Guía del usuario de Lustre

FSx para Lustre

FSx para Lustre: Guía del usuario de Lustre

Table of Contents

¿Qué es Amazon FSx for Lustre?

FSx for Lustre hace que sea fácil y rentable lanzar y ejecutar el popular sistema de Lustre archivos 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 de Lustre 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, un rendimiento de hasta un múltiplo y hasta millones TBps de IOPS. Para obtener más información sobre Lustre, consulte el sitio web de Lustre.

Como servicio totalmente gestionado, Amazon FSx facilita su uso Lustre para cargas de trabajo en las que la velocidad de almacenamiento es importante. FSx for Lustre elimina la complejidad tradicional de configurar y administrar los sistemas de Lustre archivos, 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 y clases de almacenamiento para que pueda optimizar los costes en característica de las necesidades.

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

Temas

- ¿Es la primera vez que utilizas Amazon FSx for Lustre?

Múltiples opciones de implementación y clases de almacenamiento

Amazon FSx for Lustre ofrece una variedad 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 clases de implementación y almacenamiento FSx para los sistemas de archivos Lustre.

Amazon FSx for Lustre ofrece clases de almacenamiento en unidades de estado sólido (SSD) y unidades de disco duro (HDD) optimizadas para diferentes requisitos de procesamiento de datos: AWS Interconnect

- La clase de almacenamiento SSD está optimizada para cargas de trabajo que tienen operaciones de archivos pequeñas y aleatorias y que necesitan un rendimiento TBps máximo. Proporciona un acceso uniforme con una latencia inferior a un milisegundo a todo el conjunto de datos.
- La clase de almacenamiento Intelligent-Tiering es adecuada y recomendada para la mayoría de las cargas de trabajo que no necesitan una baja latencia constante en todo el conjunto de datos. Proporciona un almacenamiento totalmente elástico y rentable, con un rendimiento de hasta un múltiplo y un acceso TBps de latencia inferior a un milisegundo a los datos a los que se accede con frecuencia con una caché de lectura SSD opcional.
- La clase de almacenamiento en disco duro se puede utilizar con cargas de trabajo que necesitan una latencia constante en ms de un solo dígito y un rendimiento de hasta decenas de veces para todo el conjunto de datos. GBps También puede aprovisionar una caché de lectura en SSD con un tamaño del 20 % de la capacidad de almacenamiento de su disco duro.

Para obtener más información, consulte FSx para las clases de almacenamiento de Lustre.

FSx para Lustre y repositorios de datos

Puede vincular los sistemas FSx de archivos de Lustre a los repositorios de datos de Amazon S3 o a los almacenes de datos locales.

FSx para la integración del repositorio de datos de Lustre S3

FSx for Lustre se integra con Amazon S3, lo que facilita el procesamiento de conjuntos de datos en la nube mediante el sistema de archivos de Lustre alto rendimiento. Cuando se vincula a un bucket de Amazon S3, un sistema de archivos FSx for Lustre presenta de forma transparente los objetos S3 como archivos. Amazon FSx importa listados de todos los archivos existentes en su bucket de S3 al crear el sistema de archivos. Amazon también FSx 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 su sistema de archivos FSx for Lustre y su repositorio de datos duradero en Amazon S3. Para obtener más información, consulte Uso de repositorios de datos con Amazon FSx for Lustre y Tareas de repositorio de datos.

FSx para repositorios de datos locales y de Lustre

Con Amazon FSx for Lustre, puede dividir sus cargas de trabajo de procesamiento de datos del entorno local en el entorno local importando datos Nube de AWS mediante o. Direct Connect Site-to-Site VPN Para obtener más información, consulte Uso de Amazon FSx con tus datos locales.

Acceso a los sistemas de archivos FSx Lustre

Puede mezclar y combinar los tipos de instancias de procesamiento y las Amazon Machine Images (AMIs) de Linux que están conectadas a un único sistema de archivos FSx for Lustre.

Se puede acceder a los sistemas de archivos de Amazon FSx for Lustre desde cargas de trabajo informáticas que se ejecutan en instancias de Amazon Elastic Compute Cloud (Amazon EC2), en contenedores Docker de Amazon Elastic Container Service (Amazon ECS) y en contenedores que se ejecutan en Amazon Elastic Kubernetes Service (Amazon EKS).

- Amazon EC2: accede a su sistema de archivos desde sus instancias EC2 informáticas de Amazon mediante el Lustre cliente de código abierto. EC2 Las instancias de Amazon pueden acceder a su sistema de archivos desde otras zonas de disponibilidad dentro de la misma Amazon Virtual Private Cloud (Amazon VPC), siempre que la configuración de red permita el acceso a través de subredes de la VPC. Una vez montado el sistema de archivos Amazon FSx for Lustre, podrá trabajar con sus archivos y directorios del mismo modo que lo haría con un sistema de archivos local.

- Amazon EKS: puede acceder a Amazon FSx for Lustre desde contenedores que se ejecutan en Amazon EKS mediante el controlador CSI de código abierto FSx para Lustre, tal y como se describe en la Guía del usuario de Amazon EKS. Los contenedores que se ejecutan en Amazon EKS pueden usar volúmenes persistentes de alto rendimiento (PVs) respaldados por Amazon FSx for Lustre.
- Amazon ECS: accede a Amazon FSx for Lustre desde los contenedores Docker de Amazon ECS en las instancias de Amazon EC2 . Para obtener más información, consulte Montaje de Amazon Elastic Container Service.

Amazon FSx for Lustre es compatible con los sistemas Linux más populares, AMIs incluidos Amazon Linux 2023 y Amazon Linux 2, Red Hat Enterprise Linux (RHEL), Centos, Ubuntu y SUSE Linux. El cliente de Lustre se incluye en Amazon Linux 2023 y Amazon Linux 2. Para RHEL, Centos y Ubuntu, AWS Lustre un repositorio de clientes proporciona clientes que son compatibles con estos sistemas operativos.

Con FSx Lustre, puede distribuir sus cargas de trabajo con un uso intensivo de cómputo desde las instalaciones locales importando datos a través de o. Nube de AWS Direct Connect AWS Virtual Private Network Puede acceder a su sistema de FSx archivos de Amazon desde las instalaciones, copiar los datos en su sistema de archivos según sea necesario y ejecutar cargas de trabajo con un uso intensivo de recursos informáticos en instancias en la nube.

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

Integraciones con servicios AWS

Amazon FSx for Lustre se integra con Amazon SageMaker AI como fuente de datos de entrada. Al utilizar la SageMaker IA 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 la SageMaker IA? en la Guía para desarrolladores de Amazon SageMaker AI. Para ver un tutorial sobre cómo utilizar Amazon FSx for Lustre como fuente de datos para la SageMaker IA, consulte Acelere la formación sobre Amazon SageMaker AI con los sistemas de archivos Amazon FSx for Lustre y Amazon EFS en el blog AWS Machine Learning.

FSx porque Lustre se integra con AWS Batch el uso de plantillas de lanzamiento. EC2 AWS Batch le permite ejecutar cargas de trabajo informáticas por lotes en el entorno Nube de AWS, incluidas cargas de trabajo de computación de alto rendimiento (HPC), aprendizaje automático (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 ¿Qué es AWS Batch? en la Guía AWS Batch del usuario.

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

Seguridad y conformidad

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

Suposición

En esta guía, hacemos las siguientes suposiciones:

- Si utilizas Amazon Elastic Compute Cloud (Amazon EC2), asumimos que estás familiarizado con ese servicio. Para obtener más información sobre cómo usar Amazon EC2, consulta la EC2 documentación de Amazon.
- 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 su EC2 instancia de Amazon a su sistema de archivos Amazon FSx for Lustre. Para obtener más información, consulta Control de acceso al sistema de archivos con Amazon VPC.

Precios de Amazon FSx for Lustre

Con Amazon FSx for 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 las tarifas asociadas al servicio, consulta los precios de Amazon FSx for Lustre.

Foros FSx de Amazon for Lustre

Si tienes problemas al usar Amazon FSx for Lustre, consulta los foros.

¿Es la primera vez que utilizas Amazon FSx for Lustre?

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

1. Si está listo para crear su primer sistema de archivos Amazon FSx for Lustre, inténteloIntroducción a Amazon FSx para Lustre.
2. Para obtener más información sobre el desempeño, consulte Rendimiento de Amazon FSx for 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 for Lustre.
4. Para ver los detalles de seguridad de Amazon FSx for Lustre, consulteSeguridad en Amazon FSx para Lustre.
5. Para obtener información sobre los límites de escalabilidad de Amazon FSx for Lustre, incluidos el rendimiento y el tamaño del sistema de archivos, consulte. Service Quotas para Amazon FSx para Lustre
6. Para obtener información sobre la API de Amazon FSx for Lustre, consulte la referencia de la API de Amazon FSx for Lustre.

Cómo configurar Amazon FSx for Lustre

Antes de usar Amazon FSx for Lustre por primera vez, complete las tareas de la Inscribirse en Amazon Web Services sección. 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 configurarlo AWS, complete las siguientes tareas:

1. Inscríbase en una Cuenta de AWS
2. Creación de un usuario con acceso administrativo

Inscríbase en una Cuenta de AWS

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

Para suscribirse a una Cuenta de AWS

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

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

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

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a https://aws.amazon.com/y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

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

Proteja su Usuario raíz de la cuenta de AWS

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

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In .
2. Active la autenticación multifactor (MFA) para el usuario raíz.

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

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

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

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

Inicio de sesión como usuario con acceso de administrador

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

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

Concesión de acceso a usuarios adicionales

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

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

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

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

Agregar permisos para utilizar repositorios de datos en Amazon S3

Amazon FSx for Lustre está profundamente integrado con Amazon S3. Esta integración significa que las aplicaciones que acceden a su sistema de archivos FSx for 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 for Lustre.

Para utilizar los repositorios de datos, primero debe conceder a Amazon FSx for 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 Consola de administración de AWS IAM 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 AWS Servicios que funcionan con IAM 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.

   JSON

```
{
    "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 comprueba Lustre el acceso a los buckets S3 enlazados?

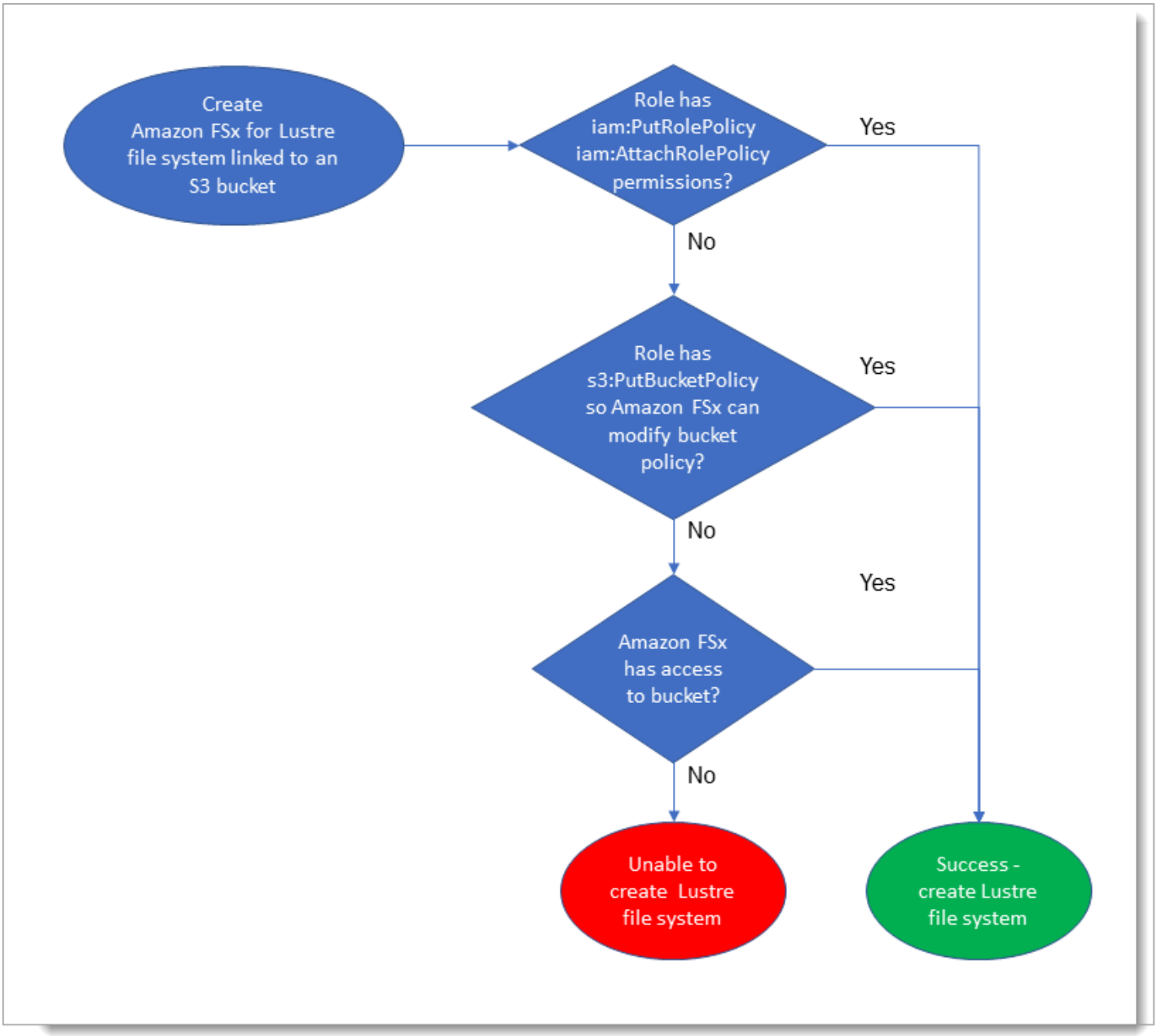
Si la función de IAM que utilizas FSx para crear el sistema de archivos de Lustre no tiene los `iam:PutRolePolicy` permisos `iam:AttachRolePolicy` and, Amazon FSx comprueba si puede

actualizar tu política de bucket de S3. Amazon FSx puede actualizar tu política de buckets si el `s3:PutBucketPolicy` permiso está incluido en tu rol de IAM para permitir que el sistema de FSx archivos de Amazon importe o exporte datos a tu bucket de S3. Si se le permite modificar la política de bucket, Amazon FSx añade los siguientes permisos a la política de bucket:

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

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

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



Siguiente paso

Para empezar a usarloFSx for Lustre, consulta las instrucciones Introducción a Amazon FSx para Lustre para crear tus recursos de Amazon FSx for 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 cuenta AWS con los permisos necesarios para crear un sistema de archivos de Amazon FSx para Lustre y una instancia de Amazon EC2. Para obtener más información, consulte Cómo configurar Amazon FSx for Lustre.
- Cree un grupo de seguridad de Amazon VPC para asociarlo al sistema de archivos de FSx para 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 de 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, recomendamos que use Amazon Linux 2023. Instalará el cliente Lustre en esta instancia de EC2 y, luego, montará el sistema de archivos de FSx para Lustre en la instancia de EC2. Para obtener más información sobre cómo crear una instancia de EC2, consulte Introducción: inicializar una instancia o Inicializar la instancia en la Guía del usuario de Amazon EC2.

Además de Amazon Linux 2023, el cliente de Lustre es compatible con los sistemas operativos Amazon Linux 2, Red Hat Enterprise Linux (RHEL), CentOS, Rocky Linux, SUSE Linux Enterprise Server y Ubuntu. Para obtener más información, consulte Compatibilidad con sistemas de archivos de Lustre y kernel de clientes.

- 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.
- Determine qué tipo de sistema de archivos Amazon FSx para Lustre desea crear, scratch o persistent. Para obtener más información, consulte Opciones de clases de implementación y almacenamiento FSx para los sistemas de archivos Lustre.
- Cada sistema de archivos de FSx para Lustre requiere una dirección IP para cada servidor de metadatos (MDS) y una dirección IP para cada servidor de almacenamiento (OSS). Para obtener más información, consulte Direcciones IP para sistemas de archivos.
- 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.

Paso 1: crear un sistema de archivos FSx para Lustre

Crea el sistema de archivos en la consola de Amazon FSx. Tenga en cuenta que 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.

Cómo 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 for Lustre y, luego, Siguiente para abrir la página Crear sistema de archivos.

   Comience la configuración con la sección de File system details.
4. 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 + - = . _ : /.

5. Para Clase de implementación y almacenamiento, elija una de las siguientes opciones:

   - Elija SSD persistente para un almacenamiento a largo plazo y para cargas de trabajo sensibles a la latencia. Con el almacenamiento SSD, se le facturará por la cantidad de almacenamiento que aprovisione.

     Si lo desea, elija compatible con Elastic Fabric Adapter (EFA) para habilitar la compatibilidad con el EFA para el sistema de archivos. Para obtener más información sobre EFA, consulte Cómo trabajar con sistemas de archivos compatibles con EFA.

   - Elija Intelligent-Tiering persistente para un almacenamiento a largo plazo. La clase de almacenamiento Intelligent-Tiering proporciona un almacenamiento totalmente elástico y rentable que es adecuado para la mayoría de las cargas de trabajo, así como una caché de lectura SSD opcional que proporciona latencias de SSD para leer datos a los que se accede con frecuencia. Con Intelligent-Tiering, se le facturarán los datos que almacene, en característica del tamaño del conjunto de datos, y no necesitará especificar el tamaño del sistema de archivos.

     Si lo desea, elija compatible con Elastic Fabric Adapter (EFA) para habilitar la compatibilidad con el EFA para el sistema de archivos.

   - Elija la implementación SSD scratch para el almacenamiento temporal y el tratamiento de datos a corto plazo. Con el almacenamiento SSD, se le facturará por la cantidad de almacenamiento que aprovisione.

6. Elija la cantidad de rendimiento para el sistema de archivos. Usted paga la cantidad de rendimiento aprovisionada.

   - Para el almacenamiento SSD persistente, elija un Rendimiento por unidad de valor de almacenamiento. El rendimiento por unidad de almacenamiento es la cantidad de rendimiento de lectura y escritura por cada 1 tebibyte (TiB) de almacenamiento aprovisionado.
   - Para el almacenamiento SSD Scratch, elija un Rendimiento por unidad de valor de almacenamiento.
   - Para el almacenamiento Intelligent-Tiering, elija un valor de capacidad de rendimiento.

7. Para la capacidad de almacenamiento (solo clase de almacenamiento SSD), defina la cantidad de capacidad de almacenamiento del sistema de archivos en TB:

   - 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 SSD persistente y compatibles con EFA, establezca este valor en incrementos de 4,8 TiB, 9,6 TiB, 19,2 TiB y 38,4 TiB para los niveles de rendimiento de 1000, 500, 250 y 125 Mbps/TiB, respectivamente.

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.

8. Para la Configuración de metadatos, elija una de las siguientes opciones para aprovisionar la cantidad de IOPS de metadatos para el sistema de archivos:

   - Elija Automático (solo clase de almacenamiento SSD) si desea que Amazon FSx para Lustre aprovisione y escale automáticamente las IOPS de metadatos en el sistema de archivos en característica de la capacidad de almacenamiento del sistema de archivos.
   - Elija Aprovisionado por el usuario si desea especificar la cantidad de IOPS de metadatos por aprovisionar al sistema de archivos con la clase de almacenamiento SSD o Intelligent-Tiering. Los valores válidos son los siguientes:
     - Para los sistemas de archivos SSD, los valores válidos son `1500`, `3000`, `6000`, `12000` y múltiplos de `12000`, hasta un máximo de `192000`.
     - Para los sistemas de archivos Intelligent-Tiering, los valores válidos son `6000` y `12000`.

   Para obtener más información sobre las IOPS de metadatos, consulte Configuración del rendimiento de los metadatos de Lustre.

9. Para la caché de lectura SSD (solo Intelligent-Tiering), seleccione Automática (proporcional a la capacidad de rendimiento) o Personalizada (proporcionada por el usuario). Con la opción automática, Amazon FSx para Lustre elige automáticamente un tamaño de caché de lectura en característica del rendimiento aprovisionado. Si conoce el tamaño aproximado de su conjunto de datos de trabajo activo, puede seleccionar Personalizado para personalizar el tamaño de la caché de lectura de la SSD. Para obtener más información, consulte Administración de la caché de lectura SSD aprovisionada.

10. 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.

11. 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	Intervalo de puertos	Origen	Descripción
Todos los TCP	TCP	0-65535	Personalizado *the_ID_of_this_security_group*	Regla de tráfico entrante de Lustre

> **Important**
>
> - Corrobore que el grupo de seguridad que use siga las instrucciones de configuración que se incluyen 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.
> - Si va a crear un sistema de archivos compatible con EFA, asegúrese de especificar un Grupo de seguridad con EFA.

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

12. 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, puedes 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 Scratch, 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.

13. 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.
> - Los sistemas de archivos Intelligent-Tiering no admiten la vinculación a los repositorios de datos de Amazon S3.

14. Para el Registro opcional, el registro está activado de forma predeterminada. Cuando está habilitado, los fallos y advertencias de la actividad del repositorio de datos en su sistema de archivos se registran en los Registros de Amazon CloudWatch. Para obtener información sobre la configuración de los registros, consulte Administración de registros.
15. En Copia de seguridad y mantenimiento opcional, puede hacer lo siguiente.
    - 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.

- Defina la hora de inicio de la Ventana de mantenimiento semanal o manténgala en el valor predeterminado Sin preferencia.

Para obtener más información, consulte Protección de los datos con copias de seguridad y Períodos de mantenimiento de Amazon FSx para Lustre.

16. En el caso de Root Squash opcional, la característica root squash está deshabilitada de forma predeterminada. Para obtener más información sobre cómo habilitar y configurar root squash, consulte Para habilitar la característica root squash al crear un sistema de archivos (consola).
17. Cree las etiquetas que desee aplicar a su sistema de archivos.
18. Seleccione Siguiente para mostrar la página de Resumen de creación del sistema de archivos.
19. 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 Sistemas de archivos y luego seleccionando Adjuntar.

Paso 2: instalar y configurar el cliente Lustre

Antes de poder acceder al sistema de archivos de Amazon FSx para Lustre desde la instancia de Amazon EC2, debe hacer lo siguiente:

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

Para comprobar la versión del kernel y descargar el cliente Lustre

1. Abra una ventana de la terminal en la instancia de 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 siguientes acciones:

   - Si el comando devuelve `6.1.79-99.167.amzn2023.x86_64` para instancias de EC2 basadas en x86, o `6.1.79-99.167.amzn2023.aarch64` o superior para instancias de 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. A continuación, descargue e instale el cliente Lustre como se describió anteriormente.

Para obtener información sobre cómo instalar el cliente Lustre en otras distribuciones de Linux, consulte Instalación del cliente de Lustre.

Paso 3: montar 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 este 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.

- Sustituya *mountname* por el nombre de montaje del sistema de archivos, que puede obtener ejecutando el comando describe-file-systems command AWS CLI o la operación de la API DescribeFileSystems.

```
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.

Paso 4: 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 el sistema de archivos a un bucket de Amazon 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.

Paso 5: Limpieza de recurso

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

Cómo 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 Finalizar una instancia en la Guía del usuario de Amazon EC2.
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 clases de implementación y almacenamiento FSx para los sistemas de archivos Lustre

Amazon FSx for Lustre ofrece dos opciones de implementación de sistemas de archivos: persistente y temporal. Ofrece tres clases de almacenamiento: SSD (unidad de estado sólido) y HDD (unidad de disco duro). AWS Interconnect

Usted elige el tipo de implementación del sistema de archivos y la clase de almacenamiento al crear un nuevo sistema de archivos mediante la Consola de administración de AWS API, AWS Command Line Interface (AWS CLI) o Amazon FSx for Lustre. Para obtener más información, consulta Paso 1: crear un sistema de archivos FSx para Lustre y consulta CreateFileSystemla Amazon FSx API Reference.

Sistemas de archivos persistentes

Los sistemas de archivos persistentes están diseñados para cargas de trabajo y almacenamiento a largo plazo, y los servidores de archivos tienen alta disponibilidad. Para los sistemas de archivos basados en SSD y HDD, los datos se replican automáticamente dentro de la misma Zona de Disponibilidad en la que se encuentra el sistema de archivos. En el caso de los sistemas de archivos Intelligent-Tiering, los datos se replican en varias zonas de disponibilidad. 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 monitorea FSx continuamente 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 fallo. 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.

Los tipos de despliegue persistentes cifran automáticamente los datos en tránsito cuando se accede a ellos desde EC2 instancias de Amazon que admiten el cifrado en tránsito.

Amazon FSx for Lustre admite dos tipos de despliegues persistentes: Persistent 1 y Persistent 2.

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 que requieren los más altos niveles de IOPS y rendimiento. Los dos sistemas de archivos Persistent 2 admiten las clases de almacenamiento SSD e Intelligent-Tiering.

Puede crear sistemas de archivos Persistent 2 con una configuración de metadatos y un EFA habilitado mediante la FSx consola de Amazon y la FSx API de Amazon. AWS Command Line Interface

Tipo de implementación Persistent 1

El tipo de implementación Persistent 1 es adecuado para casos de uso que requieren almacenamiento a largo plazo. Los tipos de implementación Persistent 1 admiten clases de almacenamiento en SSD (unidad de estado sólido) y en HDD (unidad de disco duro).

Solo puedes crear tipos de despliegue Persistent 1 mediante la API AWS CLI y la FSx API de Amazon.

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 ofrecen un alto rendimiento de ráfaga de hasta seis veces el rendimiento básico de 200 por MBps TiB de capacidad de almacenamiento. Para obtener más información, consulte Características de rendimiento de las clases de almacenamiento en SSD y HDD.

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

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 los datos que se encuentran en el servidor o disco no disponible, se produce un error inmediato. I/O

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%

Direcciones IP para sistemas de archivos

Cada FSx sistema de archivos de Lustre requiere una dirección IP para cada servidor de metadatos (MDS) y una dirección IP para cada servidor de almacenamiento (OSS).

Sistemas de archivos que utilizan la clase de almacenamiento SSD o HDD

Tipo de sistema de archivos	Rendimiento, /TiB MBps	Almacenamiento por OSS
Persistent 2 con EFA*	125	38,4 TiB por OSS
	250	19,2 TiB por OSS
	500	9,6 TiB por OSS

Tipo de sistema de archivos	Rendimiento, /TiB MBps	Almacenamiento por OSS
	1 000	4,8 TiB por OSS
Persistent 2 sin EFA*	125, 250, 500, 1000	2,4 TiB por OSS
Persistent 1 SSD	50, 100, 200	2,4 TiB por OSS
Persistent HDD	12	6 TiB por OSS
	40	1,8 TiB por OSS
Scratch 2	200	2,4 TiB por OSS
Scratch 1	200	3,6 TiB por OSS

Sistemas de archivos que utilizan la clase de almacenamiento Intelligent-Tiering

Tipo de sistema de archivos	Rendimiento por OSS
Intelligent-Tiering*	4000 MBps por sistema operativo

> **Note**
>
> * Amazon FSx aprovisiona un servidor de metadatos por cada 12 000 IOPS de metadatos en los sistemas de archivos Persistent 2 SSD e Intelligent-Tiering configurados con una configuración de metadatos.
> Los sistemas de archivos Amazon FSx for Lustre Intelligent-Tiering admiten un máximo de 512 TiB de almacenamiento por OSS.

FSx para las clases de almacenamiento de Lustre

Amazon FSx for Lustre ofrece clases de almacenamiento en unidades de estado sólido (SSD) y unidades de disco duro (HDD) optimizadas para diferentes requisitos de procesamiento de datos: AWS Interconnect

- La clase de almacenamiento SSD proporciona acceso de baja latencia (submilisegundos) a todo el conjunto de datos. La clase de almacenamiento SSD está aprovisionada, lo que significa que debe especificar el tamaño del sistema de archivos y pagar los costes de almacenamiento correspondientes a la cantidad de almacenamiento aprovisionada. Utilice la clase de almacenamiento SSD para cargas de trabajo sensibles a la latencia que requieren el rendimiento del almacenamiento basado íntegramente en tecnología flash en todos los datos.

  Los sistemas de archivos Persistent 2 con almacenamiento SSD admiten niveles más altos de rendimiento por unidad de almacenamiento (es decir, 250, 500 o 1000 MBps por TiB) en comparación con los sistemas de archivos Persistent 1. Para un sistema de archivos Persistent 1 con almacenamiento SSD, el rendimiento por unidad de almacenamiento es de 50, 100 o 200 MBps por TiB. Para un sistema de archivos Scratch con almacenamiento SSD, el rendimiento por unidad de almacenamiento es de 200 MBps por TiB.
- La clase de almacenamiento por niveles inteligentes proporciona un almacenamiento en niveles totalmente elástico e inteligente. La elasticidad significa que usted paga por la cantidad de datos que almacena y no tiene que especificar el tamaño del sistema de archivos. La organización inteligente en niveles significa que usted paga menos automáticamente por almacenar datos a los que no ha accedido recientemente. Esta clase de almacenamiento optimiza automáticamente los costos al organizar los datos inactivos en niveles de almacenamiento de menor costo. Puede aprovisionar una caché de lectura SSD opcional para acceder con baja latencia (submilisegundos) a los datos a los que accede con frecuencia. La clase de almacenamiento Intelligent-Tiering proporciona el mejor equilibrio entre precio y rendimiento para la mayoría de las cargas de trabajo. Utilice la clase de almacenamiento Intelligent-Tiering para cargas de trabajo compatibles con la caché en memoria y que no requieran el rendimiento del almacenamiento basado íntegramente en tecnología flash en todos los datos. Los sistemas de archivos Intelligent-Tiering admiten capacidades de rendimiento en incrementos de 4000. MBps
- La clase de almacenamiento en HDD se puede utilizar con cargas de trabajo que necesitan una latencia de ms uniforme de un solo dígito en todos los datos. Puede aprovisionar una caché de lectura SSD opcional con un tamaño equivalente al 20 % de la capacidad de almacenamiento de su disco duro para proporcionar acceso de baja latencia a los datos a los que se accede con frecuencia. Con el almacenamiento HDD, usted especifica el tamaño del sistema de archivos y

paga por la cantidad de almacenamiento que aprovisiona. Para un sistema de archivos Persistent 1 con almacenamiento en disco duro, el rendimiento por unidad de almacenamiento es de 12 o 40 MBps por TiB.

Para obtener más información sobre el rendimiento de estas clases de almacenamiento, consulte Características de rendimiento de las clases de almacenamiento en SSD y HDD y Características de rendimiento de la clase de almacenamiento Intelligent-Tiering.

Cómo clasifica los datos la clase de almacenamiento Intelligent-Tiering

La clase de almacenamiento Amazon FSx Intelligent-Tiering almacena automáticamente los datos en tres niveles de acceso. Se ha diseñado para optimizar los costos de almacenamiento mediante el desplazamiento automático de los datos a la capa de acceso de almacenamiento más rentable, sin que afecte al rendimiento ni se produzca sobrecarga operativa. La clase de almacenamiento Intelligent-Tiering clasifica automáticamente los datos en característica de la hora del último acceso, lo que optimiza automáticamente los costos de los datos menos activos:

- Los datos a los que se accedió en los últimos 30 días se almacenan en la capa de acceso frecuente.
- Los datos a los que no se accedió en 30 días consecutivos pasan automáticamente a la capa de acceso poco frecuente y cuestan menos que los datos de la capa de acceso frecuente.
- Los datos a los que no se accedió en 90 días consecutivos pasan automáticamente al nivel Acceso instantáneo a archivos y cuestan menos que los datos del nivel de Acceso poco frecuente.

Cuando acceda a los datos del Acceso poco frecuente o Acceso instantáneo de archivos, los datos se desplazan automáticamente al nivel de Acceso frecuente. Todos los accesos a datos no almacenados en caché tienen las mismas características de rendimiento, independientemente del nivel de los datos, y no implican costes adicionales de IOPS, recuperación o transición más allá de los costes operativos normales. read/write

Disponibilidad del tipo de implementación

Los tipos de implementación Scratch 2, Persistent 1 y Persistent 2 están disponibles de la siguiente manera: Regiones de AWS

Región de AWS	Persistent 2	Persistent 1	Scratch 2
Este de EE. UU. (Ohio)	✓	✓	✓
Este de EE. UU. (Norte de Virginia)	✓	✓	✓
Zona local del Este de EE. UU. (Atlanta)	✓ *		
Zona local del Este de EE. UU. (Dallas)	✓ *		
Oeste de EE. UU. (Norte de Californi a)	✓	✓	✓
Zona local del Oeste de EE. UU. (Los Ángeles)		✓	✓
Oeste de EE. UU. (Oregón)	✓	✓	✓
Zona en las instalaciones del Oeste de EE. UU. (Phoenix)	✓ *		
Africa (Cape Town)		✓	✓
Asia-Pacífico (Hong Kong)	✓	✓	✓
Asia-Pacífico (Hyderabad)		✓	✓
Asia-Pacífico (Yakarta)		✓	✓
Asia-Pacífico (Malasia)	✓ *		
Asia-Pacífico (Melbourne)		✓	✓
Asia-Pacífico (Mumbai)	✓	✓	✓
Asia-Pacífico (Osaka)		✓	✓
Asia-Pacífico (Seúl)	✓	✓	✓

Región de AWS	Persistent 2	Persistent 1	Scratch 2
Asia-Pacífico (Singapur)	✓	✓	✓
Asia-Pacífico (Sídney)	✓	✓	✓
Asia-Pacífico (Taipéi)	✓ *		
Asia-Pacífico (Tailandia)	✓ *		
Asia-Pacífico (Tokio)	✓	✓	✓
Canadá (centro)	✓	✓	✓
Oeste de Canadá (Calgary)	✓ *		
Europa (Fráncfort)	✓	✓	✓
Europa (Irlanda)	✓	✓	✓
Europa (Londres)	✓	✓	✓
Europa (Milán)		✓	✓
Europa (París)		✓	✓
Europa (España)		✓	✓
Europa (Estocolmo)	✓	✓	✓
Europa (Zúrich)		✓	✓
Israel (Tel Aviv)	✓ *		✓
México (centro)	✓ *		
Middle East (Bahrain)		✓	✓
Medio Oriente (EAU)		✓	✓
América del Sur (São Paulo)		✓	✓

Región de AWS	Persistent 2	Persistent 1	Scratch 2
AWS GovCloud (Este de EE. UU.)		✓	✓
AWS GovCloud (Estados Unidos-Oeste)		✓	✓

> **Note**
>
> * Son Regiones de AWS compatibles con los sistemas de archivos Persistent-125 y Persistent-250 con clase de almacenamiento SSD sin EFA.

Uso de repositorios de datos con Amazon FSx for Lustre

Amazon FSx for 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 a largo plazo en Amazon S3. FSx for Lustre está integrado de forma nativa con Amazon S3, lo que facilita el procesamiento de conjuntos de datos con el Lustre sistema de archivos.

> **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 de Amazon S3. Para obtener más información, consulte Protección de los datos con copias de seguridad.
> - Los sistemas de archivos Intelligent-Tiering no admiten la vinculación a los repositorios de datos de Amazon S3.

Temas

Información general de los repositorios de datos

Cuando utiliza Amazon FSx for Lustre con repositorios de datos, puede ingerir y procesar grandes volúmenes de datos de archivos en un sistema de archivos de alto rendimiento mediante tareas automáticas de importación e importación 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 o FSx sistemas de archivos Lustre 2.10. `Scratch 1`

FSx for 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 for Lustre. También puede ejecutar sus cargas de trabajo con un uso intensivo de recursos informáticos en EC2 instancias de Amazon 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 and/or eliminan los 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 for Lustre también admite cargas de trabajo repletas de nubes con sistemas de archivos locales, ya que le permite copiar datos de clientes locales mediante una VPN. Direct Connect

> **Important**
>
> Si ha vinculado uno o más sistemas de archivos de FSx For 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 vinculados.

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 FSx archivos de Amazon y el bucket de S3 vinculado pueden estar ubicados en el mismo lugar Región de AWS o en sitios diferentes Regiones de AWS.
- La importación automática no admite configuraciones entre regiones. Tanto el sistema de FSx archivos de Amazon como el bucket de S3 vinculado deben estar ubicados en el mismo lugar Región de AWS.
- Tanto la exportación automática como la importación automática admiten configuraciones entre cuentas. El sistema de FSx archivos de Amazon y el bucket de S3 vinculado pueden pertenecer al mismo Cuenta de AWS o a uno diferente Cuentas de AWS.

Soporte de metadatos POSIX para repositorios de datos

Amazon FSx for 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. Cuando exporta los cambios de su sistema de archivos a su repositorio de datos enlazado, FSx for Lustre también exporta los cambios en los metadatos de POSIX como metadatos de objetos de S3. Esto significa que si otro sistema FSx de archivos de 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 for Lustre importa solo los objetos de S3 que tienen claves de objeto compatibles con POSIX, como las siguientes.

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

FSx En el caso de Lustre, los directorios y los enlaces simbólicos se almacenan como objetos independientes en el repositorio de datos enlazados de S3. En el caso de los directorios, FSx en

el caso de Lustre, crea un objeto de S3 con un nombre clave que termina en una barra («/»), de la siguiente manera:

- La clave del objeto de S3 se `mydir/` asigna al directorio de Lustre FSx . `mydir/`
- La clave de objeto S3 se `mydir/mysubdir/` asigna al directorio FSx for 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, en relación con el directorio de montaje FSx de Lustre
- Datos del objeto S3: la ruta de destino de este enlace simbólico
- Metadatos del objeto S3: los metadatos del enlace simbólico

FSx for Lustre almacena los metadatos POSIX, que incluyen la propiedad, los permisos y las marcas de tiempo de los archivos, directorios y enlaces simbólicos, en los objetos de 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 porque 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 `conns`; de lo contrario FSx , 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 `conns`; de lo contrario, FSx para Lustre interpreta el valor como milisegundos.

- `x-amz-meta-user-agent`— El agente de usuario, ignorado FSx durante la importación de Lustre. Durante la exportación, FSx for 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 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 for Lustre no conserva ningún metadato personalizado definido por el usuario en los objetos de S3.

Enlaces duros y exportación a Amazon 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 físicos se exportan a S3 mediante tareas de repositorio de datos (DRTs), cada enlace físico contenido en las rutas especificadas para la 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 for Lustre se vincula a un bucket de S3 al que anteriormente otro sistema de archivos FSx for Lustre, AWS DataSync o Amazon FSx File Gateway, 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 físicos en un sistema de archivos que tiene asociaciones de repositorios de datos (DRAs) 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. Si lo hace, podrá importar los permisos POSIX cuando cree un sistema de FSx archivos de Amazon que esté 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. Verifica los permisos en el sistema de FSx archivos de Amazon 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 el sistema de archivos a un bucket de Amazon S3

Puede vincular su sistema de archivos Amazon FSx for Lustre a 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 archivos FSx de 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 directorio del sistema de archivos exclusivo FSx para Lustre y un bucket o prefijo S3 único 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 Lustre 2.10 ni en FSx los sistemas de archivos. `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 el DRA o cargar los metadatos de los lotes de archivos y directorios a los que desee acceder mediante el FSx sistema de archivos de 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 de su repositorio de datos de S3, FSx for Lustre detecta los cambios y, a continuación, los importa automáticamente a su sistema de archivos. A medida que crea, modifica o elimina archivos, FSx for Lustre exporta automáticamente los cambios a Amazon S3 de forma asíncrona una vez que la aplicación termine 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 for Lustre no evita escrituras conflictivas en varias ubicaciones.
> - En el caso de los archivos marcados con un atributo inmutable, FSx for Lustre no puede sincronizar los cambios entre el sistema de archivos de FSx For Lustre y un bucket de S3 vinculado al sistema de archivos. Si se establece un indicador inmutable durante un período de tiempo prolongado, es posible que se degrade 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 a la ruta del repositorio de datos especificada one-to-one 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://bucket-name/prefix/`. Esta propiedad especifica el lugar desde el que se importarán o exportarán los archivos del repositorio de datos de S3. FSx for Lustre añadirá una «/» al final a la ruta del repositorio de datos si no la proporciona. Por ejemplo, si proporciona una ruta de repositorio de datos des`3://amzn-s3-demo-bucket/my-prefix`, FSx for Lustre la interpretará como. `s3://amzn-s3-demo-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://amzn-s3-demo-bucket/`

`my-prefix/` está vinculado al sistema de archivos, no se puede crear otra asociación de repositorio de datos con la ruta de repositorio de datos `s3://amzn-s3-demo-bucket/my-prefix/my-sub-prefix`.

- 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 FSx API AWS CLI o Amazon.
- 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 (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 FSx API AWS CLI o Amazon.

La configuración de la ruta del sistema de archivos y la ruta del repositorio de datos proporcionan un mapeo 1:1 entre las rutas en Amazon FSx y las claves de objeto en S3.

Temas

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 FSx para un sistema de archivos de Lustre con un bucket de S3 existente, mediante el comando Consola de administración de AWS and 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. Abre la FSx consola de Amazon en https://console.aws.amazon.com/fsx/.
2. Siga el procedimiento para crear un nuevo sistema de archivos que se describe en Paso 1: crear un sistema de archivos FSx para Lustre en la sección Primeros pasos.
3. Abre el repositorio Import/Export de datos (sección opcional). 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.
   - Ruta del sistema de archivos: introduzca el nombre de un directorio de alto nivel (por ejemplo`/ns1`) o subdirectorio (por ejemplo`/ns1/subdir`) del sistema de FSx archivos de Amazon que se asociará al 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://amzn-s3-demo-bucket/my-prefix`).

Dos asociaciones de repositorios de datos no pueden tener rutas de repositorios de datos superpuestas. 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. Abre la FSx consola de Amazon 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.

   - Ruta del sistema de archivos: introduzca el nombre de un directorio de alto nivel (por ejemplo `/ns1`) o subdirectorio (por ejemplo `/ns1/subdir`) del sistema de FSx archivos de Amazon que se asociará al 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://amzn-s3-demo-bucket/my-prefix`). Dos asociaciones de repositorios de datos no pueden tener rutas de repositorios de datos superpuestas. 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. Seleccione Crear.

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 FSx archivos de Amazon 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 Amazon FSx CLI`create-data-repository-association`, tal y 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://amzn-s3-demo-bucket/myprefix/ \
    --s3
"AutoImportPolicy={Events=[NEW,CHANGED,DELETED]},AutoExportPolicy={Events=[NEW,CHANGED,DEL
```

Amazon FSx devuelve inmediatamente la descripción en JSON del 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 Consola de administración de AWS AWS CLI, la y la FSx API de Amazon, 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.

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

1. Abre la FSx consola de Amazon 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. Elija Actualizar.

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

- Para actualizar una asociación de repositorios de datos, utilice el comando Amazon FSx CLI`update-data-repository-association`, tal y 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
```

Tras 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 por el proceso de eliminar una asociación de repositorio de datos de un sistema de FSx archivos de Amazon existente a un bucket de S3 existente, mediante el Consola de administración de AWS comando and 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. Abre la FSx consola de Amazon 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. En el cuadro de diálogo Eliminar, puede elegir Eliminar datos en el sistema de archivos para eliminar físicamente los datos del sistema de archivos que corresponden a la asociación del repositorio de datos.

   Elija esta opción si planea crear una nueva asociación de repositorios de datos utilizando la misma ruta del sistema de archivos pero apuntando a un prefijo de bucket de S3 diferente, o si ya no necesita los datos de su sistema de archivos.
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 FSx archivos de Amazon 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 Amazon FSx CLI`delete-data-repository-association`, tal y como se muestra a continuación.

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

Tras eliminar correctamente la asociación de repositorios de datos, Amazon FSx devuelve su descripción como JSON.

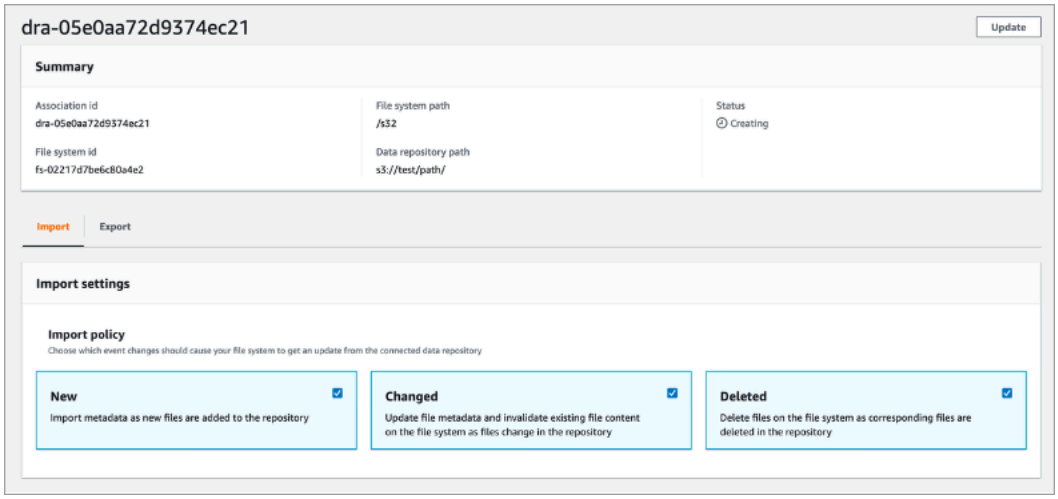
Visualización de los detalles de asociación del repositorio de datos

Puede ver los detalles de una asociación de repositorios de datos mediante FSx la consola de Lustre AWS CLI, la 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.

Cómo ver los detalles de la DRA (consola)

1. Abre la FSx consola de Amazon 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.



Cómo ver los detalles de la DRA (CLI)

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

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

  Amazon FSx devuelve la descripción de la asociación de repositorios 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:

- Creación: Amazon FSx está creando 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.
- Configuración incorrecta: 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.

  Un DRA puede configurarse incorrectamente debido a lo siguiente:

  - Amazon FSx carece de los permisos de IAM necesarios para acceder al bucket de S3.
  - La configuración de notificación de FSx eventos del bucket de S3 se elimina o modifica.
  - El bucket de S3 tiene notificaciones de eventos existentes que se superponen con los tipos de FSx eventos.

  Tras resolver el problema subyacente, el DRA vuelve automáticamente al estado Disponible en 15 minutos. También puede activar el cambio de estado inmediatamente mediante el AWS CLI comando update-data-repository-association.
- 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 FSx consola de Amazon AWS Command Line Interface, la y la FSx API de Amazon. Para obtener 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 for Lustre admite buckets de Amazon S3 que utilizan cifrado del lado del servidor con claves administradas por S3 (SSE-S3) y almacenadas en (SSE-KMS). AWS KMS keys AWS Key Management Service

Si quieres que Amazon cifre los datos FSx al escribir en tu bucket de S3, debes configurar el cifrado predeterminado de tu 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 el depósito de S3, Amazon FSx sigue la política de cifrado predeterminada del depósito de S3.

De forma predeterminada, Amazon FSx admite buckets S3 cifrados mediante SSE-S3. Si desea vincular su sistema de FSx archivos de Amazon 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 FSx a Amazon cifrar y descifrar los objetos de su bucket de S3 con su clave de KMS.

La siguiente declaración permite que un sistema de FSx archivos de Amazon específico cifre y descifre 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 FSx archivos de Amazon de tu 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:ViaService": "s3.bucket-region.amazonaws.com",
          "kms:CallerAccount": "aws_account_id"
        },
        "StringLike": {
            "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::bucket_name/*"
        },
        "ArnLike": {
          "aws:PrincipalArn": "arn:aws_partition:iam::aws_account_id:role/aws-service-
role/s3.data-source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_fs-*"
        }
      }
}
```

Acceder a buckets de Amazon S3 cifrados del lado del servidor en una VPC diferente Cuenta de AWS o desde una VPC compartida

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

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

Utilice la función de IAM para llamar a la siguiente AWS KMS API a fin de crear una concesión para la SLR de S3, de modo que la 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

Puedes importar los cambios en los datos y metadatos POSIX desde un repositorio de datos vinculado a tu sistema de FSx archivos de Amazon. 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 obtener 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 obtener 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 for Lustre copia automáticamente el contenido de un archivo de su repositorio de datos y lo carga en el sistema de archivos cuando su aplicación accede por primera vez al archivo del sistema de archivos. For Lustre gestiona este movimiento de datos y es transparente FSx 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 obtener más información, consulte Precargar los archivos en el sistema de archivos. Si solicita la precarga de varios archivos simultáneamente, Lustre carga FSx los archivos del repositorio de datos de Amazon S3 en paralelo.

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

> **Note**
>
> FSx for Lustre no admite la importación de metadatos para enlaces simbólicos (enlaces simbólicos) de las clases de almacenamiento S3 Glacier Flexible Retrieval y S3 Glacier Deep Archive. Los metadatos de los objetos S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive que no sean enlaces simbólicos se pueden importar (es decir, se crea un inodo en el FSx sistema de archivos de 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 de la clase de almacenamiento S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive a FSx for Lustre.

Importe automáticamente actualizaciones desde un bucket de S3

Puede configurar Lustre FSx para que actualice automáticamente los metadatos del sistema de archivos a medida que se añadan, modifiquen o eliminen objetos de su bucket de S3. FSx for 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 for Lustre mantiene los valores de metadatos actuales del archivo, incluidos los permisos actuales.

> **Note**
>
> El sistema FSx de archivos de Lustre y el depósito de S3 vinculado deben estar ubicados en el mismo lugar Región de AWS para que las actualizaciones se importen automáticamente.

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

> **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 este tipo de conflictos. FSx for Lustre no evita escrituras conflictivas en varias ubicaciones.

La política de importación especifica cómo desea FSx que 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:

- Nuevo: FSx para Lustre, solo actualiza automáticamente los metadatos de los archivos y directorios cuando se añaden nuevos objetos al repositorio de datos de S3 vinculado.
- Modificado: FSx ya que Lustre actualiza automáticamente los metadatos de los archivos y directorios solo cuando se cambia un objeto existente en el repositorio de datos.
- Eliminado: FSx ya que Lustre actualiza automáticamente los metadatos de los archivos y directorios solo cuando se elimina un objeto del repositorio de datos.
- Cualquier combinación de nuevo, modificado y eliminado: FSx para Lustre, se actualizan automáticamente los metadatos de los 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.
- Sin política configurada, FSx ya que Lustre no actualiza los metadatos de los archivos y directorios del sistema de archivos cuando se añaden, 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 vinculado FSx a Lustre:
>
> - 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.

Al establecer 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 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 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 for Lustre hace todo lo posible por actualizar su sistema de archivos. FSx for Lustre no puede actualizar el sistema de archivos en las siguientes situaciones:

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

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

Requisitos previos

Se requieren las siguientes condiciones FSx para que 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 obtener 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 for 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), FSx Lustre eliminará 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 obtener 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 obtener más información, consulte Actualización de la configuración de asociación de repositorios de datos.

Monitorización de la importación automática

Si la velocidad de cambio de 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 de FSx For 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 del repositorio de S3 de FSx para Lustre.

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 supervisando los cambios en su FSx sistema de archivos de Lustre. Sin embargo, los cambios adicionales no se sincronizan desde su sistema de archivos FSx de Lustre con 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 de su 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 su sistema de archivos de FSx For Lustre que no se hayan importado o que procedan de cuando la asociación

de repositorios de datos estaba mal configurada, ejecute una tarea de importación del repositorio de datos. Las tareas de importación del repositorio de datos no sincronizan las eliminaciones del depósito de S3 con el sistema de archivos de For Lustre FSx . 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 FSx sistema de archivos de Lustre conectado a un depósito de S3 con una sola partición que envíe de forma continua el máximo número de cambios posibles desde S3, y que solo se ejecute la importación automática en el sistema de archivos de FSx For Lustre, la importación automática puede procesar una acumulación de 7 horas de cambios de S3 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 depósito de S3 y desea que se sincronice con su sistema de archivos de FSx For Lustre, para evitar que los cambios de importación automática superen los 14 días, debe eliminar su sistema de archivos y volver a crearlo una vez que se haya completado el cambio de S3.

Si su `AgeOfOldestQueuedMessage` métrica está aumentando, revise su bucket `GetRequests` de S3 y sus `DeleteRequests` métricas para `PostRequests` ver si hay cambios de actividad que puedan provocar un aumento en el and/or número de cambios que se envían a la importación automática. `PutRequests` Para obtener información sobre las métricas de S3 disponibles, consulte Monitorización de Amazon S3 en la Guía del usuario de Amazon S3.

Para ver una lista de todas las métricas FSx de Lustre disponibles, consulteSupervisión 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 FSx consola y la CLI de Amazon. Tenga en cuenta que puede usar una tarea de repositorio de datos para varias DRAs.

Para importar cambios en los metadatos (consola)

1. Abre la FSx consola de Amazon en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación, elija Sistemas de archivos y, a continuación, elija el sistema de archivos de 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 FSx que Amazon entregará el informe, introduce una ruta relativa en un repositorio de datos de S3 vinculado para la ruta del informe.
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`CLI para importar los cambios de metadatos en su sistema de archivos de FSx for 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
  ```

  Tras 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

Si lo desea, puede precargar el contenido, archivos individuales o directorios en su sistema de archivos.

Importación de archivos mediante comandos de HSM

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. *path/to/file*Sustitúyalos por la ruta del archivo que está precargando en su 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 los archivos del 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 -P 8 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 obtener más información, consulte Administración de la capacidad de almacenamiento.

Paso de validación

Puede ejecutar el script de bash que se indica a continuación para ayudarle a descubrir cuántos archivos u objetos están archivados (liberados).

Para mejorar el rendimiento del script, especialmente en los sistemas de archivos con un gran número de archivos, los subprocesos de la CPU se determinan automáticamente en característica del archivo `/proc/cpuproc`. Es decir, obtendrás un rendimiento más rápido con una instancia de Amazon EC2 con un mayor número de vCPU.

1. Configure el script de bash.

```
#!/bin/bash
```

```
# Check if a directory argument is provided
if [ $# -ne 1 ]; then
    echo "Usage: $0 /path/to/lustre/mount"
    exit 1
fi

# Set the root directory from the argument
ROOT_DIR="$1"

# Check if the provided directory exists
if [ ! -d "$ROOT_DIR" ]; then
    echo "Error: Directory $ROOT_DIR does not exist."
    exit 1
fi

# Automatically detect number of CPUs and set threads
if command -v nproc &> /dev/null; then
    THREADS=$(nproc)
elif [ -f /proc/cpuinfo ]; then
    THREADS=$(grep -c ^processor /proc/cpuinfo)
else
    echo "Unable to determine number of CPUs. Defaulting to 1 thread."
    THREADS=1
fi

# Output file
OUTPUT_FILE="released_objects_$(date +%Y%m%d_%H%M%S).txt"

echo "Searching in $ROOT_DIR for all released objects using $THREADS threads"
echo "This may take a while depending on the size of the filesystem..."

# Find all released files in the specified lustre directory using parallel
# If you  get false positives for file names/paths that include the word
 'released',
# you can grep 'released exists archived' instead of just 'released'
time sudo lfs find "$ROOT_DIR" -type f | \
parallel --will-cite -j "$THREADS" -n 1000 "sudo lfs hsm_state {} | grep released"
 > "$OUTPUT_FILE"

echo "Search complete. Released objects are listed in $OUTPUT_FILE"
echo "Total number of released objects: $(wc -l <"$OUTPUT_FILE")"
```

2. Haga que el script sea ejecutable:

```
$ chmod +x find_lustre_released_files.sh
```

3. Ejecute el script, como en el siguiente ejemplo:

```
$ ./find_lustre_released_files.sh /fsxl/sample
Searching in /fsxl/sample for all released objects using 16 threads
This may take a while depending on the size of the filesystem...
real 0m9.906s
user 0m1.502s
sys 0m5.653s
Search complete. Released objects are listed in
 released_objects_20241121_184537.txt
Total number of released objects: 30000
```

Si hay objetos liberados, realice una restauración masiva en los directorios deseados para llevar los archivos a FSx Lustre desde S3, como en el siguiente ejemplo:

```
$ DIR=/path/to/lustre/mount
$ nohup find $DIR -type f -print0 | xargs -0 -n 1 -P 8 sudo lfs hsm_restore &
```

Tenga en cuenta que `hsm_restore` llevará un tiempo si hay millones de archivos.

Exportación de los cambios al repositorio de datos

Puede exportar los cambios en los datos y los cambios en los metadatos POSIX desde su sistema de archivos de FSx for Lustre a un repositorio de datos vinculado. 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 obtener 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 obtener más información, consulte Soporte de metadatos POSIX para repositorios de datos.

> **Important**
>
> - Para garantizar que FSx 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 for Lustre no exportará archivos cuya clave de objeto de 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

- Uso de las tareas del repositorio de datos para exportar los cambios
- Exportación de archivos mediante comandos de HSM

Exporte automáticamente las actualizaciones a su bucket de S3

Puede configurar su sistema de archivos de FSx For Lustre para que actualice automáticamente el contenido de un bucket de S3 vinculado a medida que se añaden, modifican o eliminan archivos del sistema de archivos. FSx for 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 los sistemas de archivos Lustre 2.10 ni en los sistemas de archivos. `Scratch 1`

Puede exportar a un repositorio de datos que esté en el Región de AWS mismo sistema de archivos o en uno diferente. Región de AWS

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 FSx administración AWS CLI, la API y la AWS API.

> **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 este tipo de conflictos. FSx for Lustre no evita escrituras conflictivas en varias ubicaciones.

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

- Nuevo: FSx para Lustre, solo actualiza automáticamente el repositorio de datos de S3 cuando se crea un nuevo archivo, directorio o enlace simbólico en el sistema de archivos.
- Modificado: FSx para Lustre, solo actualiza automáticamente el repositorio de datos de S3 cuando se cambia 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.
- Eliminado: FSx porque Lustre actualiza automáticamente el repositorio de datos de S3 solo cuando se elimina un archivo, directorio o enlace simbólico del sistema de archivos.
- Cualquier combinación de nuevo, modificado y eliminado: FSx ya que Lustre actualiza automáticamente el repositorio de datos de S3 cuando se produce alguna de las acciones especificadas 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.
- Sin política configurada, FSx ya que 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 obtener más información, consulte Registros de eventos del repositorio de datos.

> **Note**
>
> Si bien la hora de acceso (`atime`) y la hora de modificación (`mtime`) se sincronizan con S3 durante las operaciones de exportación, los cambios en estas marcas de tiempo por sí solos no activan la exportación automática. Solo los cambios en el contenido del archivo u otros metadatos (como la propiedad o los permisos) activarán una exportación automática a S3.

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 obtener 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 obtener 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 obtener más información, consulte Métricas del repositorio de S3 de FSx para Lustre.

> **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 S3 vinculados mediante la FSx consola de Amazon y la CLI. Tenga en cuenta que puede usar una tarea de repositorio de datos para varias DRAs.

Para exportar cambios (consola)

1. Abre la FSx consola de Amazon en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación, elija Sistemas de archivos y, a continuación, elija el sistema de archivos de 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) Especifica hasta 32 directorios o archivos para exportar desde tu sistema de FSx archivos de Amazon proporcionando las rutas a esos directorios o archivos en Rutas del sistema de archivos a exportar. 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 FSx que Amazon entregará el informe, introduce una ruta relativa en el repositorio de datos S3 vinculado al sistema de archivos para la ruta del informe.
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`CLI para exportar los cambios de datos y metadatos a su sistema de archivos FSx for 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
```

Tras 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 de su sistema de archivos FSx for Lustre a un repositorio de datos duradero en Amazon S3, utilice la función de exportación automática que se describe enExporte 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 for 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

Mediante las tareas de importación y exportación de repositorios de datos, puede gestionar la transferencia de datos y metadatos entre su sistema de archivos FSx for 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 su sistema FSx de archivos de Lustre y un repositorio de datos de S3. Una forma de hacerlo es mediante el seguimiento de los cambios entre tu sistema de FSx archivos de Amazon y su repositorio de datos enlazado. También lo hacen mediante el uso de técnicas de transferencia paralela para transferir datos a velocidades de hasta cientos de GBps. Las tareas del repositorio de datos se crean y visualizan mediante la FSx consola de Amazon AWS CLI, la y la FSx API de Amazon.

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 su sistema de archivos de FSx For 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 leen el archivo publicado, FSx for 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 Exportar del repositorio de datos exportan desde el sistema de archivos de Lustre a un bucket de S3 vinculado.
- Las tareas Importar del repositorio de datos importan desde un bucket de S3 vinculado al sistema de archivos de Lustre.
- Las tareas Liberar del repositorio de datos liberan archivos exportados a un bucket de S3 vinculado desde el sistema de archivos de Lustre.

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

Temas

Comprender el estado y los detalles de una tarea

Una tarea de repositorio de datos tiene información descriptiva y un estado del ciclo de vida.

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

- 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.

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

- PENDIENTE indica que Amazon no FSx ha iniciado la tarea.
- EJECUTAR indica que Amazon FSx está procesando la tarea.
- FALLIDO indica que Amazon FSx no ha procesado 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.
- SUCEDED indica que Amazon FSx ha completado la tarea correctamente.
- CANCELED indica que la tarea se canceló y no se completó.

- CANCELAR indica que Amazon FSx está cancelando la tarea.

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

En las siguientes secciones, encontrará información detallada sobre cómo administrar las tareas del repositorio de datos. Puede crear, duplicar, ver los detalles y cancelar las tareas del repositorio de datos mediante la FSx consola, la CLI o la API de Amazon.

Temas

Creación de una tarea de repositorio de datos

Puede crear una tarea de repositorio de datos mediante la FSx consola, la CLI o la API de Amazon. 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 Exportar del repositorio de datos exporta desde el sistema de archivos de Lustre a un bucket de S3 vinculado. Para obtener más información, consulte Uso de las tareas del repositorio de datos para exportar los cambios.
- La tarea Importar del repositorio de datos importa desde un bucket de S3 vinculado al sistema de archivos de Lustre. Para obtener más información, consulte Uso de las tareas del repositorio de datos para importar los cambios.
- La tarea Liberar del repositorio de datos libera los archivos del sistema de archivos de Lustre que se hayan exportado a un bucket de S3 vinculado. Para obtener más información, consulte Utilizar las tareas del repositorio de datos para liberar archivos.

Duplicación de una tarea

Puedes duplicar una tarea de repositorio de datos existente en la FSx consola de Amazon. 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

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

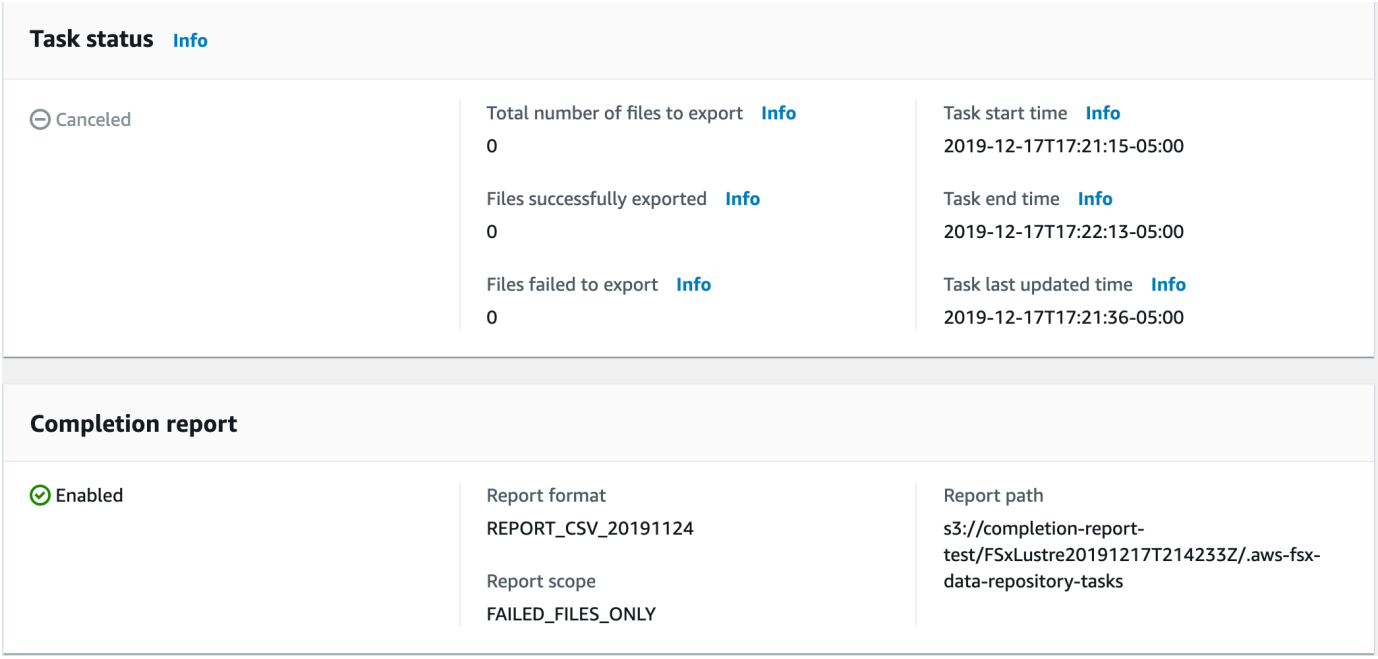
- Todas las tareas existentes.

- 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 del repositorio de datos existentes en su cuenta mediante la FSx consola, la CLI o la API de Amazon, tal y como se describe a continuación.

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

1. Abre la FSx consola de Amazon en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación, 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.
4. Para ver los detalles de una tarea, elija el ID de la tarea o el Nombre de la tarea en el panel 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 Amazon FSx `describe-data-repository-tasks`CLI, puede 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 se ejecuta correctamente, 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 FSx consola, la CLI o la API de Amazon, tal y como se describe a continuación.

Cómo 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 se ejecuta correctamente, 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 cola para ser procesado.
- Amazon FSx continúa procesando todos los archivos que estén 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. Abre la FSx consola de Amazon 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 Amazon FSx `cancel-data-repository-task`CLI 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 se ejecuta correctamente, 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 envía el informe al repositorio de datos enlazados del sistema de archivos en Amazon S3, utilizando la ruta que especifique 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 de 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, puedes encontrar el número de archivos que Amazon FSx no ha podido procesar en Files failed to export en la página de 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 opcionalmente información sobre los archivos y directorios específicos en los que se produjo un error en un informe de finalización. El informe de finalización de tareas 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 FSx archivos de Amazon durante una tarea de importación, exportación o publicación. Por lo general, este código de error significa que el sistema de FSx archivos de Amazon en el que se ejecutó la tarea fallida se encuentra en un estado de ciclo de vida FALLIDO. Cuando esto

Código de error	Explicación
	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.
`OperationNotPermitted`	Amazon FSx no pudo 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 modificad o por otro cliente del sistema de archivos. Puedes volver a intentarlo cuando tu flujo DataRepositoryTask de trabajo haya terminado de escribirse 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. Para las tareas de exportación, el sistema de FSx archivos de Amazon debe tener permiso para realizar la `S3:PutObject` operación de exportación a un repositorio de datos vinculado 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. 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` . Para las tareas de importación, el sistema de FSx archivos de Amazon debe tener permiso para realizar `S3:HeadObject` las `S3:GetObject` operaciones de importación desde un repositorio de datos vinculado en S3. Para las tareas de importación, si su bucket de S3 utiliza 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

Código de error	Explicación
	política que se indican en. Trabajo con buckets de Amazon S3 cifrados del lado del servidor 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 encontró un error relacionado con S3 que no era así. `S3AccessDenied`
`S3FileDeleted`	Amazon no FSx ha podido exportar un archivo de enlace duro porque el archivo fuente no existe en el repositorio de datos.

Código de error	Explicación
`S3ObjectInUnsupportedTier`	Amazon importó FSx correctamente un objeto sin enlace simbólico de 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 no FSx ha podido importar ni 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 no FSx ha podido importar un objeto de enlace simbólico porque se encuentra en una clase de almacenamiento de Amazon S3 que no es compatible, como una 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 no FSx ha podido liberar el archivo del sistema de archivos porque se ha eliminado del repositorio de datos antes de que pudiera publicarse.

Liberación de archivos

Las tareas de repositorio de datos liberan los datos de los archivos de su sistema de archivos FSx para Lustre a fin de 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 liberado, 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 publicación del repositorio de datos no están disponibles en los FSx sistemas de archivos Lustre 2.10.

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

- Rutas del sistema de archivos por publicar: especifica la ruta desde la que se publicarán los archivos.
- Duración mínima desde el último acceso: especifica la duración, en días, de modo que se libere cualquier archivo al que no se haya accedido durante ese periodo. 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 `atime`, `mtime` y `ctime`).

Los archivos solo se liberarán por 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. Indicar una duración mínima de `0` días desde el último acceso liberará los archivos independientemente de la duración desde el último acceso.

> **Note**
>
> No se admite el uso de caracteres comodín para incluir o excluir archivos para 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 característica de exportación automática, una tarea de exportación de un repositorio de datos o los comandos del HSM. Para comprobar que un archivo se haya exportado al 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 del HSM como usuario raíz o mediante `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 FSx consola Amazon 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. Abre la FSx consola de Amazon en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación izquierdo, elija Sistemas de archivos, a continuación, elija el sistema de archivos de 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.
6. En Rutas del sistema de archivos que se van a liberar, especifica hasta 32 directorios o archivos que se van a liberar de tu sistema de FSx archivos de Amazon 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 en la FSx que Amazon entregará el informe, introduce una ruta relativa en el repositorio de datos S3 vinculado al sistema de archivos para la ruta del informe.
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`CLI para crear una tarea que libere archivos en su sistema de archivos FSx for 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.
  - Establece `--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
```

Tras 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 tus datos locales

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

FSx Para usar Lustre con sus datos locales

1. Cree un sistema de archivos. Para más información, consulte Paso 1: crear un sistema de archivos FSx para Lustre en el ejercicio de introducción.
2. Monte el sistema de archivos desde clientes en las instalaciones. Para obtener más información, consulte Montaje de sistemas de FSx archivos de Amazon desde una VPC local o interconectada.
3. Copie los datos que desee procesar en su sistema de archivos de FSx for Lustre.

4. Ejecute su carga de trabajo de cómputo intensivo en instancias de EC2 Amazon en la nube montando su sistema de archivos.
5. Cuando termines, copia los resultados finales de tu sistema de archivos a tu ubicación de datos local y elimina tu sistema de archivos FSx para Lustre.

Registros de eventos del repositorio de datos

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

> **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.

Temas

Cómo importar eventos

Tipo de error	Nivel de registro	Mensajes de registro	Causa raíz	Código de error al finalizar el informe
Error en la enumeración de objetos	ERROR	`No se pudieron enumerar los objetos`	Amazon FSx no pudo enumerar los objetos de S3	N/A

Tipo de error	Nivel de registro	Mensajes de registro	Causa raíz	Código de error al finalizar el informe
		de S3 en el bucket de S3 bucket_name con el prefijo.	en el bucket de S3. Esto puede ocurrir si la política del bucket de S3 no proporcio na suficient es permisos a Amazon FSx.	
Clase de almacenamiento de S3 no compatible	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 S3 en un nivel no admitido *S3_tier_name* .	Amazon FSx no pudo importar un objeto de S3 porque se encuentra en una clase de almacenam iento de Amazon S3 que no se admite, como la clase de almacenam iento S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive.	`S3ObjectInUnsupportedTier`

Tipo de error	Nivel de registro	Mensajes de registro	Causa raíz	Código de error al finalizar el informe
Clase de almacenamiento de enlaces simbólicos no admitida	ERROR	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`

Tipo de error	Nivel de registro	Mensajes de registro	Causa raíz	Código de error al finalizar el informe
Acceso denegado a S3	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. 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. Para las tareas de importación, si su bucket de S3 utiliza cifrado del lado	`S3AccessDenied`

Tipo 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.	

Tipo de error	Nivel de registro	Mensajes de registro	Causa raíz	Código de error al finalizar el informe
Eliminación del acceso denegado	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

Tipo de error	Nivel de registro	Mensajes de registro	Causa raíz	Código de error al finalizar el informe
Objeto no compatible con POSIX	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`

Tipo de error	Nivel de registro	Mensajes de registro	Causa raíz	Código de error al finalizar el informe
Discrepancia de tipos de objeto	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`
Error de actualización de metadatos del directorio	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

Tipo de error	Nivel de registro	Mensajes de registro	Causa raíz	Código de error al finalizar el informe
No se ha encontrado el objeto S3	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`
Bucket de S3 no encontrado	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

Tipo de error	Nivel de registro	Mensajes de registro	Causa raíz	Código de error al finalizar el informe
Bucket de S3 no encontrado	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
Error de creación de directorio	ERROR	No se pudo crear el directorio local debido a un error interno.	Amazon FSx no pudo importar automátic amente la creación de un directorio en el sistema de archivos debido a un error interno.	N/A

Tipo de error	Nivel de registro	Mensajes de registro	Causa raíz	Código de error al finalizar el informe
El espacio en el disco está lleno	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

Tipo de error	Nivel de registro	Mensajes de registro	Causa raíz	Código de error al finalizar el informe
Acceso denegado	ERROR	No se pudo exportar el archivo porque se denegó el acceso al objeto de S3 con la clave *key_value* en el bucket de S3 *bucket_name* .	Se denegó el acceso a Amazon S3 para una tarea de exportación de un repositorio de datos. Para las tareas de exportación, el sistema de archivos de Amazon	`S3AccessDenied`

Tipo de error	Nivel de registro	Mensajes de registro	Causa raíz	Código de error al finalizar el informe
			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. Como la tarea de exportación requiere que los datos fluyan fuera de la VPC de un sistema	

Tipo de error	Nivel de registro	Mensajes de registro	Causa raíz	Código de error al finalizar el informe
			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`. Si su bucket de S3 contiene objetos cargados desde una Cuenta de AWS diferente a la de su cuenta de bucket de S3 vinculada al sistema de archivos, puede asegurarse de que sus tareas de repositorio de datos puedan modificar los metadatos de	

Tipo de error	Nivel de registro	Mensajes de registro	Causa raíz	Código de error al finalizar el informe
			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 bucket-owner-full-control` predefinida. Para habilitar la propiedad de objetos de S3, elija la opción que prefiera el	

Tipo de error	Nivel de registro	Mensajes de registro	Causa raíz	Código de error al finalizar el informe
			propietario del bucket en su bucket de S3. Para obtener más informaci ón, consulte Control de la propiedad de objetos cargados mediante la propiedad de objetos de S3 en la Guía del usuario de Amazon S3.	
La ruta de exportación es demasiado larga	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`

Tipo de error	Nivel de registro	Mensajes de registro	Causa raíz	Código de error al finalizar el informe
El archivo es demasiado grande	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`

Tipo de error	Nivel de registro	Mensajes de registro	Causa raíz	Código de error al finalizar el informe
No se encuentra la clave de KMS	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

Tipo de error	Nivel de registro	Mensajes de registro	Causa raíz	Código de error al finalizar el informe
Recurso ocupado	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`
Archivo publicado	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

Tipo de error	Nivel de registro	Mensajes de registro	Causa raíz	Código de error al finalizar el informe
La ruta del repositorio de datos no coincide	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
Internal Failure (Error interno)	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
Error de carga del informe de finalización	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

Tipo de error	Nivel de registro	Mensajes de registro	Causa raíz	Código de error al finalizar el informe
Error de validación del informe de finalización	ERROR	No se pudo cargar el informe de finalizac ión de la tarea del repositor io de datos en el bucket *bucket_na me* 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

Eventos de restauración de HSM

Tipo de error	Nivel de registro	Mensajes de registro	Causa raíz
Acceso denegado	ERROR	No se pudo restaurar el archivo porque se denegó el acceso al objeto de S3 con la clave *object_name* en el bucket de S3 *bucket_name* .	Se denegó el acceso al S3 de Amazon al intentar restaurar un archivo mediante comandos de HSM. El sistema de archivos Amazon FSx debe

Tipo de error	Nivel de registro	Mensajes de registro	Causa raíz
			tener permiso para realizar las operaciones `s3:HeadObject` y `s3:GetObject` para restaurar desde el repositorio de datos enlazados en S3.
Clase de almacenamiento de S3 no compatibles	WARN	No se pudo restaurar el archivo porque el objeto S3 *`object_name`* de del bucket *`bucket_name`* estaba en un *`S3_storage_class _name`* no compatible.	Amazon FSx no pudo restaurar el archivo porque el objeto de S3 correspondiente se encuentra en una clase de almacenamiento de S3 que no se admite, como S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. Primero debe restaurar el objeto de la clase de almacenamiento Glacier antes de usar `hsm_restore` .

Tipo de error	Nivel de registro	Mensajes de registro	Causa raíz
No se ha encontrado el objeto S3	ERROR	No se pudo restaurar el archivo porque el objeto S3 con la clave *key_value* no se encontró en el bucket de S3 *bucket_name* .	Amazon FSx no pudo restaurar el archivo porque el objeto S3 correspondiente no existe en el repositorio de datos.
Bucket de S3 no encontrado	ERROR	No se pudo restaurar el archivo porque el bucket de S3 *bucket_name* no existe.	Amazon FSx no puede restaurar el archivo porque el bucket del S3 vinculado ya no existe.
El espacio en el disco está lleno	ERROR	No se pudo restaurar el archivo porque no había espacio de almacenamiento disponible en el sistema de archivos.	El sistema de archivos se quedó sin espacio de almacenamiento disponible al intentar restaurar los datos del archivo desde el S3. Considere aumentar la capacidad de almacenamiento del sistema de archivos o liberar archivos para liberar espacio.

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. Tenga en cuenta que la exportación y la compatibilidad de muchos repositorios de datos no están disponibles en los sistemas de archivos de FSx para Lustre que no usan asociaciones de repositorios de datos.

Temas

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 de 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://amzn-s3-demo-bucket/`.

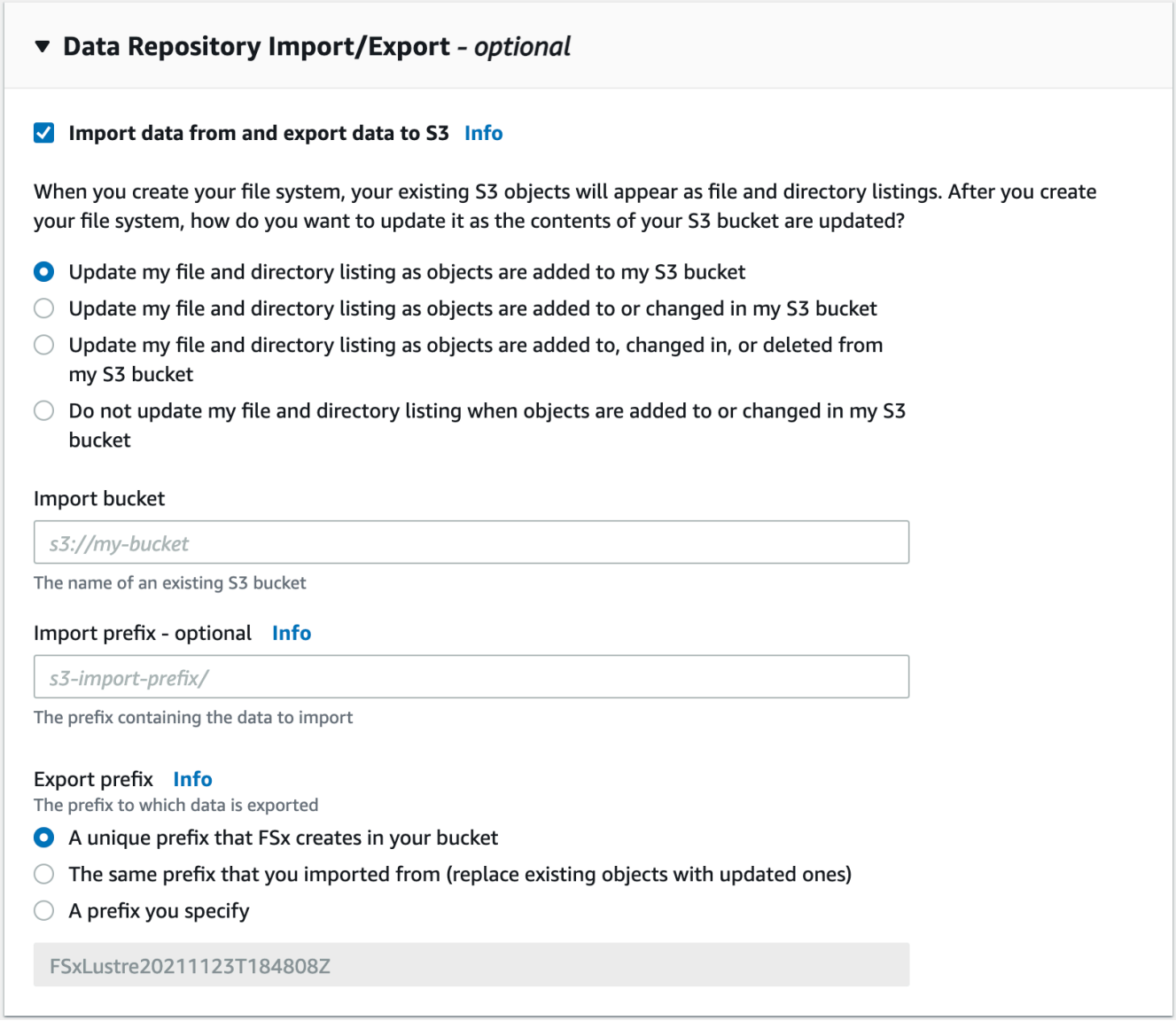
Utilizando este método, puede incluir un prefijo de importación cuando especifique la ruta de importación, y no afecta a una asignación 1:1 para las exportaciones.

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 Paso 1: crear un sistema de archivos FSx para 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 de 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 usar 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 `amzn-s3-demo-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 de 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://amzn-s3-demo-bucket/,ExportPath=s3://amzn-s3-demo-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://amzn-s3-demo-bucket/",
                    "ExportPath": "s3://amzn-s3-demo-bucket/export",
                    "ImportedFileChunkSize": 1024
                },
                "PerUnitStorageThroughput": 50
            }
        }
    ]
}
```

Visualización de la ruta de exportación de un sistema de archivos

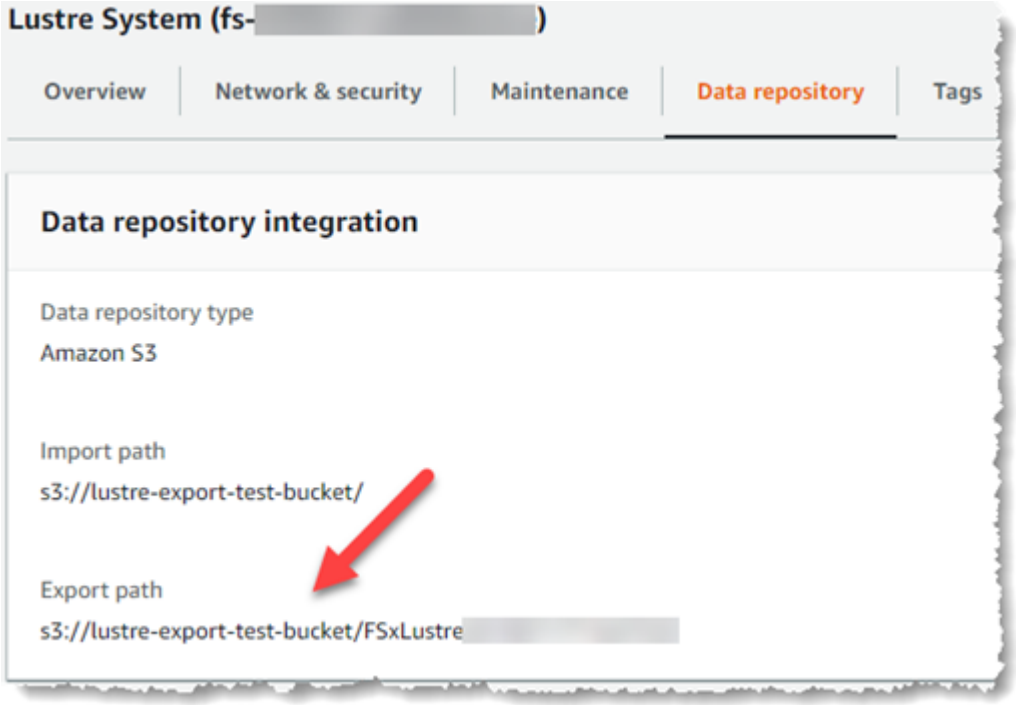
Puede ver la ruta de exportación de un sistema de archivos mediante la consola FSx para Lustre, la CLI AWS y la API.

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 de 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-systems`AWS.

```
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://amzn-s3-demo-bucket/",
    "ExportPath": "s3://amzn-s3-demo-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 de 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 de 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 de 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 usar 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 el sistema de archivos a un bucket de Amazon 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://amzn-s3-demo-bucket/",
                    "ExportPath": "s3://amzn-s3-demo-bucket/export",
                    "ImportedFileChunkSize": 1024
                }
                "PerUnitStorageThroughput": 50,
                "WeeklyMaintenanceStartTime": "2:04:30"
            }
        }
    ]
}
```

Rendimiento de Amazon FSx for Lustre

En este capítulo se proporcionan temas sobre el rendimiento de Amazon FSx for Lustre, incluidos algunos consejos y recomendaciones importantes para maximizar el rendimiento de su sistema de archivos.

Temas

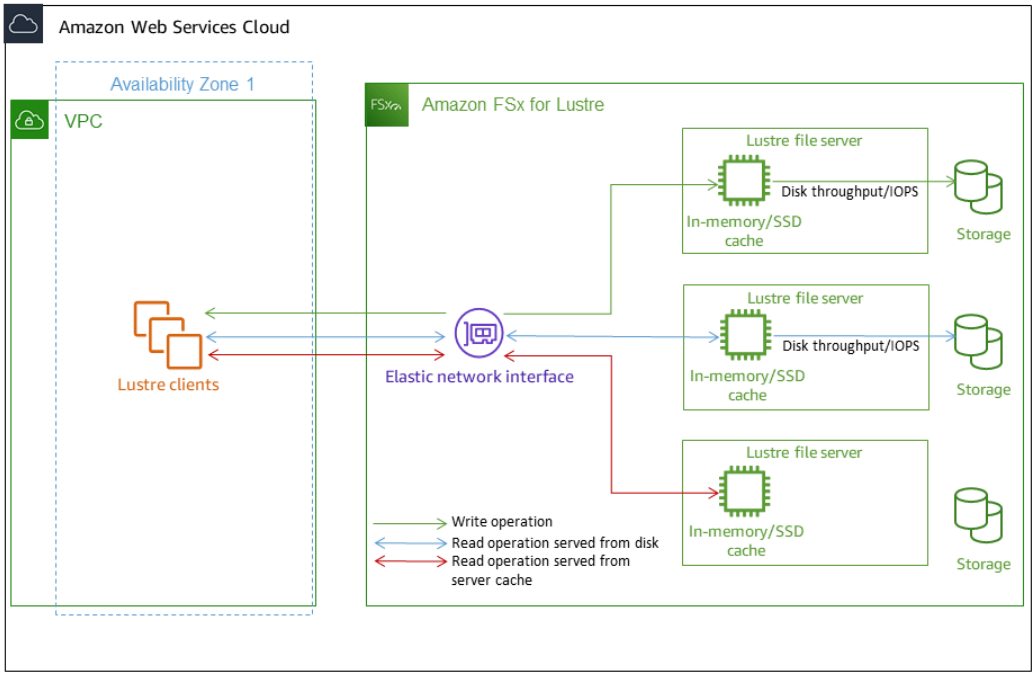
Descripción general de

Amazon FSx for Lustre, basado en Lustre el popular sistema de archivos de alto rendimiento, ofrece un rendimiento de escalado horizontal que aumenta linealmente con el tamaño del sistema de archivos. Lustrelos sistemas de archivos se escalan horizontalmente en varios discos y servidores de archivos. 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 for Lustre se basa en la arquitectura Lustre escalable para soportar altos niveles de rendimiento en un gran número de clientes.

¿Cómo funcionan FSx los sistemas de archivos de Lustre

Cada sistema FSx de archivos de Lustre consta de los servidores de archivos con los que se comunican los clientes y de un conjunto de discos conectados a cada servidor de archivos

que almacena los 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. Según la clase de almacenamiento, el servidor de archivos se puede aprovisionar con una caché de lectura de la SSD opcional. 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.

Para obtener más información sobre el rendimiento de la red, el rendimiento del disco y las características de IOPS de las clases de almacenamiento SSD y HDD, consulte Características de rendimiento de las clases de almacenamiento en SSD y HDD y Características de rendimiento de la clase de almacenamiento Intelligent-Tiering.

Rendimiento de los metadatos del sistema de archivos

Las operaciones de E/S por segundo (IOPS) de los metadatos del sistema de archivos determinan la cantidad de archivos y directorios que puede crear, enumerar, leer y eliminar por segundo.

Los sistemas de archivos Persistent 2 le permiten aprovisionar las IOPS de metadatos independientemente de la capacidad de almacenamiento y proporcionan una mayor visibilidad de la cantidad y el tipo de IOPS de metadatos que incorporan las instancias de cliente al sistema de archivos. Con los sistemas de archivos SSD, las IOPS de metadatos se aprovisionan automáticamente en característica de la capacidad de almacenamiento que aprovisione. El modo automático no es compatible con los sistemas de archivos Intelligent-Tiering.

En FSx el caso de los sistemas de archivos Lustre Persistent 2, la cantidad de IOPS de metadatos que aprovisione y el tipo de operación de metadatos determinan la tasa de operaciones de metadatos que su sistema de archivos puede admitir. El nivel de IOPS de metadatos que aprovisione determina la cantidad de IOPS aprovisionadas para los discos de metadatos del sistema de archivos.

Tipo de operación	Operaciones que puede realizar por segundo para cada IOPS de metadatos aprovisionadas
Crear, abrir y cerrar archivos	2
Eliminar archivos	1
Crear y renombrar directorios	0.1
Eliminar directorios	0.2

En el caso de los sistemas de archivos SSD, puede elegir aprovisionar las IOPS de metadatos mediante el modo automático. En el modo automático, Amazon aprovisiona FSx automáticamente las IOPS de los metadatos en función de la capacidad de almacenamiento del sistema de archivos según la siguiente tabla:

Capacidad de almacenamiento del sistema de archivos	IOPS de metadatos incluidas en el modo automático
1200 GiB	1500

Capacidad de almacenamiento del sistema de archivos	IOPS de metadatos incluidas en el modo automático
2400 GiB	3 000
De 4800 a 9600 GiB	6000
De 12 000 a 45 600 GiB	12000
≥48 000 GiB	12 000 IOPS por 24 000 GiB

En el modo aprovisionado por el usuario, puede optar por especificar la cantidad de IOPS de metadatos por aprovisionar. Los valores válidos son los siguientes:

- Para los sistemas de archivos SSD, los valores válidos son `1500`, `3000`, `6000`, `12000` y múltiplos de `12000`, hasta un máximo de `192000`.
- Para los sistemas de archivos Intelligent-Tiering, los valores válidos son `6000` y `12000`.

Para obtener información acerca de cómo configurar la IOPS de los metadatos, consulte Administración del rendimiento de los metadatos. Tenga en cuenta que usted paga por las IOPS de metadatos aprovisionadas por encima de la cantidad predeterminada de IOPS de metadatos en el sistema de archivos.

Rendimiento de las instancias de clientes individuales

Si va a crear un sistema de archivos con una capacidad GBps de rendimiento superior al 10%, le recomendamos que habilite Elastic Fabric Adapter (EFA) para optimizar el rendimiento por instancia de cliente. Para optimizar aún más el rendimiento por instancia de cliente, los sistemas de archivos compatibles con EFA también admiten el GPUDirect almacenamiento para instancias de cliente basadas en GPU NVIDIA compatibles con EFA y ENA Express para instancias de cliente habilitadas para ENA Express.

El rendimiento que puede transferir a una única instancia de cliente depende del tipo de sistema de archivos que elija y de la interfaz de red de la instancia de cliente.

Tipo de sistema de archivos	Interfaz de red de la instancia de cliente	Rendimiento máximo por cliente, GBps
No compatible con EFA	Cualquiera	100 GBps*
Compatible con EFA	ENA	100 GBps*
Compatible con EFA	ENA Express	100 Gbps
Compatible con EFA	EFA	700 Gbps
Compatible con EFA	EFA con GDS	1200 Gbps

> **Note**
>
> * El tráfico entre una instancia de cliente individual y una instancia individual del servidor FSx de almacenamiento de objetos Lustre está limitado a 5 Gbps. Consulte el número de servidores Direcciones IP para sistemas de archivos de almacenamiento de objetos en los que se basa su sistema de archivos FSx para Lustre.

Disposición de almacenamiento del sistema de archivos

Todos los datos de los archivos Lustre se almacenan en volúmenes de almacenamiento denominados destinos de almacenamiento de objetos (). OSTs Todos los metadatos de los archivos (incluidos los nombres de los archivos, las marcas de tiempo, los permisos, etc.) se almacenan en volúmenes de almacenamiento denominados destinos de metadatos (MDTs). Los sistemas de archivos de Amazon FSx for Lustre se componen de uno o varios OSTs sistemas MDTs de archivos. Amazon FSx for Lustre distribuye los datos de sus archivos entre los elementos OSTs 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 del MDT y los elementos OSTs que componen su sistema de archivos, ejecute el siguiente comando desde un cliente que tenga el sistema de archivos montado.

```
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 for Lustre distribuye automáticamente los archivos para garantizar que los datos se OSTs envíen desde todos los servidores de almacenamiento. Puede aplicar el mismo concepto a nivel de archivo configurando la forma en que los archivos se dividen en varios. OSTs

La división en bandas significa que los archivos se pueden dividir en varios fragmentos que luego se almacenan en diferentes partes. OSTs Cuando un archivo se divide en varias secciones OSTs, las solicitudes de lectura o escritura del archivo se distribuyen entre ellas OSTs, lo que aumenta el rendimiento total o las IOPS que las aplicaciones pueden procesar.

Los siguientes son los diseños predeterminados de los sistemas de archivos Amazon FSx for 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 for 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 1 se `ImportedFileChunkSize` almacenarán en varios OSTs 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 es el número de franjas OSTs que abarca 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 archivos de varios gigabytes OSTs y un gran número de ellos puede obtener un rendimiento superior al dividir los archivos en secciones superiores al valor de cinco franjas predeterminado. OSTs La creación de archivos grandes con un número reducido de franjas puede provocar cuellos de botella en I/O el rendimiento y también puede provocar que se llenen. OSTs 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 servidores OSTs y sus servidores asociados aporten IOPS, ancho de banda de red y recursos de CPU al leer y escribir archivos de gran tamaño.
- Reduce la probabilidad de que un pequeño subconjunto de ellos OSTs se convierta en puntos críticos 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 bandas de 2 y un tamaño de banda de 1 MiB, Lustre escribe fragmentos alternativos de 1 MiB de un archivo en cada uno de los dos. OSTs
- 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 gran número de fragmentos 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 del diseño, incluso si el archivo es demasiado pequeño para ocupar espacio en todos los volúmenes de 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 que se muestra arriba, si crea un archivo de 1 MiB y, a continuación, añade datos al final, el diseño del archivo se ampliará hasta tener un recuento de franjas de -1, es decir, todas las del sistema. OSTs 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. Como los archivos de registro suelen crecer al incorporar nuevos registros, Amazon FSx for Lustre asigna un recuento de franjas predeterminado de 1 a cualquier archivo creado en modo de incorporación, independientemente de la configuración de franjas predeterminada especificada en su directorio principal.

La configuración de PFL predeterminada en los sistemas de archivos Amazon FSx for 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 muy simultáneo a archivos medianos y grandes probablemente se beneficien de un diseño con más franjas en los tamaños más pequeños y con más franjas en todos los archivos más grandes, como se muestra en el OSTs ejemplo de diseño 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 `DataReadBytes` estadística indica el rendimiento total de lectura visto por todos los componentes de un sistema de OSTs 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 sistemas de archivos de Amazon FSx para Lustre.

Características de rendimiento de las clases de almacenamiento en SSD y HDD

El rendimiento que admite un sistema FSx de archivos Lustre equipado con una clase de almacenamiento SSD o HDD es proporcional a su capacidad de almacenamiento. Los sistemas de archivos Amazon FSx for Lustre se escalan a varios TBps niveles de rendimiento y millones de IOPS. Amazon FSx for Lustre también admite el acceso simultáneo al mismo archivo o directorio desde miles de instancias informáticas. 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 Los sistemas de archivos for Lustre proporcionan un rendimiento de lectura en ráfagas mediante un mecanismo de I/O crédito de red para asignar el ancho de banda de la red en función de 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 FSx para el que están diseñadas las opciones de despliegue de Lustre con clases de almacenamiento SSD y HDD.

Rendimiento del sistema de archivos para opciones de almacenamiento SSD

Tipo de implementación	Rendimiento de la red (MBps/TiB de almacenamiento aprovisionado)		IOPS de red (IOPS/TiB de almacenamiento aprovisionado)	Almacenamiento en caché (GiB RAM/TiB del almacenamiento aprovisionado)	Latencias de disco por operación de archivo (milisegundos, P50)	Rendimiento del disco (MBps/TiB de almacenamiento o caché SSD aprovisionados)	
	Referencia	Ráfaga				Referencia	Ráfagas
SCRATCH_2	200	1300	Base de decenas de miles Ráfaga de cientos de miles	6.7	Metadatos: sub-ms Datos: sub-ms	200 (lectura) 100 (escritura)	-
PERSISTENTE-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		1 000	-

Rendimiento del sistema de archivos para opciones de almacenamiento HDD

Tipo de implementación	Rendimiento de la red (MBps/TiB de almacenamiento o caché SSD aprovisionada)		IOPS de red (IOPS/TiB de almacenamiento aprovisionado)	Almacenamiento en caché (GiB RAM/TiB del almacenamiento aprovisionado)	Latencias de disco por operación de archivo (milisegundos, P50)	Rendimiento del disco (MBps/TiB de almacenamiento o caché SSD aprovisionados)	
	Referencia	Ráfaga				Referencia	Ráfagas
PERSISTENT-12							
Almacenamiento en HDD	40	375*	Base de decenas de miles Ráfaga de cientos de miles	0.4 de memoria	Metadatos: sub-ms Datos: ms de un dígito	12	80 (lectura) 50 (escritura)
Caché de lectura SSD	200	1900		Caché SSD 200	Datos: sub-ms	200	-
PERSISTENT-40							
Almacenamiento en HDD	150	1.300*	Base de decenas de miles Ráfaga de cientos de miles	1.5	Metadatos: sub-ms Datos: ms de un dígito	40	250 (lectura) 150 (escritura)
Caché de lectura SSD	750	6500		Caché SSD 200	Datos: sub-ms	200	-

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

Tipo de implementación	Rendimiento de red (MBps 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 (MBps por TiB de almacenamiento o caché SSD aprovisionado)	
	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*	Ráfaga de cientos de miles	4,4 RAM	Datos: sub-ms	100	240
PERSISTENT-200	750	1.300*		8,8 RAM		200	240

> **Note**
>
> * Los siguientes sistemas de archivos persistentes Regiones de AWS proporcionan una ráfaga de red de hasta 530 MBps por TiB de almacenamiento: África (Ciudad del Cabo), Asia Pacífico (Hong Kong), Asia Pacífico (Osaka), Asia Pacífico (Singapur), Canadá (Central), Europa (Fráncfort), Europa (Londres), Europa (Milán), Europa (Estocolmo), Oriente Medio (Baréin), Sudamérica (São Paulo), China China y US West (Los Ángeles).

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 por MBps TiB de rendimiento por unidad de almacenamiento proporciona un rendimiento de disco base agregado de 240 MBps y un rendimiento de disco en ráfaga de 1,152. GBps

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

Características de rendimiento de la clase de almacenamiento Intelligent-Tiering

La clase de almacenamiento Intelligent-Tiering de FSx for Lustre ofrece un almacenamiento elástico y rentable para las cargas de trabajo que tradicionalmente se ejecutan en sistemas de archivos de almacenamiento de archivos de alto rendimiento basados en HDD o en sistemas mixtos de HDD/SD. Los sistemas de archivos que utilizan la clase de almacenamiento por niveles inteligentes utilizan un almacenamiento regional totalmente elástico e inteligente en niveles, que crece y se reduce automáticamente para adaptarse a la carga de trabajo a medida que cambia. Para obtener información sobre cómo estratifica los datos, consulte Cómo clasifica los datos la clase de almacenamiento Intelligent-Tiering.

El rendimiento que admite un sistema de archivos Lustre con la clase de almacenamiento Intelligent-Tiering es independiente FSx del almacenamiento. Los sistemas de archivos Intelligent-Tiering se escalan hasta alcanzar varios niveles de rendimiento y millones de IOPS. TBps Los sistemas de archivos que utilizan la clase de almacenamiento Intelligent-Tiering también proporcionan una caché de lectura de la SSD aprovisionada opcional para el acceso de baja latencia a los datos a los que se

accede con frecuencia. De forma predeterminada, Amazon FSx for Lustre aprovisiona una caché de lectura SSD para los metadatos a los que se accede con frecuencia. Como la mayoría de las cargas de trabajo suelen ser de lectura intensiva y funcionan activamente solo con un pequeño subconjunto del conjunto de datos en un momento dado, el modelo híbrido de almacenamiento por niveles inteligente y cachés de lectura de la SSD permite que los sistemas de archivos que utilizan la clase de almacenamiento por niveles inteligentes proporcionen un almacenamiento con un rendimiento comparable al de los sistemas de archivos SSD para la mayoría de las cargas de trabajo, al tiempo que ofrece ahorros en los costos de almacenamiento en relación con las clases de almacenamiento SSD y HDD.

Al leer y escribir datos en un sistema de archivos Intelligent-Tiering, especialmente los datos a los que no se ha accedido recientemente o con la frecuencia suficiente como para estar en la caché en memoria del servidor de archivos, el rendimiento depende del tamaño de la caché de lectura de la SSD. El acceso a los datos desde el almacenamiento en niveles inteligentes tiene time-to-first-byte latencias de aproximadamente decenas de milisegundos, así como costes por solicitud, mientras que los accesos desde la caché de lectura de la SSD se devuelven con una latencia inferior a un milisegundo y sin costes por solicitud.

Al configurar el tamaño de la caché de lectura de la SSD para su sistema de archivos, debe tener en cuenta tanto el tamaño del conjunto de datos al que se accede con frecuencia dentro de la carga de trabajo como la sensibilidad de la carga de trabajo a una mayor latencia para las lecturas de los datos a los que se accede con menos frecuencia. Puede cambiar entre los modos de tamaño de la caché de lectura de la SSD una vez creado el sistema de archivos y escalar la caché hacia arriba o hacia abajo. Para obtener más información sobre cómo modificar la caché de lectura de la SSD, consulte Administración de la caché de lectura SSD aprovisionada.

Una solicitud de escritura se produce cuando, FSx para Lustre, escribe un bloque de datos en el almacenamiento Intelligent-Tiering. Al escribir datos en el sistema de archivos, las solicitudes de escritura se agregan y se escriben en el almacenamiento Intelligent-Tiering, lo que aumenta el rendimiento y reduce los costos de las solicitudes. Las lecturas se pueden realizar desde la caché en memoria del servidor de archivos, la caché de lectura de la SSD o directamente desde el almacenamiento Intelligent-Tiering. Cuando se realiza una lectura desde un almacenamiento Intelligent-Tiering, se produce una solicitud de lectura para cada bloque de datos recuperados. Al leer los datos de forma secuencial, Lustre los capturará previamente FSx para mejorar el rendimiento.

Los datos de la caché en memoria de los sistemas de archivos que utilizan la clase de almacenamiento Intelligent-Tiering se envían directamente al cliente solicitante como E/S de red. Cuando un cliente accede a datos que no están en la caché en memoria, se leen desde la caché

de lectura de SSD o el almacenamiento Intelligent-Tiering como E/S de disco y, a continuación, se envían al cliente como E/S de red.

Rendimiento del sistema de archivos para Intelligent-Tiering

La siguiente tabla muestra el rendimiento FSx para el que están diseñados los sistemas de archivos Intelligent-Tiering de Lustre.

Capacidad de rendimiento aprovisionada () MBps	Rendimiento de red () MBps		IOPS de red	Almacenamiento en caché en memoria (GB)	Rendimiento máximo del disco caché SSD () MBps	Cantidad máxima de IOPS en disco caché SSD	
	Referencia	Ráfaga				Referencia	Ráfaga
Cada 4000	12500	-	Cientos de miles	76,8	4000	160000	-

Consejos de rendimiento

Cuando utilices Amazon FSx for Lustre, ten en cuenta los siguientes consejos de rendimiento. Para conocer los límites de servicio, consulte Service Quotas para Amazon FSx para Lustre.

- I/O Tamaño medio: dado que Amazon FSx for Lustre es un sistema de archivos de red, cada operación de archivos pasa por un viaje de ida y vuelta entre el cliente y Amazon FSx for Lustre, lo que supone una pequeña sobrecarga de latencia. Debido a esta latencia por operación, el rendimiento general generalmente aumenta a medida que aumenta el I/O tamaño promedio, ya que la sobrecarga se amortiza con una mayor cantidad de datos.
- Modelo de solicitud: al habilitar las escrituras asíncronas en su sistema de archivos, las operaciones de escritura pendientes se almacenan en búfer en la instancia de Amazon antes de que se escriban en EC2 Amazon for Lustre de forma asíncrona FSx . 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 ha habilitado la escritura sincrónica emite solicitudes sincrónicas a Amazon FSx for Lustre. Cada operación pasa por un viaje de ida y vuelta entre el cliente y Amazon FSx for Lustre.

  > **Note**
  >
  > El modelo de solicitud que elijas tiene desventajas en cuanto a coherencia (si utilizas varias EC2 instancias de Amazon) y velocidad.

- Limite el tamaño del directorio: para lograr un rendimiento óptimo de los metadatos en los sistemas de archivos Persistent 2 FSx for Lustre, limite cada directorio a menos de 100 000 archivos. Al limitar el número de archivos de un directorio, se reduce el tiempo requerido para que el sistema de archivos bloquee el directorio principal.
- EC2 Instancias de Amazon: las aplicaciones que realizan una gran cantidad de operaciones de lectura y escritura probablemente necesiten más memoria o capacidad informática que las aplicaciones que no lo hacen. Al lanzar tus EC2 instancias de Amazon para tu carga de trabajo con un uso intensivo de recursos informáticos, elige tipos de instancias que tengan la cantidad de estos recursos que necesita tu aplicación. Las características de rendimiento de los sistemas de archivos Amazon FSx for Lustre no dependen del uso de instancias optimizadas para Amazon EBS.
- Se recomienda ajustar las instancias de cliente para obtener un rendimiento óptimo
  1. Para tipos de instancia de cliente con memoria de más de 64 GiB, recomendamos aplicar el siguiente ajuste:

```
sudo lctl set_param ldlm.namespaces.*.lru_max_age=600000
sudo lctl set_param ldlm.namespaces.*.lru_size=<100 * number_of_CPUs>
```

2. 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
```

3. Para optimizar el rendimiento de las listas de directorios (ls), es necesario aplicar los siguientes ajustes:

```
sudo lctl set_param llite.*.statahead_max=512
sudo lctl set_param llite.*.statahead_agl=1
if sudo lctl get_param llite.*.statahead_xattr > /dev/null 2>&1; then
    sudo lctl set_param llite.*.statahead_xattr=1
else
    echo "Warning: Xattr statahead is not supported on this Lustre client. Please
 upgrade to the latest Lustre 2.15 client to apply this tuning"
fi
```

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 entre las cargas de trabajo OSTs: en algunos casos, la carga de trabajo no impulsa el rendimiento total que puede ofrecer el sistema de archivos (200 MBps por TiB de almacenamiento). Si es así, puede utilizar CloudWatch las métricas para solucionar problemas si el rendimiento se ve afectado por un desequilibrio en los patrones de la carga de trabajo. I/O

Para identificar si esta es la causa, consulta la CloudWatch métrica Maximum de Amazon FSx for Lustre.

En algunos casos, esta estadística muestra una carga igual o superior al 240% del rendimiento (la capacidad MBps de rendimiento de un solo disco Amazon for Lustre de 1,2 TiB). FSx 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, separe los archivos con requisitos de alto rendimiento en todos los componentes de su sistema de archivos. OSTs

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 sus archivos. OSTs Para ello, puede modificar el `ImportedFileChunkSize` parámetro al crear su próximo sistema de archivos Amazon FSx for Lustre.

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

- Lustrecliente para IOPS de metadatos: si su sistema de archivos tiene una configuración de metadatos especificada, le recomendamos que instale un cliente Lustre 2.15 o Lustre 2.12 con una de estas versiones de sistema operativo: Amazon Linux 2023; Amazon Linux 2; Red Hat/Rocky Linux 8.9, 8.10 o 9.x; CentOS 8.9 u 8.10; Ubuntu 22+ con kernel 6.2, 6.5 o 6.8; o Ubuntu 20.

Consideraciones sobre el rendimiento de Intelligent-Tiering

Estas son algunas consideraciones importantes sobre el rendimiento cuando se trabaja con sistemas de archivos que utilizan la clase de almacenamiento Intelligent-Tiering:

- Las cargas de trabajo que leen datos con I/O tamaños más pequeños requerirán una mayor simultaneidad e incurrirán en más costos de solicitud para lograr el mismo rendimiento que las cargas de trabajo que utilizan I/O tamaños grandes debido a la mayor latencia de los niveles de almacenamiento de Intelligent-Tiering. Recomendamos configurar la caché de lectura de la SSD con un tamaño lo suficientemente grande como para soportar una mayor simultaneidad y rendimiento cuando se trabaja con tamaños de E/S más pequeños.
- La cantidad máxima de IOPS de disco que sus clientes pueden manejar con un sistema de archivos de nivel inteligente depende de los patrones de acceso específicos de su carga de trabajo

y de si usted ha aprovisionado una caché de lectura SSD. En el caso de las cargas de trabajo con acceso aleatorio, los clientes suelen generar IOPS mucho más altas si los datos se almacenan en caché en la caché de lectura de la SSD que si no están en la caché.

- La clase de almacenamiento Intelligent-Tiering admite la lectura anticipada para optimizar el rendimiento de las solicitudes de lectura secuencial. Recomendamos configurar el patrón de acceso a los datos de forma secuencial siempre que sea posible para permitir la obtención previa de los datos y aumentar el rendimiento.

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. Direct Connect Puede acceder a su sistema de FSx archivos de Amazon desde las instalaciones, copiar los datos a su sistema de archivos según sea necesario y ejecutar cargas de trabajo con un uso intensivo de recursos informáticos en instancias en la nube.

En la siguiente sección, puede obtener información sobre cómo acceder a su sistema de archivos Amazon FSx for Lustre en una instancia de 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 la instancia de procesamiento.

Temas

Compatibilidad con sistemas de archivos de Lustre y kernel de clientes

Le recomendamos encarecidamente que utilice la Lustre versión de su sistema de archivos FSx para 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 para clientes de Lustre	Versión del sistema de archivos Lustre		
					2.10	2.12	2.15
Amazon Linux 202	6.12	*	*	2.15	no	sí	sí
	6.1	6.1.79-99.167	6.1.79-99.167+	2.15	no	sí	sí
Amazon Linux 2	5.10	5.10.144-127.601	5.10.144-127.601+	2.12	yes	sí	sí
			<5.10.144-127.601	(2.10)	yes	sí	no
	5.4	5.4.214-120.368	5.4.214-120.368+	2.12	yes	sí	sí
			5.4.214-120.368	(2.10)	yes	sí	no
	4.14	4.14.294-220.533	4.14.294-220.533+	2.12	yes	sí	sí
			<4.14.294-220.533	(2.10)	yes	sí	no

Clientes de Ubuntu

Sistema operativo	Versión del sistema operativo	Versión mínima del kernel	Versión máxima del kernel	Versión para clientes de Lustre	Versión del sistema de archivos Lustre		
					2.10	2.12	2.15
Ubuntu	24	6.14.0-1012	6.14.0*	2.15	no	sí	sí
		6.8.0-1024	6.8.0*	2.15	no	sí	sí
	22	6.8.0-1017	6.8.0*	2.15	no	sí	sí
		6.5.0-1023	6.5.0*	2.15	no	sí	sí
		6.2.0-1017	6.2.0*	2.15	no	sí	sí
		5.15.0-1015-aws	5.15.0-1051-aws	2.12	yes	sí	sí
	20	5.15.0-1015-aws	5.15.0*	2.12	yes	sí	sí
		5.4.0-1011-aws	5.13.0-1031-aws	(2.10)	yes	sí	no

RHEL/CentOS/RockyClientes Linux

Sistema operativo	Versión del sistema operativo	Arquitectura	Versión mínima del kernel	Versión máxima del kernel	Versión para clientes de Lustre	Versión del sistema de archivos Lustre		
						2.10	2.12	2.15
RHEL/ Rocky Linux	9.7	Arm + x86	5.14,0-61 1.5.1	5.14.0-61 1*	2.15	no	sí	sí
	9.6	Arm + x86	5.14.0-57 0,12.1	5.14.0-57 0*	2.15	no	sí	sí
	9.5	Arm + x86	5.14.0-50 3.19.1	5.14.0-50 3*	2.15	no	sí	sí
	9.4	Arm + x86	5.14.0-42 7.13.1	5.14.0-42 7*	2.15	no	sí	sí
	9.3	Arm + x86	5.14.0-36 2.18.1	5.14.0-36 2.18.1	2.15	no	sí	sí
	9.0	Arm + x86	5.14.0-70 .13.1	5.14.0-70 .30.1	2.15	no	sí	sí
RHEL/ CentOS/ RockyLinux	8.10	Arm + x86	4.18.0-553	4.18.0-553*	2.12	yes	sí	sí
	8.9	Arm + x86	4.18.0-513*	4.18.0-513*	2.12	yes	sí	sí

Sistema operativo	Versión del sistema operativo	Arquitectura	Versión mínima del kernel	Versión máxima del kernel	Versión para clientes de Lustre	Versión del sistema de archivos Lustre		
	8.8	Arm + x86	4.18.0-477*	4.18.0-477*	2.12	yes	sí	sí
	8.7	Arm + x86	4.18.0-425*	4.18.0-425*	2.12	yes	sí	sí
	8.6	Arm + x86	4.18.0-372*	4.18.0-372*	2.12	yes	sí	sí
	8.5	Arm + x86	4.18.0-348*	4.18.0-348*	2.12	yes	sí	sí
	8.4	Arm + x86	4.18.0-305*	4.18.0-305*	2.12	yes	sí	sí
RHEL/ CentOS	8.3	Arm + x86	4.18.0-240*	4.18.0-240*	(2.10)	yes	sí	no
	8.2	Arm + x86	4.18.0-193*	4.18.0-193*	(2.10)	yes	sí	no
	7.9	x86	3.10.0-1160*	3.10.0-1160*	2.12	yes	sí	sí
	7.8	x86	3.10.0-1127*	3.10.0-1127*	(2.10)	yes	sí	no
	7.7	x86	3.10.0-1062*	3.10.0-1062*	(2.10)	yes	sí	no
CentOS	7.9	Arm	4.18.0-193*	4.18.0-193*	2.12	yes	sí	sí

Sistema operativo	Versión del sistema operativo	Arquitectura	Versión mínima del kernel	Versión máxima del kernel	Versión para clientes de Lustre	Versión del sistema de archivos Lustre		
	7.8	Arm	4.18.0-147*	4.18.0-147*	2.12	yes	sí	sí

Instalación del cliente de Lustre

Para montar el sistema de archivos Amazon FSx for Lustre desde una instancia de Linux, instale primero el cliente de código abiertoLustre. A continuación, dependiendo de la versión de su sistema operativo, utilice uno de los siguientes procedimientos. Para obtener información sobre el soporte del kernel, consulte Compatibilidad con sistemas de archivos de Lustre y kernel de clientes.

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

Amazon Linux

Para instalar el cliente de 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 kernel para instalar el cliente de Lustre en Amazon Linux 2023:

   - Requisito mínimo del kernel 6.12 - 6.12*
   - Requisito mínimo del kernel 6.1: 6.1.79-99.167.amzn2023

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

Si el comando devuelve un resultado inferior al requisito mínimo del núcleo, actualiza el núcleo y reinicia la EC2 instancia de Amazon 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 de Lustre con el siguiente comando.

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

Para instalar el cliente de 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 kernel para instalar el cliente de 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 la EC2 instancia cumple con los requisitos mínimos del núcleo, continúa con el paso e instala el Lustre cliente.

   Si el comando devuelve un resultado inferior al requisito mínimo del núcleo, actualiza el núcleo y reinicia la EC2 instancia de Amazon 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 de 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 de 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 de Lustre requiere un kernel de Amazon Linux `4.14, version 104` o superior.

```
uname -r
```

3. Realice una de las siguientes acciones:

   - Si el comando devuelve `4.14.104-78.84.amzn1.x86_64` o una versión superior a 4.14, descargue e instale el cliente de Lustre usando 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`, actualiza el kernel y reinicia tu EC2 instancia de Amazon 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 de Lustre como se ha descrito anteriormente.

CentOS, Rocky Linux y Red Hat

Para instalar el Lustre cliente en Red Hat y Rocky Linux 9.0 o 9.3—9.7

Puede instalar y actualizar paquetes de Lustre cliente compatibles con Red Hat Enterprise Linux (RHEL) y Rocky Linux desde el repositorio de paquetes yum para FSx Lustre clientes de Amazon. 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 añadir el repositorio de paquetes yum del FSx Lustre cliente Amazon

1. Abra un terminal en su cliente de Linux.
2. Instale la clave pública FSx rpm de Amazon mediante 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 FSx Lustre del cliente de Amazon

El repositorio de paquetes yum del FSx Lustre cliente de Amazon está configurado de forma predeterminada para instalar el Lustre cliente que es compatible con la versión del núcleo que se incluyó inicialmente con la última versión compatible de Rocky Linux y RHEL 9. Para instalar un cliente de Lustre que sea compatible con la versión del kernel que está usando, 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 siguientes acciones:

   - Si el comando devuelve `5.14.0-611*`, no necesita modificar la configuración del repositorio. Continúe con el procedimiento Para instalar el cliente de Lustre.
   - Si el comando vuelve a `5.14.0-570*` aparecer, debe editar la configuración del repositorio para que apunte Lustre al cliente de la versión 9.6 de Rocky Linux y RHEL.
   - Si el comando vuelve a `5.14.0-503*` aparecer, debe editar la configuración del repositorio para que apunte Lustre al cliente de la versión 9.5 de Rocky Linux y RHEL.
   - Si el comando vuelve a `5.14.0-427*` aparecer, debe editar la configuración del repositorio para que apunte Lustre al cliente de la versión 9.4 de Rocky Linux y RHEL.
   - Si el comando devuelve `5.14.0-362.18.1`, debe editar la configuración del repositorio para que apunte al cliente de Lustre para la versión Rocky Linux y RHEL 9.3.
   - Si el comando devuelve `5.14.0-70*`, debe editar la configuración del repositorio para que apunte al cliente de Lustre para la versión 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. Sustituya *`specific_RHEL_version`* por la versión de RHEL que necesite usar.

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

   Por ejemplo, para apuntar a la versión 9.6, *`specific_RHEL_version`* sustitúyala por `9.6` en el comando, como en el siguiente ejemplo.

```
sudo sed -i 's#9#9.6#' /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 (Rocky Linux y Red Hat 9.0 y posterior)

Los comandos anteriores instalan los dos paquetes necesarios para montar tu sistema de FSx archivos de Amazon e interactuar con él. El repositorio incluye paquetes de Lustre adicionales, como un paquete que contiene el código fuente y paquetes que contienen pruebas, los cuales puede instalar de forma opcional. 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 de Lustre en CentOS y Red Hat 8.2 a 8.10 o en Rocky Linux 8.4 a 8.10

Puede instalar y actualizar paquetes de Lustre cliente compatibles con Red Hat Enterprise Linux (RHEL), Rocky Linux y Centos desde el repositorio de paquetes yum para clientes de FSx Lustre Amazon. 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 añadir el repositorio de paquetes yum del FSx Lustre cliente Amazon

1. Abra un terminal en su cliente de Linux.
2. Instale la clave pública FSx rpm de Amazon mediante 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 FSx Lustre del cliente de Amazon

El repositorio de paquetes yum del FSx Lustre cliente de Amazon está configurado de forma predeterminada para instalar el Lustre cliente que es compatible con la versión del núcleo que se incluyó inicialmente con la última versión compatible de CentOS, Rocky Linux y RHEL 8. Para instalar un cliente de Lustre que sea compatible con la versión del kernel que está usando, 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 siguientes acciones:

   - Si el comando devuelve `4.18.0-553*`, no necesita modificar la configuración del repositorio. Continúe con el procedimiento Para instalar el cliente de Lustre.

- Si el comando devuelve `4.18.0-513*`, debe editar la configuración del repositorio para que apunte al cliente de Lustre para la versión CentOS, Rocky Linux y RHEL 8.9.
- Si el comando devuelve `4.18.0-477*`, debe editar la configuración del repositorio para que apunte al cliente de Lustre para la versión 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 de 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 de 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 de 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 de 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 de Lustre para la versión CentOS y RHEL 8.3.
- Si el comando devuelve `4.18.0-193*`, debe editar la configuración del repositorio para que apunte al cliente de Lustre para la versión CentOS 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 señalar la versión 8.9, sustituya *`specific_RHEL_version`* por `8.9` en el comando.

```
sudo sed -i 's#8#8.9#' /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 tu sistema de FSx archivos de Amazon e interactuar con él. El repositorio incluye paquetes de Lustre adicionales, como un paquete que contiene el código fuente y paquetes que contienen pruebas, los cuales puede instalar de forma opcional. 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 de Lustre en CentOS y Red Hat 7.7, 7.8 o 7.9 (instancias x86_64)

Puede instalar y actualizar paquetes de Lustre cliente que sean compatibles con Red Hat Enterprise Linux (RHEL) y Centos desde el repositorio de paquetes yum para clientes de FSx Lustre Amazon. 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 añadir el repositorio de paquetes yum del FSx Lustre cliente Amazon

1. Abra un terminal en su cliente de Linux.
2. Instale la clave pública FSx rpm de Amazon mediante 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 FSx Lustre del cliente de Amazon

El repositorio de paquetes yum del FSx Lustre cliente de Amazon está configurado de forma predeterminada para instalar el Lustre cliente que sea compatible con la versión del núcleo que se incluyó inicialmente con la última versión compatible de CentOS y RHEL 7. Para instalar un cliente de Lustre que sea compatible con la versión del kernel que está usando, 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 siguientes acciones:

   - Si el comando devuelve `3.10.0-1160*`, no necesita modificar la configuración del repositorio. Continúe con el procedimiento Para instalar el cliente de Lustre.
   - Si el comando devuelve `3.10.0-1127*`, debe editar la configuración del repositorio para que apunte al cliente de Lustre para la versión CentOS y RHEL 7.8.
   - Si el comando devuelve `3.10.0-1062*`, debe editar la configuración del repositorio para que apunte al cliente de Lustre para la versión CentOS 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 de Lustre desde el repositorio usando 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 tu sistema de FSx archivos de Amazon e interactuar con él. El repositorio incluye paquetes de Lustre adicionales, como un paquete que contiene el código fuente y paquetes que contienen pruebas, los cuales puede instalar de forma opcional. 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 Lustre cliente en Centos 7.8 o 7.9 (instancias basadas en ARM con AWS tecnología Graviton)

Puede instalar y actualizar los paquetes de Lustre cliente desde el repositorio de paquetes yum para FSx Lustre clientes de Amazon que sean compatibles con CentOS 7 para instancias con tecnología Graviton basadas en AWS ARM EC2 . 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 añadir el repositorio de paquetes yum del FSx Lustre cliente Amazon

1. Abra un terminal en su cliente de Linux.
2. Instale la clave pública FSx rpm de Amazon mediante 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 FSx Lustre del cliente de Amazon

El repositorio de paquetes yum del FSx Lustre cliente de Amazon está configurado de forma predeterminada para instalar el Lustre cliente que es compatible con la versión del núcleo que se incluyó inicialmente con la última versión compatible de CentOS 7. Para instalar un cliente de Lustre que sea compatible con la versión del kernel que está usando, 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 siguientes acciones:

   - Si el comando devuelve `4.18.0-193*`, no necesita modificar la configuración del repositorio. Continúe con el procedimiento Para instalar el cliente de Lustre.
   - Si el comando devuelve `4.18.0-147*`, debe editar la configuración del repositorio para que apunte al cliente de 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 basadas en ARM con AWS tecnología Graviton) EC2

Los comandos anteriores instalan los dos paquetes necesarios para montar tu sistema de FSx archivos de Amazon e interactuar con él. El repositorio incluye paquetes de Lustre adicionales, como un paquete que contiene el código fuente y paquetes que contienen pruebas, los cuales puede instalar de forma opcional. 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 18.04, 20.04, 22.04 o 24.04

Puede obtener Lustre paquetes del repositorio de Amazon FSx Ubuntu. 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 de cliente, descargue e instale la clave pública requerida. 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. Añade el repositorio de FSx paquetes de Amazon a tu gestor 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 $(lsb_release -cs) 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. Para obtener una lista de los núcleos necesarios para el Lustre cliente en Ubuntu, tanto para las instancias basadas en x86 como para EC2 las instancias basadas en ARM con procesadores EC2 AWS Graviton, consulte. Clientes de Ubuntu

   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 del kernel de Ubuntu y Lustre y reinicie.

   ```
   sudo apt install -y linux-aws lustre-client-modules-aws && sudo reboot
   ```

   Si la versión del núcleo es superior a la versión mínima del núcleo tanto para las EC2 instancias basadas en x86 como para las basadas en Graviton EC2 , y no desea actualizar a la última versión del núcleo, puede realizar la instalación Lustre para el núcleo actual con el siguiente comando.

   ```
   sudo apt install -y lustre-client-modules-$(uname -r)
   ```

   Están instalados los dos Lustre paquetes necesarios para montar su sistema de archivos FSx for Lustre e interactuar con él. 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 del cliente de Lustre, corrobore que el paquete de `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 lustre-client-modules paquete e instale el núcleo correspondiente. 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 de Lustre mediante el siguiente comando.

```
sudo apt-get install -y lustre-client-modules-$(uname -r)
```

SUSE Linux

Para instalar el Lustre cliente en SUSE Linux 12 SP3 SP4, o SP5

Para instalar el Lustre cliente en SUSE Linux 12 SP3

1. Abra un terminal en su cliente de Linux.
2. Instale la clave pública FSx rpm de Amazon mediante 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. Agregue el repositorio para el cliente de Lustre mediante 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 de 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 Lustre cliente en SUSE Linux 12 SP4

1. Abra un terminal en su cliente de Linux.
2. Instale la clave pública FSx rpm de Amazon mediante 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. Agregue el repositorio para el cliente de Lustre mediante 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 siguientes acciones:
   - Si la instaló SP4 directamente, descargue e instale el Lustre cliente 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 migraste desde SP3 al FSx repositorio de Amazon SP4 y lo agregaste anteriormente SP3, descarga e instala el Lustre cliente 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 Lustre cliente en SUSE Linux 12 SP5

1. Abra un terminal en su cliente de Linux.
2. Instale la clave pública FSx rpm de Amazon mediante 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. Agregue el repositorio para el cliente de Lustre mediante 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 siguientes acciones:

   - Si la instaló SP5 directamente, descargue e instale el Lustre cliente con los siguientes comandos.

     ```
     sudo zypper ar --gpgcheck-strict fsx-lustre-client.repo
     sudo zypper refresh
     sudo zypper in lustre-client
     ```

   - Si migraste desde SP4 al FSx repositorio de Amazon SP5 y lo agregaste anteriormente SP4, descarga e instala el Lustre cliente 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

Puedes montar tu sistema de archivos desde una EC2 instancia de Amazon.

Para montar tu sistema de archivos desde Amazon EC2

1. Conéctate a tu EC2 instancia de Amazon.
2. Cree un directorio en su sistema de archivos de FSx For Lustre para el punto de montaje con el siguiente comando.

```
$ sudo mkdir -p /fsx
```

3. Monte el sistema de archivos Amazon FSx for Lustre en el directorio que creó. 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 FSx archivos de Amazon montado en /fsx.

Configuración de clientes de EFA

Utilice los siguientes procedimientos para configurar su cliente de Lustre para acceder a un sistema de archivos FSx para Lustre mediante el Elastic Fabric Adapter (EFA).

EFA es compatible con los clientes de Lustre que ejecutan los siguientes sistemas operativos:

- Amazon Linux 2023 (AL2023)
- Red Hat Enterprise Linux (RHEL) 9.5 o posterior
- Ubuntu 22.04 o posterior con kernel versión 6.8+

El EFA es compatible con los clientes de Lustre que se indican a continuación. Para obtener más información, consulte Instalación del cliente de Lustre.

El EFA se admite en las instancias EC2 de Nitro v4 (o superior) que admiten EFA, excluida la familia de instancias trn2. Consulte Tipos de instancias compatibles en la Guía del usuario de Amazon EC2.

Temas

Paso 1: Instalar los controladores necesarios

> **Note**
>
> Si utiliza una AMI de aprendizaje profundo, puede omitir este paso, ya que tanto el controlador EFA como el controlador GPUDirect Storage (GDS) de NVIDIA vienen preinstalados.

Instalación del controlador EFA

Siga las instrucciones del Paso 3: instalación del software EFA de la Guía del usuario de Amazon EC2.

Instale el controlador GDS (opcional)

Este paso solo es necesario si planea usar GDS de NVIDIA con FSx para Lustre.

Requisitos:

- Instancia de Amazon EC2 de P5, P5e, P5en, P6 B200 o P6 de GB200
- Controlador GDS de NVIDIA, versión 2.24.2 o superior

Para instalar el controlador de almacenamiento GPS de NVIDIA en su instancia de cliente

1. Clona el repositorio GDS de NVIDIA:

```
git clone https://github.com/NVIDIA/gds-nvidia-fs.git
```

2. Compile e instale el controlador:

```
cd gds-nvidia-fs/src/
export NVFS_MAX_PEER_DEVS=128
export NVFS_MAX_PCI_DEPTH=16
sudo -E make
sudo insmod nvidia-fs.ko
```

Paso 2: configure EFA para el cliente de Lustre

Para acceder a un sistema de archivos FSx para Lustre mediante una interfaz EFA, debe instalar los módulos EFA de Lustre y configurar las interfaces EFA.

Configuración rápida

Para configurar rápidamente su cliente Lustre

1. Conéctese a la instancia de Amazon EC2.
2. Descargue y descomprima el archivo que contiene el script de configuración:

```
curl -O https://docs.aws.amazon.com/fsx/latest/LustreGuide/samples/configure-efa-
fsx-lustre-client.zip
unzip configure-efa-fsx-lustre-client.zip
```

3. Cambie a la carpeta de `configure-efa-fsx-lustre-client` y ejecute el script de configuración:

```
cd configure-efa-fsx-lustre-client
sudo ./setup.sh
```

El script hace lo siguiente de forma automática:

- Importa módulos de Lustre.
- Configura las interfaces TCP y EFA.
- Crea un servicio systemd para la configuración automática al reiniciar.

Para ver una lista de opciones y ejemplos de uso que puede usar con el script de `setup.sh`, consulte el archivo de `README.md` en el archivo zip.

Administrar el servicio systemd manualmente

El archivo de servicio systemd se crea en /etc/systemd/system/configure-efa-FSx-lustre-client.service. Los siguientes son algunos comandos útiles relacionados con systemd:

```
# Check status
sudo systemctl status configure-efa-fsx-lustre-client.service

# View logs
sudo journalctl -u configure-efa-fsx-lustre-client.service
# View warnings/errors from dmesg
sudo dmesg
```

Para obtener más información, consulte el archivo de `README.md` en el archivo zip.

Configuración de montaje automático (opcional)

Para obtener más información sobre el Montaje automático del sistema de archivos de Amazon FSx para Lustre en el arranque, consulte Montaje automático del sistema FSx de archivos de Amazon.

Paso 3: interfaces de EFA

Cada sistema de archivos de FSx para Lustre tiene un límite máximo de 1024 conexiones EFA en todas las instancias de cliente.

El script de `configure-efa-fsx-lustre-client.sh` configura automáticamente las interfaces EFA en característica del tipo de instancia.

Tipo de instancia	Número predeterminado de interfaces EFA
p6e-gb200.36xlarge	8
p6-b200.48xlarge	8
p5en.48xlarge	8

Tipo de instancia	Número predeterminado de interfaces EFA
p5e.48xlarge	8
p5.48xlarge	8
Otras instancias con varias tarjetas de red	2
Otras instancias con una sola tarjeta de red	1

Cada interfaz EFA configurada en una instancia de cliente cuenta como una conexión frente al límite de 1024 conexiones EFA cuando se conecta a un sistema de archivos FSx para Lustre.

Administración manual de las interfaces EFA

Las instancias con más interfaces EFA suelen admitir un mayor rendimiento. Puede personalizar la cantidad de interfaces para optimizar el rendimiento de sus cargas de trabajo específicas, siempre y cuando se mantenga dentro del límite total de conexiones de la EFA.

Puede administrar manualmente las interfaces EFA mediante los siguientes comandos:

1. Vea los dispositivos EFA disponibles:

```
for interface in /sys/class/infiniband/*; do
    if [ ! -e "$interface/device/driver" ]; then continue; fi
    driver=$(basename "$(realpath "$interface/device/driver")")
    if [ "$driver" != "efa" ]; then continue; fi
    echo $(basename $interface)
done
```

2. Vea las interfaces actualmente configuradas:

```
sudo lnetctl net show
```

3. Agregue una interfaz EFA:

```
sudo lnetctl net add --net efa --if device_name –peer-credits 32
```

Sustituya *device_name* por un nombre de dispositivo real de la lista del paso 1.

4. Elimine una interfaz EFA:

```
sudo lnetctl net del --net efa --if device_name
```

Sustituya *device_name* por un nombre de dispositivo real de la lista del paso 2.

Montaje de Amazon Elastic Container Service

Puede acceder a su sistema de archivos FSx for Lustre desde un contenedor 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 FSx for Lustre desde la EC2 instancia de Amazon 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 usar la opción 1 (Montaje desde una EC2 instancia de Amazon que aloja tareas de Amazon ECS) porque permite un mejor uso de los recursos, especialmente si inicia muchos contenedores (más de cinco) en la misma EC2 instancia o si sus tareas son de corta duración (menos de 5 minutos).

Usa la opción 2 (Montaje desde un contenedor de Docker) si no puedes configurar la EC2 instancia o si tu aplicación requiere la flexibilidad del contenedor.

> **Note**
>
> No se FSx admite el montaje de Lustre en un tipo de lanzamiento AWS Fargate.

En las siguientes secciones se describen los procedimientos de cada una de las opciones para montar el sistema de archivos FSx for Lustre desde un contenedor de Amazon ECS.

Temas

- Montaje desde una EC2 instancia de Amazon que aloja tareas de Amazon ECS
- Montaje desde un contenedor de Docker

Montaje desde una EC2 instancia de Amazon que aloja tareas de Amazon ECS

Este procedimiento muestra cómo puede configurar una EC2 instancia de Amazon ECS para montar localmente su sistema de archivos FSx for 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 de Lustre.

Para montar el sistema de archivos desde Amazon ECS en una EC2 instancia

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 `lustre-client` paquete y montar su sistema de archivos FSx for Lustre en él. 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 Docker, instale el `lustre-client` paquete y monte su sistema de archivos 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. Añada `SYS_ADMIN` capacidad a su contenedor para autorizarlo a montar su sistema de archivos FSx para Lustre mediante la propiedad. `linuxParameters`

```
"linuxParameters": {
  "capabilities": {
      "add": [
        "SYS_ADMIN"
      ]
   }
}
```

Montaje de sistemas de FSx archivos de Amazon desde una VPC local o interconectada

Puedes acceder al sistema de FSx archivos de Amazon de dos maneras. Una de ellas proviene de EC2 instancias de Amazon ubicadas en una VPC de Amazon enlazada a la VPC del sistema de archivos. La otra proviene de clientes locales que están conectados a la VPC de su sistema de archivos Direct Connect mediante una VPN.

Conecta la VPC del cliente y la VPC de su sistema de FSx archivos de Amazon mediante una conexión de emparejamiento de VPC o una pasarela de tránsito de VPC. Cuando utilizas una conexión de peering de VPC o una pasarela de tránsito para conectarte, las EC2 instancias de VPCs Amazon que se encuentran en una VPC pueden acceder a los sistemas de archivos de FSx Amazon en otra VPC, incluso si pertenecen a cuentas diferentes. VPCs

Antes de utilizar el siguiente procedimiento, debe configurar una conexión de emparejamiento de VPC o una puerta de enlace de tránsito de VPC.

Una pasarela de tránsito es un centro de tránsito de red que puede utilizar para interconectar sus redes con las locales. VPCs 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. VPCs Este tipo de conexión permite enrutar el tráfico entre ellas mediante direcciones privadas del Protocolo de Internet

versión 4 (IPv4) o del Protocolo de Internet versión 6 (IPv6). Puede usar la interconexión de VPC para conectarse VPCs 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 `aws fsx describe-file-systems` AWS CLI comando. También puede obtener esta dirección IP desde la consola de administración de Amazon Web Services.

En la siguiente tabla se muestran los requisitos de dirección IP para acceder a los sistemas de FSx archivos de Amazon mediante un cliente que se encuentra 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
Emparejado VPCs mediante emparejamiento de VPC o AWS Transit Gateway	Los clientes con direccion es IP dentro un rango de direcciones IP privadas de acuerdo con la norma RFC 1918: • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	✓
Redes interconectadas mediante o Direct Connect Site-to-Site VPN		✓

Si necesitas acceder a tu sistema de FSx archivos de Amazon creado antes del 17 de diciembre de 2020 mediante un rango de direcciones IP no privadas, puedes crear un nuevo sistema de archivos restaurando una copia de seguridad del sistema de archivos. Para obtener más información, consulte Protección de los datos con copias de seguridad.

Para recuperar la dirección IP de la interfaz de red primaria de un sistema de archivos

1. Abre la FSx consola de Amazon 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, accederás a la EC2 consola de Amazon.
6. En la pestaña Detalles, busca la IPv4 IP privada principal. Esta es la dirección IP de su interfaz de red principal.

> **Note**
>
> No puedes usar la resolución de nombres del Sistema de nombres de dominio (DNS) al montar un sistema de FSx archivos de Amazon desde fuera de la VPC a la que está asociado.

Montaje automático del sistema FSx de archivos de Amazon

Puedes actualizar el `/etc/fstab` archivo de tu EC2 instancia de Amazon después de conectarte a la instancia por primera vez para que monte tu sistema de FSx archivos de Amazon cada vez que se reinicie.

Usando /etc/fstab para montar Lustre automáticamente FSx

Para montar automáticamente el directorio del sistema de FSx archivos de Amazon cuando la EC2 instancia de Amazon se reinicie, puedes usar el `fstab` archivo. 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 poder actualizar el `/etc/fstab` archivo de la EC2 instancia, asegúrate de que ya has creado el sistema de FSx archivos de Amazon. Para obtener más información, consulte Paso 1: crear un sistema de archivos FSx para Lustre en el Ejercicio de introducción.
> - Para los sistemas de archivos compatibles con EFA, la configuración de systemd es un requisito previo. Para obtener más información, consulte Configuración rápida.

Para actualizar el archivo /etc/fstab de tu instancia EC2

1. Conéctese a su EC2 instancia y abra el `/etc/fstab` archivo en un editor.
2. Añada la línea siguiente al archivo `/etc/fstab`.

   Monte el sistema de archivos Amazon FSx for Lustre en el directorio que creó. Utilice el siguiente comando y sustituya lo siguiente:

   - *`/fsx`*Sustitúyalo por el directorio en el que desee montar el sistema de FSx archivos de Amazon.
   - 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.

   Para sistemas de archivos no compatibles con EFA:

   ```
   file_system_dns_name@tcp:/mountname /fsx lustre defaults,relatime,flock,_netdev,x-
   systemd.automount,x-systemd.requires=network.service 0 0
   ```

   Para sistemas de archivos compatibles con EFA:

   ```
   file_system_dns_name@tcp:/mountname /fsx lustre defaults,relatime,flock,_netdev,x-
   systemd.automount,x-systemd.requires=configure-efa-fsx-lustre-client.service,x-
   systemd.after=configure-efa-fsx-lustre-client.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` es posible que la EC2 instancia deje 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 EC2 instancia ahora está configurada para montar el sistema de FSx archivos de Amazon cada vez que se reinicie.

> **Note**
>
> En algunos casos, es posible que la EC2 instancia de Amazon deba iniciarse independientemente del estado del sistema de FSx archivos de Amazon 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	Description (Descripción)
file_system_dns_name `@tcp:/`	El nombre DNS de tu sistema de FSx archivos de Amazon, que identifica el sistema de archivos. Puede 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 del sistema de FSx archivos de Amazon en tu EC2 instancia.
`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: • `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`. • `relatime` – Esta opción mantiene los datos `atime` (tiempos de acceso al inodo), pero no para cada vez que se accede a un

Campo	Description (Descripción)
	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`. • `flock` – monta tu sistema de archivos con el bloqueo de archivos activado. Si no desea habilitar el bloqueo de archivos, use la opción de montaje `noflock` en su lugar. • `_netdev` – el valor indica al sistema operativo que el sistema de archivos reside en un dispositivo que requiere acceso a la red. Esta 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 para sistemas de archivos no compatibles con EFA garantizan que el montador automático no se ejecute hasta que la conectividad de red esté en línea. **Note** Para Amazon Linux 2023 y Ubuntu 22.04 o posteriores, use la opción `x-systemd.requires=systemd-networkd-wait-online.service` en lugar de la opción `x-systemd.requires=network.service`.

Campo	Description (Descripción)
`x-systemd.automount,x-systemd.requires=configure-efa-fsx-lustre-client.service,x-systemd.after=configure-efa-fsx-lustre-client.service`	Estas opciones para los sistemas de archivos compatibles con EFA garantizan que el montador automático no se ejecute hasta que se complete la configuración del cliente de EFA.
`0`	Un valor que indica si el sistema de archivos debe ser respaldado por `dump`. En el caso de 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. En el caso de los sistemas de FSx archivos de Amazon, este valor debe `0` indicar que no se `fsck` deben ejecutar al inicio.

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: montar un conjunto de archivos de Lustre

1. Suponga que tiene un sistema de archivos 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 use la característica del conjunto de archivos de 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 usar un conjunto de archivos, es posible que algunos comandos administrativos de Lustre que requieren acceso al directorio de `.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 FSx para Lustre, asegúrese de que esté desmontado de todas las EC2 instancias de Amazon que lo hayan montado y, antes de cerrar o terminar cualquier instancia de EC2 Amazon, asegúrese de que cualquier sistema de archivos FSx montado para Lustre esté desmontado de esa instancia.

FSx en el caso de Lustre, los servidores otorgan bloqueos temporales de archivos y directorios a los clientes durante I/O las operaciones, y los clientes deben responder con prontitud cuando los servidores les pidan que liberen sus bloqueos para desbloquear las operaciones. I/O operations from

other clients. If clients become non-responsive, they may be forcefully evicted after several minutes to allow other clients to proceed with their requested I/O Para evitar estos períodos de espera, siempre debe desmontar el sistema de archivos de las instancias cliente antes de cerrarlas o cerrarlas, y antes de FSx eliminarlas en el caso de los sistemas de archivos de Lustre.

Puedes desmontar un sistema de archivos en tu EC2 instancia de Amazon ejecutando el `umount` comando en la propia instancia. No puedes desmontar un sistema de FSx archivos de Amazon a través de AWS CLI Consola de administración de AWS, el o a través de ninguno de los AWS SDKs. Para desmontar un sistema de FSx archivos de Amazon conectado a una EC2 instancia de Amazon que ejecute Linux, utilice el siguiente `umount` comando:

```
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.

Puedes comprobar que tu sistema de FSx archivos de Amazon se ha desmontado ejecutando el `df` comando. Este comando muestra las estadísticas de uso del disco de los sistemas de archivos montados actualmente en la instancia de Amazon EC2 basada en Linux. Si el sistema de FSx archivos de Amazon que deseas desmontar no aparece en el resultado del `df` comando, significa que el sistema de archivos está desmontado.

Example — Identificar el estado de montaje de un sistema de FSx archivos de Amazon y desmontarlo

```
$ 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% /
```

Cómo trabajar con Amazon EC2 Spot Instances

FSx for Lustre se puede utilizar con instancias EC2 puntuales para reducir considerablemente EC2 los costes de Amazon. Una instancia puntual es una EC2 instancia no utilizada que está disponible por un precio inferior al precio bajo demanda. Amazon EC2 puede interrumpir su instancia puntual cuando el precio puntual supere su precio máximo, cuando la demanda de instancias puntuales aumente o cuando disminuya la oferta de instancias puntuales.

Cuando Amazon EC2 interrumpe una instancia puntual, proporciona un aviso de interrupción de la instancia puntual, que avisa a la instancia de dos minutos antes de que Amazon la EC2 interrumpa. Para obtener más información, consulte Spot Instances en la Guía del EC2 usuario de Amazon.

Para garantizar que los sistemas de FSx archivos de Amazon no se vean afectados por las interrupciones de las instancias EC2 puntuales, recomendamos desmontar los sistemas de archivos de FSx Amazon antes de finalizar o EC2 hibernar las instancias puntuales. Para obtener más información, consulte Desmontaje de sistemas de archivos.

Gestión de las interrupciones de Amazon EC2 Spot Instance

FSx for Lustre es un sistema de archivos distribuido en el que las instancias de servidor y cliente cooperan para proporcionar un sistema de archivos fiable y de alto rendimiento. Mantienen un estado distribuido y coherente en las instancias del cliente y del servidor. FSx en el caso de Lustre, los servidores delegan los permisos de acceso temporal a los clientes mientras estos se ocupan activamente de almacenar en caché I/O los 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 clientes malintencionados, los servidores pueden expulsar a los clientes de Lustre que no respondan después de unos minutos. Para evitar tener que esperar varios minutos para que un cliente que no responde responda a la solicitud del servidor, es importante desmontar los Lustre clientes sin problemas, especialmente antes de cerrar las instancias puntuales. EC2

EC2 Spot envía las notificaciones de terminación con 2 minutos de antelación antes de cerrar una instancia. Le recomendamos que automatice el proceso de desmontaje limpio de los Lustre clientes antes de cerrar las instancias puntuales. EC2

Example — Secuencia de comandos para desmontar de forma limpia las instancias puntuales que están finalizando EC2

Este script de ejemplo desmonta de forma limpia las instancias puntuales que terminan haciendo lo EC2 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 prácticas recomendadas para gestionar las interrupciones de las instancias puntuales, consulte Prácticas recomendadas para gestionar las interrupciones de las instancias puntuales. 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/spot/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/spot/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 "${FSXPATH}"; then
        echo "Error unmounting '$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 copias de seguridad en un momento dado, administrar las cuotas de almacenamiento del sistema de archivos, administrar la capacidad de rendimiento y almacenamiento, administrar la compresión de datos y establecer períodos de mantenimiento para realizar parches de software rutinarios en el sistema.

Puede administrar sus sistemas de archivos de FSx para 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

Cómo trabajar con sistemas de archivos compatibles con EFA

Si va a crear un sistema de archivos con una capacidad GBps de rendimiento superior al 10%, le recomendamos que habilite Elastic Fabric Adapter (EFA) para optimizar el rendimiento por instancia de cliente. La EFA es una interfaz de red de alto rendimiento que utiliza una técnica de elusión del

sistema operativo personalizada y el protocolo de red AWS Scalable Reliable Datagram (SRD) para aumentar el rendimiento. Para obtener información sobre EFA, consulte el adaptador Elastic Fabric para cargas AI/ML de trabajo de HPC en Amazon en EC2 la Guía del usuario de Amazon EC2 .

Los sistemas de archivos compatibles con EFA admiten dos funciones de rendimiento adicionales: GPUDirect Storage (GDS) y ENA Express. La compatibilidad con GDS se basa en el EFA para mejorar aún más el rendimiento al permitir la transferencia directa de datos entre el sistema de archivos y la memoria de la GPU, sin pasar por la CPU. Esta ruta directa elimina la necesidad de copias de memoria redundantes y la intervención de la CPU en las operaciones de transferencia de datos. Con la compatibilidad con EFA y GDS, puede lograr un mayor rendimiento en las instancias de cliente individuales compatibles con EFA. ENA Express proporciona una comunicación de red optimizada para EC2 las instancias de Amazon mediante un algoritmo avanzado de selección de rutas y un mecanismo de control de congestión mejorado. Con la compatibilidad con ENA Express, puede lograr un mayor rendimiento en las instancias de cliente individuales compatibles con ENA Express. Para obtener información sobre ENA Express, consulte Mejorar el rendimiento de la red entre EC2 instancias con ENA Express en la Guía del EC2 usuario de Amazon.

Temas

Consideraciones a la hora de utilizar sistemas de archivos compatibles con EFA

Estos son algunos elementos importantes que se deben tener en cuenta al crear sistemas de archivos compatibles con EFA:

- Múltiples opciones de conectividad: los sistemas de archivos compatibles con EFA pueden comunicarse con las instancias de los clientes mediante ENA, ENA Express y EFA.
- Tipo de implementación: el EFA es compatible con los sistemas de archivos Persistent 2 con una configuración de metadatos especificada, incluidos los sistemas de archivos que utilizan la clase de almacenamiento Intelligent-Tiering.
- Actualización de la configuración de EFA: puede optar por habilitar la EFA al crear un nuevo sistema de archivos, pero no puede habilitar ni deshabilitar la EFA en un sistema de archivos existente.

- Escalado del rendimiento con la capacidad de almacenamiento: puede escalar la capacidad de almacenamiento en un sistema de archivos basado en SSD compatible con EFA para aumentar la capacidad de rendimiento, pero no puede cambiar el nivel de rendimiento de un sistema de archivos compatible con EFA.
- Regiones de AWS: Para obtener una lista de Regiones de AWS los sistemas de archivos Persistent 2 compatibles con EFA, consulte. Disponibilidad del tipo de implementación

Requisitos previos para utilizar sistemas de archivos compatibles con EFA

A continuación se indican los requisitos previos para utilizar sistemas de archivos compatibles con EFA:

Para crear un sistema de archivos compatible con EFA:

- Preparación de un grupo de seguridad compatibles con EFA Para obtener más información, consulte Grupos de seguridad compatibles con EFA.
- Utilice la misma zona de disponibilidad y /16 CIDR que las instancias de cliente compatibles con EFA en su Amazon VPC.
- En los sistemas de archivos Intelligent-Tiering, el EFA solo se admite con una capacidad de procesamiento de 4000 o incrementos de 4000. MBps MBps

Para acceder con el sistema de archivos mediante Elastic Fabric Adapter (EFA):

- Utilice instancias Nitro v4 (o superior) que admitan EFA, excepto la familia de EC2 instancias trn2. Consulta los tipos de instancias compatibles en la Guía del EC2 usuario de Amazon.
- Ejecuta AL2 023, RHEL 9.5 y versiones posteriores, o Ubuntu 22+ con la versión de kernel 6.8 o posterior. Para obtener más información, consulte Instalación del cliente de Lustre.
- Instale los módulos EFA y configure las interfaces EFA en las instancias de sus clientes. Para obtener más información, consulte Configuración de clientes de EFA.

Para acceder al sistema de archivos mediante el GPUDirect almacenamiento (GDS):

- Utilice una instancia de cliente Amazon EC2 P5, P5e, P5en, P6-B200 o P6e- 00. GB2
- Instale el paquete NVIDIA Compute Unified Device Architecture (CUDA), el controlador NVIDIA de código abierto y el controlador de almacenamiento NVIDIA en la instancia de cliente. GPUDirect Para obtener más información, consulte Instale el controlador GDS (opcional).

Para acceder al sistema de archivos mediante ENA Express:

- Usa EC2 instancias de Amazon compatibles con ENA Express. Consulta los tipos de instancias compatibles con ENA Express en la Guía del EC2 usuario de Amazon.
- Actualización de las configuraciones para la instancia de Linux. Consulte los requisitos previos para las instancias de Linux en la Guía del EC2 usuario de Amazon.
- Habilite ENA Express en las interfaces de red de las instancias de su cliente. Para obtener más información, consulta Revisa la configuración de ENA Express para tu EC2 instancia en la Guía del EC2 usuario de Amazon.

Cómo crear un sistema de archivos compatibles con EFA

Esta sección contiene instrucciones sobre cómo crear un sistema de archivos compatible con EFA FSx para Lustre utilizando el. AWS CLI Para obtener información sobre cómo crear un sistema de archivos compatible con EFA mediante la FSx consola de Amazon, consulte. Paso 1: crear un sistema de archivos FSx para Lustre

Para crear un sistema de archivos compatibles con EFA (CLI)

Utilice el comando create-file-systemCLI (o la operación CreateFileSystemAPI equivalente). El siguiente ejemplo crea un sistema de archivos compatible con EFA FSx para Lustre con un `PERSISTENT_2` tipo de implementación.

```
aws fsx create-file-system\
   --storage-capacity 4800 \
   --storage-type SSD \
   --file-system-type LUSTRE \
   --file-system-type-version 2.15 \
   --subnet-ids subnet-01234567890 \
   --security-group-ids sg-0123456789abcdefg \
   --lustre-configuration '{"DeploymentType": "PERSISTENT_2", "EfaSupport": true}'
```

Tras crear correctamente el sistema de archivos, Amazon FSx devuelve la descripción del sistema de archivos en formato JSON.

Uso de cuotas de almacenamiento de Lustre

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 cuenta AWS 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 Lustre versión 2.15 den los sistemas de archivos de FSx para 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

Establece cuotas de almacenamiento mediante los comandos `lfs` del sistema de archivos de Lustre en la terminal de 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 comando y el grupo primario del usuario.
`lfs quota -u username /mount_point`	Información general sobre las cuotas de un usuario específic

Ver comando de cuotas	Se muestra información de cuota
	o. Los usuarios con credencia les de usuario raíz de la cuenta AWS pueden ejecutar este comando para cualquier usuario, pero los usuarios que no son raíz 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 cuenta AWS pueden ejecutar este comando para cualquier usuario, pero los usuarios que no son raíz no pueden ejecutar este comando para obtener información sobre las cuotas de otros usuarios.
`lfs quota -g groupname /mount_point`	Información general sobre cuotas para un grupo específic o.
`lfs quota -p projectid /mount_point`	Información general sobre cuotas para un proyecto específico.

Ver comando de cuotas	Se muestra información de cuota
`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 el sistema de archivos a un bucket de Amazon 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 de la SSD o HDD 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 aumentar nuevamente la capacidad del almacenamiento en un sistema de archivos hasta 6 horas después de haber solicitado el último aumento.
- 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 Administrar la capacidad de rendimiento aprovisionada.

- Tipo de implementación: puede aumentar la capacidad de almacenamiento de todos los tipos de implementación, excepto los sistemas de archivos Scratch 1.

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 métrica `FreeStorageCapacity` de CloudWatch para controlar la cantidad de almacenamiento libre disponible en el sistema de archivos. Puede crear una alarma de Amazon CloudWatch en esta métrica y recibir una notificación cuando caiga por debajo de un umbral específico. Para obtener más información, consulte Supervisión con Amazon CloudWatch.

Puede utilizar las métricas de CloudWatch para supervisar los niveles de uso de rendimiento continuos de su 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 de CloudWatch en Amazon FSx para Lustre. Para obtener información sobre cómo la capacidad de almacenamiento afecta a la capacidad de rendimiento, consulte Rendimiento de Amazon FSx for 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.

Aumento de 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 MBps/TiB y múltiplos de 1800 GiB para sistemas de archivos de 40 MBps/TiB.

- Para un sistema de archivos compatible con EFA, este valor debe estar expresado en múltiplos de 38 400 GiB para sistemas de archivos de 125 Mbps/TiB, múltiplos de 19 200 GiB para sistemas de archivos de 250 MBPS/TiB, múltiplos de 9600 GiB para sistemas de archivos de 500 Mbps/TiB y múltiplos de 4800 GiB para sistemas de archivos de 1000 MBPS/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 de FSx para Lustre, 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 `--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 persistentes, 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 con el comando AWS CLI 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.

Estado

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 las solicitudes de aumento de la capacidad de almacenamiento del sistema de archivos mediante el comando de la AWS CLI describe-file-systems y la acción de la API DescribeFilesystems. 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 caché de lectura SSD aprovisionada

Al crear un sistema de archivos con la clase de almacenamiento Intelligent-Tiering, tiene la opción de aprovisionar también una caché de lectura basada en SSD que proporciona latencias de SSD para las lecturas de los datos a los que se accede con frecuencia, hasta 3 IOPS por GiB.

Puede configurar la caché de lectura de la SSD para los datos a los que se accede con frecuencia con una de estas opciones de modo de dimensionamiento:

- Automático (proporcional a la capacidad de rendimiento). Con Automático, Amazon FSx para Lustre selecciona automáticamente el tamaño de la caché de lectura de datos de una SSD en característica de la capacidad de rendimiento aprovisionada.
- Personalizado (aprovisionado por el usuario). Con Personalizado, puede personalizar el tamaño de la caché de lectura de su SSD y escalarla o reducirla en cualquier momento en característica de las necesidades de su carga de trabajo.
- Elija Sin caché si no desea utilizar una caché de lectura de datos de SSD con su sistema de archivos.

En el modo automático (proporcional a la capacidad de rendimiento), Amazon FSx aprovisiona el siguiente tamaño de caché de lectura predeterminado según la capacidad de rendimiento del sistema de archivos.

Capacidad de rendimiento aprovisionada (MBps)	Caché de lectura SSD en modo automático (proporcional a la capacidad de rendimiento) (GiB)	Tamaño de caché de lectura SSD compatible	
		mínimo (GiB)	máximo (GiB)
Cada 4000	20000	32	131072

Después de crear el sistema de archivos, puede modificar el modo de tamaño y la capacidad de almacenamiento de la caché de lectura en cualquier momento.

Temas

Consideraciones a la hora de actualizar la caché de lectura de la SSD

A continuación, presentamos algunas consideraciones importantes a la hora de modificar la caché de lectura de la SSD:

- Cada vez que modifique la caché de lectura de la SSD, se borrará todo su contenido. Esto significa que puede ver una reducción en los niveles de rendimiento hasta que la caché de lectura de la SSD vuelva a llenarse.
- Puede aumentar o reducir el tamaño de la capacidad de la caché de lectura de la SSD. Sin embargo, solo podrá realizar esta acción una vez cada seis horas. No hay ninguna restricción de tiempo a la hora de añadir o eliminar una caché de lectura de la SSD de su sistema de archivos.
- Debe aumentar o reducir el tamaño de la caché en memoria de lectura de su SSD en un mínimo de un 10 % cada vez que la modifique.

Actualización de una caché de lectura SSD aprovisionada

Puede actualizar la caché de lectura de datos de una SSD con la consola Amazon FSx, la AWS CLI o la API de Amazon FSx.

Para actualizar la caché de lectura de la SSD de un sistema de archivos Intelligent-Tiering (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación, elija Sistemas de archivos. En la lista sistemas de archivos, elija el sistema de archivos de FSx para la que quiere actualizar la caché de lectura de la SSD.
3. SSD En el panel de resumen, seleccione Actualizar junto al valor de la caché de lectura de la SSD del sistema de archivos.

   Aparecerá el cuadro de diálogo Actualizar la caché de lectura de la SSD.

4. Seleccione el nuevo modo de dimensionamiento que desee para la caché de lectura de datos, de la siguiente manera:
   - Elija Automático (proporcional a la capacidad de rendimiento) para ajustar automáticamente el tamaño de la caché de lectura de datos en característica de su capacidad de rendimiento.
   - Elija Personalizado (aprovisionado por el usuario) si conoce el tamaño aproximado de su conjunto de datos y desea personalizar su caché de lectura de datos. Si selecciona Personalizado, también tendrá que especificar la capacidad de caché de lectura deseada en GiB.
   - Elija Ninguno si no desea utilizar una caché de lectura de datos SSD con su sistema de archivos Intelligent-Tiering.
5. Elija Actualizar.

Para actualizar la caché de lectura de la SSD para un sistema de archivos Intelligent-Tiering (CLI)

Para actualizar la caché de lectura SSD para un sistema de archivos de nivel inteligente, use el comando update-file-system de AWS CLI o la acción de API equivalente UpdateFileSystem. Establezca los siguientes parámetros:

- Establezca `--file-system-id` en el ID del sistema de archivos que va a actualizar.
- Para modificar la caché de lectura de la SSD, utilice la propiedad `--lustre-configuration DataReadCacheConfiguration`. Esta propiedad tiene dos parámetros, `SizeGiB` y `SizingMode`:
  - SizeGib: establece el tamaño de la caché de lectura de la SSD en GiB cuando se utiliza el modo `USER_PROVISIONED`.
  - SizingMode: establece el modo de dimensionamiento de la caché de lectura de la SSD.
    - Configúrelo en `NO_CACHE` si no desea utilizar una caché de lectura SSD con su sistema de archivos Intelligent-Tiering.
    - Configúrelo en `USER_PROVISIONED` para especificar el tamaño exacto de la caché de lectura de su SSD.
    - Configúrelo en `PROPORTIONAL_TO_THROUGHPUT_CAPACITY` para que el tamaño de la caché en memoria de lectura de datos de la SSD se ajuste automáticamente en característica de su capacidad de rendimiento.

En el siguiente ejemplo, se actualiza la caché de lectura de la SSD al modo `USER_PROVISIONED` y se establece el tamaño en 524 288 GiB.

```
aws fsx update-file-system \
   --file-system-id fs-0123456789abcdef0 \
   --lustre-configuration
 'DataReadCacheConfiguration={SizeGiB=524288,SizingMode=USER_PROVISIONED}'
```

Para supervisar el progreso de la actualización, utilice el comando describe-file-systemsAWS CLI. Busque la sección `AdministrativeActions` en la salida.

Para obtener más información, consulte AdministrativeAction en la referencia de la API de Amazon FSx.

Monitoreo de las actualizaciones de la caché de lectura de la SSD

Puede monitorear el progreso de la actualización de la caché de lectura de la SSD con la consola Amazon FSx, la API o AWS CLI.

Supervisión de las actualizaciones en la consola

Puede monitorear las actualizaciones del sistema de datos en la pestaña Actualizaciones de la página Detalles del sistema de archivos.

Para las actualizaciones de la caché de lectura de la SSD, puede ver la siguiente información:

Tipo de actualización

Los tipos compatibles son el modo de dimensionamiento de la caché de lectura de la SSDl y el tamaño de la caché de lectura de la SSD.

Valor de destino

El valor actualizado para el modo de dimensionamiento de la caché de lectura de la SSD del sistema de archivos o el tamaño de la caché de lectura de la SSD.

Estado

Estado actual de la actualización. 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.
- Completada: la actualización finalizó correctamente.

- Error: la solicitud de actualización falló. Elija el signo de interrogación (?) para ver información sobre la causa de un error en la solicitud.

Tiempo de solicitud

La hora en que Amazon FSx recibió la solicitud de acción de actualización.

Monitoreo de las actualizaciones de la caché de lectura de la SSD con AWS CLI y la API

Puede ver y monitorear las solicitudes de actualización de la caché de lectura de las SSD del sistema de archivos con el comando describe-file-systemsAWS CLI y la acción de la API DescribeFilesystems. La matriz de `AdministrativeActions` enumera las 10 acciones de actualización más recientes para cada tipo de acción administrativa. Al actualizar la caché de lectura de la SSD de un sistema de archivos, se genera un `FILE_SYSTEM_UPDATE` `AdministrativeActions`.

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 acción administrativa pendiente para cambiar el modo de tamaño de la caché de lectura de la SSD a `USER_PROVISIONED` y el tamaño de la caché de lectura de la SSD a 524 288.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586797629.095,
        "Status": "PENDING",
        "TargetFileSystemValues": {
            "LustreConfiguration": {
                "DataReadCacheConfiguration": {
                     "SizingMode": "USER_PROVISIONED"
                     "SizeGiB": 524288,
                }
            }
        }
    }
]
```

Cuando la configuración de la caché de lectura de la SSD tiene disponible el nuevo almacenamiento, el estado de `FILE_SYSTEM_UPDATE` cambia a `COMPLETED`. Si se produce un error en la solicitud

de actualización de la caché de lectura de la SSD, el estado de la acción `FILE_SYSTEM_UPDATE` cambia a `FAILED`.

Administración del rendimiento de los metadatos

Puede actualizar la configuración de metadatos del sistema de archivos de FSx para Lustre sin interrumpir a los usuarios finales o las aplicaciones mediante la consola de Amazon FSx, la API de Amazon FSx o la AWS Command Line Interface (AWS CLI). El procedimiento de actualización aumenta la cantidad de IOPS de metadatos aprovisionadas para el sistema de archivos.

> **Note**
>
> Los metadatos mejorados solo están disponibles para los sistemas de archivos 2.15. Puede aumentar el rendimiento de metadatos solo en los sistemas de archivos de FSx para Lustre creados con el tipo de implementación Persistent 2 y una configuración de metadatos especificada. No puede añadir ni actualizar la configuración de metadatos de un sistema de archivos FSx para Lustre si la configuración de metadatos no se especificó en el momento de la creación del sistema de archivos. Esto también se aplica a los sistemas de archivos restaurados a partir de copias de seguridad de sistemas de archivos de la versión 2.12 que no permitían mejorar el rendimiento de los metadatos, o de sistemas de archivos de la versión 2.15 que no tenían una configuración de metadatos especificada.

El aumento del rendimiento de los metadatos del sistema de archivos estará disponible para su uso en cuestión de minutos. Puede actualizar el rendimiento de los metadatos en cualquier momento, siempre que las solicitudes de aumento del rendimiento de los metadatos se realicen con al menos 6 horas de diferencia. Mientras se escala el rendimiento de los metadatos, 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 del rendimiento de los metadatos. Se le facturará el nuevo aumento del rendimiento de los metadatos una vez que estén disponibles para usted.

Puede realizar un seguimiento del progreso del aumento del rendimiento de los metadatos en cualquier momento mediante la consola, la CLI y la API de Amazon FSx. Para obtener más información, consulte Supervisión de las actualizaciones de configuración de los metadatos.

Temas

Configuración del rendimiento de los metadatos de Lustre

La cantidad de IOPS de metadatos aprovisionadas determina la tasa máxima de operaciones de metadatos que puede admitir el sistema de archivos.

Al crear el sistema de archivos, debe elegir un modo de configuración de metadatos:

- Para los sistemas de archivos SSD, elija Modo automático si desea que Amazon FSx aprovisione y escale automáticamente las IOPS de metadatos en el sistema de archivos en característica de la capacidad de almacenamiento del sistema de archivos. Tenga en cuenta que los sistemas de archivos Intelligent-Tiering no admiten el modo automático.
- Para los sistemas de archivos SSD, puede elegir Aprovisionado por el usuario si desea especificar la cantidad de IOPS de metadatos por aprovisionar al sistema de archivos.
- Para los sistemas de archivos Intelligent-Tiering, debe elegir el modo aprovisionado por el usuario. Con el modo aprovisionado por el usuario, puede especificar la cantidad de IOPS de metadatos por aprovisionar al sistema de archivos.

En los sistemas de archivos SSD, puede cambiar del modo automático al modo aprovisionado por el usuario en cualquier momento. También puede cambiar del modo aprovisionado por el usuario al modo automático si la cantidad de IOPS de metadatos aprovisionadas en el sistema de archivos coincide con la cantidad predeterminada de IOPS de metadatos que se aprovisionaron en modo automático. Los sistemas de archivos Intelligent-Tiering solo admiten el modo aprovisionado por el usuario, por lo que no puede cambiar los modos de configuración de los metadatos.

Los valores de IOPS de metadatos válidos son los siguientes:

- Para los sistemas de archivos SSD, los valores de IOPS de metadatos válidas son 1500, 3000, 6000 y múltiplos de 12 000 hasta un máximo de 192 000.

- Para los sistemas de archivos Intelligent-Tiering, los valores de IOPS de metadatos válidos son 6000 y 12 000.

Si el rendimiento de los metadatos de la carga de trabajo supera la cantidad de IOPS de metadatos aprovisionadas en modo automático, puede usar el modo aprovisionado por el usuario para aumentar el valor de las IOPS de metadatos para el sistema de archivos.

Puede ver el valor actual de la configuración del servidor de metadatos del sistema de archivos de la siguiente manera:

- Mediante la consola: en el panel de resumen de la página de detalles del sistema de archivos, el campo IOPS de metadatos muestra el valor actual de las IOPS de metadatos aprovisionadas y el modo de configuración de metadatos actual del sistema de archivos.
- Uso de la CLI o la API: utilice el comando de la CLI describe-file-systems o la operación de la API DescribeFileSystems y busque la propiedad `MetadataConfiguration`.

Consideraciones al aumentar el rendimiento de los metadatos

A continuación, presentamos algunas consideraciones importantes a la hora de aumentar el rendimiento de los metadatos:

- Solo aumento del rendimiento de los metadatos: solo puede aumentar la cantidad de IOPS de metadatos del sistema de archivos; no puede disminuir la cantidad de IOPS de metadatos.
- Especificación de IOPS de metadatos en modo automático no permitida: no puede especificar la cantidad de IOPS de metadatos en un sistema de archivos que está en modo automático. Tendrá que cambiar al modo aprovisionado por el usuario y, a continuación, realizar la solicitud. Para obtener más información, consulte Cambio del modo de configuración de los metadatos.
- Las IOPS de metadatos para datos escritos antes de escalar: al escalar las IOPS de metadatos a más de 12 000, FSx para Lustre agrega nuevos servidores de metadatos a su sistema de archivos. Los nuevos metadatos se distribuyen automáticamente en todos los servidores para mejorar el rendimiento. Sin embargo, los metadatos y subdirectorios existentes creados antes del escalado permanecen en los servidores de origen, sin que aumenten las IOPS de los metadatos.
- Tiempo entre aumentos: no puede aumentar nuevamente el rendimiento de los metadatos en un sistema de archivos hasta 6 horas después de haber solicitado el último aumento.

- Aumentos del rendimiento de metadatos y del almacenamiento en SSD al mismo tiempo: no se puede escalar el rendimiento de metadatos y la capacidad de almacenamiento del sistema de archivos al mismo tiempo.

¿Cuándo aumentar el rendimiento de los metadatos?

Aumente la cantidad de IOPS de metadatos cuando necesite ejecutar cargas de trabajo que requieran niveles de rendimiento de metadatos superiores a los aprovisionados de forma predeterminada en el sistema de archivos. Puede supervisar el rendimiento de metadatos en la Consola de administración de AWS mediante el gráfico `Metadata IOPS Utilization` que proporciona el porcentaje del rendimiento del servidor de metadatos aprovisionado que consume en el sistema de archivos.

También puede supervisar el rendimiento de los metadatos mediante métricas de CloudWatch más detalladas. Las métricas de CloudWatch incluyen `DiskReadOperations` y `DiskWriteOperations`, que proporcionan el volumen de operaciones del servidor de metadatos que requieren E/S del disco, así como métricas detalladas para las operaciones de metadatos, como la creación de archivos y directorios, las estadísticas, las lecturas y las eliminaciones. Para obtener más información, consulte Métricas de metadatos de FSx para Lustre.

Aumento del rendimiento de metadatos

Puede aumentar el rendimiento de metadatos del sistema de archivos mediante la consola de Amazon FSx, la AWS CLI o la API de Amazon FSx.

Para aumentar el rendimiento de los metadatos de un sistema de archivos (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación, elija Sistemas de archivos. En la lista Sistemas de archivos, elija el sistema de archivos de FSx para Lustre al que desee aumentarle el rendimiento de metadatos.
3. En Acciones, elija Actualizar IOPS de metadatos. O bien, en el panel Resumen, seleccione Actualizar junto al campo IOPS de metadatos del sistema de archivos.

   Aparecerá el cuadro de diálogo Actualizar IOPS de metadatos.
4. Elija Aprovisionada por el usuario.
5. Para las IOPS de metadatos deseadas, elija el nuevo valor de IOPS de metadatos. El valor que ingrese debe ser igual o mayor que el valor actual de IOPS de metadatos.

- Para los sistemas de archivos SSD, los valores válidos son `1500`, `3000`, `6000`, `12000` y múltiplos de `12000`, hasta un máximo de `192000`.
- Para los sistemas de archivos Intelligent-Tiering, los valores válidos son `6000` y `12000`.

6. Elija Actualizar.

Para aumentar el rendimiento de los metadatos de un sistema de archivos (CLI)

Para aumentar el rendimiento de los metadatos de un sistema de archivos de FSx para Lustre, use el comando update-file-system de la AWS CLI (UpdateFileSystem es la acción de la API equivalente). Establezca los siguientes parámetros:

- Establezca `--file-system-id` en el ID del sistema de archivos que va a actualizar.
- Para aumentar el rendimiento de los metadatos, use la propiedad `--lustre-configuration MetadataConfiguration`. Esta propiedad tiene dos parámetros, `Mode` y `Iops`.
  1. Si el sistema de archivos está en modo USER_PROVISIONED, el uso de `Mode` es opcional (si se usa, se establece `Mode` en `USER_PROVISIONED`).

     Si el sistema de archivos SSD está en modo AUTOMÁTICO, establezca `Mode` en `USER_PROVISIONED` (lo que cambia el modo del sistema de archivos a USER_PROVISIONED además de aumentar el valor de IOPS de los metadatos).
  2. Para los sistemas de archivos SSD, establezca `Iops` en un valor de `1500`, `3000`, `6000`, `12000` o múltiplos de `12000` hasta un máximo de `192000`. Para los sistemas de archivos Intelligent-Tiering, establézcalo en `Iops` a `6000`, o `12000`. El valor que ingrese debe ser igual o mayor que el valor actual de IOPS de metadatos.

En el siguiente ejemplo, se actualizan las IOPS de metadatos aprovisionadas a 12 000.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration 'MetadataConfiguration={Mode=USER_PROVISIONED,Iops=12000}'
```

Cambio del modo de configuración de los metadatos

Para los sistemas de archivos basados en SSD, puede cambiar el modo de configuración de metadatos de un sistema de archivos existente mediante la consola y la CLI de AWS, como se explica en los siguientes procedimientos.

Al cambiar del modo automático al modo aprovisionado por el usuario, debe proporcionar un valor de IOPS de metadatos mayor o igual al valor de IOPS de metadatos actual del sistema de archivos.

Si solicita cambiar del modo aprovisionado por el usuario al modo automático y el valor actual de IOPS de metadatos es superior al predeterminado automático, Amazon FSx rechaza la solicitud porque no se admite la reducción de las IOPS de metadatos. Para desbloquear el cambio de modo, debe aumentar la capacidad de almacenamiento para que coincida con las IOPS de metadatos actuales en modo automático para poder volver a activar el cambio de modo.

Puede cambiar la configuración de metadatos del sistema de archivos mediante la consola de Amazon FSx, la AWS CLI o la API de Amazon FSx.

Cómo cambiar el modo de configuración de los metadatos de un sistema de archivos (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación, elija Sistemas de archivos. En la lista sistemas de archivos, elija el sistema de archivos de FSx para Lustre cuyo rendimiento de metadatos desea cambiar.
3. En Acciones, elija Actualizar IOPS de metadatos. O bien, en el panel Resumen, seleccione Actualizar junto al campo IOPS de metadatos del sistema de archivos.

   Aparecerá el cuadro de diálogo Actualizar IOPS de metadatos.
4. Aplique alguna de las siguientes acciones.

   - Para cambiar del modo aprovisionado por el usuario al modo automático, seleccione Automático.
   - Para cambiar del modo automático al modo aprovisionado por el usuario, seleccione Aprovisionado por el usuario. A continuación, para las IOPS de metadatos deseadas, proporcione un valor de IOPS de metadatos superior o igual al valor actual de IOPS de metadatos del sistema de archivos.
5. Elija Actualizar.

Cómo cambiar el modo de configuración de los metadatos de un sistema de archivos SSD (CLI)

Para cambiar el modo de configuración de los metadatos de un sistema de archivos SSD de FSx para Lustre, use el comando update-file-system de la AWS CLI (UpdateFileSystem es la acción de la API equivalente). Establezca los siguientes parámetros:

- Establezca `--file-system-id` en el ID del sistema de archivos que va a actualizar.

- Para cambiar el modo de configuración de los metadatos en los sistemas basados en archivos SSD, use la propiedad de `--lustre-configuration MetadataConfiguration`. Esta propiedad tiene dos parámetros, `Mode` y `Iops`.
  - Para cambiar del sistema de archivos SSD del modo automático al modo aprovisionado por el usuario, debe establecer `Mode` en `USER_PROVISIONED` y `Iops` para proporcionar un valor de IOPS de metadatos mayor o igual al valor de IOPS de metadatos actual del sistema de archivos. Por ejemplo:

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration
 'MetadataConfiguration={Mode=USER_PROVISIONED,Iops=96000}'
```

  - Para cambiar del modo aprovisionado por el usuario al modo automático, establezca `Mode` en `AUTOMATIC` y no use el parámetro `Iops`. Por ejemplo:

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration 'MetadataConfiguration={Mode=AUTOMATIC}'
```

Supervisión de las actualizaciones de configuración de los metadatos

Puede supervisar el progreso de las actualizaciones mediante la consola de Amazon FSx, la API o la AWS CLI.

Supervisión de las actualizaciones de configuración de los metadatos (consola)

Puede supervisar las actualizaciones de la configuración de los metadatos en la pestaña actualizaciones de la página de detalles del sistema de archivos.

Para obtener información sobre las actualizaciones de la configuración de los metadatos, puede ver la siguiente información:

Tipo de actualización

Los tipos admitidos son las IOPS de metadatos y el modo de configuración de metadatos.

Valor de destino

El valor actualizado para las IOPS de metadatos o el modo de configuración de metadatos del sistema de archivos.

Estado

Estado actual de la actualización. 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.
- Completada: la actualización finalizó correctamente.
- Error: la solicitud de actualización falló. Elija el signo de interrogación (?) para ver información sobre la causa de un error en la solicitud.

Tiempo de solicitud

La hora en que Amazon FSx recibió la solicitud de acción de actualización.

Supervisión de las actualizaciones de configuración de los metadatos (CLI)

Puede ver y supervisar las solicitudes de actualización de lac configuración de los metadatos mediante el comando describe-file-systems de la AWS CLI y la operación de la API DescribeFileSystems. La matriz de `AdministrativeActions` enumera las 10 acciones de actualización más recientes para cada tipo de acción administrativa. Cuando actualice el rendimiento o el modo de configuración de los metadatos de un sistema de archivos, se genera una `AdministrativeActions` `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 una acción administrativa pendiente para aumentar las IOPS de los metadatos a 96 000 y el modo de configuración de los metadatos a aprovisionado por el usuario.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1678840205.853,
        "Status": "PENDING",
        "TargetFileSystemValues": {
            "LustreConfiguration": {
                "MetadataConfiguration": {
                    "Iops": 96000,
                    "Mode": USER_PROVISIONED
                }
            }
        }
```

```
    }
]
```

Amazon FSx procesa la acción `FILE_SYSTEM_UPDATE` y modifica las IOPS y el modo de configuración de metadatos del sistema de archivos. Cuando los nuevos recursos de metadatos están disponibles para el sistema de archivos, el estado de `FILE_SYSTEM_UPDATE` cambia a `COMPLETED`.

Si se produce un error en la solicitud de actualización de la configuración de metadatos, el estado de la acción `FILE_SYSTEM_UPDATE` cambia a `FAILED`, como se muestra en el siguiente ejemplo. La propiedad `FailureDetails` proporciona información sobre el fallo.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1678840205.853,
        "Status": "FAILED",
        "TargetFileSystemValues": {
            "LustreConfiguration": {
                "MetadataConfiguration": {
                    "Iops": 96000,
                    "Mode": USER_PROVISIONED
                }
            }
        },
        "FailureDetails": {
            "Message": "failure-message"
        }
    }
]
```

Administrar la capacidad de rendimiento aprovisionada

Todos los sistemas de archivos de FSx para Lustre tienen una capacidad de rendimiento que se configura al crear el sistema de archivos. Para los sistemas de archivos que utilizan almacenamiento SSD o HDD, la capacidad de rendimiento se mide en megabytes por segundo por tebibyte (MBps/TiB). En el caso de los sistemas de archivos que utilizan almacenamiento por niveles inteligente, la capacidad de rendimiento del sistema de archivos se mide en megabytes por segundo (MBps). 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 for 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 MBps/TiB.
- Para los tipos de implementación basados en SSD Persistent 2, los valores válidos son 125, 250, 500 y 1000 MBps/TiB.

Puede modificar la capacidad de rendimiento de un sistema de archivos Intelligent-Tiering aumentando el valor de la capacidad de rendimiento total del sistema de archivos. Los valores válidos son 4000 MBps o incrementos de 4000 MBps, hasta un máximo de 2 000 000 MBps.

Puede ver el valor actual de la capacidad de rendimiento del sistema de archivos por unidad de almacenamiento, como se indica a continuación:

- Uso de la consola: en el panel Resumen de la página de detalles del sistema de archivos, el campo Rendimiento por unidad de almacenamiento muestra el valor actual para los sistemas de archivos basados en SSD, mientras que el campo capacidad de rendimiento muestra el valor actual para los sistemas de archivos Intelligent-Tiering.
- Uso de la CLI o la API: utilice el comando de la CLI describe-file-systems o la operación de la API DescribeFileSystems y busque la propiedad `PerUnitStorageThroughput`.

Al modificar la capacidad de rendimiento del sistema de archivos, entre bastidores, Amazon FSx cambia los servidores de archivos a sistemas de archivos SSD o agrega nuevos servidores de archivos a los sistemas de archivos Intelligent-Tiering. 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

- Modificación de la capacidad de rendimiento
- Monitoreo de los cambios en la capacidad de rendimiento

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 reducir: puede aumentar o reducir la capacidad de rendimiento de un sistema de archivos basado en SSD. Solo se puede aumentar la capacidad de rendimiento de un sistema de archivos Intelligent-Tiering.
- Actualice los incrementos: al modificar la capacidad de rendimiento, utilice los incrementos que aparecen en el cuadro de diálogo Actualizar el nivel de rendimiento para los sistemas de archivos basados en SSD o en el cuadro de diálogo Actualizar la capacidad de rendimiento para los sistemas de archivos Intelligent-Tiering.
- 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.
- Escalado automático de la caché de lectura de la SSD: para el modo predeterminado de la caché de lectura de la SSD (proporcional a la capacidad de rendimiento), Amazon FSx aprovisiona automáticamente 5 GiB de almacenamiento de datos por cada MBps de capacidad de rendimiento que aprovisione. A medida que escala la capacidad de rendimiento de su sistema de archivos, Amazon FSx escala automáticamente la caché de datos de su SSD al adjuntar almacenamiento en caché adicional a cualquier servidor de archivos recién agregado.
- Tipo de implementación: solo puede actualizar la capacidad de rendimiento de los tipos de implementación persistentes basados en SSD o Intelligent-Tiering. No puede modificar la capacidad de rendimiento de los sistemas de archivos basados en SSD compatibles con EFA.

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 del 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 de CloudWatch en Amazon FSx para Lustre. Para obtener información acerca de las métricas de CloudWatch, consulte Supervisión con Amazon CloudWatch.

Modificación de la capacidad de rendimiento

Puede modificar una capacidad de rendimiento de un sistema de archivos de FSx para Lustre con la consola de Amazon FSx, AWS Command Line Interface (AWS CLI) o la API de Amazon FSx.

Cómo modificar la capacidad de rendimiento de un sistema de archivos SSD (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, seleccione Actualizar nivel de rendimiento. O bien, en el panel Resumen, seleccione Actualizar junto a la capacidad de rendimiento del sistema de archivos.

   Aparecerá 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.

Cómo modificar la capacidad de rendimiento (CLI) de un sistema de archivos SSD

- Para modificar la capacidad de rendimiento de un sistema de archivos, utilice el comando CLI update-file-system (o la operación API UpdateFileSystem 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` MBps/TiB para sistemas de archivo Persistent 1 SSD, o a un valor de `125`, `250`, `500` o un sistema de archivo `1000` MBps/TiB for Persistent 2 SSD.

Este comando especifica que la capacidad de rendimiento se establezca en 1000 MBps/TiB para el sistema de archivos.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration PerUnitStorageThroughput=1000
```

Cómo modificar la capacidad de rendimiento de un sistema de archivos Intelligent-Tiering (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 Actions (Acciones), seleccione Update throughput capacity (Actualizar capacidad de rendimiento). O bien, en el panel Summary (Resumen), seleccione Update (Actualizar) junto a la Throughput capacity (Capacidad de rendimiento) del sistema de archivos.

   Aparece el cuadro de diálogo Actualizar la capacidad de rendimiento.
4. Seleccione el valor nuevo para la Capacidad de rendimiento deseado de la lista.

   Amazon FSx escalará automáticamente la caché de lectura de datos para evitar borrar el contenido de la caché.
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.

Cómo modificar la capacidad de rendimiento (CLI) de un sistema de archivos

- Para modificar la capacidad de rendimiento de un sistema de archivos, utilice el comando CLI update-file-system (o la operación API UpdateFileSystem equivalente). Establezca los siguientes parámetros:
  - Establezca `--file-system-id` en el ID del sistema de archivos que va a actualizar.

- Si la caché de lectura de datos está configurada en un modo proporcional a la capacidad de rendimiento, establezca `--lustre-configuration ThroughputCapacity` en un nivel de rendimiento de incrementos de `4000` MBps, hasta un máximo de `2000000` MBps.

  Si la caché de lectura de datos está configurada en el modo aprovisionado por el usuario, también debe usar la propiedad `--lustre-configuration DataReadCacheConfiguration` para especificar la caché de lectura de datos. Debe mantener la misma proporción de almacenamiento en caché por servidor y especificar el nuevo SizeGib o se rechazará la solicitud.

Este comando especifica que la capacidad de rendimiento se establezca en 8000 MBps para un sistema de archivos que utilice una caché en memoria de lectura configurada en modo proporcional al modo de capacidad de rendimiento.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration '{
      "ThroughputCapacity": 8000
      }'
```

Este comando especifica que la capacidad de rendimiento se establezca en 8000 MBps para un sistema de archivos que utilice una caché de lectura configurada en modo aprovisionado por el usuario.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration {
        "ThroughputCapacity": 8000,
        "DataReadCacheConfiguration": '{
             "SizingMode":"USER_PROVISIONED"
             "SizeGiB":1000
             # New size should be cache storage allocated per server multiplied by
 number of file servers
         }
}'
```

Monitoreo 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)

- 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.

  Estado

  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 de la CLI describe-file-systems y la acción de la API DescribeFileSystems. 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 MBps/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 usar la característica de compresión de datos de Lustre para ahorrar costos en los 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. 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 MBps por TiB de almacenamiento. El rendimiento del disco tiene una base de 50 MBps por TiB. Con la compresión de datos, el rendimiento del disco podría aumentar de 50 MBps por TiB a un máximo de 250 MBps 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 Características de rendimiento de las clases de almacenamiento en SSD y HDD. 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 de Amazon FSx for Lustre en el Blog sobre almacenamiento de AWS.

Temas

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 Paso 1: crear un sistema de archivos FSx para 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.
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 de 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 de 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 más información sobre la supervisión del rendimiento del sistema de archivos, consulte Supervisión de sistemas de archivos de Amazon FSx para Lustre.

Root squash de Lustre

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 de 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 de 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 identificador de usuario (UID) y el identificador de grupo (GID) del usuario raíz a un UID y GID especificados por el administrador del sistema de 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 de 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 de 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 usar la consola de Amazon FSx para proporcionar los valores UID y GID del root squash en la propiedad Root Squash, como se muestra en Para habilitar la característica root squash al crear un sistema de archivos (consola). También puede usar el parámetro `RootSquash` con la AWS CLI o la API para proporcionar los valores 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 de Lustre usado 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 NID estándar de Lustre especificando la dirección IP del cliente seguida del identificador de red de 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 usar la propiedad Excepciones a Root Squash de la consola de Amazon FSx para proporcionar la lista de NID de los clientes. En la AWS CLI o la API,

use el parámetro `NoSquashNids`. Para obtener más información, consulte los procedimientos en Administración de root squash.

Administración de root squash

De forma predeterminada, root squash está deshabilitada durante la creación de sistemas de archivos. Puede habilitar la característica root squash al crear un nuevo sistema de archivos de Amazon FSx para Lustre desde la consola de Amazon FSx, la AWS CLI o la API.

Para habilitar la característica 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 Paso 1: crear un sistema de archivos FSx para Lustre en la sección Primeros pasos.
3. Abra la sección Root Squash: opcional.
4. En el caso de Root Squash, proporcione los identificadores de usuario y grupo con los que el usuario raíz puede acceder al sistema de archivos. Puede especificar cualquier número entero en el rango de `1` a `4294967294`:
   1. Para identificador de usuario, especifique el identificador de usuario que debe usar el usuario raíz.
   2. Para identificador de grupo, especifique el identificador de grupo que debe usar el usuario raíz.
5. (Opcional) Para las excepciones a Root Squash, haga lo siguiente:
   1. Seleccione 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. Para obtener información sobre el formato de la dirección IP, consulte Cómo funciona Root Squash.
   3. Repita el procedimiento según sea necesario para agregar 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 activada.

Para habilitar la característica root squash al crear un sistema de archivos (CLI)

- Para crear un sistema de archivos de 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 de 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 del sistema de archivos actual mediante la consola de Amazon FSx, la AWS CLI o la API. Por ejemplo, puede cambiar los valores de UID y GID de root squash, añadir o eliminar los NID de cliente o deshabilitar root squash.

Cómo 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 de Lustre para el que desee gestionar root squash.
3. En Acciones, elija Actualizar root squash. 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 configuración de Root Squash.
4. En el caso de Root Squash, actualice los identificadores de usuario y grupo con los que el usuario raíz puede acceder al sistema de archivos. Puede especificar cualquier número entero en el rango de `0` a `4294967294`. Para deshabilitar root squash, especifique `0` (cero) para ambos identificadores.
   1. Para identificador de usuario, especifique el identificador de usuario que debe usar el usuario raíz.
   2. Para identificador de grupo, especifique el identificador de grupo que debe usar el usuario raíz.
5. Para las excepciones a Root Squash, haga lo siguiente:
   1. Seleccione Agregar dirección de cliente.
   2. En el campo Direcciones de clientes, especifique la dirección IP de un cliente al que no se aplica root squash.
   3. Repita el procedimiento según sea necesario para agregar más direcciones IP de clientes.
6. Elija Actualizar.

> **Note**
>
> Si la función root squash está habilitada y desea deshabilitarla, elija Deshabilitar 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.

Cómo actualizar la configuración de root squash en un sistema de archivos (CLI) existente

Para actualizar la configuración de root squash para un sistema de ficheros FSx para Lustre existente, utilice el comando AWS CLI 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 del sistema de archivos en el panel de Resumen de la página de detalles del sistema de archivos de la consola de Amazon FSx o en respuesta a un comando de `describe-file-systems` de la CLI (la acción de API equivalente es `DescribeFileSystems`).

Estado del sistema de archivos de FSx para Lustre

Puede visualizar el estado de un sistema de archivos de Amazon FSx mediante la consola de Amazon FSx, el comando de AWS CLI describe-file-systems o la operación de API 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: • El sistema de archivos ha generado un error y Amazon FSx no puede recuperarlo. • Al crear un nuevo sistema de archivos, Amazon FSx no pudo crear el sistema de archivos.

Etiquetar los recursos de Amazon FSx para Lustre

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 de 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 tus FSx recursos de Amazon.

Períodos de mantenimiento de Amazon FSx para Lustre

Amazon FSx para Lustre realiza parches de software rutinarios para el software de Lustre que administra. Los parches se aplican con poca frecuencia, normalmente una vez cada varias semanas. 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. 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.

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. 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 mantenimiento. Tenga en cuenta que la caché en memoria se borrará durante el mantenimiento, lo que generará latencias más altas hasta que se complete el mantenimiento.

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
```

Administración de versiones de Lustre

FSx para Lustre actualmente admite varias versiones de Lustre con soporte a largo plazo (LTS) publicadas por la comunidad de Lustre. Las versiones LTS más recientes ofrecen ventajas como mejoras de rendimiento, nuevas características y compatibilidad con las versiones más recientes del núcleo de Linux para sus instancias de cliente. Puede actualizar sus sistemas de archivos a las

versiones más recientes de Lustre en cuestión de minutos con los SDK Consola de administración de AWS, AWS CLI o AWS.

FSx para Lustre actualmente es compatible con las versiones LTS 2.10, 2.12 y 2.15 de Lustre. Puede determinar la versión LTS de sus sistemas de archivos FSx para Lustre mediante Consola de administración de AWS o mediante el comando AWS CLI describe-file-systems.

Antes de realizar la actualización de una versión de Lustre, recomendamos que siga los pasos descritos en Prácticas recomendadas para la actualización de versiones de Lustre.

Temas

Prácticas recomendadas para la actualización de versiones de Lustre

Recomendamos seguir estas prácticas recomendadas antes de actualizar la versión de Lustre de su sistema de archivos FSx para Lustre:

- Pruebe en un entorno que no sea de producción: pruebe una actualización de la versión de Lustre en un duplicado de su sistema de archivos de producción antes de actualizar su sistema de archivos de producción. Esto garantiza un proceso de actualización fluido para su carga de trabajo de producción.
- Garantice la compatibilidad con los clientes: compruebe que las versiones del núcleo de Linux que se ejecutan en sus instancias cliente sean compatibles con la versión de Lustre a la que planea actualizar. Para obtener más información, consulte Compatibilidad con sistemas de archivos de Lustre y kernel de clientes.
- Haga una copia de seguridad de sus datos:
  - Para sistemas de archivos no vinculados a S3: es recomendable que cree una copia de seguridad de FSx antes de actualizar la versión de Lustre a fin de tener un punto de restauración conocido para el sistema de archivos. Si las copias de seguridad diarias automáticas están habilitadas en su sistema de archivos, Amazon FSx creará automáticamente una copia de seguridad de su sistema de archivos antes de la actualización.
  - Para los sistemas de archivos vinculados a S3, le recomendamos que se asegure de que todos los cambios se hayan exportado a S3 antes de realizar la actualización. Si ha activado la exportación automática, compruebe que la métrica `AgeOfOldestQueuedMessage` de exportación automática sea cero para confirmar que todos los cambios se han exportado

correctamente a S3. Si no ha activado la exportación automática, puede ejecutar una exportación manual de tareas de repositorio de datos (DRT) para sincronizar el sistema de archivos con el bucket de S3 antes de realizar la actualización.

Aplicación de la actualización

Para actualizar su sistema de archivos FSx para Lustre a una versión más reciente, siga los pasos que se indican:

1. Desmonte todos los clientes: antes de iniciar la actualización, debe desmontar el sistema de archivos de todas las instancias de clientes que accedan a su sistema de archivos. Puede comprobar que todos los clientes se han desmontado correctamente mediante la métrica `ClientConnections` de Amazon CloudWatch; esta métrica debe mostrar cero conexiones. El proceso de actualización no continuará si algún cliente permanece conectado al sistema de archivos.

   Puede ver la lista de identificadores de red (NID) de los clientes conectados al sistema de archivos en el archivo de `.fsx/clientConnections` almacenado en la raíz del sistema de archivos. Este archivo se actualiza cada 5 minutos. Puede utilizar el comando `cat` para mostrar el contenido del archivo, como en este ejemplo:

   ```
   cat /test/.fsx/clientConnections
   ```

2. Actualización de la versión de FSx: puede actualizar la versión de Lustre de su sistema de archivos de FSx para Lustre mediante la consola Amazon FSx, la AWS CLI o la API de Amazon FSx. Le recomendamos que actualice sus sistemas de archivos a la última versión de Lustre compatible con FSx para Lustre.

   Para actualizar la versión de Lustre de un sistema de archivos (consola)

   a. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
   b. En el panel de navegación, elija Sistemas de archivos. En la lista Sistemas de archivos, elija el sistema de archivos de FSx para Lustre al que desee actualizar la versión de Lustre.
   c. En Acciones, seleccione Actualizar la versión de Lustre del sistema de archivos. O bien, en el panel Resumen, seleccione Actualizar junto al campo IOPS de metadatos del sistema de archivos. Aparece el cuadro de diálogo Actualizar la versión de Lustre del sistema de archivos. Aparece el cuadro de diálogo Actualizar la versión de Lustre del sistema de archivos.

d. En el campo Seleccione una nueva versión de Lustre, elija una versión de Lustre. El valor que elija debe ser más reciente que la versión actual de Lustre.

e. Elija Actualizar.

Para actualizar la versión Lustre de un sistema de archivos (CLI)

Para actualizar la versión Lustre de un sistema de archivos de FSx para Lustre, utilice el comando de AWS CLI update-file-system. (La acción de API equivalente es UpdateFileSystem). Establezca los siguientes parámetros:

- Establezca `--file-system-id` en el ID del sistema de archivos que va a actualizar.
- Establezca `--file-system-type-version` a una versión de Lustre más reciente para el sistema de archivos que está actualizando.

El siguiente ejemplo actualiza la versión Lustre del sistema de archivos de la 2.12 a la 2.15:

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --file-system-type-version "2.15"
```

3. Montar todos los clientes: puede monitorear el progreso de las actualizaciones de las versiones de Lustre mediante la pestaña Actualizaciones de la consola Amazon FSx o `describe-file-systems` en AWS CLI. Una vez que el estado de la actualización de la versión de Lustre sea `Completed`, podrá volver a montar de forma segura el sistema de archivos en las instancias de sus clientes y reanudar su carga de trabajo.

Eliminación de un sistema de archivos

Puede eliminar un sistema de archivos Amazon FSx para Lustre mediante la consola Amazon FSx, la AWS CLI, y la API de 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 enlazados 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 métrica AgeOfoldestQueuedMessage sea cero (si utiliza la exportación automática) o puede ejecutar una tarea de exportación de repositorios 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 Paso 5: Limpieza de recurso.
- Usando la API o la CLI: utilice la operación de la API DeleteFileSystem o el comando CLI delete-file-system.

Protección de los datos con copias de seguridad

Con Amazon FSx for Lustre, puede realizar copias de seguridad automáticas diarias y copias de seguridad iniciadas por el usuario de sistemas de archivos persistentes que no estén vinculados a un repositorio de datos duradero de Amazon S3. Las FSx copias de seguridad file-system-consistent de Amazon son muy duraderas e incrementales. Para garantizar una alta durabilidad, Amazon FSx for Lustre almacena las copias de seguridad en Amazon Simple Storage Service (Amazon S3) con una durabilidad del 99,19% (11 9 unidades).

FSx En el caso de Lustre, las copias de seguridad del sistema de archivos son copias de seguridad incrementales y basadas en bloques, independientemente de que se generen mediante la función de copia de seguridad automática diaria o mediante la función de copia de seguridad iniciada por el usuario. Esto significa que cuando realizas una copia de seguridad, Amazon FSx compara los datos de tu sistema de archivos con la copia de seguridad anterior a nivel de bloque. A continuación, Amazon FSx guarda 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 nuevo sistema de archivos realizada después TBs de cargar los datos tarda horas en completarse.
- Una segunda copia de seguridad del sistema de archivos con datos que TBs implique 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 Lustre contiene toda la información necesaria FSx para crear un nuevo sistema de archivos a partir de la copia de seguridad y restaurar de forma efectiva una point-in-time 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 for Lustre realiza en el sistema de archivos. FSx Las copias de seguridad de Amazon ayudan a satisfacer sus necesidades de cumplimiento y retención de copias de seguridad. Trabajar con las copias de seguridad de Amazon FSx for 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 este 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 Backup FSx para Lustre

Las copias de seguridad solo se admiten en FSx los sistemas de archivos persistentes de Lustre que no estén vinculados a un repositorio de datos de Amazon S3.

Amazon FSx no admite copias de seguridad en sistemas de archivos temporales porque los sistemas de archivos temporales están diseñados para el almacenamiento temporal y el procesamiento de datos a corto plazo. Amazon FSx no admite copias de seguridad en sistemas de archivos vinculados a un bucket de Amazon S3 porque el bucket 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 clase de implementación y almacenamiento y Uso de repositorios de datos.

Trabajo con copias de seguridad diarias automáticas

Amazon FSx for Lustre puede realizar una copia de seguridad automática diaria 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. En algún momento durante el período de copias de seguridad diarias, I/O es posible que el almacenamiento se suspenda brevemente mientras se inicializa el proceso de copia de seguridad (normalmente durante menos de unos 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 utilizar uno de ellos AWS SDKs para cambiar la AWS CLI ventana de copia de seguridad y el período de retención de la copia 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 for Lustre le permite realizar copias de seguridad manuales de sus sistemas de archivos en cualquier momento. Puede hacerlo mediante la consola, la API o la AWS Command Line Interface (CLI) de Amazon FSx for Lustre. Las copias de seguridad de los sistemas de FSx archivos de Amazon iniciadas por los usuarios nunca caducan y están disponibles durante el tiempo que desees 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. Solo puede

eliminar las copias de seguridad iniciadas por el usuario mediante la consola, la API o la CLI de Amazon FSx for Lustre, y Amazon nunca las elimina automáticamente. FSx 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 FSx consola de Amazon para un sistema de archivos existente.

Cómo crear una copia de seguridad iniciada por el usuario del sistema de archivos

1. Abre la consola Amazon FSx for 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 tus copias de seguridad en la consola de Amazon FSx for Lustre, selecciona Backups en la barra de navegación de la izquierda. Si escribe el nombre de la copia de seguridad, la tabla filtra los resultados y mostrar solo los coincidentes.

Al crear una copia de seguridad iniciada por el usuario como se describe en este procedimiento`USER_INITIATED`, tiene el tipo y el estado Creating mientras 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 AWS Backup con Amazon FSx

AWS Backup es una forma sencilla y rentable de proteger sus datos mediante la realización de copias de seguridad de los sistemas de FSx archivos de Amazon. AWS Backup es un servicio de copias de seguridad unificado diseñado para simplificar la creación, copia, restauración y eliminación de copias de seguridad y, al mismo tiempo, mejorar la elaboración de informes y la auditoría. AWS Backup facilita el desarrollo de una estrategia de respaldo centralizada para garantizar el

cumplimiento legal, reglamentario y profesional. AWS Backup también simplifica la protección AWS de sus volúmenes de almacenamiento, bases de datos y sistemas de archivos al proporcionar un lugar central donde puede hacer lo siguiente:

- Configure y audite los AWS recursos de los que desea hacer una copia de seguridad.
- Automatizar la programación de copias de seguridad.
- Establecer políticas de retención.
- Copie las copias de seguridad en todas AWS las regiones y AWS cuentas.
- Monitorizar toda la actividad reciente de copias de seguridad y restauración.

AWS Backup utiliza la función de copia de seguridad integrada de Amazon FSx. Las copias de seguridad realizadas desde la AWS Backup consola 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 FSx consola de Amazon. Si se utilizan AWS Backup para gestionar estas copias de seguridad, se obtienen funciones 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 conserva las copias de seguridad inmutables incluso después de eliminar el sistema de archivos de origen. Esto protege contra la eliminación accidental o malintencionada.

Las copias de seguridad creadas por AWS Backup tienen el tipo de copia de seguridad `AWS_BACKUP` y son incrementales en relación con cualquier otra copia de FSx seguridad de Amazon que realices de tu sistema de archivos. Las copias de seguridad realizadas por se AWS Backup 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 AWS Backup en la FSx consola, la CLI y la API de Amazon. Sin embargo, no puedes eliminar las copias de seguridad realizadas AWS Backup en la FSx consola, CLI o API de Amazon. Para obtener más información sobre cómo AWS Backup realizar copias de seguridad de los sistemas de FSx archivos de Amazon, consulte Trabajar con Amazon FSx File Systems en la Guía para AWS Backup desarrolladores.

Copiar copias de seguridad

Puedes usar Amazon FSx para copiar manualmente las copias de seguridad de la misma AWS cuenta a otra Región de AWS (copias entre regiones) o dentro de la misma Región de AWS (copias dentro de la región). Solo puede realizar copias entre regiones dentro de la misma partición.

AWS Puedes crear copias de seguridad iniciadas por el usuario mediante la FSx consola o la API de Amazon. AWS CLI Cuando crea una copia de seguridad iniciada por el usuario, tiene el tipo`USER_INITIATED`.

También puedes utilizarlas AWS Backup para copiar copias de seguridad entre AWS cuentas Regiones de AWS y entre ellas. 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 AWS región para, en caso de que se produzca un desastre en la región principal Región de AWS, poder restaurarlas a partir de las copias de seguridad y recuperar rápidamente la disponibilidad en la otra AWS región. 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 en la misma AWS cuenta (entre regiones o dentro de una región) mediante la FSx consola de Amazon o la API AWS CLI de Amazon FSx for 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 si utiliza el AWS Backup AWS Organizations soporte. Las políticas definen los límites de las cuentas para las copias multicuentas. AWS Organizations Para obtener más información sobre cómo AWS Backup realizar copias de seguridad entre cuentas, consulta Cómo crear copias de seguridad Cuentas de AWS en la Guía para AWS Backup desarrolladores.

Limitaciones de las copias de seguridad

A continuación se indican algunas limitaciones al copiar copias de seguridad:

- Las copias de seguridad de los sistemas de archivos que utilizan la clase de almacenamiento Intelligent-Tiering no admiten copias de seguridad.
- Las copias de seguridad entre regiones solo se admiten entre dos regiones comerciales Regiones 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 una región, dentro de cualquier región. 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 un único destino de Región de AWS 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 AWS región de origen y solicitar una copia de seguridad 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 de origen. AWS

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.

JSON

```
{
    "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 AWS cuenta 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 FSx los sistemas de archivos Lustre mediante la Consola de administración de AWS CLI y la API, como se describe en los siguientes procedimientos.

Cómo copiar una copia de seguridad dentro de la misma cuenta (entre regiones o dentro de una región) mediante la consola

1. Abre la FSx consola de Amazon 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 de regiones de destino, selecciona una AWS región de destino en la que copiar la copia de seguridad. El destino puede estar en otra AWS región (copia entre regiones) o dentro de la misma AWS región (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 el cifrado, elija la clave de AWS KMS cifrado 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.

Cómo 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 FSx consola de Amazon o mediante programación mediante el comando `describe-backups` CLI o la operación de DescribeBackupsAPI.

Restauración de copias de seguridad

Puede utilizar una copia de seguridad disponible para crear un nuevo sistema de archivos y restaurar de forma eficaz una point-in-time instantánea de otro sistema de archivos. Puede restaurar una copia de seguridad mediante la consola o una de las AWS SDKs. AWS CLI 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.

> **Note**
>
> Solo puede restaurar la copia de seguridad en un sistema de archivos del mismo tipo de implementación, clase de almacenamiento, capacidad de rendimiento, capacidad de almacenamiento, tipo de compresión de datos y Región de AWS que el original. Puede aumentar la capacidad de almacenamiento del sistema de archivos restaurado una vez que esté disponible.

Para restaurar un sistema de archivos a partir de una copia de seguridad mediante la consola

1. Abre la consola Amazon FSx for 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.

   El asistente de creación de sistemas de archivos se abre con la mayoría de los ajustes preconfigurados en característica de la configuración del sistema de archivos desde el que se creó la copia de seguridad. Si lo desea, puede modificar la configuración de la VPC o elegir una versión de Lustre más reciente. Tenga en cuenta que otros ajustes de configuración, como el tipo de implementación y el rendimiento por unidad de almacenamiento, no se pueden modificar durante la restauración.
4. Complete el asistente igual que cuando crea un nuevo sistema de archivos.
5. Elija Review and create.
6. Revisa la configuración que has elegido para el sistema de archivos de Amazon FSx for Lustre y, a continuación, selecciona Crear sistema de archivos.

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 puedes eliminar las copias de seguridad realizadas AWS Backup en la FSx consola, la CLI o la API de Amazon.

Para eliminar una copia de seguridad

1. Abre la consola Amazon FSx for Lustre en https://console.aws.amazon.com/fsx/.
2. En el panel de la consola, elija Copias de seguridad 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.

Supervisión de sistemas de archivos de Amazon FSx para Lustre

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento del sistema de archivos de FSx para Lustre y de las demás soluciones de AWS. Recopilar datos de supervisión de todas las partes de la solución de AWS permite que depure con más facilidad un error de punto múltiple si se produjera. Puede supervisar el sistema de archivos de FSx para Lustre, informar cuando algo no funciona y tomar medidas automáticamente cuando proceda mediante las siguientes herramientas:

- Amazon CloudWatch: supervisa los recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real. Puede recopilar métricas y realizar su seguimiento, crear paneles personalizados y definir alarmas que le adviertan o que tomen medidas cuando una métrica determinada alcance el umbral que se especifique. Por ejemplo, puede hacer que CloudWatch haga un seguimiento de la capacidad de almacenamiento u otras métricas de las instancias de Amazon FSx para Lustre e iniciar nuevas instancias automáticamente cuando sea necesario.
- Registro de Lustre: supervisa los eventos de registro habilitados para el sistema de archivos. El registro de Lustre escribe estos eventos en los Registros de Amazon CloudWatch.
- AWS CloudTrail: captura las llamadas a la API y otros eventos relacionados que realiza la Cuenta de AWS o se realizan en nombre de esta. Además, entrega los archivos de registros a un bucket de Amazon S3 especificado. También pueden identificar qué usuarios y cuentas llamaron a AWS, la dirección IP de origen de las llamadas y el momento en que estas se realizaron.

En las siguientes secciones, se proporciona información sobre cómo usar las herramientas con los sistemas de archivos de FSx para Lustre.

Temas

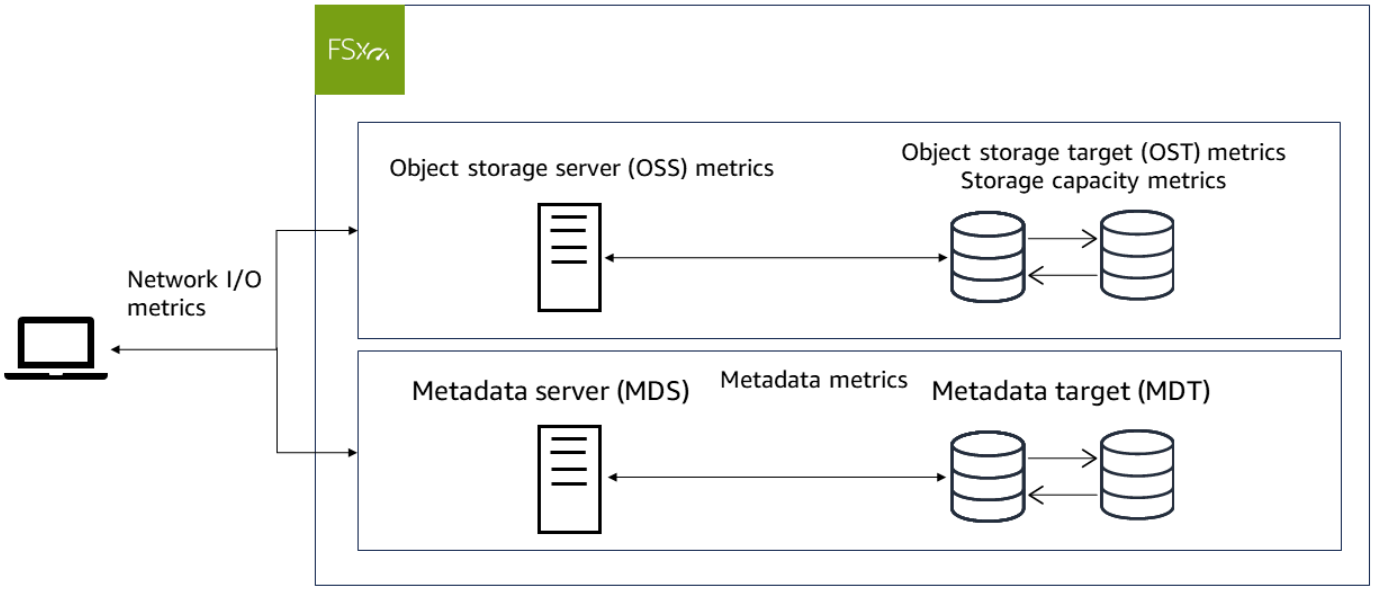
Supervisión con Amazon CloudWatch

Puede supervisar Amazon FSx para Lustre mediante 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 periodo de 15 meses, de forma que pueda acceder a información de historial y obtener una mejor perspectiva acerca del desempeño de su aplicación o servicio. Para obtener más información acerca de CloudWatch, consulte ¿Qué es Amazon CloudWatch? en la Guía del usuario de Amazon CloudWatch.

Las métricas de CloudWatch para FSx para Lustre se organizan en seis categorías:

- Métricas de E/S de la red: mida la actividad entre los clientes y el sistema de archivos.
- Métricas del servidor de almacenamiento de objetos: mida el rendimiento de la red del servidor de almacenamiento de objetos (OSS) y la utilización del rendimiento del disco.
- Métricas del objetivo de almacenamiento de objetos: mida el rendimiento del disco de objetivo de almacenamiento de objetos (OST) y la utilización de las IOPS del disco.
- Métricas de metadatos: mida la utilización de la CPU del servidor de metadatos (MDS), la utilización de las IOPS del objetivo de metadatos (MDT) y las operaciones de metadatos del cliente.
- Métricas de capacidad de almacenamiento: mida la utilización de la capacidad de almacenamiento.
- Métricas del repositorio de datos de S3: mida la antigüedad del mensaje más antiguo en espera de ser importado o exportado y cambie el nombre procesado por el sistema de archivos.

En el siguiente diagrama, se muestra un sistema de archivos de FSx para Lustre, sus componentes y sus categorías de métricas.



FSx para Lustre envía datos de métricas a CloudWatch en intervalos de un minuto.

> **Note**
>
> Es posible que las métricas no se publiquen durante los periodos de mantenimiento del sistema de archivos de Amazon FSx para Lustre.

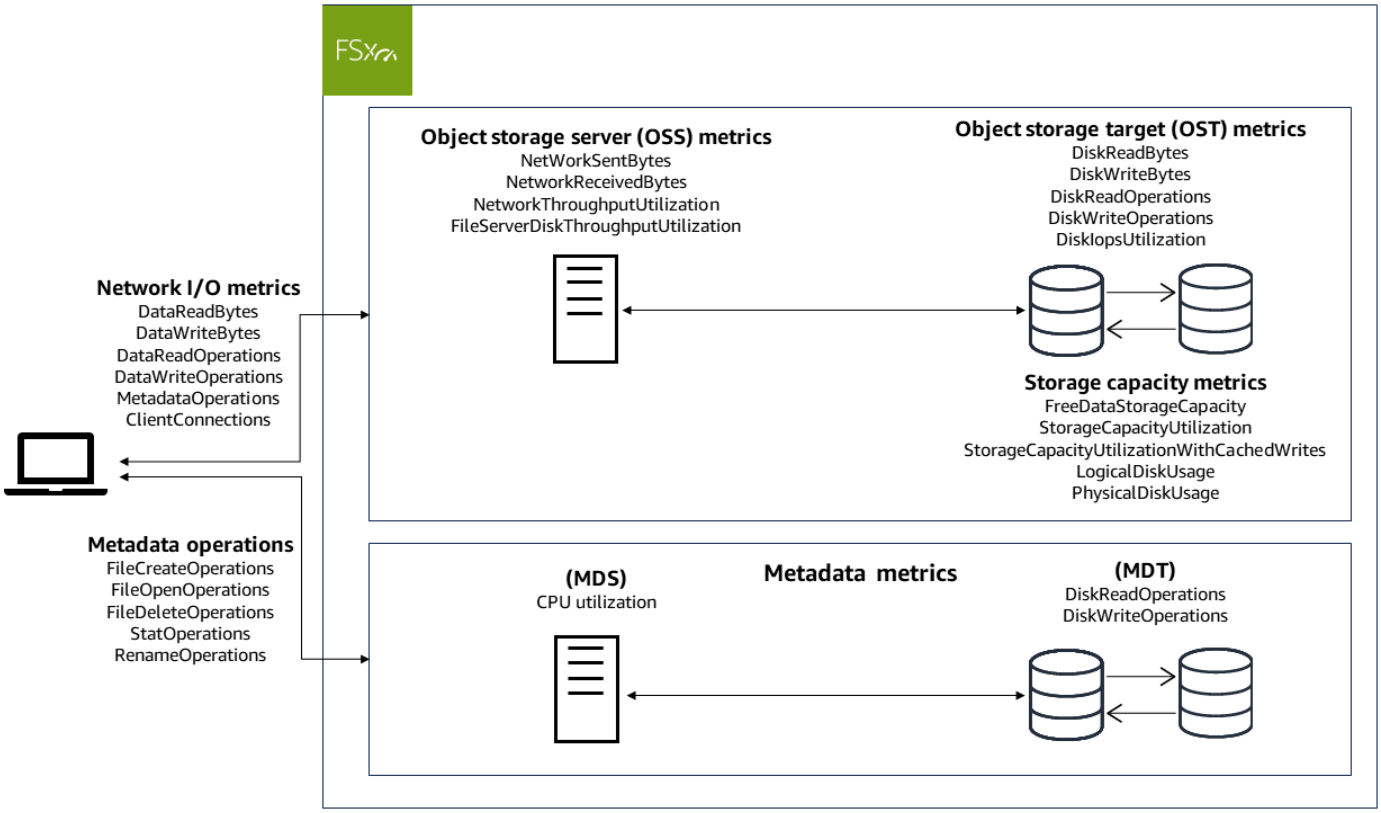
Temas

Cómo usar las métricas de CloudWatch en Amazon FSx para Lustre

Hay dos componentes arquitectónicos principales de cada sistema de archivos de Amazon FSx para Lustre:

- Uno o más servidores de almacenamiento de objetos (OSS) que proporcionan datos a los clientes que acceden al sistema de archivos. Cada OSS está conectado a uno o más volúmenes de almacenamiento, denominados destinos de almacenamiento de objetos (OST), que alojan los datos en el sistema de archivos.
- Uno o más servidores de metadatos (MDS) que proporcionan metadatos a los clientes que acceden al sistema de archivos. Cada MDS está conectado a un volumen de almacenamiento, denominado destino de metadatos (MDT), que almacena metadatos como nombres de archivos, directorios, permisos de acceso y diseños de archivos.

FSx para Lustre notifica métricas en CloudWatch que rastrean el rendimiento y el uso de recursos del almacenamiento y los servidores de metadatos del sistema de archivos y sus volúmenes de almacenamiento asociados. En el siguiente diagrama, se ilustra un sistema de archivos de Amazon FSx para Lustre con los componentes arquitectónicos y las métricas de CloudWatch de rendimiento y recursos, que se ofrecen para supervisar.



Puede usar el panel Supervisión y rendimiento del panel de control del sistema de archivos en la consola de Amazon FSx para Lustre para ver las métricas que se describen en las siguientes tablas. Para obtener más información, consulte Acceso a métricas de CloudWatch.

Actividad del sistema de archivos (en la pestaña “Resumen”)

¿Cómo...?	Gráfico	Métricas relevantes
... determino la cantidad de capacidad de almacenamiento disponible en mi sistema de archivos?	Capacidad de almacenamiento disponible (en bytes)	`FreeDataStorageCapacity`
... determinar el rendimiento total de los clientes de mi sistema de archivos?	Rendimiento total del cliente (bytes/seg)	SUMA (`DataReadBytes` + `DataWriteBytes`) / PERÍODO (en segundos)
…determinar el total de IOPS de cliente en mi sistema de archivos?	IOPS totales de los clientes (operaciones/segundo)	`SUM(DataReadOperations + DataWriteOperations + MetadataOperations )/PERIOD (in seconds)`
…determinar la cantidad de conexiones que se establecen entre los clientes y el servidor de archivos?	Conexiones de cliente (recuento)	`ClientConnections`
…determinar la utilización del rendimiento de los metadatos de mi sistema de archivos?	Utilización de IOPS de metadatos (porcentaje)	`MAX(MDT Disk IOPS)`

Pestaña “Almacenamiento”

¿Cómo...?	Gráfico	Métricas relevantes
…determinar cuánto almacenamiento está disponible?	Capacidad de almacenamiento disponible (en bytes)	`FreeDataStorageCapacity`
…determinar el porcentaje de almacenamiento usado en mi sistema de archivos, sin contar el espacio reservado para las escrituras en caché en los clientes?	Utilización de la capacidad de almacenamiento total (porcentaje)	`StorageCapacityUtilization`
…determinar el porcentaje de almacenamiento usado en mi sistema de archivos, incluido el espacio reservado para las escrituras en caché en los clientes?	Utilización de la capacidad de almacenamiento total (porcentaje)	`StorageCapacityUtilizationWithCachedWrites`
…determinar el porcentaje de almacenamiento usado en los OST de mi sistema de archivos, sin contar el espacio reservado para las escrituras en caché en los clientes?	Utilización de la capacidad de almacenamiento total por OST (porcentaje)	`StorageCapacityUtilization`

¿Cómo...?	Gráfico	Métricas relevantes
…determinar el porcentaje de almacenamiento usado en los OST de mi sistema de archivos, incluido el espacio reservado para las escrituras en caché en los clientes?	Utilización de la capacidad de almacenamiento total por OST con permisos de cliente (porcentaje)	`StorageCapacityUtilizationWithCachedWrites`
…determinar la relación de compresión de datos de mi sistema de archivos?	Ahorros por compresión	100 * (`LogicalDiskUsage` - `PhysicalDiskUSage`)/`LogicalDiskUsage`

Rendimiento del almacenamiento de objetos (en la pestaña “Rendimiento”)

¿Cómo...?	Gráfico	Métricas relevantes
…determinar el rendimiento de la red entre los clientes y los OSS como porcentaje del límite aprovisionado?	Rendimiento de la red (porcentaje)	`NetworkThroughputUtilization`
…determinar el rendimiento del disco entre los OSS y sus OST como porcentaje del límite aprovisionado?	Rendimiento del disco (porcentaje)	`FileServerDiskThroughputUtilization`
…determinar las IOPS para las operaciones que acceden a los OST como porcentaje del límite aprovisionado?	IOPS del disco	`DiskIopsUtilization`

¿Cómo...?	Gráfico	Métricas relevantes
	(porcentaje)	

Rendimiento de los metadatos (en la pestaña “Rendimiento”)

¿Cómo...?	Gráfico	Métricas relevantes
…determinar el porcentaje de utilización de la CPU del servidor de metadatos?	Utilización de la CPU (porcentaje)	`CPUUtilization`
…determinar la utilización de IOPS de metadatos como porcentaje del límite aprovisionado?	Utilización de IOPS de metadatos	`MAX(MDT Disk IOPS)`

Acceso a métricas de CloudWatch

Puede acceder a las métricas de Amazon FSx para Lustre en CloudWatch de las siguientes maneras:

- La consola de Amazon FSx para Lustre.
- La consola de CloudWatch.
- La interfaz de la línea de comandos (CLI) de CloudWatch.
- La API de CloudWatch.

Los siguientes procedimientos le muestran cómo acceder a las métricas con estas herramientas.

Uso de la consola de Amazon FSx para Lustre

Cómo ver las métricas mediante la consola de Amazon FSx para Lustre

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

2. Desde el panel de navegación, elija Sistemas de archivos y, a continuación, elija el sistema de archivos cuyas métricas desee ver.
3. En la página Resumen, seleccione Supervisión y rendimiento para ver las métricas del sistema de archivos.

   Hay cuatro pestañas en el panel Monitoring & performance (Monitoreo y rendimiento).

   - Seleccione Resumen (la pestaña predeterminada) para mostrar las advertencias activas, las alarmas de CloudWatch y los gráficos de la actividad del Sistema de archivos.
   - Elija Almacenamiento para ver la capacidad del almacenamiento, las métricas de utilización y las advertencias activas.
   - Elija Rendimiento para ver las métricas de rendimiento del almacenamiento y los servidores de archivos y las advertencias activas.
   - Elija las alarmas de CloudWatch para ver los gráficos de cualquier alarma configurada para su sistema de archivos.

Uso de la consola de CloudWatch

Cómo 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. (Opcional) Para explorar las métricas, seleccione la categoría que mejor se adapte a su pregunta.

Uso de AWS CLI

Cómo 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.

Uso de API de CloudWatch

Para obtener acceso a las métricas desde la API de CloudWatch

- Llamar a `GetMetricStatistics`. Para obtener más información, consulte la referencia de la API de Amazon CloudWatch.

Métricas y dimensiones de Amazon FSx para Lustre

Amazon FSx para Lustre publica las métricas descritas en las siguientes tablas en el espacio de nombres de `AWS/FSx` de Amazon CloudWatch para todos los sistemas de archivos de FSx para Lustre.

Temas

Métricas de E/S de la red de FSx para Lustre

El espacio de nombres `AWS/FSx` incluye las siguientes métricas de E/S de red. Todas estas métricas tienen una dimensión, `FileSystemId`.

Métrica	Descripción
`DataReadBytes`	La cantidad de bytes que los clientes leen en el sistema de archivos. La estadística `Sum` es el número total de bytes asociados a operacion es de lectura durante el periodo especificado. La estadística `Minimum` es la cantidad mínima de bytes asociados a las operaciones de lectura en un solo OST. La estadística `Maximum` es la cantidad máxima de bytes asociados a las operaciones de lectura en el OST. La estadística

Métrica	Descripción
	`Average` es la cantidad promedio de bytes asociados a las operacion es de lectura por OST. La estadística `SampleCount` es la cantidad de OST. Para calcular el rendimiento medio (bytes por segundo) de un período, divida la estadística `Sum` por el número de segundos del período. Unidades: • Bytes para `Sum`, `Minimum`, `Maximum` y `Average`. • Recuento de , , , y . `SampleCount` . Estadísticas válidas: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCou nt`
`DataWriteBytes`	La cantidad de bytes que los clientes escriben en el sistema de archivos. La estadística `Sum` es el número total de bytes asociados a las operaciones de escritura. La estadística `Minimum` es la cantidad mínima de bytes asociados a las operaciones de escritura en un solo OST. La estadística `Maximum` es la cantidad máxima de bytes asociados a las operaciones de escritura en el OST. La estadística `Average` es la cantidad promedio de bytes asociados a las operaciones de escritura por OST. La estadística `SampleCount` es la cantidad de OST. Para calcular el rendimiento medio (bytes por segundo) de un período, divida la estadística `Sum` por el número de segundos del período. Unidades: • Bytes para `Sum`, `Minimum`, `Maximum` y `Average`. • Recuento de , , , y . `SampleCount` . Estadísticas válidas: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCou nt`

Métrica	Descripción
`DataReadOperations`	El número de operaciones de lectura. La estadística `Sum` es el número total de operaciones de lectura. La estadística `Minimum` es la cantidad mínima de operaciones de lectura en un solo OST. La estadística `Maximum` es la cantidad máxima de operaciones de lectura en el OST. La estadística `Average` es la cantidad promedio de operaciones de lectura por OST. La estadística `SampleCount` es la cantidad de OST. 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. Unidades: • Recuento de `Sum`, `Minimum`, `Maximum`, `Average` y `SampleCount` . Estadísticas válidas: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`

Métrica	Descripción
`DataWriteOperations`	El número de operaciones de escritura. La estadística `Sum` es el número total de operaciones de escritura. La estadística `Minimum` es la cantidad mínima de operaciones de escritura en un solo OST. La estadística `Maximum` es la cantidad máxima de operaciones de escritura en el OST. La estadística `Average` es la cantidad promedio de operaciones de escritura por OST. La estadística `SampleCount` es la cantidad de OST. 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. Unidades: • Recuento de `Sum`, `Minimum`, `Maximum`, `Average` y `SampleCount` . Estadísticas válidas: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`

Métrica	Descripción
`MetadataOperations`	El número de operaciones de metadatos. La estadística `Sum` es el recuento de operaciones de metadatos. La estadística `Minimum` es la cantidad mínima de operaciones de metadatos por MDT. La estadística `Maximum` es la cantidad máxima de operaciones de metadatos por MDT. La estadística `Average` es la cantidad promedio de operaciones de metadatos por MDT. La estadística `SampleCount` es la cantidad de MDT. 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. Unidades: • Recuento de `Sum`, `Minimum`, `Maximum`, `Average` y `SampleCount` . Estadísticas válidas: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`
`ClientConnections`	La cantidad de conexiones activas entre los clientes y el sistema de archivos. Unidad: recuento

Métricas del servidor de almacenamiento de objetos de FSx para Lustre

El espacio de nombres de `AWS/FSx` incluye las siguientes métricas del servidor de almacenamiento de objetos (OSS). Todas estas métricas tienen dos dimensiones, `FileSystemId` y `FileServer`.

- `FileSystemId`: el identificador del recurso de AWS del sistema de archivos.
- `FileServer`: el nombre del servidor de almacenamiento de objetos (OSS) del sistema de archivos de Lustre. Cada OSS está aprovisionado con uno o más destinos de almacenamiento de objetos (OST). Los OSS usan la convención de nomenclatura de OSS <HostIndex>, en la que *`HostIndex`* representa un valor hexadecimal de 4 dígitos (por ejemplo, `OSS0001`). El identificador de un OSS es el identificador del primer OST conectado a él. Por ejemplo, el primer

OSS conectado a `OST0000` y `OST0001` usará `OSS0000` y el segundo OSS conectado a `OST0002` y `OST0003` usará `OSS0002`.

Métrica	Descripción
`NetworkThroughputUtilization`	Utilización del rendimiento de la red como porcentaje del rendimiento de la red disponible para el sistema de archivos. Esta métrica equivale a la suma de `NetworkSentBytes` y `NetworkReceivedBytes` como porcentaje de la capacidad de rendimiento de la red de un OSS del sistema de archivos. Se emite una métrica por minuto para cada uno de los OSS del sistema de archivos. La estadística `Average` es la utilización promedia del rendimiento de la red para el OSS determinado durante un periodo específico. La estadística `Minimum` es la utilización más baja del rendimiento de la red para el OSS determinado por un minuto, durante un periodo específico. La estadística `Maximum` es la utilización más alta del rendimiento de la red para el OSS determinado por un minuto, durante un periodo específico. Unidad: porcentaje Estadísticas válidas: `Average`, `Minimum`, `Maximum`
`NetworkSentBytes`	La cantidad de bytes enviados por el sistema de archivos. En esta métrica, se tiene en cuenta todo el tráfico, incluido el movimiento de datos hacia y desde los repositorios de dato vinculados. Se emite una métrica por minuto para cada uno de los OSS del sistema de archivos.

Métrica	Descripción
	La estadística `Sum` es la cantidad total de bytes enviados a través de la red por el OSS en cuestión durante un periodo específico. La estadística `Average` es la cantidad promedio de bytes enviados a través de la red por el OSS en cuestión durante un periodo específico. La estadística `Minimum` es la cantidad más baja de bytes enviados a través de la red por el OSS en cuestión durante un periodo específico. La estadística `Maximum` es la cantidad más alta de bytes enviados a través de la red por el OSS en cuestión durante un periodo específico. Para calcular el rendimiento enviado (bytes por segundo) de cualquier estadística, divídala por los segundos del periodo especificado. Unidades: bytes Estadísticas válidas: `Sum`, `Average`, `Minimum`, `Maximum`

Métrica	Descripción
`NetworkReceivedBytes`	La cantidad de bytes recibidos por el sistema de archivos. En esta métrica, se tiene en cuenta todo el tráfico, incluido el movimiento de datos hacia y desde los repositorios de dato vinculados. Se emite una métrica por minuto para cada uno de los OSS del sistema de archivos. La estadística `Sum` es la cantidad total de bytes recibidos a través de la red por el OSS en cuestión durante un periodo específico. La estadística `Average` es la cantidad promedio de bytes recibidos a través de la red por el OSS en cuestión durante un periodo específico. La estadística `Minimum` es la cantidad más baja de bytes recibidos a través de la red por el OSS en cuestión durante un periodo específico. La estadística `Maximum` es la cantidad más alta de bytes recibidos a través de la red por el OSS en cuestión durante un periodo específico. Para calcular el rendimiento (bytes por segundo) de cualquier estadística, divídala por los segundos del periodo especificado. Unidades: bytes Estadísticas válidas: `Sum`, `Average`, `Minimum`, `Maximum`

Métrica	Descripción
`FileServerDiskThroughputUtilization`	El rendimiento del disco entre el OSS y los OST asociados, como porcentaje del límite aprovisionado determinado por la capacidad de rendimiento. Esta métrica equivale a la suma de `DiskReadBytes` y `DiskWriteBytes` como porcentaje de la capacidad de rendimiento del disco red de un OSS del sistema de archivos. Se emite una métrica por minuto para cada uno de los OSS del sistema de archivos. La estadística `Average` es la utilización promedio del rendimiento del disco del OSS en cuestión durante un periodo específico. La estadística `Minimum` es la utilización más baja del rendimiento del disco del OSS en cuestión durante un periodo específico. La estadística `Maximum` es la utilización más alta del rendimiento del disco del OSS en cuestión durante un periodo específico. Unidad: porcentaje Estadísticas válidas: `Average`, `Minimum`, `Maximum`

Métricas del destino de almacenamiento de objetos de FSx para Lustre

El espacio de nombres de `AWS/FSx` incluye las siguientes métricas del destino de almacenamiento de objetos (OST). Todas estas métricas tienen dos dimensiones, `FileSystemId` y `StorageTargetId`.

> **Note**
>
> Las métricas `DiskReadOperations` y `DiskWriteOperations` no están disponibles en sistemas de archivos Scratch y las métricas `DiskIopsUtilization` no están disponibles en sistemas de archivos Scratch y Persistent en HDD.

Métrica	Descripción
`DiskReadBytes`	La cantidad de bytes (E/S del disco) de cualquier disco que se lee en este OST. Se emite una métrica por minuto para cada uno de los OST del sistema de archivos. La estadística `Sum` es la cantidad total de bytes leídos en un minuto desde el OST en cuestión durante un periodo específico. La estadística `Average` es la cantidad promedio de bytes leídos en un minuto desde el OST en cuestión durante un periodo específico. La estadística `Minimum` es la cantidad más baja de bytes leídos en un minuto desde el OST en cuestión durante un periodo específico. La estadística `Maximum` es la cantidad más alta de bytes leídos en un minuto desde el OST en cuestión durante un periodo específico. Para calcular el rendimiento de lectura en disco (bytes por segundo) de cualquier estadística, divídala por los segundos del periodo. Unidades: bytes Estadísticas válidas: `Sum`, `Average`, `Minimum` y `Maximum`
`DiskWriteBytes`	La cantidad de bytes (E/S del disco) de cualquier disco que se escribe en este OST. Se emite una métrica por minuto para cada uno de los OST del sistema de archivos. La estadística `Sum` es la cantidad total de bytes escritos en un minuto desde el OST en cuestión durante un periodo específico.

Métrica	Descripción
	La estadística `Average` es la cantidad promedio de bytes escritos en un minuto desde el OST en cuestión durante un periodo específico. La estadística `Minimum` es la cantidad más baja de bytes escritos en un minuto desde el OST en cuestión durante un periodo específico. La estadística `Maximum` es la cantidad más alta de bytes escritos en un minuto desde el OST en cuestión durante un periodo específico. Para calcular el rendimiento de lectura en disco (bytes por segundo) de cualquier estadística, divídala por los segundos del periodo Unidades: bytes Estadísticas válidas: `Sum`, `Average`, `Minimum` y `Maximum`

Métrica	Descripción
`DiskReadOperations`	La cantidad de operaciones de lectura (E/S del disco) de este OST. Se emite una métrica por minuto para cada uno de los OST del sistema de archivos. La estadística `Sum` es la cantidad total de operaciones de lectura realizadas por el OST en cuestión durante un periodo específico. La estadística `Average` es la cantidad promedio de operaciones de lectura realizadas por minuto por el OST en cuestión durante un periodo específico. La estadística `Minimum` es la cantidad más baja de operaciones de lectura realizadas por minuto por el OST en cuestión durante un periodo específico. La estadística `Maximum` es la cantidad más alta de operaciones de lectura realizadas por minuto por el OST en cuestión durante un periodo específico. Para calcular las IOPS promedio del disco durante el periodo, use la estadística `Average` y divida el resultado por 60 (segundos). Unidades: recuento Estadísticas válidas: `Sum`, `Average`, `Minimum` y `Maximum`

Métrica	Descripción
`DiskWrite Operations`	La cantidad de operaciones de escritura (E/S del disco) de este OST. Se emite una métrica por minuto para cada uno de los OST del sistema de archivos. La estadística `Sum` es la cantidad total de operaciones de escritura realizadas por el OST en cuestión durante un periodo específico. La estadística `Average` es la cantidad promedio de operaciones de escritura realizadas por minuto por el OST en cuestión durante un periodo específico. La estadística `Minimum` es la cantidad más baja de operaciones de escritura realizadas por minuto por el OST en cuestión durante un periodo específico. La estadística `Maximum` es la cantidad más alta de operaciones de escritura realizadas por minuto por el OST en cuestión durante un periodo específico. Para calcular las IOPS promedio del disco durante el periodo, use la estadística `Average` y divida el resultado por 60 (segundos). Unidades: recuento Estadísticas válidas: `Sum`, `Average`, `Minimum` y `Maximum`

Métrica	Descripción
`DiskIopsUtilization`	Utilización de IOPS del disco de un OST, expresado como porcentaje del límite de IOPS del disco del OST. Se emite una métrica por minuto para cada uno de los OST del sistema de archivos. La estadística `Average` es la utilización promedio de IOPS del disco del OST en cuestión durante un periodo específico. La estadística `Minimum` es la utilización más baja de IOPS del disco del OST en cuestión durante un periodo específico. La estadística `Maximum` es la utilización más alta de IOPS del disco del OST en cuestión durante un periodo específico. Unidad: porcentaje Estadísticas válidas: `Average`, `Minimum` y `Maximum`

Métricas de metadatos de FSx para Lustre

El espacio de nombres de `AWS/FSx` incluye las siguientes métricas de metadatos. La métrica `CPUUtilization` toma las dimensiones `FileSystemId` y `FileServer`, mientras que las demás métricas toman las dimensiones `FileSystemId` y `StorageTargetId`.

- `FileSystemId`: el identificador del recurso de AWS del sistema de archivos.
- `StorageTargetId`: el nombre del destino de los metadatos (MDT). Los MDT usan la convención de nomenclatura de los MDT <MDTIndex> (por ejemplo, `MDT0001`).
- `FileServer`: el nombre del servidor de metadatos (MDS) del sistema de archivos de Lustre. Cada MDS se aprovisiona con un destino de metadatos (MDT). Los MDS usan la convención de nomenclatura de MDS <HostIndex>, en la que `HostIndex` representa un valor hexadecimal de 4 dígitos derivado del índice MDT del servidor. Por ejemplo, el primer MDS aprovisionado con `MDT0000` usará `MDS0000` y el segundo MDS aprovisionado con `MDT0001` usará `MDS0001`. El sistema de archivos contiene varios servidores de metadatos si el sistema de archivos tiene una configuración de metadatos especificada.

Métrica	Descripción
`CPUUtilization`	El porcentaje de utilización de los recursos de CPU de MDS del sistema de archivos. Se emite una métrica por minuto para cada uno de los MDS del sistema de archivos. La estadística `Average` es la utilización promedio de la CPU del MDS durante un periodo específico. La estadística `Minimum` es la utilización más baja de la CPU del MDS en cuestión durante un periodo específico. La estadística `Maximum` es la utilización más alta de la CPU del MDS en cuestión durante un periodo específico. Unidad: porcentaje Estadísticas válidas: `Average`, `Minimum` y `Maximum`
`FileCreateOperations`	Cantidad total de operaciones de creación de archivos. Unidad: recuento
`FileOpenOperations`	Cantidad total de operaciones de apertura de archivos. Unidad: recuento
`FileDeleteOperations`	Cantidad total de operaciones de eliminación de archivos. Unidad: recuento
`StatOperations`	Cantidad total de operaciones de estado.

Métrica	Descripción
	Unidad: recuento
`RenameOperations`	Cantidad total de cambios de nombre de directorio, ya sean cambios de nombre de directorio locales o cruzados. Unidad: recuento

Métricas de la capacidad de almacenamiento de FSx para Lustre

El espacio de nombres `AWS/FSx` incluye las siguientes métricas de la capacidad de almacenamiento. Todas estas métricas tienen dos dimensiones, `FileSystemId` y `StorageTargetId`, excepto `LogicalDiskUsage` y `PhysicalDiskUsage`, que toman la dimensión `FileSystemId`.

Métrica	Descripción
`FreeDataStorageCapacity`	La cantidad de capacidad de almacenamiento disponible en este OST. Se emite una métrica por minuto para cada uno de los OST del sistema de archivos. La estadística `Sum` es la cantidad total de bytes disponibl es en el OST en cuestión durante un periodo específico. La estadística `Average` es la cantidad promedio de bytes disponibles en el OST en cuestión durante un periodo específico. La estadística `Minimum` es la cantidad más baja de bytes disponibles en el OST en cuestión durante un periodo específico. La estadística `Maximum` es la cantidad más alta de bytes disponibles en el OST en cuestión durante un periodo específico. Unidades: bytes

Métrica	Descripción
	Estadísticas válidas: `Sum`, `Average`, `Minimum` y `Maximum`
`StorageCapacityUtilization`	La utilización de la capacidad de almacenamiento del OST de un sistema de archivos determinado. Se emite una métrica por minuto para cada uno de los OST del sistema de archivos. La estadística `Average` es la cantidad promedio de utilización de la capacidad de almacenamiento del OST en cuestión durante un periodo específico. La estadística `Minimum` es la cantidad mínima de utilización de la capacidad de almacenamiento del OST en cuestión durante un periodo específico. La estadística `Maximum` es la cantidad máxima de utilización de la capacidad de almacenamiento del OST en cuestión durante un periodo específico. Unidad: porcentaje Estadísticas válidas: `Average`, `Minimum`, `Maximum`

Métrica	Descripción
`StorageCapacityUtilizationWithCachedWrites`	La utilización de la capacidad de almacenamiento del OST de un sistema de archivos determinado, incluido el espacio reservado para las escrituras en caché en el cliente. Se emite una métrica por minuto para cada uno de los OST del sistema de archivos. La estadística `Average` es la cantidad promedio de utilización de la capacidad de almacenamiento del OST en cuestión durante un periodo específico. La estadística `Minimum` es la cantidad mínima de utilización de la capacidad de almacenamiento del OST en cuestión durante un periodo específico. La estadística `Maximum` es la cantidad máxima de utilización de la capacidad de almacenamiento del OST en cuestión durante un periodo específico. Unidad: porcentaje Estadísticas válidas: `Average`, `Minimum`, `Maximum`

Métrica	Descripción
`LogicalDiskUsage`	La cantidad de datos lógicos almacenados (sin comprimir). La estadística `Sum` es el número total de bytes lógicos almacenados en el sistema de archivos. La estadísti ca `Minimum` es la menor cantidad de bytes lógicos almacenados en un OST del sistema de archivos. La estadística `Maximum` es el mayor número de bytes lógicos almacenados en un OST del sistema de archivos. La estadística `Average` es la cantidad promedio de bytes lógicos almacenados por OST. La estadística `SampleCount` es la cantidad de OST. Unidades: • Bytes para `Sum`, `Minimum`, `Maximum`. • Recuento de , , , y . `SampleCount` . Estadísticas válidas: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`

Métrica	Descripción
`PhysicalDiskUsage`	La cantidad de almacenamiento ocupada físicamente por los datos del sistema de archivos (comprimidos). La estadística `Sum` es la cantidad total de bytes ocupados en OST del sistema de archivos. La estadística `Minimum` es la cantidad total de bytes ocupados en el OST más vacío. La estadística `Maximum` es la cantidad total de bytes ocupados en el OST más lleno. La estadística `Average` es la cantidad promedio de bytes ocupados por OST. La estadística `SampleCount` es la cantidad de OST. Unidades: • Bytes para `Sum`, `Minimum`, `Maximum`. • Recuento de , , , y . `SampleCount` . Estadísticas válidas: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`

Métricas del repositorio de S3 de FSx para Lustre

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` Dimensión: `AutoExport`	La antigüedad, en segundos, del mensaje más antiguo en espera de ser exportado. La estadística `Average` es la edad media del mensaje más antiguo en espera de ser exportado. La estadística `Maximum`

Métrica	Descripción
	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 mensaje ha permanecido en la cola. Un valor de cero indica que no hay mensajes esperando a ser exportados. Unidades: segundos Estadísticas válidas: `Average`, `Minimum`, `Maximum`
`RepositoryRenameOperations` Dimensión: `AutoExport`	El número de cambios de nombre procesado s por el sistema de archivos en respuesta a un cambio de nombre de directorio mayor. 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. Unidades: recuento Estadísticas válidas: `Sum`, `Average`, `Minimum` y `Maximum`

Métrica	Descripción
`AgeOfOldestQueuedMessage` Dimensión: `AutoImport`	La antigüedad, en segundos, del mensaje más antiguo en espera de ser importado. 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. Unidades: segundos Estadísticas válidas: `Average`, `Minimum`, `Maximum`

Dimensiones de FSx para Lustre

Las métricas de Amazon FSx para Lustre usan el espacio de nombres de `AWS/FSx` y las siguientes dimensiones.

- La dimensión `FileSystemId` indica el identificador de un sistema de archivos y filtra las métricas que usted solicita a ese sistema de archivos individual. Puede encontrar el identificador en la consola de Amazon FSx en el panel Resumen de la página de detalles del sistema de archivos, en el campo Identificador del sistema de archivos. El identificador del sistema de archivos adopta la forma de *`fs-01234567890123456`*. También puede ver el identificador en la respuesta del comando `describe-file-systems` de la CLI (la acción de API equivalente es `DescribeFileSystems`).
- La dimensión `StorageTargetId` indica qué OST (destino de almacenamiento de objetos) o MDT (destino de metadatos) publicó las métricas de metadatos. Un `StorageTargetId` adopta la forma de `OSTxxxx` (por ejemplo, `OST0001`) o `MDTxxxx` (por ejemplo, `MDT0001`).
- La dimensión `FileServer` denota lo siguiente

- Para las métricas de OSS: el nombre del servidor de almacenamiento de objetos (OSS). Los OSS usan la convención de nomenclatura `OSSxxxx` (por ejemplo, `OSS0002`).
- Para la métrica de utilización de la CPU: el nombre de un servidor de metadatos (MDS). Los MDS usan la convención de nomenclatura `MDSxxxx` (por ejemplo, `MDS0002`).
- La dimensión `Publisher` está disponible en CloudWatch y la AWS CLI para las métricas `AutoImport` y `AutoImport` para denotar qué servicio publicó las métricas.

Para obtener más información acerca de las dimensiones, consulte Dimensiones en la Guía del usuario de Amazon CloudWatch.

Advertencias y recomendaciones de rendimiento

FSx para Lustre muestra una advertencia para las métricas de CloudWatch cada vez que una de estas métricas se acerca o supera un umbral predeterminado para varios puntos de datos consecutivos. Estas advertencias le brindan recomendaciones prácticas que puede utilizar para optimizar el rendimiento del sistema de archivos.

Se puede acceder a las advertencias en varias áreas del panel Supervisión y rendimiento en la consola de Amazon FSx para Lustre. Todas las advertencias de rendimiento de Amazon FSx activas o recientes y todas las alarmas de CloudWatch configuradas para el sistema de archivos que se encuentre en estado de alarma aparecen en el panel Supervisión y rendimiento de la sección Resumen. La advertencia también aparece en la sección del panel de control donde se muestra el gráfico métrico. Estas advertencias desaparecen automáticamente del panel de control 24 horas después de que las métricas subyacentes caigan por debajo del umbral de advertencia.

Puede crear alarmas de CloudWatch para cualquiera de las métricas de Amazon FSx. Para obtener más información, consulte Creación de alarmas de CloudWatch para monitorizar las métricas de .

Utilice las advertencias de rendimiento para mejorar el rendimiento del sistema de archivos

Amazon FSx ofrece recomendaciones prácticas que puede utilizar para optimizar el rendimiento de su sistema de archivos. Puede tomar las medidas recomendadas si espera que el proble continúe o si está afectando al rendimiento del sistema de archivos. En función de la métrica que haya provocado la advertencia, puede resolverla aumentando la capacidad de rendimiento, la capacidad de almacenamiento o las IOPS de metadatos del sistema de archivos, tal y como se describe en la siguiente tabla.

Sección del panel	Si hay una advertencia para esta métrica	Haga lo siguiente
Almacenamiento	`Storage capacity utilization`	Aumente la capacidad de almacenamiento del sistema de archivos. Si la utilización de la capacidad de almacenamiento solo es mayor para un subconjunto de los destinos de almacenamiento de objetos (OST) del sistema de archivos, también puede reequilibrar la carga de trabajo para que la utilización de la capacidad de almacenamiento se equilibre de manera más uniforme en todo el sistema de archivos.
	`Storage capacity utilization with cached writes`	Reduzca el tamaño de la memoria caché de escritura de los clientes configurando el parámetro max_dirty_mb en los clientes.
Rendimiento del almacenamiento de objetos	`Network throughput`	Aumente la capacidad de rendimiento del sistema de archivos. Si la utilización del rendimiento es mayor para un subconjunto de los servidores de almacenamiento de objetos (OSS) del sistema de archivos, también puede reequilibrar la carga de trabajo para que la utilización

Sección del panel	Si hay una advertencia para esta métrica	Haga lo siguiente
		del rendimiento se equilibre de manera más uniforme en todo el sistema de archivos.
	`Disk throughput`	Aumente la capacidad de rendimiento del sistema de archivos. Si la utilización de rendimien to del disco es mayor para un subconjunto de los servidores de almacenamiento de objetos (OSS) del sistema de archivos, también puede reequilibrar la carga de trabajo para que la utilización de rendimiento del disco se equilibre de manera más uniforme en todo el sistema de archivos.
	`Disk IOPS`	Aumente la capacidad de almacenamiento del sistema de archivos. Si la utilización de IOPS del disco es mayor para un subconjunto de los destinos de almacenamiento de objetos (OST) del sistema de archivos, también puede reequilibrar la carga de trabajo para que la utilización de IOPS del disco se equilibre de manera más uniforme en todo el sistema de archivos.

Sección del panel	Si hay una advertencia para esta métrica	Haga lo siguiente
Rendimiento de metadatos	`CPU utilization`	Aumente la capacidad de almacenamiento del sistema de archivos. Si necesita escalar el rendimiento de los metadatos independientemente de la capacidad de almacenamiento, puede migrar a un nuevo sistema de archivos que permita aprovisionar el rendimiento de metadatos más allá de la capacidad de almacenamiento mediante el parámetro MetadataConfiguration.
	`Metadata IOPS`	Aumente las IOPS de metadatos del sistema de archivos.

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

Creación de alarmas de CloudWatch para monitorizar las métricas de

Puede crear una alarma de CloudWatch que envíe un mensaje de Amazon SNS cuando la alarma cambie de estado. Una alarma controla una única métrica durante el periodo que especifique y realiza una o varias acciones en función del valor de la métrica relativo a un determinado umbral durante un periodo. La acción es una notificación que se envía a un tema de Amazon SNS o a una política de Auto Scaling.

Las alarmas invocan acciones únicamente para los cambios de estado prolongados. Las alarmas de CloudWatch no invocan acciones simplemente porque estén en un estado particular. El estado debe

cambiar y permanecer modificado durante un periodo específico. Puede crear alarmas con la consola de Amazon FSx o la consola de CloudWatch.

Los siguientes procedimientos describen cómo crear alarmas para Amazon FSx para Lustre con la consola, la AWS CLI y la API.

Cómo establecer alarmas con la consola de Amazon FSx para Lustre

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación, elija Sistemas de archivos y, a continuación, elija el sistema de archivos para el que desea crear la alarma.
3. En la página Resumen, seleccione Supervisión y rendimiento.
4. Seleccione Crear alarma de CloudWatch. Se lo redirigirá a la consola de CloudWatch.
5. Elija Seleccionar métricas y, luego, Siguiente.
6. En la sección de Métricas, elija FSX.
7. Elija Métricas del sistema de archivos, seleccione la métrica para la que desea configurar la alarma y, a continuación, elija Seleccionar métrica.
8. En la sección Condiciones, elija las condiciones para la alarma, y luego, Siguiente.

   > **Note**
   >
   > Es posible que las métricas no se publiquen durante el mantenimiento del sistema de archivos. Para evitar cambios innecesarios y engañosos en el estado de las alarmas y configurar las alarmas 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.

9. Si desea que CloudWatch le envíe un correo electrónico o una notificación SNS cuando el estado de la alarma activa la acción, elija Siempre que ocurra este estado de alarma.

   En Seleccionar un tema de SNS, elija un tema de SNS existente. Si selecciona 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 el campo para futuras alarmas. Elija Siguiente.

> **Warning**
>
> Si utiliza Crear tema para crear un nuevo tema de Amazon SNS, debe verificar las direcciones de correo electrónico para que reciban 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 reciben una notificación.

10. Rellene los valores de Nombre, Descripción, y Siempre que de la métrica, y luego seleccione Siguiente.
11. En la página Vista previa y crear, revise la alarma y elija Crear alarma.

Cómo establecer alarmas utilizando la consola de CloudWatch

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. Elija Crear alarma para iniciar el Asistente de creación de alarmas.
3. Elija Métricas de FSx para localizar una métrica. Para filtrar los resultados, puede buscar el identificador del sistema de archivos. Seleccione la métrica para la que desea crear una alarma y elija Siguiente.
4. Escriba valores para Nombre y Descripción y, luego, seleccione Siempre que para la métrica.
5. Si desea que CloudWatch le envíe un correo electrónico cuando se alcance el estado de la alarma, elija El estado es ALARMA para Siempre que esta alarma. En Enviar notificación a, elija un tema de SNS existente. Si selecciona Crear tema, puede definir los nombres y las direcciones de correo electrónico de una nueva lista de suscripción de correo electrónico. Esta lista se guarda y aparece en el campo para futuras alarmas.

> **Warning**
>
> Si utiliza Crear tema para crear un nuevo tema de Amazon SNS, debe verificar las direcciones de correo electrónico para que reciban 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 reciben una notificación.

6. Vea la vista previa de la alarma y, a continuación, seleccione Crear alarma o regrese para realizar cambios.

Cómo 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.

Cómo configurar una alarma mediante CloudWatch

- Llamar a `PutMetricAlarm`. Para obtener más información, consulte la Referencia de la API de Amazon CloudWatch.

Registro con los Registros de Amazon CloudWatch

FSx para Lustre permite registrar en los Registros de Amazon CloudWatch los eventos de error y advertencia de los repositorios de datos asociados a su sistema de archivos.

> **Note**
>
> El registro con los Registros de Amazon CloudWatch solo está disponible en los sistemas de archivos de Amazon FSx para 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 de FSx para Lustre, puede habilitar el registro de los eventos del repositorio de datos en los Registros de Amazon CloudWatch.

Los eventos de error y advertencia se pueden registrar para los eventos de importación, exportación y restauración. 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 for 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 para Lustre debe configurarse con un destino de los Registros de Amazon CloudWatch. El destino de registro de eventos es un grupo de registro de los Registros de Amazon CloudWatch y Amazon FSx crea un flujo de registro para su sistema de archivos dentro de este grupo de registro. Los registros de CloudWatch le permite almacenar, ver y buscar registros de eventos de auditoría en la consola de Amazon CloudWatch, ejecutar consultas en los registros mediante CloudWatch Logs Insights y activar alarmas de CloudWatch o funciones de 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 registro de los Registros de CloudWatch predeterminado en su cuenta como destino del registro de eventos. Si quiere usar un grupo de registro de los Registros de CloudWatch personalizados 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 registro de los Registros de Amazon CloudWatch debe empezar por el prefijo `/aws/fsx/`.
- Si no tiene un grupo de registro de los Registros de CloudWatch existente al crear o actualizar un sistema de archivos en la consola, Amazon FSx para Lustre puede crear y usar un flujo de registro predeterminado en el grupo de registro `/aws/fsx/lustre` de los Registros de CloudWatch. 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 registro predeterminado, la interfaz de usuario de configuración le permite crear un grupo de registro de los Registros de CloudWatch al crear o actualizar el sistema de archivos en la consola.
- El grupo de registro de los Registros de CloudWatch de destino debe estar en la misma partición de AWS, Región de AWS y Cuenta de AWS como su sistema de archivos de Amazon FSx para Lustre.

Puede cambiar el destino del registro de eventos en cualquier momento. Al hacerlo, los nuevos registros de eventos se envían solo al nuevo destino.

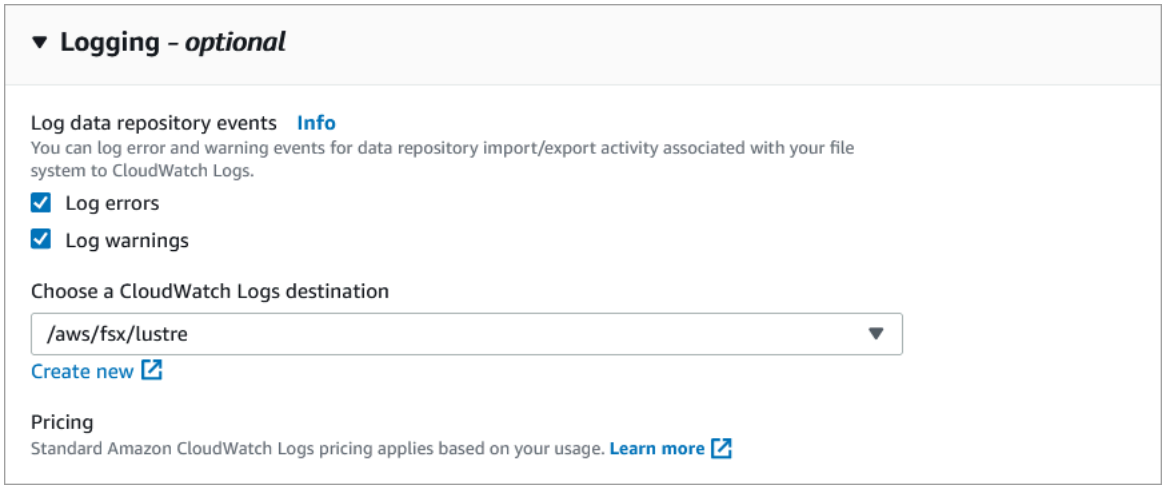
Administración de registros

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 de 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, AWS CLI, o la API 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 Paso 1: crear un sistema de archivos FSx para 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 propiedad `LogConfiguration` con la operación CreateFileSystem 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.

Cómo 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 Data repository.
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 los Registros de CloudWatch existente o cree uno nuevo.

6. Seleccione Save.

Cómo 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:

- Puede ver los registros accediendo a la consola de Amazon CloudWatch y seleccionando el grupo de registro y el flujo de registro al que se envían los registros de eventos. Para obtener más información, consulte Ver los datos de registro enviados a CloudWatch Log en la Guía del usuario de Registros de Amazon Cloudwatch.
- Puede utilizar la Información de registros de CloudWatch para buscar y analizar de forma interactiva los datos de registro. Para obtener más información, consulte Analizar los datos de registro con Información de registros de CloudWatch en la Guía del usuario de Registros de Amazon CloudWatch.
- También puede exportar registros a Amazon S3. Para obtener más información, consulte Exportar datos de registros a Amazon S3 en la Guía del usuario de Registros de Amazon CloudWatch.

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 en la consola de CloudTrail en el Historial de eventos. Mediante la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a Amazon 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 sobre 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 Visualización de 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

- Recepción de archivos de registro de CloudTrail de varias regiones y Recepción de 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 lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario de AWS Identity and Access Management (IAM) o credenciales de usuario raíz.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para 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 de registro de CloudTrail pueden contener una o varias entradas de registro. Un evento representa una solicitud específica realizada desde un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

El siguiente ejemplo muestra una entrada de registro de CloudTrail que demuestra la operación `TagResource` cuando se 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 demuestra la acción `UntagResource` cuando una etiqueta para un sistema de archivos se elimina de 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"
}
```

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 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 con AWS DataSync? en la guía del usuario de 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 Configuración inicial de AWS DataSync en la guía del usuario de AWS DataSync.

- Ha creado un sistema de archivo FSx para Lustre de destino. Para obtener más información, consulte Paso 1: crear un sistema de archivos FSx para 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 Site-to-Site 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 mediante DataSync implica los siguientes pasos básicos:

1. Descargue e implemente un agente en su entorno y actívelo (no es necesario si se realiza una transferencia entre Servicios de AWS uno y otro).
2. Cree una ubicación de origen y de destino.
3. Cree una tarea.
4. 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 de AWS DataSync con Amazon FSx para Lustre.
- Implementación del agente en Amazon EC2

Seguridad en Amazon FSx para Lustre

La seguridad en AWS es la principal prioridad. Como cliente de AWS, se beneficiará de una arquitectura de red y de centros de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y el usuario. 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 los servicios de AWS en Amazon Web Services Cloud. AWS también brinda 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 sobre los programas de conformidad que se aplican a Amazon FSx for Lustre, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad se determina según el servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida a la hora de utilizar Amazon FSx for Lustre. En los siguientes temas, se mostrará cómo configurar Amazon FSx para satisfacer sus objetivos de seguridad y conformidad. También puede aprender a usar otros servicios de Amazon que ayudan a supervisar y proteger los recursos de Amazon FSx for Lustre.

A continuación encontrará una descripción de las consideraciones de seguridad para trabajar con Amazon FSx.

Temas

Protección de los datos en Amazon FSx for Lustre

El modelo de responsabilidad compartida, y de AWS se aplica a la protección de datos de Amazon FSx for Lustre. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres 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, consulta las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta 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, recomendamos proteger las credenciales de la Cuenta de AWS y configurar cuentas de usuario individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Utiliza SSL/TLS para comunicarse con los recursos de AWS. Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure los registros de API y de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre cómo utilizar registros de seguimiento de CloudTrail para capturar actividades de AWS, consulta Working with CloudTrail trails en la Guía del usuario de AWS CloudTrail.
- Utiliza las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los servicios de Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-3 al acceder a AWS a través de una interfaz de línea de comandos o una API, utiliza un punto de conexión de FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulta Estándar de procesamiento de la información federal (FIPS) 140-3.

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 las situaciones en las que debe trabajar con la Amazon FSx u otros Servicios de AWS a través de la consola, la API, la AWS CLI o los SDK de AWS. Cualquier

dato que ingrese en etiquetas o campos de texto 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 for Lustre

Amazon FSx for Lustre admite dos formas de cifrado para sistemas de archivos, el cifrado de datos en reposo y el 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 el sistema de archivos de Amazon FSx for Lustre.

Temas

Cifrado de datos en reposo

El cifrado de los datos en reposo se habilita automáticamente al crear un sistema de archivos de Amazon FSx for Lustre mediante la Consola de administración de AWS, la AWS CLI o mediante programación a través de la API de Amazon FSx o uno de los SDK de 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 clave AWS KMS 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 el sistema de archivos de Amazon FSx for Lustre.

> **Note**
>
> La infraestructura de gestión de claves de AWS utiliza algoritmos criptográficos aprobados por el estándar de procesamiento de la información federal (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 FSx para Lustre utiliza AWS KMS, consulte Cómo Amazon FSx for Lustre usa 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 for Lustre de forma transparente, por lo que no tiene que modificar sus aplicaciones.

Amazon FSx for Lustre usa 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 de AWS Key Management Service.

Cómo Amazon FSx for Lustre usa AWS KMS

Amazon FSx for Lustre cifra datos de manera automática antes de escribirse en el sistema de archivos y los descifra de la misma manera a medida que se leen. Los datos se cifran mediante un cifrado de bloques XTS-AES-256. Todos los sistemas de archivos scratch de FSx para Lustre se cifran en reposo mediante claves administradas por AWS KMS. Amazon FSx for Lustre se integra con AWS KMS para 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 de KMS usada 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 AWSpara 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 acerca de la creación de claves administradas por el cliente, consulte la Creación de claves en la Guía para desarrolladores de AWS Key Management Service.

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 se activa la rotación de claves, AWS KMS rota automáticamente su clave 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 de claves 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 datos del lado del servidor con una nueva clave de KMS, sin exponer el texto no cifrado de los datos en el 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 de 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 utilizar la clave 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 acerca de la clave de KMS especificada. Este permiso está incluido en la política de claves predeterminada.
- kms:ListAliases: (opcional) muestra todos los alias de 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

Los sistemas de archivos persistentes y scratch 2 pueden cifrar automáticamente los datos en tránsito cuando se accede a ellos desde instancias de Amazon EC2 que admiten el cifrado en tránsito. También lo hacen para todas las comunicaciones entre hosts en el sistema de archivos. Para saber qué instancias de EC2 admiten el cifrado en tránsito, consulte Cifrado en tránsito en la guía del usuario de Amazon EC2.

Para obtener una lista de las Regiones de AWS en las que Amazon FSx para Lustre está disponible, consulte Disponibilidad del tipo de implementación.

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

Tiene dos opciones de conectividad entre su red privada y AWS:

- Una conexión de AWS Site-to-Site VPN. Para obtener más información, consulte ¿Qué es AWS Site-to-Site VPN?
- Una conexión de AWS Direct Connect. Para obtener más información, consulte ¿Qué es AWS Direct Connect?

Puede acceder a FSx para Lustre a través de la red para acceder a las operaciones de API publicadas por AWS 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 de API publicadas AWS, los clientes deben ser compatibles con la seguridad de la capa de transporte (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 for Lustre

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos de Amazon FSx . El IAM es un Servicio de AWS servicio que puede utilizar sin coste adicional.

Temas

- Cómo funciona Amazon FSx for Lustre con IAM
- Ejemplos de políticas basadas en identidad para Amazon for Lustre FSx
- Políticas administradas de AWS para Amazon FSx para Lustre
- Solución de problemas de identidad y acceso a Amazon FSx for Lustre
- Uso de etiquetas con Amazon FSx
- Uso de roles vinculados a servicios para Amazon FSx

Público

La forma de usar AWS Identity and Access Management (IAM) varía según la función que desempeñes:

- Usuario del servicio: solicita permisos al administrador si no se puede acceder a las características (consulte Solución de problemas de identidad y acceso a Amazon FSx for Lustre).
- Administrador del servicio: determina el acceso de los usuarios y envía las solicitudes de permiso (consulte Cómo funciona Amazon FSx for Lustre con IAM).
- Administrador de IAM: escribe las políticas para administrar el acceso (consulte Ejemplos de políticas basadas en identidad para Amazon for Lustre FSx).

Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Debe autenticarse como usuario de Usuario raíz de la cuenta de AWS IAM o asumir una función de IAM.

Puede iniciar sesión como una identidad federada con las credenciales de una fuente de identidad, como AWS IAM Identity Center (IAM Identity Center), la autenticación de inicio de sesión único o las credenciales. Google/Facebook Para obtener más información sobre el inicio de sesión, consulte Cómo iniciar sesión en la Cuenta de AWS en la Guía del usuario de AWS Sign-In .

Para el acceso programático, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte AWS Signature Version 4 para solicitudes de API en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear un Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz que tiene acceso completo a todos Servicios de AWS los recursos.

Recomendamos encarecidamente que no utilice el usuario raíz para las tareas cotidianas. Para ver las tareas que requieren credenciales de usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio empresarial, del proveedor de identidades web o al Directory Service que se accede Servicios de AWS mediante credenciales de una fuente de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, recomendamos AWS IAM Identity Center. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad con permisos específicos para una sola persona o aplicación. Recomendamos utilizar credenciales temporales en lugar de usuarios de IAM con credenciales a largo plazo. Para obtener más información, consulte Exigir a los usuarios humanos que utilicen la federación con un proveedor de identidad para acceder AWS mediante credenciales temporales en la Guía del usuario de IAM.

Un grupo de IAM especifica un conjunto de usuarios de IAM y facilita la administración de los permisos para grupos grandes de usuarios. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad con permisos específicos que proporciona credenciales temporales. Puede asumir un rol cambiando de un rol de usuario a uno de IAM (consola) o llamando a una AWS CLI operación de AWS API. Para obtener más información, consulte Métodos para asumir un rol en la Guía del usuario de IAM.

Las funciones de IAM son útiles para el acceso de usuarios federados, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon. EC2 Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Administración del acceso con políticas

AWS Para controlar el acceso, puede crear políticas y adjuntarlas a identidades o recursos. AWS Una política define los permisos cuando están asociados a una identidad o un recurso. AWS evalúa estas políticas cuando un director hace una solicitud. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre los documentos de políticas de JSON, consulte Información general de políticas de JSON en la Guía del usuario de IAM.

Mediante las políticas, los administradores especifican quién tiene acceso a qué, definiendo qué entidad principal puede realizar acciones sobre qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM crea políticas de IAM y las agrega a roles, que los usuarios pueden asumir posteriormente. Las políticas de IAM definen permisos independientemente del método que se utilice para realizar la operación.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de política de permisos JSON que asocia a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Las políticas basadas en identidad pueden ser políticas insertadas (incrustadas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener información sobre cómo elegir entre políticas administradas e insertadas, 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 políticas JSON que se asocian a un recurso. Son ejemplos 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. Debe especificar una entidad principal en una política basada en recursos.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer los permisos máximos que conceden los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM. Para obtener más información, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations .
- Políticas de control de recursos (RCPs): establece los permisos máximos disponibles para los recursos de tus cuentas. Para obtener más información, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para obtener más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona Amazon FSx for Lustre con IAM

Antes de utilizar IAM para gestionar el acceso a Amazon FSx, consulta qué funciones de IAM están disponibles para su uso con Amazon. FSx

Funciones de IAM que puedes usar con Amazon FSx for Lustre

Característica de IAM	FSx Soporte de Amazon
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No

Característica de IAM	FSx Soporte de Amazon
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
ACLs	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 visión general de cómo funcionan Amazon FSx y otros AWS servicios con la mayoría de las funciones de IAM, consulta AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en la identidad de Amazon FSx

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente 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. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de la política 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 de Amazon FSx basadas en la identidad, consulta. Ejemplos de políticas basadas en identidad para Amazon for Lustre FSx

Políticas basadas en recursos en Amazon FSx

Admite políticas basadas en recursos: no

Acciones políticas para Amazon FSx

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de FSx las acciones de Amazon, consulta Acciones definidas por Amazon FSx para Lustre en la Referencia de autorización de servicio.

Las acciones políticas en Amazon FSx usan 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 de Amazon FSx basadas en la identidad, consulta. Ejemplos de políticas basadas en identidad para Amazon for Lustre FSx

Recursos de políticas para Amazon FSx

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). En el caso de las acciones que no admiten permisos por recurso, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de los tipos de FSx recursos de Amazon y sus tipos ARNs, consulte Recursos definidos por Amazon FSx for Lustre en la Referencia de autorización de servicio. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte Acciones definidas FSx por Amazon for Lustre.

Para ver ejemplos de políticas de Amazon FSx basadas en la identidad, consulta. Ejemplos de políticas basadas en identidad para Amazon for Lustre FSx

Claves de condición de la política para Amazon FSx

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puede crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de claves de FSx estado de Amazon, consulta Claves de estado de Amazon FSx for Lustre en la Referencia de autorización de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por Amazon FSx for Lustre.

Para ver ejemplos de políticas de Amazon FSx basadas en la identidad, consulta. Ejemplos de políticas basadas en identidad para Amazon for Lustre FSx

Listas de control de acceso (ACLs) en Amazon FSx

Soporta ACLs: 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 denominados etiquetas. Puede adjuntar etiquetas a las entidades y AWS los recursos de IAM y, a continuación, diseñar políticas de ABAC para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso.

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 Definición de permisos con la autorización de 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 FSx los recursos de Amazon, consulteEtiquetar los recursos de Amazon FSx para Lustre.

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 tus FSx recursos de Amazon.

Uso de credenciales temporales con Amazon FSx

Compatibilidad con credenciales temporales: sí

Las credenciales temporales proporcionan acceso a AWS los recursos a corto plazo y se crean automáticamente cuando utilizas la federación o cambias de rol. AWS recomienda generar

credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM y Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Sesiones de acceso directo para Amazon FSx

Admite sesiones de acceso directo (FAS): sí

Las sesiones de acceso directo (FAS) utilizan los permisos del operador principal que realiza la llamada Servicio de AWS, junto con los de solicitud, Servicio de AWS para realizar solicitudes a los servicios descendentes. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Sesiones de acceso directo.

Funciones 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 Crear 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 FSx funcionalidad de Amazon. Edita las funciones de servicio solo cuando Amazon te FSx dé instrucciones para hacerlo.

Funciones vinculadas a servicios para Amazon FSx

Compatible con roles vinculados al servicio: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información sobre la creación y la gestión de funciones FSx vinculadas a los servicios de Amazon, consulte. Uso de roles vinculados a servicios para Amazon FSx

Ejemplos de políticas basadas en identidad para Amazon for Lustre FSx

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar FSx los recursos de Amazon. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por Amazon FSx, incluido el ARNs formato de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de Amazon FSx for Lustre en la Referencia de autorización de servicio.

Temas

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear, acceder o eliminar FSx los recursos de Amazon de tu cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos

como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.

- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de la FSx consola de Amazon

Para acceder a la consola Amazon FSx for Lustre, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirte enumerar y ver detalles sobre los FSx recursos de Amazon que tienes Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la AWS API AWS CLI o a la misma. En su lugar, permita el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la FSx consola de Amazon, adjunta también la política `AmazonFSxConsoleReadOnlyAccess` AWS gestionada a las entidades. Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Puedes ver esta `AmazonFSxConsoleReadOnlyAccess` y otras políticas de servicios FSx gestionados de Amazon enPolíticas administradas de AWS para Amazon FSx para Lustre.

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

Políticas administradas de AWS para Amazon FSx para Lustre

Una política administrada de AWS es una política independiente que AWS crea y administra. Las políticas administradas de AWS se diseñan para ofrecer permisos para muchos casos de uso comunes, por lo que puede empezar a asignar permisos a los usuarios, grupos y roles.

Considere que es posible que las políticas administradas de AWS no concedan permisos de privilegio mínimo para los casos de uso concretos, ya que están disponibles para que las utilicen todos los clientes de AWS. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puede cambiar los permisos definidos en las políticas administradas de AWS. Si AWS actualiza los permisos definidos en una política administrada de AWS, la actualización afecta a todas las identidades de entidades principales (usuarios, grupos y roles) a las que está adjunta la política. Lo más probable es que AWS actualice una política administrada de AWS cuando se lance un nuevo Servicio de AWS o las operaciones de la API nuevas estén disponibles para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

AmazonFSxServiceRolePolicy (Política de rol de servicio de Amazon FSx)

Permite a Amazon FSx administrar recursos de AWS en su nombre. Consulte Uso de roles vinculados a servicios para Amazon FSx para obtener más información.

Política administrada por AWS: AmazonFSxDeleteServiceLinkedRoleAccess

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 en `iam` que permiten a Amazon FSx ver, eliminar y ver el estado de eliminación de las funciones vinculadas al servicio FSx para el acceso a Amazon S3.

Para ver los permisos de esta política, consulte AmazonFSxDeleteServiceLinkedRoleAccess en la guía de referencia de políticas administradas por AWS.

Política administrada por AWS: AmazonFSxFullAccess

Puede asociar AmazonFSxFullAccess a las entidades IAM. Amazon FSx también asocia esta política a un rol de servicio que permite a Amazon FSx realizar acciones en su nombre.

Proporciona acceso completo a Amazon FSx y acceso a los servicios AWS relacionados.

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 que las entidades principales vean información sobre los directorios de Directory Service.
- `ec2`
  - Permite que las entidades principales creen etiquetas en las condiciones especificadas.
  - Para proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una nube privada virtual (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 administrar los recursos de AWS en nombre del usuario.
- `firehose`: permite que las entidades principales escriban los registros en Amazon Data Firehose. Esto es necesario para que los usuarios puedan supervisar el acceso al sistema de archivos de FSx para Windows File Server al enviar los registros de acceso de auditoría a Firehose.
- `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 monitorear el acceso al sistema de archivos de FSx para Windows File Server al enviar los registros de acceso de auditoría a los registros de CloudWatch.

Para ver los permisos de esta política, consulte AmazonFSxFullAccess en la guía de referencia de políticas administradas por AWS.

Política administrada por AWS: AmazonFSxConsoleFullAccess

Puede adjuntar la política `AmazonFSxConsoleFullAccess` a las identidades de IAM.

Esta política concede permisos administrativos que brindan acceso completo a Amazon FSx y a los servicios relacionados de AWS a través de la Consola de administración de AWS.

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 que las entidades principales vean las alarmas y métricas de CloudWatch en la consola de administración de Amazon FSx.
- `ds`: permite que las entidades principales creen listas de información sobre un directorio de Directory Service.
- `ec2`
  - Permite que las entidades principales creen etiquetas en tablas de enrutamiento, interfaces de red de listas, tablas de enrutamiento, grupos de seguridad, subredes y la VPC asociada a un sistema de archivos de Amazon FSx.
  - Permite a las entidades principales que proporcionen una validación mejorada de grupos de seguridad de todos los que se pueden usar con una VPC.
  - Permite a los directores ver las interfaces de red elásticas asociadas a un sistema de archivos Amazon FSx.
- `kms`: permite que las entidades principales creen listas de los alias para las claves de 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, consulte AmazonFSxConsoleFullAccess en la guía de referencia de políticas administradas por AWS.

Política administrada por AWS: AmazonFSxConsoleReadOnlyAccess

Puede adjuntar la política `AmazonFSxConsoleReadOnlyAccess` a las identidades de IAM.

Esta política concede permisos de solo lectura a Amazon FSx y a los servicios relacionados de AWS para que los usuarios puedan ver información sobre estos servicios en la Consola de administración de AWS.

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 que las entidades principales vean las alarmas y métricas de CloudWatch en la consola de administración de Amazon FSx.
- `ds`: permite que las entidades principales vean información sobre un directorio de Directory Service en la consola de administración de Amazon FSx.
- `ec2`
  - Permite que las entidades principales vean 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.
  - Permite a las entidades principales que proporcionen una validación mejorada de grupos de seguridad de todos los que se pueden usar con una VPC.
  - Permite a los directores ver las interfaces de red elásticas asociadas a un sistema de archivos Amazon FSx.
- `kms`: permite que las entidades principales vean los alias de las claves de AWS Key Management Service en la consola de administración de Amazon FSx.
- `log`: permite que las entidades principales describan los grupos de registro de los Registros de Amazon CloudWatch 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 que las entidades principales describan 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 AmazonFSxConsoleReadOnlyAccess en la guía de referencia de políticas administradas por AWS.

Política administrada de AWS: AmazonFSxReadOnlyAccess

Puede adjuntar la política `AmazonFSxReadOnlyAccess` a las identidades de IAM.

- `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`: para 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 AmazonFSxReadOnlyAccess en la guía de referencia de políticas administradas por AWS.

Las actualizaciones de Amazon FSx a las políticas administradas de AWS

Es posible consultar los detalles sobre las actualizaciones de las políticas administradas de AWS para Amazon FSx desde que este servicio comenzó a hacer un 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
AmazonFSxServiceRolePolicy: actualización de una política existente	Amazon FSx agregó un nuevo permiso de `ec2:AssignIpv6Addresses` que permite a las entidades principales asignar direcciones IPv6 a las interfaces de red del cliente que tienen	22 de julio de 2025

Cambio	Descripción	Fecha
	una etiqueta `AmazonFSx.FileSystemId` .	
AmazonFSxServiceRolePolicy: actualización de una política existente	Amazon FSx agregó un nuevo permiso de `ec2:UnassignIpv6Addresses` que permite a las entidades principales anular la asignación de direcciones IPv6 de las interfaces de red de los clientes que tienen una etiqueta `AmazonFSx.FileSystemId` .	22 de julio de 2025
AmazonFSxConsoleFullAccess: actualización de una política existente	Amazon FSx agregó un nuevo permiso de `fsx:CreateAndAttachS3AccessPoint` que permite a las entidades principales crear un punto de acceso S3 y adjuntarlo a un volumen FSx.	25 de junio de 2025
AmazonFSxConsoleFullAccess: actualización de una política existente	Amazon FSx agregó un nuevo permiso de `fsx:DescribeS3AccessPointAttachments` que permite a las entidades principales enumerar todos los puntos de acceso S3 de forma Cuenta de AWS a Región de AWS.	25 de junio de 2025

Cambio	Descripción	Fecha
AmazonFSxConsoleFullAccess: actualización de una política existente	Amazon FSx agregó un nuevo permiso de `fsx:DetachAndDeleteS3AccessPoint` que permite a las entidades principales eliminar un punto de acceso S3.	25 de junio de 2025
AmazonFSxFullAccess: actualización de una política existente	Amazon FSx agregó un nuevo permiso de `fsx:CreateAndAttachS3AccessPoint` que permite a las entidades principales crear un punto de acceso S3 y adjuntarlo a un volumen FSx.	25 de junio de 2025
AmazonFSxFullAccess: actualización de una política existente	Amazon FSx agregó un nuevo permiso de `fsx:DescribeS3AccessPointAttachments` que permite a las entidades principales enumerar todos los puntos de acceso S3 de forma Cuenta de AWS a Región de AWS.	25 de junio de 2025
AmazonFSxFullAccess: actualización de una política existente	Amazon FSx agregó un nuevo permiso de `fsx:DetachAndDeleteS3AccessPoint` que permite a las entidades principales eliminar un punto de acceso S3.	25 de junio de 2025

Cambio	Descripción	Fecha
AmazonFSxConsoleReadOnlyAccess: actualización de una política existente	Amazon FSx agregó un nuevo permiso de `ec2:DescribeNetworkInterfaces` que permite a las entidades principales ver las interfaces de red elásticas asociadas a su sistema de archivos.	25 de febrero de 2025
AmazonFSxConsoleFullAccess: actualización de una política existente	Amazon FSx agregó un nuevo permiso de `ec2:DescribeNetworkInterfaces` que permite a las entidades principales ver las interfaces de red elásticas asociadas a su sistema de archivos.	7 de febrero de 2025
AmazonFSxServiceRolePolicy: actualización de una política existente	Amazon FSx agregó un nuevo permiso, `ec2:GetSecurityGroupsForVpc`, que permite que las entidades principales proporcionen 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
AmazonFSxReadOnlyAccess: actualización a una política existente	Amazon FSx agregó un nuevo permiso, `ec2:GetSecurityGroupsForVpc`, que permite que las entidades principales proporcionen 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
AmazonFSxConsoleReadOnlyAccess: actualización de una política existente	Amazon FSx agregó un nuevo permiso, `ec2:GetSecurityGroupsForVpc`, que permite que las entidades principales proporcionen 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
AmazonFSxFullAccess: actualización de una política existente	Amazon FSx agregó un nuevo permiso, `ec2:GetSecurityGroupsForVpc`, que permite que las entidades principales proporcionen 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
AmazonFSxConsoleFullAccess: actualización de una política existente	Amazon FSx agregó un nuevo permiso, `ec2:GetSecurityGroupsForVpc`, que permite que las entidades principales proporcionen 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
AmazonFSxFullAccess: 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 sistemas de archivos de FSx para OpenZFS.	20 de diciembre de 2023
AmazonFSxConsoleFullAccess: 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 sistemas de archivos de FSx para OpenZFS.	20 de diciembre de 2023
AmazonFSxFullAccess: actualización de una política existente	Amazon FSx agregó un nuevo permiso para permitir a los usuarios realizar la replicación de volúmenes bajo demanda de FSx para sistemas de archivos de OpenZFS.	26 de noviembre de 2023

Cambio	Descripción	Fecha
AmazonFSxConsoleFullAccess: actualización de una política existente	Amazon FSx agregó un nuevo permiso para permitir a los usuarios realizar la replicación de volúmenes bajo demanda de FSx para sistemas de archivos de OpenZFS.	26 de noviembre de 2023
AmazonFSxFullAccess: actualización de una política existente	Amazon FSx agregó nuevos permisos para que los usuarios puedan ver, activar y desactivar la compatibilidad de VPC compartida de FSx para sistemas de archivos Multi-AZ de ONTAP.	14 de noviembre de 2023
AmazonFSxConsoleFullAccess: actualización de una política existente	Amazon FSx agregó nuevos permisos para que los usuarios puedan ver, activar y desactivar la compatibilidad de VPC compartida de FSx para sistemas de archivos Multi-AZ de ONTAP.	14 de noviembre de 2023
AmazonFSxFullAccess: 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

Cambio	Descripción	Fecha
Política administrada por AWS: AmazonFSxServiceRolePolicy: actualización de una política existente	Amazon FSx modificó el permiso de `cloudwatch:PutMetricData` existente para que Amazon FSx publique las métricas de CloudWatch en el espacio de nombres de `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
AmazonFSxConsoleFullAccess: 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
AmazonFSxConsoleReadOnlyAccess: actualización de 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

Cambio	Descripción	Fecha
AmazonFSxConsoleFullAccess: actualización de 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
AmazonFSxReadOnlyAccess: política de seguimiento iniciada	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
AmazonFSxDeleteServiceLinkedRoleAccess: política de seguimiento iniciada	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
AmazonFSxServiceRolePolicy: actualización de una política existente	Amazon FSx añadió permisos nuevos para que Amazon FSx administre las configuraciones de red para los sistemas de archivos de Amazon FSx para NetApp ONTAP.	2 de septiembre de 2021

Cambio	Descripción	Fecha
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
AmazonFSxConsoleFullAccess: actualización de una política existente	Amazon FSx añadió permisos nuevos que permiten que Amazon FSx cree los sistemas de archivos Multi-AZ Amazon FSx para NetApp ONTAP.	2 de septiembre de 2021
AmazonFSxConsoleFullAccess: 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
AmazonFSxServiceRolePolicy: actualización de una política existente	Amazon FSx añadió permisos nuevos para permitir a Amazon FSx describir y escribir en los flujos de registros de los registros de CloudWatch. Esto es necesario para que los usuarios puedan ver los registros de auditoría de acceso a los archivos de los sistemas de archivos de FSx para Windows File Server mediante los registros de CloudWatch.	8 de junio de 2021
AmazonFSxServiceRolePolicy: actualización de una política existente	Amazon FSx agregó nuevos permisos para permitir a Amazon FSx describir y escribir en los flujos de entrega de Amazon Data Firehose. Esto es necesario para que los usuarios puedan ver los registros de auditoría de acceso de un sistema de archivos de FSx para Windows File Server mediante Amazon Data Firehose.	8 de junio de 2021

Cambio	Descripción	Fecha
AmazonFSxFullAccess: actualización de una política existente	Amazon FSx añadió nuevos permisos para permitir a las entidades principales describir y crear grupos de registros de los registros de CloudWatch, registrar flujos y escribir eventos en flujos de registro. Esto es necesario para que las entidades principales puedan ver los registros de auditoría de acceso a los archivos de los sistemas de archivos de FSx para Windows File Server mediante los registros de CloudWatch.	8 de junio de 2021
AmazonFSxFullAccess: actualización de una política existente	Amazon FSx agregó nuevos permisos para permitir a las entidades principales describir y escribir registros en Amazon Data Firehose. Esto es necesario para que los usuarios puedan ver los registros de auditoría de acceso de un sistema de archivos de FSx para Windows File Server mediante Amazon Data Firehose.	8 de junio de 2021

Cambio	Descripción	Fecha
AmazonFSxConsoleFullAccess: actualización de una política existente	Amazon FSx añadió nuevos permisos para que las entidades principales puedan describir los grupos de registros de los registros de Amazon CloudWatch asociados a la cuenta que realiza la solicitud. Esto es necesario para que las entidades principales puedan elegir un grupo de registro de los registros de CloudWatch existente al configurar la auditoría de acceso a los archivos para un sistema de archivos de FSx para Windows File Server.	8 de junio de 2021
AmazonFSxConsoleFullAccess: actualización de una política existente	Amazon FSx agregó nuevos permisos para que las entidades principales puedan 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 elegir un flujo de entrega existente de Firehose al configurar la auditoría de acceso a los archivos para un sistema de archivos de FSx para Windows File Server.	8 de junio de 2021

Cambio	Descripción	Fecha
AmazonFSxConsoleReadOnlyAccess: actualización de una política existente	Amazon FSx añadió nuevos permisos para que las entidades principales puedan describir los grupos de registros de los registros de Amazon CloudWatch 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.	8 de junio de 2021
AmazonFSxConsoleReadOnlyAccess: actualización de una política existente	Amazon FSx agregó nuevos permisos para que las entidades principales puedan 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.	8 de junio de 2021

Cambio	Descripción	Fecha
Amazon FSx inició un seguimiento de los cambios	Amazon FSx inició el seguimiento de los cambios en las políticas administradas de AWS.	8 de junio de 2021

Solución de problemas de identidad y acceso a Amazon FSx for Lustre

Utiliza la siguiente información para ayudarte a diagnosticar y solucionar los problemas habituales que puedes encontrar al trabajar con Amazon FSx e IAM.

Temas

- No estoy autorizado a realizar ninguna acción en Amazon FSx
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis FSx recursos de Amazon

No estoy autorizado a realizar ninguna 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 necesitas ayuda, ponte en contacto con tu AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibes un error que indica que no estás autorizado a realizar la `iam:PassRole` acción, debes actualizar tus políticas para que puedas transferir una función a Amazon FSx.

Algunas te Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada al servicio. Para ello, debe tener permisos para transferir la función al servicio.

El siguiente ejemplo de 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 otorguen un rol de servicio. Mary no tiene permisos para transferir la función 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 AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis FSx recursos de Amazon

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admiten políticas basadas en recursos o listas de control de acceso (ACLs), puedes usar esas políticas para permitir que las personas accedan a tus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si Amazon FSx admite estas funciones, consultaCómo funciona Amazon FSx for Lustre con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en la Guía del usuario de IAM.

- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (federación de identidades) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Uso de etiquetas con Amazon FSx

Puedes usar etiquetas para controlar el acceso a FSx los recursos de Amazon e implementar el control de acceso basado en atributos (ABAC). Para aplicar etiquetas a FSx los recursos de Amazon durante la creación, los usuarios deben tener ciertos permisos AWS Identity and Access Management (de IAM).

Conceder permisos para etiquetar recursos durante la creación

Con algunas acciones de la API de Amazon FSx for Lustre que crean recursos, puedes 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, consulta ¿Para qué sirve ABAC? 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`.

El siguiente ejemplo de política permite a los usuarios crear sistemas de archivos y aplicarles etiquetas durante la creación de un sistema específico Cuenta de AWS.

```
{
  "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 sobre el etiquetado de FSx los recursos de Amazon, consulte[Etiquetar los recursos de Amazon FSx para Lustre]. Para obtener más información sobre el uso de etiquetas

para controlar el acceso a los recursos de Amazon FSx for Lustre, consulteUso de etiquetas para controlar el acceso a tus FSx recursos de Amazon.

Uso de etiquetas para controlar el acceso a tus FSx recursos de Amazon

Para controlar el acceso a FSx los recursos y acciones de Amazon, puedes usar políticas de IAM basadas en etiquetas. Puede proporcionar este control de dos maneras:

- Puedes controlar el acceso a FSx los recursos de Amazon en función de las etiquetas de esos recursos.
- Puede controlar qué etiquetas se pueden pasar en una condición de solicitud IAM.

Para obtener información sobre cómo utilizar las etiquetas para controlar el acceso a AWS los recursos, consulte Controlar el acceso mediante etiquetas en la Guía del usuario de IAM. Para obtener más información sobre cómo etiquetar FSx los recursos de Amazon en el momento de la creación, consulteConceder permisos para etiquetar recursos durante la creación. Para obtener más información acerca del etiquetado de recursos, consulte Etiquetar los recursos de Amazon FSx para Lustre.

Control del acceso a un recurso en función de las etiquetas

Para controlar qué acciones puede realizar un usuario o un rol en un FSx recurso de Amazon, puedes usar 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`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333: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`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateFileSystemFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateFileSystemFromBackup"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333: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`. En el FSx caso de los sistemas de archivos de Lustre, los usuarios necesitan el `fsx:CreateBackup` privilegio de crear la copia de seguridad final.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteFileSystem"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333: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`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateDataRepositoryTask"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateDataRepositoryTask",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:task/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Uso de roles vinculados a servicios para Amazon FSx

Amazon FSx usa roles AWS Identity and Access Management vinculados a servicios (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Amazon. FSx Amazon predefine las funciones vinculadas al servicio FSx e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en tu nombre.

Un rol vinculado a un servicio facilita la configuración de Amazon FSx porque no tienes que añadir manualmente los permisos necesarios. Amazon FSx define los permisos de sus funciones vinculadas a servicios y, a menos que se defina lo contrario, solo Amazon FSx puede asumir sus funciones. 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. Esto protege tus FSx recursos de Amazon porque no puedes eliminar inadvertidamente el permiso de acceso a los recursos.

Para obtener información sobre otros servicios que admiten funciones vinculadas a servicios, consulte los AWS servicios que funcionan con IAM y busque los servicios con la palabra Sí en la columna Funciones vinculadas a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del 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 tu 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 de Amazon FSx for 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 FSx a Amazon completar las siguientes acciones administrativas en nombre del usuario en todos los AWS recursos aplicables:

Para obtener actualizaciones de esta política, consulte AmazonFSxServiceRolePolicy (Política de rol de servicio de Amazon FSx).

> **Note**
>
> AWSServiceRoleForAmazonFSx Lo utilizan todos los tipos de sistemas de FSx archivos de Amazon; algunos de los permisos enumerados no son aplicables a FSx Lustre.

- `ds`— Permite FSx a Amazon ver, autorizar y desautorizar las aplicaciones de su Directory Service directorio.
- `ec2`— Permite FSx a Amazon hacer lo siguiente:
  - Vea, cree y desasocie las interfaces de red asociadas a un sistema de FSx archivos de Amazon.
  - Vea una o más direcciones IP elásticas asociadas a un sistema de FSx archivos de Amazon.
  - Vea Amazon VPCs, los grupos de seguridad y las subredes asociados a un sistema de FSx archivos de Amazon.
  - Asigne IPv6 direcciones a las interfaces de red de los clientes que tengan una `AmazonFSx.FileSystemId` etiqueta.
  - Anule la asignación de IPv6 direcciones de las interfaces de red de los clientes que tengan una `AmazonFSx.FileSystemId` etiqueta.
  - Para proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una nube privada virtual (VPC).
  - Cree un permiso para que un usuario AWS autorizado realice determinadas operaciones en una interfaz de red.
- `cloudwatch`— Permite FSx a Amazon publicar puntos de datos métricos CloudWatch en el espacio de FSx nombres AWS/.
- `route53`— Permite FSx a Amazon asociar una Amazon VPC a una zona alojada privada.
- `logs`— Permite FSx a Amazon 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 FSx de archivos del servidor de archivos de Windows a un flujo de CloudWatch registros.
- `firehose`— Permite FSx a Amazon 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 para Windows File Server en una transmisión de entrega de Amazon Data Firehose.

JSON

```
{
    "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 Las actualizaciones de Amazon FSx a las políticas administradas de 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.

AWSServiceRoleForFSxDetalles de los permisos de S3Access

En efectoAWSServiceRoleForFSxS3Access_*file-system-id*, la política de permisos de roles permite FSx a Amazon realizar las siguientes acciones en un bucket de Amazon S3 que aloja el repositorio de datos de un sistema de archivos de 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.

Crear un rol vinculado a un servicio para Amazon FSx

No necesita crear manualmente un rol vinculado a servicios. Cuando creas un sistema de archivos en la Consola de administración de AWS AWS CLI, la o la AWS API, Amazon FSx crea el rol vinculado al servicio por ti.

> **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. Cuando creas un sistema de archivos, Amazon vuelve a FSx crear el rol vinculado al servicio para ti.

Edición de un rol vinculado a un servicio para Amazon FSx

Amazon FSx no te 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.

Eliminar 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 FSx servicio de Amazon utiliza el rol cuando intentas eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para 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 obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones compatibles con los roles vinculados a FSx los servicios de Amazon

Amazon FSx admite el uso de funciones vinculadas al servicio en todas las regiones en las que el servicio esté disponible. 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 usa grupos de seguridad de VPC para controlar el tráfico de red de los clientes de Lustre.

Grupos de seguridad compatibles con EFA

Si va a crear un FSx para Lustre compatible con EFA, primero debe crear un grupo de seguridad compatible con EFA y especificarlo como grupo de seguridad para el sistema de archivos. Un EFA requiere un grupo de seguridad que permita todo el tráfico entrante y saliente hacia y desde el propio grupo de seguridad y el grupo de seguridad de los clientes si los clientes residen en otro grupo de seguridad. Para más información, consulte Paso 1: preparar un grupo de seguridad compatibles con EFA en la Guía del usuario de Amazon EC2.

Controlar el acceso mediante reglas de entrada y salida

Para usar un grupo de seguridad para controlar el acceso al sistema de archivos de Amazon FSx y clientes de Lustre, agregue las reglas de entrada para controlar el tráfico entrante y las reglas de salida para controlar el tráfico saliente del sistema de archivos y clientes de 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.

Cómo crear un grupo de seguridad para el sistema de archivos de Amazon FSx

1. Abra la consola de 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, agregue reglas de entrada al grupo de seguridad que acaba de crear para permitir el tráfico de Lustre entre los servidores de archivos de 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 los servidores de archivos de FSx para Lustre
Regla TCP personalizada	TCP	988	Elija Personalizar e introduzca los identificadores de grupo de seguridad de los grupos de seguridad asociados a los clientes de Lustre	Permite el tráfico de Lustre entre servidores de archivos de FSx para Lustre y clientes de Lustre

Tipo	Protocolo	Rango de puertos	Origen	Descripción
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 los servidores de archivos de FSx para Lustre
Regla TCP personalizada	TCP	1018-1023	Elija Personalizar e introduzca los identificadores de grupo de seguridad de los grupos de seguridad asociados a los clientes de Lustre	Permite el tráfico de Lustre entre servidores de archivos de FSx para Lustre y clientes de 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 de FSx para Lustre y clientes de Lustre y entre servidores de archivos de 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	Permita el tráfico de Lustre entre los servidores de archivos de FSx para Lustre
Regla TCP personalizada	TCP	988	Elija Personalizar e introduzca los identificadores de grupo de seguridad del grupo de seguridad asociado a los clientes de Lustre	Permita el tráfico de Lustre entre servidores de archivos de FSx para Lustre y clientes de 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 los servidores de archivos de FSx para Lustre

Tipo	Protocolo	Rango de puertos	Origen	Descripción
Regla TCP personalizada	TCP	1018-1023	Elija Personalizar e introduzca los identificadores de grupo de seguridad de los grupos de seguridad asociados a los clientes de Lustre	Permite el tráfico de Lustre entre servidores de archivos de FSx para Lustre y clientes de 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 el sistema de archivos para ver sus detalles.
3. En la pestaña Red y seguridad, haga clic en el enlace de la consola de Amazon EC2 en Interfaces de red para ver todas las interfaces de red del sistema de archivos.
4. Para cada interfaz de red, elija Acciones y, luego, seleccione Cambiar grupos de seguridad.
5. En la caja de diálogo Cambiar grupos de seguridad, elija los grupos de seguridad que desea asociar a las interfaces de red.
6. Seleccione Save.

Reglas del grupo de seguridad de VPC del cliente de Lustre

Puede usar los grupos de seguridad de la VPC para controlar el acceso a los clientes de Lustre agregando reglas de entrada para controlar el tráfico entrante y reglas de salida para controlar el tráfico saliente de los clientes de Lustre. Procure tener las reglas de tráfico de red adecuadas en el grupo de seguridad para garantizar que el tráfico de Lustre pueda fluir entre los clientes de Lustre y los sistemas de archivos de Amazon FSx.

Agregue las siguientes reglas de entrada a los grupos de seguridad aplicados a los clientes de Lustre.

Tipo	Protocolo	Rango de puertos	Origen	Descripción
Regla TCP personalizada	TCP	988	Elegir Personalizado e introducir los identificadores de grupo de seguridad de los grupos de seguridad que se aplican a los clientes de Lustre	Permite el tráfico de Lustre entre 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 de FSx para Lustre y clientes de Lustre
Regla TCP personalizada	TCP	1018-1023	Elegir Personalizado e introducir los identificadores de grupo de seguridad de los grupos de seguridad que se aplican a los clientes de Lustre	Permite el tráfico de Lustre entre 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 de FSx para Lustre y clientes de Lustre

Agregue las siguientes reglas de salida a los grupos de seguridad aplicados a los clientes de Lustre.

Tipo	Protocolo	Rango de puertos	Origen	Descripción
Regla TCP personalizada	TCP	988	Elegir Personalizado e introducir los identificadores de grupo de seguridad de los grupos de seguridad que se aplican a los clientes de Lustre	Permite el tráfico de Lustre entre clientes de Lustre
Regla TCP personalizada	TCP	988	Elija Personalizado e introduzca los ID de los grupos de seguridad asociados a sus sistemas de	Permita el tráfico de Lustre entre servidores de archivos de FSx para Lustre y clientes de Lustre

Tipo	Protocolo	Rango de puertos	Origen	Descripción
			archivo FSx para Lustre	
Regla TCP personalizada	TCP	1018-1023	Elegir Personalizado e introducir los identificadores de grupo de seguridad de los grupos de seguridad que se aplican a los clientes de Lustre	Permite el tráfico de Lustre entre 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 archivo FSx para Lustre	Permite el tráfico de Lustre entre servidores de archivos de FSx para Lustre y clientes de 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 incluidos por programa de conformidad y escoja el programa de conformidad que le interese. Para obtener información general, consulte Programas de conformidad de AWS.

Puedes 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 confidencialidad de los datos, los objetivos de conformidad de su empresa, así como de la legislación y los reglamentos aplicables. Para obtener más información sobre la responsabilidad de conformidad al usar Servicios de AWS, consulte la Documentación de seguridad de AWS.

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 VPC de 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 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 de 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 de 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 el emparejamiento de VPC

Puede conectar una VPC a otra con puntos de conexión de VPC de interfaz usando el emparejamiento de VPC. El emparejamiento 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 emparejadas permanece en la red de AWS y no pasa por la red pública de Internet. Una vez que las VPC están emparejadas, 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 la 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 Visualización y actualización de la compatibilidad de DNS para su VPC en la Guía del usuario de Amazon VPC.

Excepto 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 principal 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.

Service Quotas para Amazon FSx para Lustre

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.

Recurso	Predeterminado/a	Descripción
Sistemas de archivos Persistent 1 de Lustre	100	El número máximo de sistemas de archivos de Amazon FSx para Lustre Persistent 1 que puede crear en esta cuenta.
Sistemas de archivos Persistent 2 de Lustre	100	El número máximo de sistemas de archivos de Amazon FSx para Lustre Persistent 2 que puede crear en esta cuenta.
Capacidad de almacenamiento en HDD de tipo Persistent de Lustre (por sistema de archivos)	102 000	La cantidad máxima de capacidad de almacenamiento HDD (en GiB) que puede configurar para un sistema de archivos persistente Amazon FSx para Lustre.

Recurso	Predeterminado/a	Descripción
Capacidad de almacenamiento de archivos de tipo Persistent 1 de Lustre	100 800	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 de tipo Persistent 2 de Lustre	100 800	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 Scratch de Lustre	100	La cantidad máxima de sistemas de archivos Scratch de Amazon FSx para Lustre que puede crear en esta cuenta.
Capacidad de almacenamiento de Scratch de Lustre	100 800	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.
Capacidad de rendimiento persistente de Intelligent-Tiering de Lustre	100000	La capacidad de rendimiento (en MBps) total permitida para todos los sistemas de archivos Intelligent-Tiering de Amazon FSx para Lustre esta cuenta.

Recurso	Predeterminado/a	Descripción
Capacidad de almacenamiento en caché de lectura en SSD persistente con Intelligent-Tiering de Lustre	100 800	La cantidad máxima de capacidad de caché de lectura SSD aprovisionado que puede configurar para todos los sistemas de archivos Amazon FSx para Lustre Intelligent-Tiering en esta cuenta.
LustreCopias de seguridad de	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.

Cómo solicitar un aumento de cuota

1. Abra la consola de Service Quotas.
2. En el panel de navegación, elija Servicios de AWS.
3. Elija Lustre.
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 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.

Recurso	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
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.

Solución de problemas de Amazon FSx para Lustre

En esta sección, se describen varios escenarios de solución de problemas y soluciones para 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 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 compatible con EFA debido a un grupo de seguridad mal configurado

Se produce un error al crear un sistema de archivos compatible con EFA de FSx para Lustre y aparece el siguiente mensaje de error:

```
Insufficient security group permissions to create an EFA-enabled file system.
Update security group to allow all internal inbound and outbound traffic.
```

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 Grupos de seguridad compatibles con EFA. Un EFA requiere un grupo de seguridad que permita todo el tráfico entrante y saliente hacia y desde el propio grupo de seguridad y el grupo de seguridad de los clientes si los clientes residen en otro grupo de seguridad.

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 de 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 debido a errores de capacidad insuficiente

Es posible que reciba un error de capacidad insuficiente al intentar crear un nuevo sistema de archivos, actualizar la capacidad de almacenamiento o modificar la capacidad de rendimiento.

Causa

Este error se produce cuando FSx para Lustre en ese momento no tiene capacidad de hardware disponible en la zona de disponibilidad solicitada para llevar a cabo la solicitud.

Solución

Para resolver este problema, pruebe lo siguiente:

- Espere unos minutos y después intente la solicitud de nuevo, ya que la disponibilidad de capacidad cambia frecuentemente.
- Vuelva a intentar la solicitud en una zona de disponibilidad diferente.
- Intente realizar la operación con un tamaño de almacenamiento más pequeño o un nivel de rendimiento inferior.

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 obtener 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 de `mountname` a partir de la respuesta del comando describe-file-systemsAWS 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 obtener 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 obtener 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 (DRA)

Al crear una asociación de repositorios de datos (DRA) desde la consola de Amazon FSx o mediante el comando CLI `create-data-repository-association` (la acción de API equivalente es CreateDataRepositoryAssociation), 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) usando la consola Amazon FSx o el comando CLI `create-file-system` (la acción de API equivalente es CreateFileSystem).

Acción que se debe ejecutar

Si el sistema de archivos de 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 de 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.

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 de 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 obtener más información, consulte Agregar permisos para utilizar repositorios de datos en Amazon S3.
2. Mediante la CLI o la API de Amazon FSx, actualice el sistema de archivos `AutoImportPolicy` con el comando CLI `update-file-system` (la acción de API equivalente es UpdateFileSystem), 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 su 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 CLI `update-file-system` (la acción de API equivalente es UpdateFileSystem), 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 obtener 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 los OST no están llenos, ajuste el tamaño del búfer de páginas sin procesar del cliente haciendo 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 de 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 de 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 métrica de Amazon CloudWatch, `OST FreeDataStorageCapacity`, compruebe `Minimum`. 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

Amazon FSx para Lustre admite el acceso desde contenedores que se ejecutan en Amazon EKS mediante el controlador de CSI de código abierto de FSx para Lustre. Para obtener más información sobre la implementación, consulte Use el almacenamiento de Amazon FSx para Lustre en la Guía del usuario de Amazon EKS.

Si tiene problemas con el controlador CSI de FSx para Lustre para contenedores que se ejecutan en Amazon EKS, consulte Solución de problemas con el controlador CSI (problemas comunes) que está 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.

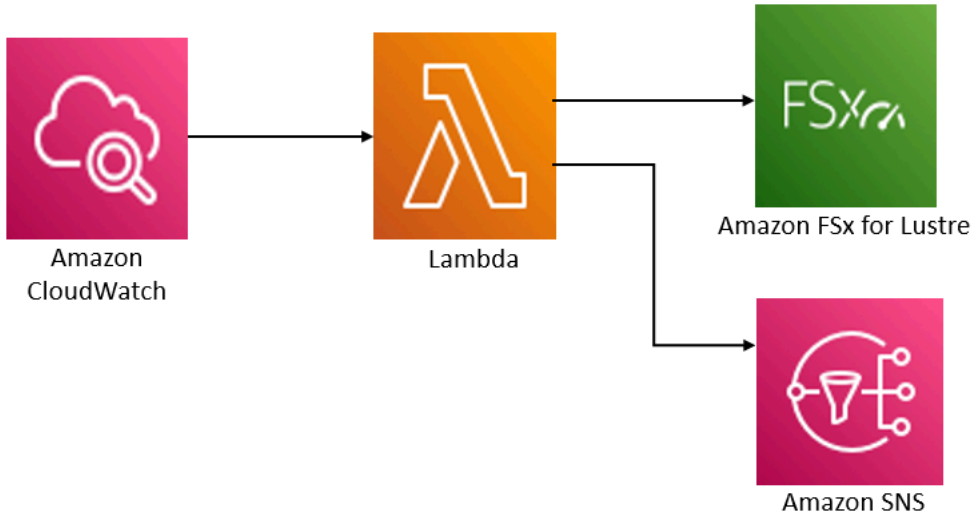
La solución despliega automáticamente todos los componentes necesarios y tiene en cuenta los siguientes parámetros:

- 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 Programar expresiones para reglas en la Guía del usuario de Amazon CloudWatch.

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 plantilla CloudFormation implementa un evento de CloudWatch, una función de 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 evento de CloudWatch se ejecuta según una programación que usted defina como 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.

CloudFormationPlantilla de

Esta solución utiliza 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 plantilla CloudFormation fsx-scheduled-backup.template.

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 plantilla CloudFormation fsx-scheduled-backup.template. Para obtener más información sobre la creación de una pila de 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 sobre Regiones de AWS y puntos de conexión en la Referencia general de AWS.

2. En Parámetros, revise los parámetros de la plantilla y modifíquelos para adaptarlos a las necesidades del sistema de archivos. Esta solución utiliza los siguientes valores predeterminados.

Parámetro	Predeterminado/a	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 evento de CloudWatch, que desencadena una nueva copia de seguridad y elimina 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/a	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 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 de Amazon FSx para Lustre en el JSON de entrada para el evento de CloudWatch. 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 CloudFormation.

```
{
 "start-backup": "true",
 "purge-backups": "true",
 "filesystem-id": "${FileSystemId}",
 "notify_on_success": "${SuccessNotification}"
```

```
}
```

Para programar copias de seguridad para un sistema de archivos de Amazon FSx para Lustre adicional, cree otra regla de eventos de CloudWatch. 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 adicionales de los eventos de CloudWatch que cree manualmente no forman parte de la pila CloudFormation de la solución de copias de seguridad programada personalizada de Amazon FSx para Lustre. Por lo tanto, no se eliminan si se elimina la pila.

Historial del documento

- Versión de la API: 2018-03-01
- Última actualización de la documentación: 30 de septiembre de 2025

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 ha agregado compatibilidad adicional en Región de AWS para el tipo de implementación Persistent 2	Los sistemas de archivos de tipo Persistent 2 en SSD de FSx para Lustre ya están disponibles en la zona en las instalaciones del Oeste de EE. UU. (Phoenix). Para obtener más información, consulte la disponibilidad de tipos de implementaciones.	30 de septiembre de 2025
Lustre Se agregó compatibilidad del cliente con Ubuntu 24 Kernel 6.14.0	El cliente FSx para Lustre ahora es compatible con instancias de Amazon EC2 que ejecutan Ubuntu 24.04 Kernel 6.14.0. Para obtener más información, consulte Instalación del cliente Lustre.	24 de septiembre de 2025
Se ha agregado compatibilidad del cliente Lustre con Kernel 6.12 de Amazon Linux 2023	El cliente FSx para Lustre ahora es compatible con instancias de Amazon EC2 que ejecutan Kernel 6.12 de Amazon Linux 2023. Para obtener más información,	9 de septiembre de 2025

	consulte Instalación del cliente Lustre.	
Se agregó soporte adicional para Región de AWS	Los sistemas de archivos de FSx para Lustre ya están disponibles en Asia-Pacífico (Taipéi). Para obtener más información, consulte la disponibilidad de tipos de implementaciones.	18 de agosto de 2025
Amazon FSx actualizó la política gestionada AmazonFSxServiceRolePolicy de AWS	Amazon FSx agregó los permisos `ec2:AssignIpv6Addresses` y `ec2:UnassignIpv6Addresses` a la AmazonFSxServiceRolePolicy. Para obtener más información, consulte Actualizaciones de Amazon FSx a políticas gestionadas de AWS.	22 de julio de 2025
Lustre Se agregó compatibilidad del cliente con Rocky Linux y Red Hat Enterprise Linux (RHEL	El cliente FSx para Lustre ahora es compatible con instancias de Amazon EC2 que ejecutan Rocky Linux y Red Hat Enterprise Linux (RHEL) 9.6. Para obtener más información, consulte Instalación del cliente Lustre.	1 de julio de 2025

Amazon FSx actualizó la política gestionada de AmazonFSxFullAccess de AWS	La política administrada de AmazonFSxFullAccess se actualizó para añadir los permisos `fsx:CreateAndAttachS3AccessPoint` , `fsx:DescribeS3AccessPointAttachments` y `fsx:DetachAndDeleteS3AccessPoint` .	25 de junio de 2025
Amazon FSx actualizó la política gestionada de AmazonFSxConsoleFullAccess de AWS	La política administrada de AmazonFSxConsoleFullAccess se actualizó para añadir los permisos `fsx:CreateAndAttachS3AccessPoint` , `fsx:DescribeS3AccessPointAttachments` y `fsx:DetachAndDeleteS3AccessPoint` .	25 de junio de 2025

Compatibilidad agregada para la clase de almacenamiento Intelligent-Tiering	Ahora puede crear sistemas de archivos de FSx para Lustre con la clase de almacenamiento Intelligent Tiering. Intelligent-Tiering proporciona un almacenamiento totalmente elástico con una caché SSD opcional para un acceso de baja latencia a los datos a los que se accede con frecuencia. Para obtener más información, consulte Características de rendimiento de la clase de almacenamiento Intelligent Tiering.	29 de mayo de 2025
Se agregó soporte adicional para Región de AWS	Los sistemas de archivos de FSx para Lustre ya están disponibles en Asia Pacífico (Tailandia) y México (centro). Para obtener más información, consulte la disponibilidad de tipos de implementaciones.	8 de mayo de 2025
Lustre Se ha agregado compatibilidad del cliente con Ubuntu	El cliente FSx for Lustre ahora es compatible con instancias de Amazon EC2 que ejecutan Ubuntu 24.04. Para obtener más información, consulte Instalación del cliente Lustre.	19 de marzo de 2025

Amazon FSx actualizó la política administrada de AmazonFSxConsoleReadOnlyAccess de AWS	Amazon FSx actualizó la política AmazonFSx ConsoleReadOnlyAccess para agregar el `ec2:DescribeNetworkInterfaces` permiso. Para obtener más información, consulte la política de AmazonFSx ConsoleReadOnlyAccess.	25 de febrero de 2025
Se ha agregado compatibilidad para actualizar la versión de Lustre	Ahora puede actualizar la versión Lustre de su sistema de archivos de FSx para Lustre a una versión más reciente. Para obtener más información, consulte Administrar la versión de Lustre.	12 de febrero de 2025
Amazon FSx actualizó la política gestionada de AmazonFSxConsoleFullAccess de AWS	Amazon FSx actualizó la política AmazonFSxConsoleFullAccess para agregar el `ec2:DescribeNetworkInterfaces` permiso. Para obtener más información, consulte la política AmazonFSxConsoleFullAccess.	7 de febrero de 2025

Se ha agregado compatibilidad adicional en Región de AWS para el tipo de implementación Persistent 2	Los sistemas de archivos de tipo Persistent 2 en SSD de FSx para Lustre ya están disponibles en el Región de AWS de Asia Pacífico (Malasia). Para obtener más información, consulte la disponibilidad de tipos de implementaciones.	2 de enero de 2025
Lustre Se agregó compatibilidad del cliente con Rocky Linux y Red Hat Enterprise Linux (RHEL	El cliente FSx para Lustre ahora es compatible con instancias de Amazon EC2 que ejecutan Rocky Linux y Red Hat Enterprise Linux (RHEL) 9.5. Para obtener más información, consulte Instalación del cliente Lustre.	26 de diciembre de 2024
Soporte añadido para Elastic Fabric Adapter (EFA)	Ahora puede crear un sistema de archivos de FSx para Lustre Persistent 2 con soporte para Elastic Fabric Adapter (EFA), que proporciona un mayor rendimiento de red para las instancias de cliente que admiten EFA. La activación de EFA también proporciona compatibilidad con GPUDirect Storage (GDS) y ENA Express. Para obtener más información, consulte Uso de sistemas de archivos de compatibles con EFA.	27 de noviembre de 2024

Se ha agregado compatibilidad adicional en Región de AWS para el tipo de implementación Persistent 2	Los sistemas de archivos de tipo Persistent 2 en SSD de FSx para Lustre ya están disponibles en el Oeste de EE. UU. (Norte de California) Región de AWS. Para obtener más información, consulte la disponibilidad de tipos de implementaciones.	27 de noviembre de 2024
Lustre Se agregó compatibilidad del cliente con Ubuntu 22 Kernel 6.8.0	El cliente FSx para Lustre ahora es compatible con instancias de Amazon EC2 que ejecutan Ubuntu 22.04 Kernel 6.8.0. Para obtener más información, consulte Instalación del cliente Lustre.	8 de noviembre de 2024
Se agregó soporte para métricas adicionales de Amazon CloudWatch y un panel de supervisión mejorado	FSx para Lustre ahora proporciona métricas de redes, rendimiento y almacenamiento adicionales y un panel de supervisión mejorado para una mayor visibilidad de la actividad del sistema de archivos. Para obtener más información, consulte Monitorización con Amazon CloudWatch.	25 de septiembre de 2024

Se ha agregado compatibilidad adicional en Región de AWS para el tipo de implementación Persistent 2	Los sistemas de archivos de tipo Persistent 2 en SSD de FSx para Lustre ya están disponibles en la zona en las instalaciones del Este de EE. UU. (Dallas). Para obtener más información, consulte la disponibilidad de tipos de implementaciones.	20 de septiembre de 2024
Lustre Se agregó compatibilidad del cliente con Ubuntu 22 Kernel 6.5.0	El cliente FSx para Lustre ahora es compatible con instancias de Amazon EC2 que ejecutan Ubuntu 22.04 Kernel 6.5.0. Para obtener más información, consulte Instalación del cliente Lustre.	1 de agosto de 2024
Lustre Se agregó compatibilidad del cliente con CentOS, Rocky Linux y Red Hat Enterprise Linux (RHEL	El cliente FSx para Lustre ahora es compatible con instancias de Amazon EC2 que ejecutan CentOS, Rocky Linux y Red Hat Enterprise Linux (RHEL) 8.10. Para obtener más información, consulte Instalación del cliente Lustre.	18 de junio de 2024

Se agregó soporte para aumentar el rendimiento de los metadatos	Ahora puede crear un sistema de archivos de FSx para Lustre Persistent 2 con una configuración de metadatos que permita aumentar el rendimiento de los metadatos . Para obtener más informaci ón, consulte Rendimiento de los metadatos del sistema de archivos y Administración del rendimiento de los metadatos.	6 de junio de 2024
Se ha agregado compatibi lidad adicional en Región de AWS para el tipo de implementación Persistent 2	Los sistemas de archivos de tipo Persistent 2 en SSD de FSx para Lustre ya están disponibles en la zona en las instalaciones del Este de EE. UU. (Atlanta). Para obtener más información, consulte la disponibilidad de tipos de implementaciones.	29 de mayo de 2024
Lustre Se agregó compatibi lidad del cliente con Rocky Linux y Red Hat Enterprise Linux (RHEL	El cliente FSx para Lustre ahora es compatible con instancias de Amazon EC2 que ejecutan Rocky Linux y Red Hat Enterprise Linux (RHEL) 9.4. Para obtener más información, consulte Instalaci ón del cliente Lustre.	16 de mayo de 2024

Se ha agregado compatibilidad adicional en Región de AWS para el tipo de implementación Persistent 2	Los sistemas de archivos de tipo Persistent 2 en SSD de FSx para Lustre ya están disponibles en el Región de AWS del Oeste de Canadá (Calgary). Para obtener más información, consulte la disponibilidad de tipos de implementaciones.	3 de mayo de 2024
Lustre Se ha agregado compatibilidad del cliente con Amazon Linux	El cliente FSx para Lustre ahora es compatible con instancias de Amazon EC2 que ejecutan Amazon Linux 2023. Para obtener más información, consulte Instalación del cliente Lustre.	25 de marzo de 2024
Lustre Se agregó compatibilidad del cliente con CentOS, Rocky Linux y Red Hat Enterprise Linux (RHEL	El cliente FSx para Lustre ahora es compatible con instancias de Amazon EC2 que ejecutan CentOS, Rocky Linux y Red Hat Enterprise Linux (RHEL) 8.9. Para obtener más información, consulte Instalación del cliente Lustre.	9 de enero de 2024

Amazon FSx actualizó las políticas administradas por AWS AmazonFSxFullAccess, AmazonFSxConsoleFullAccess, AmazonFSx ReadOnlyAccess, AmazonFSx ConsoleReadOnlyAccess y AmazonFSxServiceRolePolicy	Amazon FSx actualizó las políticas AmazonFSxFullAccess, AmazonFSxConsoleFullAccess, AmazonFSx ReadOnlyAccess, AmazonFSx ConsoleReadOnlyAccess y AmazonFSxServiceRolePolicy para agregar el permiso `ec2:GetSecurityGroupsForVpc`. Para obtener más información, consulte Actualizaciones de Amazon FSx a políticas gestionadas de AWS.	9 de enero de 2024
Lustre Se agregó compatibilidad del cliente con Rocky Linux y Red Hat Enterprise Linux (RHEL) 9.0 y	El cliente FSx para Lustre ahora es compatible con instancias de Amazon EC2 que ejecutan Rocky Linux y Red Hat Enterprise Linux (RHEL) 9.0 y 9.3. Para obtener más información, consulte Instalación del cliente Lustre.	20 de diciembre de 2023
Amazon FSx para Lustre actualizó las políticas administradas por AWS AmazonFSxFullAccess y AmazonFSxConsoleFullAccess	Amazon FSx actualizó las políticas AmazonFSx FullAccess y AmazonFSx ConsoleFullAccess para agregar la acción `ManageCrossAccountDataReplication`. Para obtener más información, consulte Actualizaciones de Amazon FSx a políticas gestionadas de AWS.	20 de diciembre de 2023

Amazon FSx actualizó las políticas administradas por AWS AmazonFSxFullAccess y AmazonFSxConsoleFullAccess	Amazon FSx actualizó las políticas AmazonFSxFullAccess y AmazonFSxConsoleFullAccess para agregar el permiso `fsx:CopySnapshotAndUpdateVolume` . Para obtener más información, consulte Actualizaciones de Amazon FSx a políticas gestionadas de AWS.	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 Administración de la capacidad de rendimiento.	16 de noviembre de 2023
Amazon FSx actualizó las políticas administradas por AWS AmazonFSxFullAccess y AmazonFSxConsoleFullAccess	Amazon FSx actualizó las políticas AmazonFSxFullAccess y AmazonFSxConsoleFullAccess para agregar los permisos `fsx:DescribeSharedVPCConfiguration` y `fsx:UpdateSharedVPCConfiguration` . Para obtener más información, consulte Actualizaciones de Amazon FSx a políticas gestionadas de AWS.	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 agregó compatibilidad con Lustre versión 2.15	Todos los sistemas de archivos de FSx para Lustre ahora se basan en Lustre versión 2.15 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 ha agregado compatibilidad adicional en Región de AWS para el tipo de implementación Persistent 2	Los sistemas de archivos de tipo Persistent 2 de FSx para Lustre ya están disponibles en el Región de AWS de Israel (Tel Aviv). 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 AmazonFSxServiceRolePolicy de AWS	Amazon FSx actualizó el permiso `cloudwatch:PutMetricData` en la AmazonFSxServiceRolePolicy. Para obtener más información, consulte Actualizaciones de Amazon FSx a políticas gestionadas de AWS.	24 de julio de 2023
Amazon FSx actualizó la política gestionada de AmazonFSxFullAccess de AWS	Amazon FSx actualizó la política AmazonFSxFullAccess para eliminar el permiso `fsx:*` y añadir acciones específicas de `fsx`. Para obtener más información, consulte la política AmazonFSxFullAccess.	13 de julio de 2023

Amazon FSx actualizó la política gestionada de AmazonFSxConsoleFullAccess de AWS	Amazon FSx actualizó la política AmazonFSxConsoleFullAccess para eliminar el permiso `fsx:*` y añadir acciones específicas de `fsx`. Para obtener más información, consulte la política AmazonFSxConsoleFullAccess.	13 de julio de 2023
Lustre Se agregó compatibilidad del cliente con CentOS, Rocky Linux y Red Hat Enterprise Linux (RHEL	El cliente FSx para Lustre ahora es compatible con instancias de Amazon EC2 que ejecutan CentOS, Rocky Linux y Red Hat Enterprise Linux (RHEL) 8.8. Para obtener más información, consulte Instalación del cliente Lustre.	25 de mayo de 2023
Se agregó soporte para las métricas de AutoImport y AutoExport	FSx para Lustre proporciona ahora métricas de Amazon CloudWatch que monitorizan las actualizaciones automáticas de importación y exportación de sistemas de archivos vinculados a repositorios de datos. Para obtener más información, consulte Monitorización con 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 de 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
Lustre Se agregó compatibilidad del cliente con CentOS, Rocky Linux y Red Hat Enterprise Linux (RHEL	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 Lustre.	5 de diciembre de 2022
Se ha agregado compatibilidad adicional en Región de AWS para el tipo de implementación Persistent 2	La nueva generación Persistent 2 SSD FSx para sistemas de archivos Lustre ya está disponible en el Regiones de AWS Europa (Estocolmo), Asia Pacífico (Hong Kong), Asia Pacífico (Mumbai) y Asia Pacífico (Seúl). Para obtener más información, consulte Opciones de implementación para sistemas de archivos de FSx para Lustre.	10 de noviembre de 2022

Lustre Se agregó compatibilidad del cliente con CentOS, Rocky Linux y Red Hat Enterprise Linux (RHEL	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 Lustre.	8 de septiembre de 2022
Lustre Se ha agregado compatibilidad del cliente con Ubuntu	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 Lustre.	28 de julio de 2022
Lustre Se ha agregado compatibilidad del cliente con Rocky Linux	El cliente FSx para Lustre ahora soporta instancias de Amazon EC2 ejecutando Rocky Linux. Para obtener más información, consulte Instalación del cliente Lustre.	8 de julio de 2022
Se ha agregado compatibilidad con root squash de Lustre	Ahora puede usar la característica root squash de Lustre para restringir el acceso a nivel de raíz de los clientes que intentan acceder al sistema de archivos de FSx para Lustre como raíz. Para obtener más información, consulte root squash de Lustre.	25 de mayo de 2022

Se ha agregado compatibilidad adicional en Región de AWS para el tipo de implementación Persistent 2	La nueva generación Persistent 2 SSD FSx para sistemas de archivos Lustre ya está disponible en el Regiones de AWS Europa (Londres) , Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney). Para obtener más información, consulte Opciones de implementación para sistemas de archivos de FSx para Lustre.	19 de abril de 2022
Se ha agregado compatibilidad para usar AWS DataSync para migrar archivos a sus sistemas de archivos de Amazon FSx para Lustre.	Ahora puede usar AWS DataSync para migrar archivos de los sistemas de archivos existentes a los sistemas de archivos de FSx para Lustre. Para obtener más información, consulte Cómo migrar archivos existentes a FSx para Lustre usando AWS DataSync.	5 de abril de 2022
Se ha agregado compatibilidad para los puntos de conexión de VPC para la interfaz AWS PrivateLink	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 con las colas de DRA de Lustre	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
Lustre Se ha agregado compatibilidad del cliente con CentOS y Red Hat Enterprise Linux (RHEL	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 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 para Lustre para que registre los eventos de error y advertencia de los repositor ios de datos asociados a su sistema de archivos en los Registros de Amazon CloudWatch. Para obtener más información, consulte Registro con los Registros de Amazon CloudWatch.	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 agregó compatibilidad con Lustre versión 2.12	Ahora puede elegir Lustre versión 2.12 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
Lustre Se ha agregado compatibilidad del cliente con CentOS y Red Hat Enterprise Linux (RHEL	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 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	Puede usar Amazon FSx para realizar las copias de seguridad dentro 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 región). Para obtener más información, consulte Copiar copias de seguridad.	12 de abril de 2021
Lustre Compatibilidad del cliente Lustre con conjuntos de archivos de	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
Lustre Se ha agregado compatibilidad del cliente con 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 Lustre.	17 de diciembre de 2020
Lustre Se ha agregado compatibilidad del cliente con CentOS y Red Hat Enterprise Linux (RHEL	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 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 está integrado ahora con AWS Backup	Ahora puede utilizar AWS Backup para realizar copias de seguridad y restaurar sus sistemas de archivos de FSx, además de utilizar las copias de seguridad nativas de Amazon FSx. Para obtener más información, consulte Uso de 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

Lustre Se ha agregado compatibilidad del cliente con SUSE Linux SP4 y SP	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 Lustre.	20 de julio de 2020
Lustre Se ha agregado compatibilidad del cliente con CentOS y Red Hat Enterprise Linux (RHEL	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 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 las opciones de implementación de 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 las tareas de repositorios de datos.	23 de diciembre de 2019

Se agregó soporte adicional para Región de AWS	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 soporte adicional para Región de AWS	FSx para 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 agregó compatibilidad del cliente Lustre con 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 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 modificad os en un prefijo que especifiq ue. 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.