FSx.

## Consideraciones sobre los puntos de conexión de VPC de interfaz para Amazon FSx

Antes de configurar un punto de conexión de VPC de interfaz para Amazon FSx, revise el tema Propiedades y limitaciones de los puntos de conexión de interfaz en la Guía del usuario de Amazon VPC.

Puede llamar a cualquiera de las operaciones de API de Amazon FSx desde su VPC. Por ejemplo, puede crear un sistema de archivos FSx para Lustre llamando a la API CreateFileSystem desde su VPC. Para ver la lista completa de las API de Amazon FSx, consulte Actions (Acciones) en la Referencia de las API de Amazon FSx.

### Consideraciones sobre la interconexión de VPC

Puede conectar una VPC a otra con puntos de conexión VPC de interfaz usando la interconexión de VPC. La interconexión de VPC es una conexión de red entre dos VPC. Puede establecer una conexión de emparejamiento de VPC entre dos VPC propias o con una VPC en otra Cuenta de AWS. Las VPC también pueden estar en dos Regiones de AWS diferentes.

El tráfico entre las VPC interconectadas permanece en la red de AWS y no pasa por la red pública de Internet. Una vez que las VPC están interconectadas, algunos recursos como las instancias de

Amazon Elastic Compute Cloud (Amazon EC2) en ambas VPC pueden obtener acceso a la API de Amazon FSx a través de puntos de conexión de VPC de interfaz creados en una de las VPC.

## Creación de un punto de conexión de VPC de interfaz para API de Amazon FSx

Puede crear un punto de conexión de VPC para la API de Amazon FSx mediante la consola de Amazon VPC o desde AWS Command Line Interface (AWS CLI). Para obtener más información, consulte Creación de un punto de conexión de VPC de interfaz en la Guía del usuario de Amazon VPC.

Para obtener una lista completa de los puntos de conexión de Amazon FSx, consulte Puntos de conexión y cuotas de Amazon FSx en la Referencia general de Amazon Web Services.

Para crear un punto de conexión de VPC de interfaz para Amazon FSx, utilice una de las siguientes opciones:

- **`com.amazonaws.`*`region`*`.fsx`** – Crea un punto de conexión para las operaciones de la API de Amazon FSx.
- **`com.amazonaws.`*`region`*`.fsx-fips`** – Crea un punto de conexión para la API de Amazon FSx que cumple con el Estándar federal de procesamiento de información (FIPS) 140-2.

Para utilizar la opción de DNS privado, debe configurar los atributos `enableDnsHostnames` y `enableDnsSupport` de su VPC. Para obtener más información, consulte Viewing and updating DNS support for your VPC (Visualización y actualización de la compatibilidad de DNS para su VPC) en la Guía del usuario de Amazon VPC.

Salvo en Regiones de AWS en China, si habilita un DNS privado para el punto de conexión, podrá realizar solicitudes de la API a Amazon FSx con el punto de conexión de VPC mediante el nombre de DNS predeterminado para la Región de AWS, por ejemplo `fsx.us-east-1.amazonaws.com`. En las Regiones de AWS de China (Pekín) y China (Ningxia), puede realizar solicitudes de la API con el punto de conexión de VPC mediante `fsx-api.cn-north-1.amazonaws.com.cn` y `fsx-api.cn-northwest-1.amazonaws.com.cn`, respectivamente.

Para obtener más información, consulte Acceso a un servicio a través de un punto de conexión de VPC de interfaz en la Guía del usuario de Amazon VPC.

# Creación de una política de punto de conexión de VPC para Amazon FSx

Para controlar aún más el acceso a la API de Amazon FSx, puede adjuntar opcionalmente una política de AWS Identity and Access Management (IAM) a su punto de conexión de VPC. La política especifica lo siguiente:

- La entidad de seguridad que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos en los que se pueden llevar a cabo las acciones.

Para obtener más información, consulte Control del acceso a los servicios con puntos de conexión de VPC en la Guía del usuario de Amazon VPC.

# Cuotas

A continuación, puede obtener información acerca de las cuotas a la hora de trabajar con Amazon FSx para Lustre.

Temas



## Cuotas que puede aumentar

A continuación, se indican las cuotas de Amazon FSx para Lustre por cuenta AWS, por Región AWS, que puede aumentar.

| Resource | Predeterminado | Descripción |
|---|---|---|
| Sistemas de archivos Lustre Persistent_1 | 100 | El número máximo de sistemas de archivos de Amazon FSx para Lustre Persistent_1 que puede crear en esta cuenta. |
| Sistemas de archivos Lustre Persistent_2 | 100 | El número máximo de sistemas de archivos de Amazon FSx para Lustre Persistent_2 que puede crear en esta cuenta. |
| Capacidad de almacenamiento HDD persistente de Lustre (por sistema de archivos) | 102000 | La cantidad máxima de capacidad de almacenamiento HDD (en GiB) que puede configurar para un sistema de archivos persistente Amazon FSx para Lustre. |

| Resource | Predeterminado | Descripción |
| --- | --- | --- |
| Capacidad de almacenamiento de archivos Lustre Persistent_1 | 100800 | La cantidad máxima de capacidad de almacenamiento (en GiB) que puede configurar para todos los sistemas de archivos de Amazon FSx para Lustre Persistent_1 en esta cuenta. |
| Capacidad de almacenamiento de archivos Lustre Persistent_2 | 100800 | La cantidad máxima de capacidad de almacenamiento (en GiB) que puede configurar para todos los sistemas de archivos de Amazon FSx para Lustre Persistent_2 en esta cuenta. |
| Sistemas de archivos Lustre Scratch | 100 | La cantidad máxima de sistemas de archivos Scratch de Amazon FSx para Lustre que puede crear en esta cuenta. |
| Capacidad de almacenamiento de Lustre Scratch | 100800 | La cantidad máxima de capacidad de almacenamiento (en GiB) que puede configurar para todos los sistemas de archivos de Amazon FSx para Lustre Scratch en esta cuenta. |
| Copias de seguridad Lustre | 500 | El número máximo de copias de seguridad iniciados por el usuario que puede tener para todos los sistemas de archivos de Amazon FSx para Lustre en esta cuenta. |

Para solicitar un aumento de cuota

1. Abra la consola de Service Quotas de .
2. En el panel de navegación, elija Servicios de AWS.
3. Elija Amazon FSx.
4. Elija una cuota.
5. Seleccione Solicitar aumento de cuota y siga las instrucciones para solicitar un aumento de cuota.
6. Para ver el estado de la solicitud de cuota, seleccione Historial de solicitudes de cuota en el panel de navegación de la consola.

Para obtener más información, consulte Solicitud de un aumento de cuota en la Guía del usuario de Service Quotas.

## Cuotas de recursos para cada sistema de archivos

Los siguientes son los límites de los recursos de Amazon FSx para Lustre para cada sistema de archivos de una región AWS.

| Resource | Límite por sistema de archivos |
|---|---|
| Número máximo de etiquetas | 50 |
| Período máximo de retención para las copias de seguridad automatizadas | 90 días |
| Número máximo de solicitudes de copia de seguridad en curso a una única Región de destino por cuenta. | 5 |
| Número de actualizaciones de archivos desde un bucket de S3 vinculado por sistemas de archivos | 10 millones / mes |
| Capacidad mínima de almacenamiento, sistemas de archivos SSD | 1,2 TiB |
| Capacidad mínima de almacenamiento, sistemas de archivos HDD | 6 TiB |

| Resource | Límite por sistema de archivos |
| --- | --- |
| Rendimiento mínimo por unidad de almacenamiento, SSD | 50 MBps |
| Rendimiento máximo por unidad de almacenamiento, SSD | 1000 MBps |
| Rendimiento mínimo por unidad de almacenamiento, HDD | 12 MBps |
| Rendimiento máximo por unidad de almacenamiento, HDD | 40 MBps |

## Consideraciones adicionales

Además, tenga en cuenta lo siguiente:

- Puede utilizar cada clave AWS Key Management Service (AWS KMS) en un máximo de 125 sistemas de archivos de Amazon FSx para Lustre.
- Para obtener una lista de las regiones AWS en las que puede crear sistemas de archivos, consulte los Puntos de conexión y cuotas de Amazon FSx en Referencia general de AWS.

# Resolución de problemas

Utilice la información siguiente para resolver los problemas que es posible que surjan cuando trabaje con los sistemas de archivos de Amazon FSx para Lustre.

Si tiene problemas que no aparecen en la siguiente lista, haga una pregunta en el foro de Amazon FSx para Lustre.

Temas



## Error al intentar crear un sistema de archivos de Amazon FSx para Lustre

Existen varias causas posibles por las que se produce un error en una solicitud de creación de un sistema de archivos, tal como se describe en los siguientes temas.

### No se puede crear un sistema de archivos debido a un grupo de seguridad mal configurado

Se produce un error al crear un sistema de archivos FSx para Lustre y aparece el siguiente mensaje de error:

```
The file system cannot be created because the default security group in the subnet
 provided
or the provided security groups do not permit Lustre LNET network traffic on port 988
```

Acción que se debe ejecutar

Asegúrese de que el grupo de seguridad de VPC que está utilizando para la operación de creación esté configurado como se describe en Control de acceso al sistema de archivos con Amazon VPC. Debe configurar el grupo de seguridad para permitir el tráfico entrante en los puertos 988 y 1018-1023 desde el propio grupo de seguridad o la subred CIDR completa, que es necesaria para permitir que los hosts del sistema de archivos se comuniquen entre sí.

## No se puede crear un sistema de archivos que esté vinculado a un bucket de S3

Si se produce un error al crear un nuevo sistema de archivos vinculado a un bucket de S3, aparece un mensaje de error similar al siguiente.

```
User: arn:aws:iam::012345678901:user/username is not authorized to perform:
 iam:PutRolePolicy on resource: resource ARN
```

Este error puede producirse si intenta crear un sistema de archivos vinculado a un bucket de Amazon S3 sin los permisos de IAM necesarios. Los permisos de IAM necesarios admiten la función vinculada al servicio Amazon FSx para Lustre que se utiliza para acceder al bucket de Amazon S3 especificado en su nombre.

Acción que se debe ejecutar

Asegúrese de que su entidad de IAM (usuario, grupo o rol) tenga los permisos adecuados para crear sistemas de archivos. Para ello, se incluye añadir la política de permisos que admite la función vinculada al servicio Amazon FSx para Lustre. Para más información, consulte Agregar permisos para utilizar repositorios de datos en Amazon S3.

Para obtener más información acerca de los roles vinculados a servicios, consulte Uso de roles vinculados a servicios para Amazon FSx.

# Solución de problemas de montaje del sistema de archivos

Existen varias causas posibles cuando falla un comando de montaje de un sistema de archivos, como se describe en los siguientes temas.

## El montaje del sistema de archivos falla de inmediato

El comando de montaje del sistema de archivos falla de inmediato. En el siguiente código se muestra un ejemplo.

```
mount.lustre: mount fs-0123456789abcdef0.fsx.us-east-1.aws@tcp:/fsx at /lustre
failed: No such file or directory

Is the MGS specification correct?
Is the filesystem name correct?
```

Este error puede producirse si no está utilizando el valor `mountname` correcto al montar un sistema de archivos persistente o scratch 2 usando el comando mount. Puede obtener el valor `mountname` a partir de la respuesta del describe-file-systems comando AWS CLI o de la operación de la API DescribeFileSystems.

## El montaje del sistema de archivos deja de responder y luego falla con un error de tiempo de espera agotado

El comando de montaje del sistema de archivos deja de responder durante un minuto o dos y, a continuación, falla con un error de tiempo de espera agotado.

En el siguiente código se muestra un ejemplo.

```
sudo mount -t lustre file_system_dns_name@tcp:/mountname /mnt/fsx

[2+ minute wait here]
Connection timed out
```

Este error puede producirse porque los grupos de seguridad de la instancia de Amazon EC2 o el sistema de archivos no están configurados correctamente.

Acción que se debe ejecutar

Asegúrese de que sus grupos de seguridad para el sistema de archivos tienen las reglas de entrada especificadas en Grupos de seguridad de Amazon VPC.

## Se produce un error de montaje automático y la instancia no responde

En algunos casos, el montaje automático puede fallar para un sistema de archivos y su instancia de Amazon EC2 puede dejar de responder.

Este problema puede producirse si no se ha declarado la opción `_netdev`. Si falta `_netdev`, la instancia de Amazon EC2 puede dejar de responder. Este resultado se debe a que los sistemas de archivos de red se deben inicializar después de que la instancia de procesamiento inicia sus redes.

Acción que se debe ejecutar

Si se produce este problema, contáctese con AWS Support.

## Error en el montaje del sistema de archivos durante el arranque del sistema

El montaje del sistema de archivos falla durante el arranque del sistema. El montaje se realiza de forma automática usando `/etc/fstab`. Cuando el sistema de archivos no está montado, aparece el siguiente error en el syslog durante el período de arranque de la instancia.

```
LNetError: 3135:0:(lib-socket.c:583:lnet_sock_listen()) Can't create socket: port 988
 already in use
LNetError: 122-1: Can't start acceptor on port 988: port already in use
```

Este error puede producirse cuando el puerto 988 no está disponible. Cuando la instancia está configurada para montar sistemas de archivos NFS, es posible que los montajes NFS unan el puerto del cliente al puerto 988

Acción que se debe ejecutar

Puede solucionar este problema ajustando las opciones de montaje `noresvport` y `noauto` del cliente NFS siempre que sea posible.

## El montaje del sistema de archivos que utiliza el nombre de DNS falla

Los nombres del Servicio de nombres de dominio (DNS) mal configurados pueden provocar errores en el montaje del sistema de archivos, como se muestra en los siguientes escenarios.

Caso 1: se produce un error al montar un sistema de archivos que utiliza un nombre de servicio de nombres de dominio (DNS). En el siguiente código se muestra un ejemplo.

```
sudo mount -t lustre file_system_dns_name@tcp:/mountname /mnt/fsx
mount.lustre: Can't parse NID
'file_system_dns_name@tcp:/mountname'
```

Acción que se debe ejecutar

Compruebe la configuración de la nube privada virtual (VPC). Si utiliza una VPC personalizada, asegúrese de que la configuración de DNS esté habilitada. Para obtener más información, consulte Utilización de DNS con su VPC en la Guía del usuario de Amazon VPC.

Para especificar un nombre de DNS en el comando `mount`, haga lo siguiente:

- Asegúrese de que la instancia de Amazon EC2 se encuentra en la misma VPC que el sistema de archivos de Amazon FSx para Lustre.
- Conecte su instancia de Amazon EC2 dentro de una VPC configurada para utilizar el servidor DNS proporcionado por Amazon. Para obtener más información, consulte Conjuntos de opciones de DHCP en la Guía del usuario de Amazon VPC.
- Asegúrese de que la VPC de Amazon de la instancia de Amazon EC2 conectada tiene habilitados los nombres de host DNS. A fin de obtener más información, consulte Actualización de soporte de DNS para su VPC en la guía del usuario de Amazon VPC.

Caso 2: se produce un error al montar un sistema de archivos que utiliza un nombre de servicio de nombres de dominio (DNS). En el siguiente código se muestra un ejemplo.

```
mount -t lustre file_system_dns_name@tcp:/mountname /mnt/fsx
mount.lustre: mount file_system_dns_name@tcp:/mountname at /mnt/fsx failed: Input/
output error Is the MGS running?
```

Acción que se debe ejecutar

Asegúrese de que los grupos de seguridad de la VPC del cliente tienen aplicadas las reglas de tráfico saliente correctas. Esta recomendación es especialmente válida si no está utilizando el grupo de seguridad predeterminado o si lo ha modificado. Para más información, consulte Grupos de seguridad de Amazon VPC.

# No puede acceder al sistema de archivos

Existen varias causas posibles por las que no pueda acceder al sistema de archivos, cada una tiene su propia resolución, como se indica a continuación.

## Se eliminó la dirección IP elástica que está adjunta a la interfaz de red elástica del sistema de archivos

Amazon FSx no admite el acceso a los sistemas de archivos desde la Internet pública. Amazon FSx separa de manera automática cualquier dirección IP elástica, la cual es una dirección IP pública a la que se puede acceder desde Internet, que se adjunta a la interfaz de red elástica de un sistema de archivos.

## Se modificó o eliminó la interface de red elástica del sistema de archivos

No debe modificar ni eliminar la interfaz de red elástica del sistema de archivos. Si se modifica o elimina la interfaz de red, se puede provocar una pérdida permanente de la conexión entre la VPC y el sistema de archivos. Cree un nuevo sistema de archivos y no modifique ni elimine la interfaz de red elástica de FSx. Para más información, consulte Control de acceso al sistema de archivos con Amazon VPC.

# No se puede validar el acceso a un bucket de S3 al crear una asociación de repositorios de datos

Al crear una asociación de repositorios de datos (DRA) desde la consola de Amazon FSx o mediante el comando `create-data-repository-association` CLI (CreateDataRepositoryAssociationes la acción de API equivalente), se produce un error con el siguiente mensaje de error.

```
Amazon FSx is unable to validate access to the S3 bucket. Ensure the IAM role or user
you are using has s3:Get*, s3:List* and s3:PutObject permissions to the S3 bucket
 prefix.
```

> **Note**
>
> También puede aparecer el error anterior al crear un sistema de archivos Scratch 1, Scratch 2 o Persistent 1 vinculado a un repositorio de datos (bucket o prefijo de S3) mediante la consola Amazon FSx o el comando `create-file-system` CLI CreateFileSystem(es la acción de API equivalente).

Acción que se debe ejecutar

Si el sistema de archivos FSx para Lustre está en la misma cuenta que el bucket de S3, este error significa que el rol de IAM que utilizó para la solicitud de creación no tiene los permisos necesarios para acceder al bucket de S3. Asegúrese de que el rol de IAM tiene los permisos indicados en el mensaje de error. Estos permisos admiten la función vinculada al servicio Amazon FSx para Lustre que se utiliza para acceder al bucket de Amazon S3 especificado en su nombre.

Si el sistema de archivos FSx para Lustre está en una cuenta diferente a la del bucket de S3 (en el caso de varias cuentas), además de asegurarse de que el rol de IAM que utilizó tenga los permisos

necesarios, la política de bucket de S3 debe configurarse para permitir el acceso desde la cuenta en la que se creó el FSx para Lustre. La siguiente es una política de ejemplo de bucket,

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetBucketAcl",
                "s3:GetBucketNotification",
                "s3:ListBucket",
                "s3:PutBucketNotification"
            ],
            "Resource": [
                "arn:aws:s3:::bucket_name",
                "arn:aws:s3:::bucket_name/*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::file_system_account_ID:role/aws-service-role/
s3.data-source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_fs-*"
                }
            }
        }
    ]
}
```

Para obtener más información sobre cómo configurar permisos de bucket entre cuentas en Amazon S3, consulte Ejemplo 2: Concesión de permisos de bucket entre cuentas en la Guía del usuario de Amazon Simple Storage Service.

# Renombrar directorios lleva mucho tiempo

Pregunta

He renombrado un directorio en un sistema de archivos vinculado a un bucket de Amazon S3 y tengo activada la exportación automática. ¿Por qué los archivos de este directorio tardan tanto en cambiar de nombre en el bucket de S3?

Respuesta

Cuando se cambia el nombre de un directorio en el sistema de archivos, FSx para Lustre crea nuevos objetos S3 para todos los archivos y directorios dentro del directorio que fue renombrado. El tiempo que se tarda en propagar el cambio de nombre del directorio a S3 está directamente relacionado con la cantidad de archivos y directorios que descienden del directorio al que se va a cambiar el nombre.

# Resolución de problemas de un bucket de S3 vinculado mal configurado

En algunos casos, el bucket S3 vinculado de un sistema de archivos FSx para Lustre puede tener un estado de ciclo de vida de repositorio de datos mal configurado.

Causa posible

Este error puede producirse si Amazon FSx no dispone de los permisos AWS Identity and Access Management (IAM) necesarios para acceder al repositorio de datos vinculado. Los permisos de IAM necesarios admiten la función vinculada al servicio Amazon FSx para Lustre que se utiliza para acceder al bucket de Amazon S3 especificado en su nombre.

Acción que se debe ejecutar

1. Asegúrese de que su entidad de IAM (usuario, grupo o rol) tenga los permisos adecuados para crear sistemas de archivos. Para ello, se incluye añadir la política de permisos que admite la función vinculada al servicio Amazon FSx para Lustre. Para más información, consulte Agregar permisos para utilizar repositorios de datos en Amazon S3.
2. Con la API o la CLI de Amazon FSx, actualice el sistema de archivos `AutoImportPolicy` con el comando `update-file-system` CLI (UpdateFileSystemes la acción de API equivalente), de la siguiente manera.

```
aws fsx update-file-system \
--file-system-id fs-0123456789abcdef0 \
--lustre-configuration AutoImportPolicy=the_existing_AutoImportPolicy
```

Para obtener más información acerca de los roles vinculados a servicios, consulte Uso de roles vinculados a servicios para Amazon FSx.

Causa posible

Este error puede producirse si el repositorio de datos de Amazon S3 vinculado tiene una configuración de notificación de eventos existente con tipos de eventos que se solapan con la configuración de notificación de eventos de Amazon FSx (`s3:ObjectCreated:*`, `s3:ObjectRemoved:*`).

También puede ocurrir si la configuración de notificación de eventos de Amazon FSx en el bucket de S3 vinculado se eliminó o modificó.

Acción que se debe ejecutar

1. Elimine cualquier notificación de evento existente en el bucket de S3 vinculado que utilice uno o ambos tipos de eventos que utiliza la configuración de eventos de FSx, `s3:ObjectCreated:*` y `s3:ObjectRemoved:*`.
2. Asegúrese de que exista una configuración de notificación de eventos de S3 en el bucket de S3 vinculado con el nombre `FSx`, tipos de eventos `s3:ObjectCreated:*` y `s3:ObjectRemoved:*`, y envíe al tema SNS con ARN:*topic_arn_returned_in_API_response*.
3. Vuelva a aplicar la configuración de notificación de eventos FSx en el bucket de S3 mediante la CLI o la API de Amazon FSx, para actualizar el sistema de archivos de `AutoImportPolicy`. Hágalo con el comando `update-file-system` CLI (UpdateFileSystemes la acción de API equivalente), de la siguiente manera.

```
aws fsx update-file-system \
--file-system-id fs-0123456789abcdef0 \
--lustre-configuration AutoImportPolicy=the_existing_AutoImportPolicy
```

# Solución de problemas de almacenamiento

En algunos casos, es posible que surjan problemas de almacenamiento de archivos. Puede solucionar estos problemas mediante comandos `lfs`, como el comando `lfs migrate`.

## Error de escritura debido a la falta de espacio en el destino de almacenamiento

Puede comprobar el uso de almacenamiento de su sistema de archivos usando el comando `lfs df -h`, tal y como se describe en Disposición de almacenamiento del sistema de archivos. El campo `filesystem_summary` indica el uso total de almacenamiento del sistema de archivos.

Si el uso del disco del sistema de archivos es del 100 %, considere la posibilidad de aumentar la capacidad de almacenamiento del sistema de archivos. Para más información, consulte Administración de la capacidad de almacenamiento.

Si el uso del almacenamiento del sistema de archivos no es del 100 % y sigue obteniendo errores de escritura, es posible que el archivo en el que está escribiendo esté dividido en franjas en un OST que está lleno.

Acción que se debe ejecutar

- Si muchos de los OST están llenos, aumente la capacidad de almacenamiento del sistema de archivos. Compruebe si hay un almacenamiento desequilibrado en los OST siguiendo las acciones de la sección Almacenamiento desequilibrado en los OST.
- Si las OST no están llenas, ajuste el tamaño del búfer de páginas no utilizadas del cliente aplicando los siguientes ajustes a todas las instancias del cliente:

```
sudo lctl set_param osc.*.max_dirty_mb=64
```

## Almacenamiento desequilibrado en los OST

Amazon FSx para Lustre distribuye las nuevas franjas de archivos de manera uniforme entre las OST. Sin embargo, es posible que su sistema de archivos siga desequilibrado debido a los patrones de E/S o al diseño del almacenamiento de archivos. Como resultado, algunos destinos de almacenamiento pueden llenarse mientras que otros permanecen relativamente vacíos.

El comando `lfs migrate` se utiliza para mover archivos o directorios de OST más llenos a OST menos llenos. Puede utilizar el comando `lfs migrate` en modo de bloqueo o sin bloqueo.

- El modo de bloqueo es el modo por defecto del comando `lfs migrate`. Cuando se ejecuta en modo de bloqueo, `lfs migrate` primero adquiere un bloqueo de grupo en los archivos y directorios antes de la migración de datos para evitar modificaciones en los archivos, y luego libera el bloqueo cuando finaliza la migración. Al impedir que otros procesos modifiquen los archivos, el modo de bloqueo evita que estos procesos interrumpan la migración. El inconveniente es que impedir que una aplicación modifique un archivo puede provocar retrasos o errores en la aplicación.
- El modo sin bloqueo se habilita para el comando `lfs migrate` con la opción `-n`. Cuando se ejecuta `lfs migrate` en el modo sin bloqueo, otros procesos pueden seguir modificando los archivos que se están migrando. Si un proceso modifica un archivo antes de que `lfs migrate` finalice la migración, `lfs migrate` no podrá migrar ese archivo, dejando el archivo con su disposición de franjas original.

Le recomendamos que utilice el modo sin bloqueo, ya que es menos probable que interfiera con la aplicación.

Acción que se debe ejecutar

1. Inicie una instancia de cliente relativamente grande (como el tipo de instancia Amazon EC2 `c5n.4xlarge`) para montarla en el sistema de archivos.
2. Antes de ejecutar el script en modo sin bloqueo o el script en modo de bloqueo, ejecute primero los siguientes comandos en cada instancia de cliente para acelerar el proceso:

   ```
   sudo lctl set_param 'mdc.*.max_rpcs_in_flight=60'
   sudo lctl set_param 'mdc.*.max_mod_rpcs_in_flight=59'
   ```

3. Inicie una sesión de pantalla y ejecute el script de modo sin bloqueo o el script de modo de bloqueo. Asegúrese de cambiar las variables adecuadas en los scripts:

   - Script para el modo sin bloqueo:

     ```
     #!/bin/bash

     # UNCOMMENT THE FOLLOWING LINES:
     #
     # TRY_COUNT=0
     ```

```
# MAX_MIGRATE_ATTEMPTS=100
# OSTS="fsname-OST0000_UUID"
# DIR_OR_FILE_MIGRATED="/mnt/subdir/"
# BATCH_SIZE=10
# PARALLEL_JOBS=16 # up to max-procs processes, set to 16 if client is
 c5n.4xlarge with 16 vcpu
# LUSTRE_STRIPING_CONFIG="-E 100M -c 1 -E 10G -c 8 -E 100G -c 16 -E -1 -c 32" #
 should be consistent with the existing striping setup
#

if [ -z "$TRY_COUNT" -o -z "$MAX_MIGRATE_ATTEMPTS" -o -z "$OSTS" -o -z
 "$DIR_OR_FILE_MIGRATED" -o -z "$BATCH_SIZE" -o -z "$PARALLEL_JOBS" -o -z
 "$LUSTRE_STRIPING_CONFIG" ]; then
    echo "Some variables are not set."
    exit 1
fi

echo "lfs migrate starts"
while true; do
    output=$(sudo lfs find ! -L released --ost $OSTS --print0
 $DIR_OR_FILE_MIGRATED | shuf -z | /bin/xargs -0 -P $PARALLEL_JOBS -n $BATCH_SIZE
 sudo lfs migrate -n $LUSTRE_STRIPING_CONFIG 2>&1)
    if [[ $? -eq 0 ]]; then
        echo "lfs migrate succeeds for $DIR_OR_FILE_MIGRATED at the $TRY_COUNT
 attempt, exiting."
        exit 0
    elif [[ $? -eq 123 ]]; then
        echo "WARN: Target data objects are not located on these OSTs. Skipping
 lfs migrate"
        exit 1
    else
        echo "lfs migrate fails for $DIR_OR_FILE_MIGRATED at the $TRY_COUNT
 attempt, retrying..."
        if (( ++TRY_COUNT >= MAX_MIGRATE_ATTEMPTS )); then
            echo "WARN: Exceeds max retry attempt. Skipping lfs migrate for
 $DIR_OR_FILE_MIGRATED. Failed with the following error"
            echo $output
            exit 1
        fi
    fi
done
```

- Script para el modo de bloqueo:

- Sustituya los valores en `OSTS` por los valores de sus OST.
- Proporcione un valor entero a `nproc` para establecer el número de procesos max-procs que se ejecutarán en paralelo. Por ejemplo, el tipo de instancia Amazon EC2 `c5n.4xlarge` tiene 16 vCPU, por lo que puede usar 16 (o un valor < 16) para `nproc`.
- Introduzca la ruta del directorio de montaje `mnt_dir_path`.

```
# find all OSTs with usage above a certain threshold; for example, greater than
 or equal to 85% full
for OST in $(lfs df -h |egrep '( 8[5-9]| 9[0-9]|100)%'|cut -d' ' -f1); do echo
 ${OST};done|tr '\012' ','

# customer can also just pass OST values directly to OSTS variable
OSTS='dzfevbmv-OST0000_UUID,dzfevbmv-OST0002_UUID,dzfevbmv-OST0004_UUID,dzfevbmv-
OST0005_UUID,dzfevbmv-OST0006_UUID,dzfevbmv-OST0008_UUID'

nproc=<Run up to max-procs processes if client is c5n.4xlarge with 16 vcpu, this
 value can be set to 16>

mnt_dir_path=<mount dir, e.g. '/my_mnt'>

lfs find ${mnt_dir_path} --ost ${OSTS}| xargs -P ${nproc} -n2 lfs migrate -E 100M
 -c 1 -E 10G -c 8 -E 100G -c 16 -E -1 -c 32
```

Notas

- Si observa que esto afecta al rendimiento de las lecturas del sistema de archivos, puede detener las migraciones en cualquier momento utilizando `ctrl-c` o `kill -9`, y reducir el número de subprocesos (valor `nproc`) a un número inferior (por ejemplo, 8) y reanudar la migración de los archivos.
- El comando `lfs migrate` fallará en un archivo que también esté abierto por la carga de trabajo del cliente. Lanzará un error y pasará al siguiente archivo; por lo tanto, es posible que, si se está accediendo a muchos archivos, el script no pueda migrar ningún archivo, y se reflejará como que la migración avanza muy lentamente.
- Puede monitorizar el uso de OST utilizando cualquiera de los siguientes métodos
  - En el montaje de cliente, ejecute el siguiente comando para monitorizar el uso del OST y encontrar el OST con un uso superior al 85 %:

```
lfs df -h |egrep '( 8[5-9]| 9[1-9]|100)%'
```

- Comprueba la CloudWatch métrica de Amazon`OST FreeDataStorageCapacity`, compruebaMinimum. Si el script da como resultado que las OST están ocupadas en más del 85 %, cuando la métrica se acerque al 15 %, use `ctrl-c` o `kill -9` para detener la migración.

- También puede considerar cambiar la configuración de franjas de su sistema de archivos o de un directorio, de modo que los nuevos archivos sean fragmentados a través de múltiples destinos de almacenamiento. Para obtener más información, consulte Fragmentación de datos en su sistema de archivos.

## Resolución de problemas con el controlador FSx para Lustre CSI

Si tiene problemas con el controlador CSI de FSx for Lustre para contenedores que se ejecutan en Amazon EKS, consulte Solución de problemas con el controlador CSI (problemas comunes), disponible en. GitHub

# Información adicional

En esta sección se proporciona una referencia de las características de Amazon FSx compatibles, pero obsoletas.

Temas



## Configurar una programación de copias de seguridad personalizada

Le recomendamos que utilice AWS Backup para configurar un programa de copias de seguridad personalizado para su sistema de archivos. La información que se proporciona aquí es de referencia si necesita programar copias de seguridad con más frecuencia que cuando utiliza AWS Backup.

Cuando está activado, Amazon FSx realiza automáticamente una copia de seguridad de su sistema de archivos una vez al día durante un período de copia de seguridad diario. Amazon FSx aplica un período de retención que usted especifica para estas copias de seguridad automáticas. También admite copias de seguridad iniciadas por el usuario, por lo que puede realizar copias de seguridad en cualquier momento.

A continuación, encontrará los recursos y la configuración para implementar una programación de copias de seguridad personalizada. La programación de copias de seguridad personalizadas realiza las copias de seguridad iniciadas por el usuario en un sistema de archivos Amazon FSx para Lustre según una programación personalizada que usted defina. Algunos ejemplos pueden ser una vez cada seis horas, una vez a la semana, etc. Este script también configura la eliminación de las copias de seguridad anteriores al período de retención especificado.

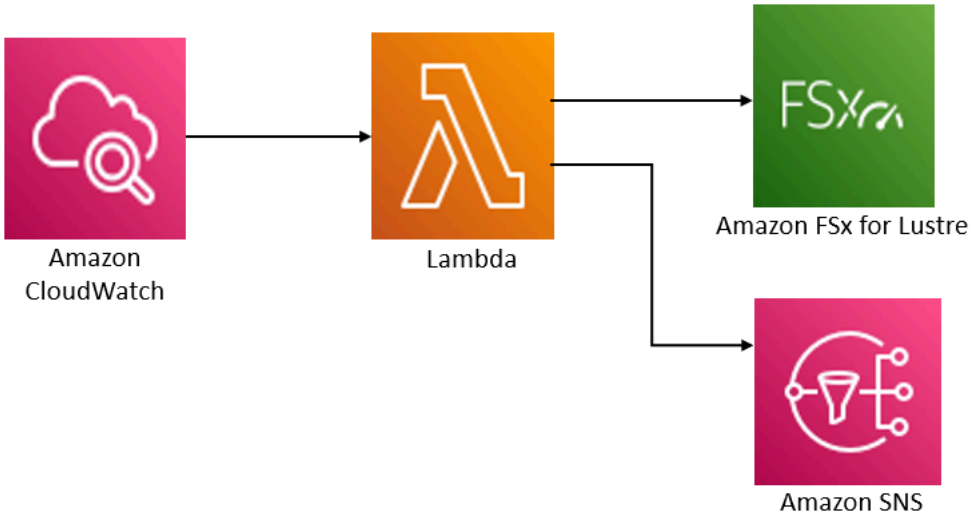
La solución despliega automáticamente todos los componentes necesarios y tiene en cuenta los siguientes parámetros:

- El ID del sistema de archivos
- Un patrón de programación CRON para realizar copias de seguridad
- El período de retención de copias de seguridad en (días)
- Las etiquetas de nombre de la copia de seguridad

Para obtener más información sobre los patrones de programación de CRON, consulte Schedule Expressions for Rules en la Guía del CloudWatch usuario de Amazon.

## Información general de la arquitectura

Al implementar esta solución, se crean los siguientes recursos en Nube de AWS.




Esta solución hace lo siguiente:

1. La AWS CloudFormation plantilla implementa un CloudWatch evento, una función Lambda, una cola de Amazon SNS y un rol de IAM. El rol de IAM otorga a la función de Lambda permiso para invocar las operaciones de la API Amazon FSx para Lustre.
2. El CloudWatch evento se ejecuta según un cronograma que usted defina como un patrón CRON durante la implementación inicial. Este evento invoca la función de Lambda del administrador de copias de seguridad de la solución, que invoca la operación de la API Amazon FSx para Lustre `CreateBackup` para iniciar una copia de seguridad.
3. El administrador de copias de seguridad recupera una lista de las copias de seguridad existentes iniciadas por el usuario para el sistema de archivos especificado usando `DescribeBackups`. Luego, elimina las copias de seguridad anteriores al período de retención, que haya especificó durante la implementación inicial.
4. El administrador de copias de seguridad envía un mensaje de notificación a la cola de Amazon SNS si la copia de seguridad se realiza correctamente si elige la opción de recibir una notificación durante la implementación inicial. En caso de error, siempre se envía una notificación.

# Plantilla de AWS CloudFormation

Esta solución utiliza AWS CloudFormation para automatizar la implementación de la solución de programación de copias de seguridad personalizada de Amazon FSx para Lustre. Para usar esta solución, descargue la fsx-scheduled-backupplantilla .template. AWS CloudFormation

## Implementación automatizada

El siguiente procedimiento configura e implementa esta solución de programación de copias de seguridad personalizada. Tarda aproximadamente cinco minutos en desplegarse. Antes de empezar, debe tener en su cuenta AWS el ID de un sistema de archivos de Amazon FSx para Lustre que se ejecute en una Amazon Virtual Private Cloud (Amazon VPC). Para más información sobre la creación de estos recursos, consulte Introducción a Amazon FSx para Lustre.

> **Note**
>
> La implementación de esta solución implica la facturación de los servicios AWS asociados. Para más información, consulte las páginas de precios de estos servicios.

Para lanzar la pila de soluciones de copia de seguridad personalizadas

1. Descargue la fsx-scheduled-backupplantilla .template. AWS CloudFormation Para obtener más información sobre la creación de una pila de AWS CloudFormation, consulte Crear una pila en la consola de AWS CloudFormation en la Guía del usuario de AWS CloudFormation.

   > **Note**
   >
   > De forma predeterminada, esta plantilla se inicia en la región Este de EE. UU. (Norte de Virginia) de AWS. En la actualidad, Amazon FSx para Lustre solo está disponible en versiones específicas de Regiones de AWS. Debe lanzar esta solución en una región AWS en la que esté disponible Amazon FSx para Lustre. Para obtener más información, consulte la sección de Amazon FSx de Regiones de AWS y Puntos de conexión en la Referencia general de AWS.

2. En el caso de los parámetros, revise los parámetros de la plantilla y modifíquelos para adaptarlos a las necesidades de su sistema de archivos. Esta solución utiliza los siguientes valores predeterminados.

| Parámetro | Predeterminado | Descripción |
| --- | --- | --- |
| ID del sistema de archivos de Amazon FSx para Lustre | Sin valor predeterminado | El ID del sistema de archivos del que desea hacer una copia de seguridad. |
| Patrón de programación CRON para las copias de seguridad. | 0 0/4 * * ? * | La programación para ejecutar el CloudWatch evento, activar una nueva copia de seguridad y eliminar las copias de seguridad antiguas fuera del período de retención. |
| Retención de copias de seguridad (días) | 7 | El número de días que se deben guardar las copias de seguridad iniciadas por el usuario. La función de Lambda elimina las copias de seguridad iniciadas por el usuario con una antigüeda d superior a este número de días. |
| Nombre de las copias de seguridad | copia de seguridad programada por el usuario | El nombre de estas copias de seguridad, que aparece en la columna Nombre de copia de seguridad de la consola de administración de Amazon FSx para Lustre. |

| Parámetro | Predeterminado | Descripción |
| --- | --- | --- |
| Notificaciones de copias de seguridad | Sí | Elija si desea recibir una notificación cuando las copias de seguridad se inicien correctamente. Siempre se envía una notificación si se produce un error. |
| Dirección de correo electrónico | Sin valor predeterminado | La dirección de correo electrónico para suscribirse a las notificaciones del SNS. |

3. Elija Siguiente.
4. En Opciones, elija Siguiente.
5. En la página Revisar, revise y confirme la configuración. Debe seleccionar la casilla de verificación que reconoce que la plantilla crea recursos IAM.
6. Elija Crear para implementar la pila.

Puede ver el estado de la pila en la consola de AWS CloudFormation en la columna Estado. Debería ver el estado CREATE_COMPLETE en aproximadamente cinco minutos.

## Opciones adicionales

Puede utilizar la función de Lambda creada por esta solución para realizar copias de seguridad programadas personalizadas de más de un sistema de archivos de Amazon FSx para Lustre. El ID del sistema de archivos se pasa a la función Amazon FSx for Lustre en el JSON CloudWatch de entrada del evento. El JSON predeterminado que se pasa a la función de Lambda es el siguiente, donde los valores para `FileSystemId` y `SuccessNotification` se transfieren desde los parámetros especificados al lanzar la pila AWS CloudFormation.

```
{
 "start-backup": "true",
 "purge-backups": "true",
 "filesystem-id": "${FileSystemId}",
 "notify_on_success": "${SuccessNotification}"
```

```
}
```

Para programar copias de seguridad para un sistema de archivos Amazon FSx for Lustre adicional, CloudWatch cree otra regla de eventos. Para ello, utilice la fuente de eventos de Programación, con la función de Lambda creada por esta solución como destino. Elija Constante (texto JSON) en Configurar entrada. Para la entrada JSON, simplemente sustituya el ID del sistema de archivos del sistema de archivo de Amazon FSx para Lustre para hacer una copia de seguridad en lugar de `${FileSystemId}`. Además, sustituya `Yes` o `No` en lugar `${SuccessNotification}` en el JSON anterior.

Las reglas de CloudWatch eventos adicionales que cree manualmente no forman parte del conjunto de soluciones de backup programado AWS CloudFormation personalizadas de Amazon FSx for Lustre. Por lo tanto, no se eliminan si se elimina la pila.

# Historial del documento

- Versión de la API: 01-03-2018
- Última actualización de la documentación: 25 de marzo de 2024

En la siguiente tabla se describen cambios importantes en la Guía del usuario de Amazon FSx para Lustre. Para obtener notificaciones sobre las actualizaciones de la documentación, puede suscribirse a la fuente RSS.

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Se agregó el soporte de cliente Lustre para Amazon Linux 2023 | El cliente FSx for Lustre ahora es compatible con instancias de Amazon EC2 que ejecutan Amazon Linux 2023. Para obtener más información, consulte Instalación del cliente de Lustre. | 25 de marzo de 2024 |
| Se agregó el soporte de cliente Lustre para Centos, Rocky Linux y Red Hat Enterprise Linux (RHEL) 8.9 | El cliente FSx for Lustre ahora es compatible con instancias de Amazon EC2 que ejecutan Centos, Rocky Linux y Red Hat Enterpris e Linux (RHEL) 8.9. Para obtener más información, consulte Instalación del cliente de Lustre. | 9 de enero de 2024 |
| Amazon FSx actualizó las políticas gestionadas de AmazonFSxFullAccess, AmazonFSxConsoleFu llAccess, AmazonF SxReadOnlyAccess y SxConsoleReadOnlyAccess | Amazon FSx actualizó las políticas de AmazonFSx FullAccess, AmazonFSx ConsoleFullAccess, AmazonF SxReadOnlyAccess y SxServiceRolePolicy AmazonF SxConsole | 9 de enero de 2024 |

| | | |
|---|---|---|
| AmazonF SxServiceRolePolicy AWS | ReadOnlyAccess para añadir el permiso. `ec2:GetSecurityGroupsForVpc` Para obtener más información, consulte Amazon FSx sobre las actualizaciones de las políticas AWS gestionadas. | |
| Se agregó el soporte de cliente Lustre para Centos, Rocky Linux y Red Hat Enterprise Linux (RHEL) 9.0 y 9.3 | El cliente FSx for Lustre ahora es compatible con instancias de Amazon EC2 que ejecutan Centos, Rocky Linux y Red Hat Enterprise Linux (RHEL) 9.0 y 9.3. Para obtener más información, consulte Instalación del cliente de Lustre. | 20 de diciembre de 2023 |
| Amazon FSx for Lustre actualizó SxFullAccess las políticas gestionadas de AmazonF y AmazonF SxConsoleFullAccess AWS | Amazon FSx actualizó las SxConsoleFullAccess políticas de AmazonF SxFullAccess y AmazonF para añadir la acción. `ManageCrossAccountDataReplication` Para obtener más información, consulte Amazon FSx sobre las actualizaciones de las políticas AWS gestionadas. | 20 de diciembre de 2023 |

| | | |
|---|---|---|
| Amazon FSx actualizó las políticas gestionadas de AmazonF SxFullAccess y AmazonF SxConsoleFullAccess AWS | Amazon FSx actualizó las SxConsoleFullAccess políticas de AmazonF SxFullAccess y AmazonF para añadir el permiso. `fsx:CopySnapshotAndUpdateVolume` Para obtener más información, consulte Amazon FSx sobre las actualizaciones de las políticas AWS gestionadas. | 26 de noviembre de 2023 |
| Se ha agregado compatibilidad para el escalado de la capacidad de rendimiento | Ahora puede modificar la capacidad de rendimiento de los sistemas de archivos existentes basados en SSD persistentes FSx para Lustre a medida que evolucionan sus requisitos de rendimiento. Para obtener más información, consulte Gestión de la capacidad de rendimiento. | 16 de noviembre de 2023 |
| Amazon FSx actualizó las políticas gestionadas de AmazonF SxFullAccess y AmazonF SxConsoleFullAccess AWS | Amazon FSx actualizó las SxConsoleFullAccess políticas de AmazonF SxFullAccess y AmazonF para añadir los permisos y. `fsx:DescribeSharedVPCConfiguration` `fsx:UpdateSharedVPCConfiguration` Para obtener más información, consulte Amazon FSx sobre las actualizaciones de las políticas AWS gestionadas. | 14 de noviembre de 2023 |

| | | |
|---|---|---|
| Se ha agregado compatibilidad para las cuotas de proyectos | Ahora puede crear cuotas de almacenamiento para proyectos. La cuota de un proyecto se aplica a todos los archivos o directorios asociados a un proyecto. Para obtener más información, consulte Cuotas de almacenamiento. | 29 de agosto de 2023 |
| Se ha agregado compatibilidad para Lustre versión 2.15 | Todos los sistemas de archivos de FSx para Lustre se basan ahora en la versión 2.15 de Lustre cuando se crean mediante la consola de Amazon FSx. Para obtener más información, consulte Paso 1: cómo crear su sistema de archivos de Amazon FSx para Lustre. | 29 de agosto de 2023 |
| Se agregó Región de AWS soporte adicional para el tipo de implementación Persistent_1 | Los sistemas de archivos Persistent_1 FSx for Lustre ya están disponibles en Israel (Tel Aviv). Región de AWS Para obtener más información, consulte Opciones de implementación para sistemas de archivos de FSx para Lustre. | 24 de agosto de 2023 |

| | | |
|---|---|---|
| Se ha agregado compatibilidad para las tareas del repositorio de datos de publicación | FSx para Lustre ahora proporciona tareas de liberación de repositorio de datos para liberar archivos guardados desde un sistema de archivos vinculado a un repositorio de datos S3. Al liberar un archivo, se retiene la lista de archivos y los metadatos, pero se elimina la copia local del contenido de ese archivo. Para obtener más información, consulte Utilizar las tareas del repositorio de datos para liberar archivos. | 9 de agosto de 2023 |
| Amazon FSx actualizó la política gestionada de SxServiceRolePolicy AWS AmazonF | Amazon FSx actualizó el `cloudwatch:PutMetricData` permiso en AmazonF. SxServiceRolePolicy Para obtener más información, consulte Amazon FSx sobre las actualizaciones de las políticas AWS gestionadas. | 24 de julio de 2023 |
| Amazon FSx actualizó la política gestionada de SxFullAccess AWS AmazonF | Amazon FSx actualizó la SxFullAccess política de AmazonF para eliminar el `fsx:*` permiso y añadir acciones específicas. `fsx` Para obtener más información, consulte la política de SxFullAccessAmazonF. | 13 de julio de 2023 |

| | | |
|---|---|---|
| Amazon FSx actualizó la política gestionada de SxConsoleFullAccess AWS AmazonF | Amazon FSx actualizó la SxConsoleFullAccess política de AmazonF para eliminar el `fsx:*` permiso y añadir acciones específicas. `fsx` Para obtener más informaci ón, consulte la política de SxConsoleFullAcces sAmazonF. | 13 de julio de 2023 |
| Se ha agregado compatibi lidad con clientes Lustre para Centos, Rocky Linux y Red Hat Enterprise Linux (RHEL) 8.8 | El cliente FSx para Lustre ahora es compatible con instancias de Amazon EC2 que ejecutan Centos, Rocky Linux y Red Hat Enterpris e Linux (RHEL) 8.8. Para obtener más información, consulte Instalación del cliente de Lustre. | 25 de mayo de 2023 |
| Support agregado AutoImport para AutoExport métricas | FSx for Lustre ahora proporcio na métricas de CloudWatch Amazon que supervisan las actualizaciones automáticas de importación y exportación para los sistemas de archivos vinculados a los repositor ios de datos. Para obtener más información, consulta Monitoring with Amazon CloudWatch. | 31 de marzo de 2023 |

| | | |
|---|---|---|
| Se ha agregado compatibilidad DRA para los tipos de implementación Persistent_1 y Scratch_2 | Ahora puede crear asociaciones de repositorios de datos para vincular repositorios de datos a sistemas de archivos Lustre 2.12 con tipos de implementación Persistent_1 o Scratch_2. Para obtener más información, consulte Uso de repositorios de datos con Amazon FSx para Lustre. | 29 de marzo de 2023 |
| Se ha agregado compatibilidad con clientes Lustre para Centos, Rocky Linux y Red Hat Enterprise Linux (RHEL) 8.7 | El cliente FSx para Lustre ahora es compatible con instancias de Amazon EC2 que ejecutan Centos, Rocky Linux y Red Hat Enterprise Linux (RHEL) 8.7. Para obtener más información, consulte Instalación del cliente de Lustre. | 5 de diciembre de 2022 |
| Se agregó Región de AWS soporte adicional para el tipo de despliegue Persistent_2 | Los FSx SSD Persistent_2 de última generación para sistemas de archivos FSx for Lustre ya están disponibles en Europa (Estocolmo), Asia Pacífico (Hong Kong), Asia Pacífico (Bombay) y Asia Pacífico (Seúl). Regiones de AWS Para obtener más información, consulte Opciones de implementación para sistemas de archivos de FSx para Lustre. | 10 de noviembre de 2022 |

| | | |
|---|---|---|
| Se ha agregado compatibilidad con clientes Lustre para Centos, Rocky Linux y Red Hat Enterprise Linux (RHEL) 8.6 | El cliente FSx para Lustre ahora es compatible con instancias de Amazon EC2 que ejecutan Centos, Rocky Linux y Red Hat Enterprise Linux (RHEL) 8.6. Para obtener más información, consulte Instalación del cliente de Lustre. | 8 de septiembre de 2022 |
| Se ha agregado compatibilidad con el cliente Lustre para Ubuntu 22 | El cliente FSx for Lustre ahora es compatible con instancias de Amazon EC2 que ejecutan Ubuntu 22.04. Para obtener más información, consulte Instalación del cliente de Lustre. | 28 de julio de 2022 |
| Se ha agregado compatibilidad con clientes Lustre para Rocky Linux | El cliente FSx para Lustre ahora soporta instancias de Amazon EC2 ejecutando Rocky Linux. Para obtener más información, consulte Instalación del cliente de Lustre. | 8 de julio de 2022 |
| Se ha agregado compatibilidad para Lustre root squash | Ahora puede utilizar la característica de bloqueo de raíz Lustre para restringir el acceso a nivel de raíz de los clientes que intentan acceder a su sistema de archivos de FSx para Lustre como root. Para obtener más información, consulte Lustre root squash. | 25 de mayo de 2022 |

| | | |
|---|---|---|
| Se agregó Región de AWS soporte adicional para el tipo de implementación Persistent_2 | Los FSx SSD Persistent_2 de última generación para sistemas de archivos FSx for Lustre ya están disponibles en Europa (Londres), Asia Pacífico (Singapur) y Asia Pacífico (Sídney). Regiones de AWS Para obtener más información, consulte Opciones de implementación para sistemas de archivos de FSx para Lustre. | 19 de abril de 2022 |
| Se agregó soporte para AWS DataSync migrar archivos a sus sistemas de archivos Amazon FSx for Lustre. | Ahora puede utilizarlos AWS DataSync para migrar archivos de los sistemas de archivos existentes a los sistemas de archivos FSx for Lustre. Para obtener más información, consulte Cómo migrar archivos existentes a FSx para Lustre usando AWS DataSync. | 5 de abril de 2022 |
| Support agregado para los puntos finales AWS PrivateLink de la interfaz de VPC | Ahora puede utilizar los puntos de conexión de VPC de interfaz para acceder a la API de Amazon FSx desde su VPC sin enviar tráfico por Internet. Para obtener más información, consulte Amazon FSx y los puntos de conexión de VPC de interfaz. | 5 de abril de 2022 |

| | | |
|---|---|---|
| Se ha agregado compatibilidad para las colas de Lustre DRA | Ahora puede crear un DRA (asociación de repositorio de datos) al crear un sistema de archivos de FSx para Lustre. La solicitud se pondrá en cola y el DRA se creará una vez que el sistema de archivos esté disponible. Para obtener más información, consulte Vincular su sistema de archivos a un bucket de S3. | 28 de febrero de 2022 |
| Se ha agregado compatibilidad con clientes Lustre para Centos y Red Hat Enterprise Linux (RHEL) 8.5 | El cliente FSx para Lustre ahora es compatible con instancias de Amazon EC2 que ejecutan Centos y Red Hat Enterprise Linux (RHEL) 8.5. Para obtener más información, consulte Instalación del cliente de Lustre. | 20 de diciembre de 2021 |

| | | |
|---|---|---|
| Soporte para exportar cambios desde FSx para Lustre a un repositorio de datos enlazados | Ahora puede configurar FSx para Lustre para exportar automáticamente los archivos nuevos, modificados y eliminados de su sistema de archivos a un repositor io de datos de Amazon S3 vinculado. Puede utilizar tareas de repositorio de datos para exportar datos y cambios de metadatos al repositorio de datos. También puede configurar enlaces a varios repositorios de datos. Para obtener más información, consulte Exportación de los cambios al repositorio de datos. | 30 de noviembre de 2021 |
| Se ha agregado soporte para el registro de Lustre | Ahora puede configurar FSx for Lustre para que registre en Amazon Logs los eventos de error y advertencia de los repositorios de datos asociados a su sistema de archivos. CloudWatch Para obtener más información, consulta Cómo iniciar sesión con Amazon CloudWatch Logs. | 30 de noviembre de 2021 |

| | | |
|---|---|---|
| Los sistemas de archivos SSD persistentes soportan un mayor rendimiento y una menor capacidad de almacenamiento | Los sistemas de archivos de FSx para Lustre con SSD persistente de próxima generación tienen opciones de mayor rendimiento y menor capacidad mínima de almacenamiento. Para obtener más información, consulte Opciones de implementación para sistemas de archivos de FSx para Lustre. | 30 de noviembre de 2021 |
| Se ha agregado compatibilidad para Lustre versión 2.12 | Ahora puede elegir la versión 2.12 de Lustre cuando cree un sistema de archivos de FSx para Lustre. Para obtener más información, consulte Paso 1: cómo crear su sistema de archivos de Amazon FSx para Lustre. | 5 de octubre de 2021 |
| Se ha agregado compatibilidad con clientes Lustre para Centos y Red Hat Enterprise Linux (RHEL) 8.4 | El cliente FSx para Lustre ahora es compatible con instancias de Amazon EC2 que ejecutan Centos y Red Hat Enterprise Linux (RHEL) 8.4. Para obtener más información, consulte Instalación del cliente de Lustre. | 9 de junio de 2021 |

| | | |
|---|---|---|
| Se ha agregado soporte para la compresión de datos | Ahora puede activar la compresión de datos al crear un sistema de archivos de FSx para Lustre. También puede activar o desactivar la compresión de datos en un sistema de archivos de FSx para Lustre existente. Para obtener más información, consulte Compresión de datos de Lustre. | 27 de mayo de 2021 |
| Se ha agregado compatibilidad para copiar copias de seguridad | Ahora puede usar Amazon FSx para copiar copias de seguridad internas Cuenta de AWS a otras Región de AWS (copias entre regiones) o dentro de las mismas Región de AWS (copias dentro de una región). Para obtener más información, consulte Copiar copias de seguridad. | 12 de abril de 2021 |
| Soporte de cliente Lustre para conjuntos de archivos Lustre | El cliente FSx para Lustre ahora admite el uso de conjuntos de archivos para montar solo un subconjunto del espacio de nombres del sistema de archivos. Para obtener más información, consulte Montaje de conjuntos de archivos específicos. | 18 de marzo de 2021 |

| | | |
|---|---|---|
| Se ha agregado soporte para el acceso de clientes mediante direcciones IP no privadas | Puede acceder a FSx para sistemas de archivos Lustre desde un cliente en las instalaciones utilizando direcciones IP no privadas. Para obtener más informaci ón, consulte Montar sistemas de archivos de Amazon FSx desde una Amazon VPC en las instalaciones o intercone ctada. | 17 de diciembre de 2020 |
| Se ha agregado compatibi lidad con clientes Lustre para Centos 7.9 basado en Arm | El cliente FSx para Lustre ahora es compatible con instancias de Amazon EC2 que ejecuten Centos 7.9 basado en Arm. Para obtener más información, consulte Instalación del cliente de Lustre. | 17 de diciembre de 2020 |
| Se ha agregado compatibi lidad con clientes Lustre para Centos y Red Hat Enterprise Linux (RHEL) 8.3 | El cliente FSx para Lustre ahora es compatible con instancias de Amazon EC2 que ejecutan Centos y Red Hat Enterprise Linux (RHEL) 8.3. Para obtener más información, consulte Instalaci ón del cliente de Lustre. | 16 de diciembre de 2020 |

| | | |
|---|---|---|
| Se ha agregado compatibilidad para el escalado de la capacidad de rendimiento y almacenamiento | Ahora puede aumentar la capacidad de rendimiento y almacenamiento de los sistemas de archivos de FSx para Lustre existentes a medida que evolucionan sus necesidades de rendimiento y almacenamiento. Para obtener más información, consulte Administración de la capacidad de rendimiento y almacenamiento. | 24 de noviembre de 2020 |
| Se ha agregado soporte para cuotas de almacenamiento | Ahora puede crear cuotas de almacenamiento para usuarios y grupos. Las cuotas de almacenamiento limitan la cantidad de espacio en disco y el número de archivos que un usuario o grupo puede consumir en su sistema de archivos de FSx para Lustre. Para obtener más información, consulte Cuotas de almacenamiento. | 9 de noviembre de 2020 |
| Amazon FSx ahora está integrado con AWS Backup | Ahora puede utilizarlos AWS Backup para realizar copias de seguridad y restaurar sus sistemas de archivos FSx, además de utilizar las copias de seguridad nativas de Amazon FSx. Para obtener más información, consulte Uso AWS Backup con Amazon FSx. | 9 de noviembre de 2020 |

| | | |
|---|---|---|
| Se ha agregado compatibilidad para opciones de almacenamiento HDD (unidad de disco duro) | Además de la opción de almacenamiento SSD (unidad de estado sólido), FSx para Lustre ahora soporta la opción de almacenamiento HDD (unidad de disco duro). Puede configurar su sistema de archivos para utilizar HDD para cargas de trabajo de alto rendimiento que normalmente tienen grandes operaciones de archivos secuenciales. Para obtener más información, consulte Múltiples opciones de almacenamiento. | 12 de agosto de 2020 |
| Soporte para importar cambios de repositorios de datos enlazados en FSx para Lustre | Ahora puede configurar su sistema de archivos de FSx para Lustre para importar automáticamente los nuevos archivos añadidos y los archivos que han cambiado en un repositorio de datos vinculados después de la creación del sistema de archivos. Para más información, consulte Importar actualizaciones automáticamente desde el repositorio de datos. | 23 de julio de 2020 |

| | | |
|---|---|---|
| Se ha agregado compatibilidad con el cliente Lustre para SUSE Linux SP4 y SP5 | El cliente FSx para Lustre ahora es compatible con las instancias de Amazon EC2 que ejecutan SUSE Linux SP4 y SP5. Para obtener más información, consulte Instalación del cliente de Lustre. | 20 de julio de 2020 |
| Se ha agregado compatibilidad con clientes Lustre para Centos y Red Hat Enterprise Linux (RHEL) 8.2 | El cliente FSx para Lustre ahora es compatible con instancias de Amazon EC2 que ejecutan Centos y Red Hat Enterprise Linux (RHEL) 8.2. Para obtener más información, consulte Instalación del cliente de Lustre. | 20 de julio de 2020 |
| Se ha agregado compatibilidad para copias de seguridad automáticas y manuales del sistema de archivos | Ahora puede realizar copias de seguridad diarias automáticas y copias de seguridad manuales de sistemas de archivos no vinculados a un repositorio de datos duraderos de Amazon S3. Para obtener más información, consulte Trabajar con copias de seguridad. | 23 de junio de 2020 |

| | | |
|---|---|---|
| Se publicaron dos nuevos tipos de implementación de sistemas de archivos | Los sistemas de archivos Scratch están diseñados para el almacenamiento temporal y el procesamiento de datos a corto plazo. Los sistemas de archivos persistentes están diseñados para cargas de trabajo y almacenamiento a largo plazo. Para obtener más información, consulte Opciones de implementación FSx para Lustre. | 12 de febrero de 2020 |
| Se ha agregado compatibilidad para metadatos POSIX | FSx para Lustre conserva los metadatos POSIX asociados al importar y exportar archivos a un repositorio de datos duraderos vinculados en Amazon S3. Para obtener más información, consulte Soporte de metadatos POSIX para repositorios de datos. | 23 de diciembre de 2019 |
| Se ha lanzado una nueva característica de tareas de repositorio de datos | Ahora puede exportar datos modificados y metadatos POSIX asociados a un repositorio de datos duraderos vinculados en Amazon S3 mediante tareas de repositorio de datos. Para obtener más información, consulte Transferencia de datos y metadatos mediante tareas de repositorio de datos. | 23 de diciembre de 2019 |

| | | |
|---|---|---|
| Se agregó Región de AWS soporte adicional | FSx para Lustre ya está disponible en la región Región de AWS de Europa (Londres) . Para conocer los límites específicos de una región FSx para Lustre, consulte Límites. | 9 de julio de 2019 |
| Se agregó Región de AWS soporte adicional | FSx for Lustre ya está disponible en Asia Pacífico (Singapur). Región de AWS Para conocer los límites específicos de una región FSx para Lustre, consulte Límites. | 26 de junio de 2019 |
| Se ha agregado compatibilidad con clientes Lustre para Amazon Linux y Amazon Linux 2 | El cliente FSx para Lustre ahora es compatible con las instancias de Amazon EC2 que ejecutan Amazon Linux y Amazon Linux 2. Para obtener más información, consulte Instalación del cliente de Lustre. | 11 de marzo de 2019 |
| Se ha añadido soporte para rutas de exportación de datos definidas por el usuario | Los usuarios ahora tienen la opción de sobrescribir los objetos originales en su bucket de Amazon S3 o escribir los archivos nuevos o modificados en un prefijo que especifique. Con esta opción, dispone de flexibilidad adicional para incorporar FSx para Lustre a sus flujos de trabajo de procesamiento de datos. Para obtener más información, consulte Exportación de datos a su bucket de Amazon S3. | 6 de febrero de 2019 |

| | | |
|---|---|---|
| Aumento del límite de almacenamiento total por defecto | El almacenamiento total por defecto para todos los sistemas de archivos de FSx para Lustre aumentó a 100.800 GiB. Para obtener más información, consulte Límites. | 11 de enero de 2019 |
| Amazon FSx para Lustre ya está disponible de forma general | Amazon FSx para Lustre es un sistema de archivos totalmente administrado que está optimizado para cargas de trabajo informáticas intensivas, como la informática de alto rendimiento, machine learning y flujos de trabajo de procesamiento de medios. | 28 de noviembre de 2018 |

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.