aws

Guía del usuario de ONTAP

FSx para ONTAP

FSx para ONTAP: Guía del usuario de ONTAP

Table of Contents

¿Qué es Amazon FSx para NetApp ONTAP?

Amazon FSx para NetApp ONTAP es un servicio totalmente gestionado que proporciona un almacenamiento de archivos altamente fiable, escalable, de alto rendimiento y rico en funciones basado en NetApp el popular sistema de archivos ONTAP. FSx for ONTAP combina las características, el rendimiento, las capacidades y las operaciones de API conocidas de los sistemas de NetApp archivos con la agilidad, la escalabilidad y la simplicidad de un sistema totalmente gestionado. Servicio de AWS

FSx para ONTAP proporciona un almacenamiento de archivos compartido rápido, flexible y rico en características al que se puede acceder fácilmente desde instancias informáticas de Linux, Windows y macOS que se ejecutan en AWS o en las instalaciones. FSx para ONTAP ofrece almacenamiento en unidades de estado sólido (SSD) de alto rendimiento con latencias de submilisegundos. Con FSx para ONTAP, puede alcanzar niveles de rendimiento de SSD para su carga de trabajo y pagar por el almacenamiento en SSD solo para una pequeña fracción de sus datos.

Administrar sus datos con FSx para ONTAP es más fácil porque puede capturar, clonar y replicar sus archivos con solo hacer clic en un botón. Además, FSx for ONTAP organiza automáticamente sus datos en niveles de almacenamiento elásticos y de menor coste, lo que reduce la necesidad de aprovisionar o gestionar la capacidad.

FSx para ONTAP también proporciona un almacenamiento duradero y de alta disponibilidad con copias de seguridad totalmente gestionadas y soporte para la recuperación de desastres entre regiones. Para facilitar la protección y la seguridad de sus datos, FSx para ONTAP es compatible con las aplicaciones antivirus y de seguridad de datos más populares.

Para los clientes que utilizan NetApp ONTAP de forma local, FSx for ONTAP es una solución ideal para migrar, realizar copias de seguridad o fragmentar sus aplicaciones basadas en archivos de forma local a otras AWS sin necesidad de cambiar el código de la aplicación ni la forma de gestionar los datos.

Como servicio totalmente gestionado, FSx para ONTAP facilita el lanzamiento y el escalado de un almacenamiento de archivos compartido fiable, seguro y de alto rendimiento en la nube. Con FSx para ONTAP, ya no tendrá que preocuparse por lo siguiente:

- Configuración y aprovisionamiento de servidores de archivos y volúmenes de almacenamiento
- Replicación de los datos
- Instalación y aplicación de parches al software del servidor de archivos

- Detección y solución de los fallos de hardware
- Gestión de la conmutación por error y la conmutación por recuperación
- Realización de copias de seguridad manualmente

FSx for ONTAP también proporciona una rica integración con otros AWS servicios, como AWS Identity and Access Management (IAM), Amazon WorkSpaces, AWS Key Management Service (AWS KMS) y. AWS CloudTrail

Temas

Características de FSx para ONTAP

Con FSx para ONTAP, obtiene una solución de almacenamiento de archivos totalmente gestionada con:

- Compatibilidad para conjuntos de datos a escala de petabytes en un único espacio de nombres
- Hasta decenas de gigabytes por segundo (GBps) de rendimiento por sistema de archivos
- Acceso multiprotocolo a los datos mediante los protocolos sistema de archivos de red (NFS), bloque de mensajes del servidor (SMB) e interfaz de sistemas informáticos pequeños de Internet (iSCSI)
- Opciones de implementación Multi-AZ y Single-AZ de alta disponibilidad y durabilidad
- Organización automática de los datos en niveles que reduce los costos de almacenamiento mediante la transición automática de los datos a los que se accede con poca frecuencia a un nivel de almacenamiento de menor costo en función de sus patrones de acceso
- Compresión, deduplicación y compactación de datos para reducir el consumo de almacenamiento
- Support for NetApp, función de SnapMirror replicación
- Support para las soluciones NetApp de almacenamiento en caché locales: NetApp Global File Cache y FlexCache

- Support para el acceso y la administración mediante operaciones de API y NetApp herramientas nativas AWS
  - AWS Management Console, AWS Command Line Interface (AWS CLI) y SDK
  - NetApp CLI de ONTAP, API REST y BlueXP
- Compatibilidad para las siguientes características de seguridad y protección de datos:
  - Cifrado de los datos del sistema de archivos y de las copias de seguridad en reposo mediante AWS KMS keys
  - Cifrado de datos en tránsito mediante claves de sesión de Kerberos de SMB
  - Análisis antivirus bajo demanda
  - Autenticación y autorización mediante Microsoft Active Directory
  - Auditoría de acceso a archivos
  - NetApp's SnapLock característica compatible con volúmenes empresariales y de cumplimiento

Seguridad y protección de datos

Amazon FSx ofrece varios niveles de seguridad y conformidad para facilitar la protección de sus datos. Cifra automáticamente los datos en reposo en los sistemas de archivos y las copias de seguridad mediante claves que usted administra en AWS Key Management Service (AWS KMS). También puede cifrar los datos en tránsito mediante Kerberos para clientes NFS y SMB.

Se ha evaluado que Amazon FSx cumple con los siguientes estándares:

- Organización Internacional de Normalización (ISO)
- La norma de seguridad de datos del sector de pagos con tarjeta (PCI DSS)
- Certificaciones de Controles del sistema y organizaciones (SOC)
- La Ley de Portabilidad y Responsabilidad de Seguros Médicos de EE. UU de 1996 (Health Insurance Portability and Accountability Act of 1996, HIPAA).

Para obtener más información, consulte Protección de datos en Amazon FSx para ONTAP NetApp .

Amazon FSx también proporciona los siguientes niveles de control de acceso:

- A nivel de sistema de archivos, Amazon FSx proporciona control de acceso mediante grupos de seguridad de Amazon Virtual Private Cloud (Amazon VPC).

- A nivel de API, Amazon FSx proporciona control de acceso mediante políticas de acceso de AWS Identity and Access Management (IAM).
- Para proporcionar control de acceso a nivel de archivos y carpetas, Amazon FSx admite permisos de Unix, listas de control de acceso (ACL) de NFS y ACL de NTFS. Al unir Amazon FSx a un Active Directory, los usuarios que acceden a los sistemas de archivos pueden autenticarse con sus credenciales de Active Directory.

Para que pueda ver las acciones realizadas por los usuarios en sus recursos de Amazon FSx, Amazon FSx se integra con AWS CloudTrail para supervisar y registrar las llamadas a la API de Amazon FSx. Para obtener más información, consulte Registro de llamadas a la API de FSx para ONTAP con AWS CloudTrail.

Además, Amazon FSx protege sus datos con copias de seguridad de sistemas de archivos de gran durabilidad. Amazon FSx realiza copias de seguridad diarias automáticas y puede realizar copias de seguridad adicionales en cualquier momento. Para obtener más información, consulte Protección de datos.

Precios de FSx para ONTAP

Los sistemas de archivos se le facturan en función de las siguientes categorías:

- Capacidad de almacenamiento SSD (por gigabyte al mes o GB al mes)
- IOPS de SSD que aprovisione por encima de tres IOPS/GB (por IOPS al mes)
- Capacidad de rendimiento (por megabytes por segundo [MBps] al mes)
- Consumo de almacenamiento del pool de capacidad (por GB al mes)
- Solicitudes de grupos de capacidad (por lectura y escritura)
- Consumo de almacenamiento de copia de seguridad (por GB al mes)

Para obtener más información sobre los precios y las tarifas asociadas al servicio, consulte los precios de Amazon FSx for NetApp ONTAP.

Foros de FSx para ONTAP

Si tiene problemas al utilizar Amazon FSx, utilice los foros de debate de FSx para ONTAP para obtener respuestas.

¿Es la primera vez que usa Amazon FSx?

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

1. Si es la primera vez que utiliza AWS, consulte Configuración de FSx para ONTAP para configurar un Cuenta de AWS.
2. Si está preparado para crear su primer sistema de archivos de Amazon FSx, siga las instrucciones que se indican en Introducción a Amazon FSx para ONTAP NetApp .
3. Para obtener más información acerca del rendimiento, consulte Amazon FSx para NetApp el rendimiento de ONTAP.
4. Para obtener información sobre la seguridad de Amazon FSx, consulte Seguridad en Amazon FSx para ONTAP NetApp .
5. Para obtener más información acerca de las API de Amazon FSx, consulte la Referencia de la API de Amazon FSx.

Cómo funciona Amazon FSx para NetApp ONTAP

En este tema se presentan las principales características de Amazon FSx para los sistemas de archivos NetApp ONTAP y su funcionamiento, con enlaces a secciones con descripciones detalladas, detalles importantes de implementación y step-by-step procedimientos de configuración.

Temas

Sistemas de archivos de FSx para ONTAP

Un sistema de archivos es el recurso FSx principal de ONTAP, de forma análoga a un clúster ONTAP local. NetApp Especifique la capacidad de almacenamiento de la unidad de estado sólido (SSD) y la capacidad de rendimiento de su sistema de archivos, y elija una nube privada virtual (VPC) de Amazon donde se cree su sistema de archivos. Para obtener más información, consulte Gestión de FSx para sistemas de archivos ONTAP.

El sistema de archivos puede tener de uno a 12 pares de alta disponibilidad (HA) en función de su configuración. Un par HA se compone de dos servidores de archivos en una configuración activo-en espera. Los sistemas de archivos con un único par de alta disponibilidad se denominan sistemas de archivos escalables. Los sistemas de archivos con varios pares de alta disponibilidad se denominan sistemas de archivos escalables. Para obtener más información, consulte Pares de alta disponibilidad (HA).

Máquinas virtuales de almacenamiento

Una máquina virtual de almacenamiento (SVM) es un servidor de archivos aislado con sus propios puntos de conexión administrativos y de acceso a los datos para administrar y acceder a los datos.

Cuando accede a los datos de su sistema de archivos de FSx for ONTAP, sus clientes y estaciones de trabajo interactúan con una SVM mediante la dirección IP del punto de conexión de la SVM. Para obtener más información, consulte Gestión de SVM.

Puede unir las SVM a un Active Directory de Microsoft para autenticar y autorizar el acceso a los archivos. Para obtener más información, consulte Uso de Microsoft Active Directory en FSx para ONTAP.

Volúmenes

Los volúmenes de FSx para ONTAP son recursos virtuales que se utilizan para organizar y agrupar los datos. Los volúmenes son contenedores lógicos que se alojan en máquinas virtuales virtuales y los datos almacenados en ellos consumen la capacidad de almacenamiento físico del sistema de archivos.

Al crear un volumen, se establece su tamaño, que determina la cantidad de datos físicos que se pueden almacenar en él, independientemente del nivel de almacenamiento en el que se almacenen los datos. También puede configurar el tipo de volumen, RW (lectura y escritura) o DP (protección de datos). Un volumen DP es de solo lectura y se puede utilizar como destino en una relación o. NetApp SnapMirror SnapVault

Los volúmenes de FSx para ONTAP tienen aprovisionamiento ligero, lo que significa que solo consumen capacidad de almacenamiento para los datos almacenados en ellos. En el caso de los volúmenes con aprovisionamiento reducido, la capacidad de almacenamiento no se reserva por adelantado. En cambio, el almacenamiento se asigna de forma dinámica, según sea necesario. El espacio libre se devuelve al sistema de archivos cuando se eliminan los datos del volumen o del LUN. Por ejemplo, puede crear tres volúmenes de 10 TiB en un sistema de archivos configurado con 10 TiB de capacidad de almacenamiento libre, siempre que la cantidad total de datos almacenados en los tres volúmenes no supere los 10 TiB en ningún momento. La cantidad de datos almacenados físicamente en un volumen se tiene en cuenta para el consumo total de capacidad de almacenamiento. Para obtener más información, consulte Gestión de volúmenes FSx para ONTAP.

Niveles de almacenamiento

Un sistema de archivos de FSx para ONTAP tiene dos niveles de almacenamiento: almacenamiento principal y almacenamiento agrupado de capacidad. El almacenamiento principal es un almacenamiento SSD aprovisionado, escalable y de alto rendimiento diseñado específicamente para

la parte activa del conjunto de datos. El almacenamiento agrupado con capacidad es un nivel de almacenamiento totalmente elástico que puede escalar hasta petabytes y tiene un coste optimizado para los datos a los que se accede con poca frecuencia. Los datos que escribe en sus volúmenes consumen capacidad en sus niveles de almacenamiento. Para obtener más información, consulte Niveles de almacenamiento de FSx para ONTAP.

Organización de datos en niveles

La organización de datos en niveles es el proceso mediante el cual Amazon FSx NetApp para ONTAP mueve automáticamente los datos entre el SSD y los niveles de almacenamiento del grupo de capacidad. Cada volumen tiene una política de estratificación que controla si los datos se mueven al nivel de capacidad cuando se vuelven inactivos (inactivos). El período de enfriamiento de la política de estratificación de un volumen determina cuándo los datos se vuelven inactivos (fríos). Para obtener más información, consulte Organización de datos de volumen en niveles.

Eficacia de almacenamiento

Amazon FSx para NetApp ONTAP es compatible con las funciones de eficiencia de almacenamiento a nivel de bloques de ONTAP (compactación, compresión y deduplicación) para reducir la capacidad de almacenamiento que consumen sus datos. Las características de eficiencia del almacenamiento pueden reducir el espacio ocupado por sus datos en el almacenamiento SSD, el almacenamiento agrupado de capacidades y las copias de seguridad. El ahorro típico de capacidad de almacenamiento en las cargas de trabajo de uso general para el uso compartido de archivos sin sacrificar el rendimiento es del 65% gracias a la compresión, la deduplicación y la compactación, tanto en el nivel de almacenamiento SSD como en el del pool de capacidad. Para obtener más información, consulte FSx para la eficiencia de almacenamiento de ONTAP.

Acceso a datos almacenados en FSx para sistemas de archivos ONTAP

Puede acceder a los datos de los volúmenes FSx para ONTAP desde varios clientes Linux, Windows o macOS simultáneamente a través de los protocolos NFS (v3, v4, v4.1, v4.2) y SMB. También puede acceder a los datos mediante el protocolo iSCSI (bloque). Para obtener más información, consulte Acceso a datos.

Gestión de FSx para ONTAP

Puede interactuar con el sistema de archivos de FSx para ONTAP de diferentes maneras y gestionar sus recursos. Puede administrar sus FSx para los recursos de ONTAP mediante ambas AWS herramientas de administración de NetApp ONTAP:

- AWS herramientas de administración
  - Las AWS Management Console
  - El AWS Command Line Interface (AWS CLI)
  - La API y los SDK de Amazon FSx
  - AWS CloudFormation
- NetApp herramientas de gestión:
  - NetApp BlueXP
  - La CLI NetApp de ONTAP
  - La API NetApp REST DE ONTAP

Para obtener más información, consulte Administración de recursos.

Configuración de FSx para ONTAP

Antes de usar Amazon FSx por primera vez, complete las siguientes tareas:

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

Temas

Registro para obtener una Cuenta de AWS

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

Cómo registrarse en una Cuenta de AWS

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

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

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

AWS le enviará un correo electrónico de confirmación luego de completar el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Crear un usuario administrativo

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

Protección de su Usuario raíz de la cuenta de AWS

1. Inicie sesión en la AWS Management Console como propietario de cuenta, elija Usuario raíz e ingrese el email de su Cuenta de AWS. En la siguiente página, escriba su contraseña.

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

2. Active la autenticación multifactor (MFA) para el usuario raíz.

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

Creación de un usuario administrativo

1. Activar IAM Identity Center

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

2. En IAM Identity Center, otorga acceso administrativo a un usuario administrativo.

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

Cómo iniciar sesión como usuario administrativo

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

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

Siguiente paso

Para empezar a usar FSx para ONTAP, consulte Introducción a Amazon FSx para ONTAP NetApp para ver las instrucciones para crear sus recursos de Amazon FSx.

Introducción a Amazon FSx para ONTAP NetApp

Obtenga información sobre cómo empezar a utilizar Amazon FSx para NetApp ONTAP. Este ejercicio introductorio incluye los siguientes pasos.

Temas

Paso 1: Crear un sistema de archivos Amazon FSx para NetApp ONTAP

La consola Amazon FSx tiene dos opciones para crear un sistema de archivos: una opción de Creación rápida y una opción de Creación estándar. Para crear rápida y fácilmente un sistema de archivos Amazon FSx para NetApp ONTAP con la configuración recomendada por el servicio, utilice la opción de creación rápida.

La opción de creación rápida crea un sistema de archivos con un único par de alta disponibilidad (HA), una sola máquina virtual de almacenamiento (SVM) y un único volumen. La opción de Creación rápida configura este sistema de archivos para permitir el acceso a los datos desde instancias de Linux a través del protocolo Network File System (NFS). Una vez creado el sistema de archivos, puede crear SVM y volúmenes adicionales según sea necesario, incluido un SVM unido a un Active Directory para permitir el acceso desde clientes Windows y macOS a través del protocolo Server Message Block (SMB).

Para obtener información sobre el uso de la opción de creación estándar para crear un sistema de archivos con una configuración personalizada y sobre el uso de la API AWS CLI y, consulte. Creación de FSx para sistemas de archivos ONTAP

Para crear su sistema de archivos

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

3. En la página Seleccione el tipo de sistema de archivos, elija Amazon FSx para NetApp ONTAP y, a continuación, elija Siguiente. Aparecerá la página Create ONTAP file system (Crear sistema de archivos ONTAP).
4. En Método de creación, seleccione Creación rápida.
5. En la sección Configuración rápida, en Nombre del sistema de archivos (opcional), ingrese un nombre para el sistema de archivos. Es más fácil encontrar y administrar los sistemas de archivos cuando les da nombre. Puede utilizar un máximo de 256 letras Unicode, espacios en blanco y números, además de los siguientes caracteres especiales: + - (guión) =. _ (guión bajo) : /
6. Para el Tipo de implementación, elija Multi-AZ o Single-AZ.

   - Los sistemas de archivos Multi-AZ replican sus datos y admiten la conmutación por error en varias zonas de disponibilidad de la misma Región de AWS.
   - Los sistemas de archivos Single-AZ replican sus datos y ofrecen una conmutación por error automática dentro de una única zona de disponibilidad.

   Para obtener más información, consulte Disponibilidad y durabilidad.
7. Para la capacidad de almacenamiento en SSD, especifique la capacidad de almacenamiento del sistema de archivos, en gibibytes (). GiBs Introduzca cualquier número entero en el rango de 1024 a 196 608. Si necesitas más capacidad de almacenamiento en SSD, puedes usar Standard create. Para obtener más información, consulte Para crear un sistema de archivos (consola).

   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. En cuanto a la capacidad de rendimiento, Amazon FSx proporciona automáticamente una capacidad de rendimiento recomendada en función del almacenamiento SSD. También puede elegir el rendimiento de su sistema de archivos (hasta 4096 MBps). Si necesita más capacidad de rendimiento, puede utilizar Standard Create.
9. Para la Nube Privada Virtual (VPC), elija la VPC de Amazon que desee asociar a su sistema de archivos.
10. En Storage efficiency (Eficiencia de almacenamiento), seleccione Enabled (Activado) para activar las funciones de eficiencia de almacenamiento de ONTAP (compresión, deduplicación y compactación) o Disabled (Desactivado) para desactivarlas.

11. (Sólo Multi-AZ) punto de conexión IP address range especifica el rango de direcciones IP en el que se crean los puntos de conexión para acceder a su sistema de ficheros.

    Elija una opción de Creación rápida para el rango de direcciones IP del punto de conexión:

    - Unallocated IP address range from your VPC: Elija esta opción para que Amazon FSx utilice las últimas 64 direcciones IP del rango CIDR principal de la VPC como rango de direcciones IP de punto de conexión para el sistema de archivos. Tenga en cuenta que este rango se comparte entre varios sistemas de archivos si elige esta opción varias veces.

      > **Note**
      >
      > - Cada sistema de archivos que cree consume dos direcciones IP de este rango: una para el clúster y otra para la primera SVM. La primera y la última dirección IP también están reservadas. Por cada SVM adicional, el sistema de archivos consume otra dirección IP. Por ejemplo, un sistema de archivos que aloja 10 SVM utiliza 11 direcciones IP. Los sistemas de archivos adicionales funcionan de la misma manera. Consumen las dos direcciones IP iniciales, más una para cada SVM adicional. El número máximo de sistemas de archivos que utilizan el mismo rango de direcciones IP, cada uno con un único SVM, es 31.
      > - Esta opción aparece atenuada si una subred utiliza alguna de las últimas 64 direcciones IP del rango CIDR principal de una subred.

    - Floating IP address range outside your VPC: Elija esta opción para que Amazon FSx utilice un rango de direcciones 198.19.x.0/24 que no esté ya utilizado por ningún otro sistema de archivos con la misma VPC y tablas de enrutamiento.

    También puede especificar su propio rango de direcciones IP en la opción de Creación estándar.

12. Seleccione Next (Siguiente) y revise la configuración del sistema de archivos en la página Create ONTAP file system (Crear sistema de archivos ONTAP). Tenga en cuenta qué configuraciones del sistema de archivos puede modificar una vez creado el sistema de archivos.
13. Seleccione Crear sistema de archivos.

La Creación rápida crea un sistema de archivos con una SVM (llamada `fsx`) y un volumen (llamada `vol1`). El volumen tiene una ruta de unión de `/vol1` y una política de niveles Automática de los grupos de capacidad (que agrupa automáticamente todos los datos a los que no se haya accedido

durante 31 días para convertirlos en un almacenamiento de grupos de capacidad más económico). La política de instantáneas predeterminada se asigna al volumen predeterminado. Los datos del sistema de archivos se cifran en reposo mediante la AWS KMS clave gestionada por el servicio predeterminada.

Paso 2: Montar el sistema de archivos desde una instancia de Linux Amazon EC2

Puede montar el sistema de archivos desde una instancia de Amazon Elastic Compute Cloud (Amazon EC2). Este procedimiento utiliza una instancia que ejecuta Amazon Linux 2.

Para montar el sistema de archivos desde Amazon EC2

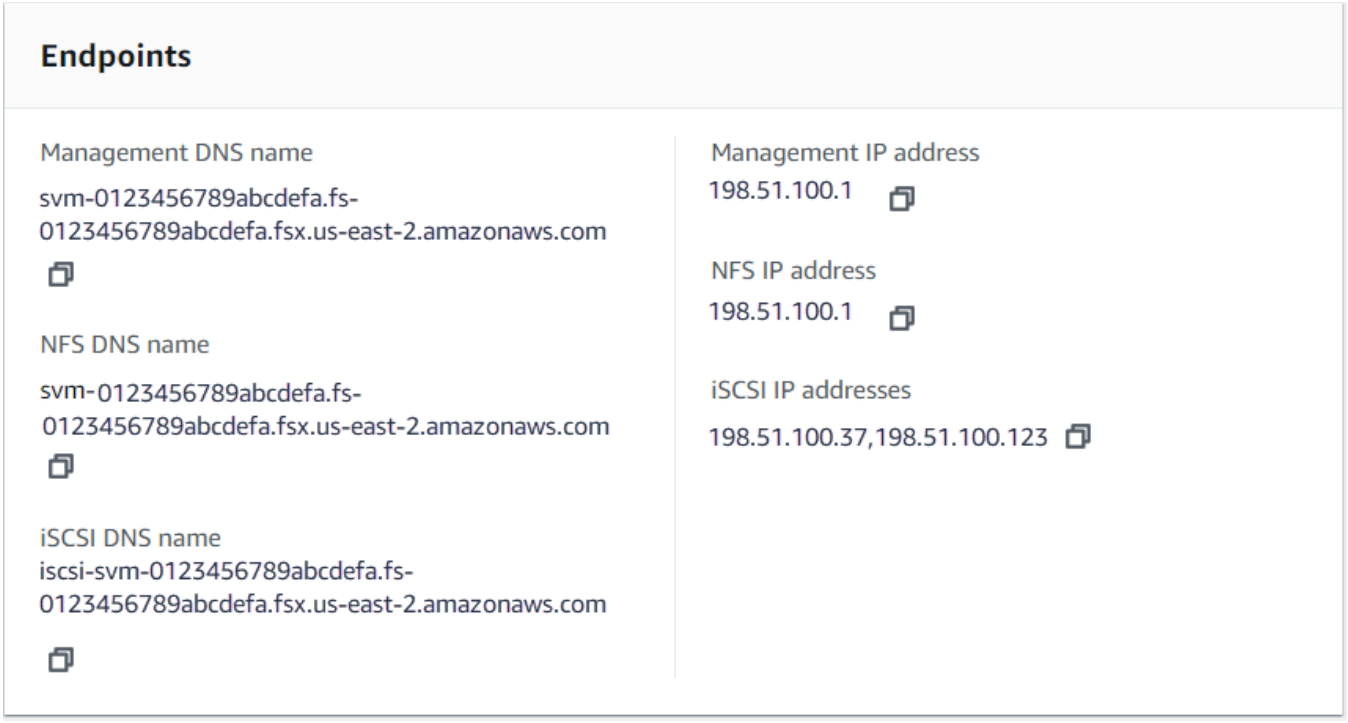
1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Cree o seleccione una instancia de Amazon EC2 que ejecute Amazon Linux 2 y que esté en la misma nube privada virtual (VPC) que el sistema de archivos. Para obtener más información sobre el lanzamiento de una instancia, consulte Paso 1: Lanzar una instancia en la Guía del usuario de Amazon EC2 para instancias Linux.
3. Conéctese a su instancia de Linux de Amazon EC2. Para obtener más información, consulte Conexión con la instancia de Linux en la Guía del usuario de Amazon EC2 para instancias de Linux.
4. Abra un terminal en su instancia de Amazon EC2 mediante un secure shell (SSH) e inicie sesión con las credenciales correspondientes.
5. Cree un directorio en su instancia de Amazon EC2 para usarlo como punto de montaje del volumen con el siguiente comando. En el siguiente ejemplo, reemplace *`mount-point`* con su propia información.

   ```
   $ sudo mkdir /mount-point
   ```

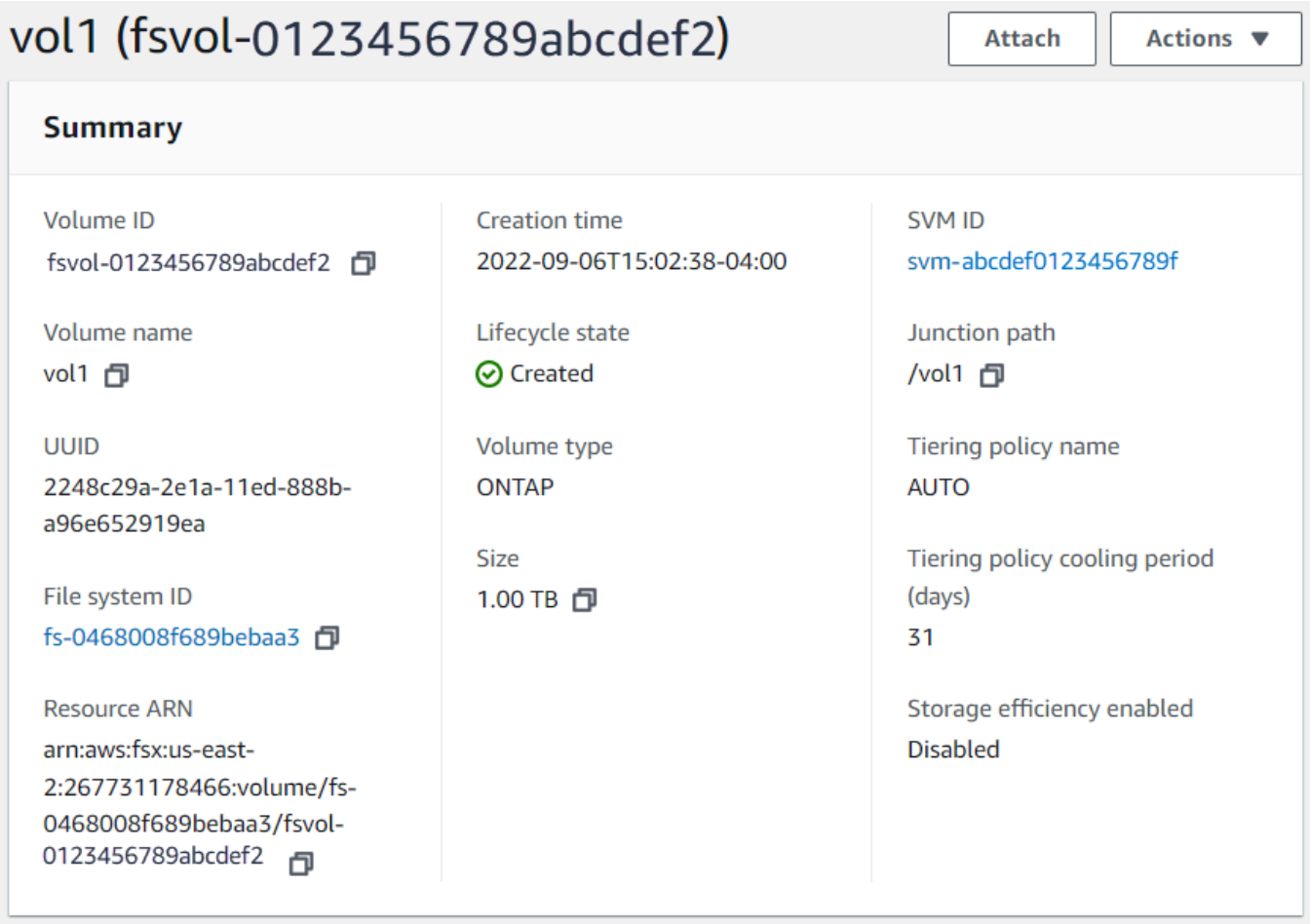
6. Monte su sistema de archivos Amazon FSx para NetApp ONTAP en el directorio que ha creado. Utilice un comando `mount` similar al del ejemplo siguiente. En el siguiente ejemplo, sustituya los siguientes valores de marcador de posición por su propia información.

   - *`nfs_version`*: la versión de NFS que está utilizando; FSx para ONTAP es compatible con las versiones 3, 4.0, 4.1 y 4.2.
   - *`nfs-dns-name`*: el nombre de DNS de NFS de la máquina virtual de almacenamiento (SVM) en el que se encuentra el volumen que va a montar. Para encontrar el nombre DNS de

NFS en la consola de Amazon FSx, seleccione Storage virtual machines y, a continuación, seleccione la SVM en la que se encuentra el volumen que va a montar. El nombre DNS de NFS se encuentra en el panel de Puntos de conexión, que se muestra en la siguiente imagen.



- *`volume-junction-path`*: la ruta de unión del volumen que está montando. Puede encontrar la ruta de unión de un volumen en la consola de Amazon FSx, en el panel Summary (Resumen) de la página de detalles del volumen, que se muestra en la siguiente imagen.



- *mount-point*: el nombre del directorio que creó en la instancia EC2 para el punto de montaje del volumen.

```
sudo mount -t nfs -o nfsvers=nfs_version nfs-dns-name:/volume-junction-path /mount-point
```

El siguiente comando utiliza valores de ejemplo.

```
sudo mount -t nfs -o nfsvers=4.1 svm-abcdef1234567890c.fs-012345abcdef6789b.fsx.us-east-2.amazonaws.com:/vol1 /fsxN
```

Si tiene problemas con su instancia de Amazon EC2 (como la interrupción de las conexiones), consulte Solución de problemas de instancias EC2 en la Guía del usuario de Amazon EC2 para instancias Linux.

Paso 3: Limpiar recursos

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

Para limpiar los recursos:

1. En la consola de Amazon EC2, termine la instancia. Para obtener más información, consulte Terminar la instancia en la Guía del usuario de Amazon EC2 para instancias de Linux.
2. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
3. En la consola de Amazon FSx, elimine todos los volúmenes de FSx para ONTAP que no sean volúmenes raíz de su SVM. Para obtener más información, consulte Eliminación de un volumen.
4. Elimine todos sus FSx para las SVM de ONTAP. Para obtener más información, consulte Eliminación de una máquina virtual de almacenamiento (SVM).
5. En la consola Amazon FSx, elimine el sistema de archivos. Al eliminar un sistema de archivos, todas las copias de seguridad automáticas se eliminan automáticamente. Sin embargo, debe eliminar todas las copias de seguridad creadas manualmente. Los pasos siguientes describen este proceso.

    a. En el panel de control de la consola, seleccione el nombre del sistema de archivos que ha creado para este ejercicio.

    b. En Acciones, seleccione Eliminar sistema de archivos.

    c. En el cuadro de diálogo Delete file system (Eliminar sistema de archivos), ingrese el ID del sistema de archivos que desee eliminar en el cuadro File system ID (ID del sistema de archivos).

    d. Seleccione Delete file system (Eliminar sistema de archivos).

    e. Mientras Amazon FSx elimina el sistema de archivos, su estado en el panel cambia a DELETING (ELIMINANDO). Una vez que se elimina el sistema de archivos, deja de aparecer en el panel de control. Todas las copias de seguridad automáticas se eliminan junto con el sistema de archivos.

    f. Ahora puede eliminar cualquier copia de seguridad creada manualmente para su sistema de archivos. En la barra de navegación de la izquierda, seleccione Backups.

    g. En el panel de control, seleccione las copias de seguridad que tengan el mismo File system ID (ID del sistema de archivos) que el sistema de archivos que ha eliminado y seleccione

Delete backup (Eliminar copia de seguridad). Asegúrese de retener la copia de seguridad final, si creó una.

h. Se abre el cuadro de diálogo Delete backups (Eliminar copias de seguridad). Mantenga la casilla de verificación seleccionada para los ID de las copias de seguridad que desea eliminar y, a continuación, seleccione Delete backups (Eliminar copias de seguridad).

Su sistema de archivos Amazon FSx y todas las copias de seguridad automáticas relacionadas ahora se eliminan, junto con las copias de seguridad manuales que haya decidido eliminar.

Acceso a datos

Puede acceder a sus sistemas de archivos Amazon FSx mediante una variedad de clientes y métodos compatibles tanto en entornos locales como locales. Nube de AWS

Cada SVM tiene cuatro puntos finales que se utilizan para acceder a los datos o administrar la SVM mediante la NetApp CLI de ONTAP o la API REST:

- `Nfs`: para conectarse mediante el protocolo sistema de archivos de red (NFS)
- `Smb`: para conectarse mediante el protocolo de bloque de mensajes de servicio (SMB) (si su SVM está unido a un Active Directory o si utiliza un grupo de trabajo).
- `Iscsi`— Para conectarse mediante el protocolo Internet Small Computer Systems Interface (iSCSI) (solo para sistemas de archivos ampliables).
- `Management`— Para gestionar las SVM mediante la NetApp CLI o la API de ONTAP, o BlueXP NetApp

Temas

Clientes compatibles

Los sistemas de archivos de FSx para ONTAP admiten el acceso a datos desde una amplia variedad de instancias informáticas y sistemas operativos. Para ello, admite el acceso mediante el protocolo de sistemas de archivos de red (NFS) (v3, v4.0, v4.1 y v4.2), todas las versiones del protocolo de bloque de mensajes de servidor (SMB) (incluidas las 2.0, 3.0 y 3.1.1) y el protocolo de interfaz de sistemas informáticos pequeños de Internet (iSCSI).

> **Important**
>
> 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, que 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 admiten las siguientes AWS instancias de procesamiento para su uso con FSx para ONTAP:

- Instancias de Amazon Elastic Compute Cloud (Amazon EC2) que ejecutan Linux con soporte para NFS o SMB, Microsoft Windows y macOS. Para obtener más información, consulte Volúmenes de montaje.
- Contenedores de Docker de Amazon Elastic Container Service (Amazon ECS) en instancias de Amazon EC2 para Windows y Linux. Para obtener más información, consulte Uso de Amazon Elastic Container Service con FSx para ONTAP.
- Amazon Elastic Kubernetes Service: para obtener más información, consulte el controlador CSI de Amazon FSx para NetApp ONTAP en la Guía del usuario de Amazon EKS.
- Red Hat OpenShift Service on AWS (ROSA): para obtener más información, consulte ¿En qué funciona Red Hat Service? OpenShift AWS en la guía del AWS usuario de Red Hat OpenShift Service on.
- WorkSpaces Instancias de Amazon. Para obtener más información, consulte Uso de Amazon WorkSpaces con FSx para ONTAP.
- Instancias de Amazon AppStream 2.0.
- AWS Lambda — Para obtener más información, consulte la entrada del AWS blog Habilitar el acceso de pequeñas y medianas empresas para cargas de trabajo sin servidor con Amazon FSx.
- Máquinas virtuales (VM) que se ejecutan en entornos de VMware Cloud. AWS Para obtener más información, consulte Configurar Amazon FSx para NetApp ONTAP como almacenamiento externo y la guía de implementación de VMware Cloud on with AWS Amazon FSx para ONTAP. NetApp

Una vez montados, los sistemas de archivos de FSx para ONTAP aparecen como un directorio local o una letra de unidad en NFS y SMB, lo que proporciona un almacenamiento de archivos en red compartido y totalmente gestionado al que pueden acceder simultáneamente hasta miles de clientes. Se puede acceder a los LUNS iSCSI como dispositivos de bloques cuando se montan sobre iSCSI.

Acceder a los datos desde dentro AWS

Cada sistema de archivos de Amazon FSx está asociado a una nube privada virtual (VPC). Puede acceder a su sistema de archivos de FSx para ONTAP desde cualquier lugar de la VPC del sistema de archivos, independientemente de la zona de disponibilidad. También puede acceder a su sistema de archivos desde otras VPC que pueden estar en AWS cuentas diferentes o Regiones de AWS. Además de los requisitos descritos en las siguientes secciones para acceder a los recursos de FSx para ONTAP, también debe asegurarse de que el grupo de seguridad de VPC del sistema de archivos esté configurado de modo que el tráfico de datos y administración pueda fluir entre el sistema de archivos y los clientes. Para obtener más información acerca de las reglas de los grupos de seguridad obligatorios, consulte Grupos de seguridad de Amazon VPC.

Temas

Acceso a los datos desde la misma VPC

Al crear su sistema de archivos Amazon FSx para NetApp ONTAP, debe seleccionar la Amazon VPC en la que se encuentra. Todas las SVM y los volúmenes asociados al sistema de archivos Amazon FSx NetApp for ONTAP también se encuentran en la misma VPC. Al montar un volumen, si el sistema de archivos y el cliente que monta el volumen están ubicados en la misma VPC Cuenta de AWS, puede utilizar el nombre DNS y la unión de volúmenes de la SVM o el recurso compartido SMB, según el cliente. Para obtener más información, consulte Volúmenes de montaje.

Puede lograr un rendimiento óptimo si el cliente y el volumen se encuentran en la misma zona de disponibilidad que la subred del sistema de archivos o en la subred preferida para los sistemas de archivos Multi-AZ. Para identificar la subred o la subred preferida de un sistema de archivos, en la consola de Amazon FSx, elija Sistemas de archivos y, a continuación, elija el sistema de archivos de ONTAP cuyo volumen va a montar y la subred o subred preferida (Multi-AZ) aparecerá en el panel Subred o Subred preferida.

Acceso a los datos desde fuera de la VPC de implementación

En esta sección se describe cómo acceder a un FSx para los puntos finales del sistema de archivos ONTAP desde AWS ubicaciones fuera de la VPC de despliegue del sistema de archivos.

Acceso a los puntos de conexión de administración de NFS, SMB y ONTAP en sistemas de archivos Multi-AZ

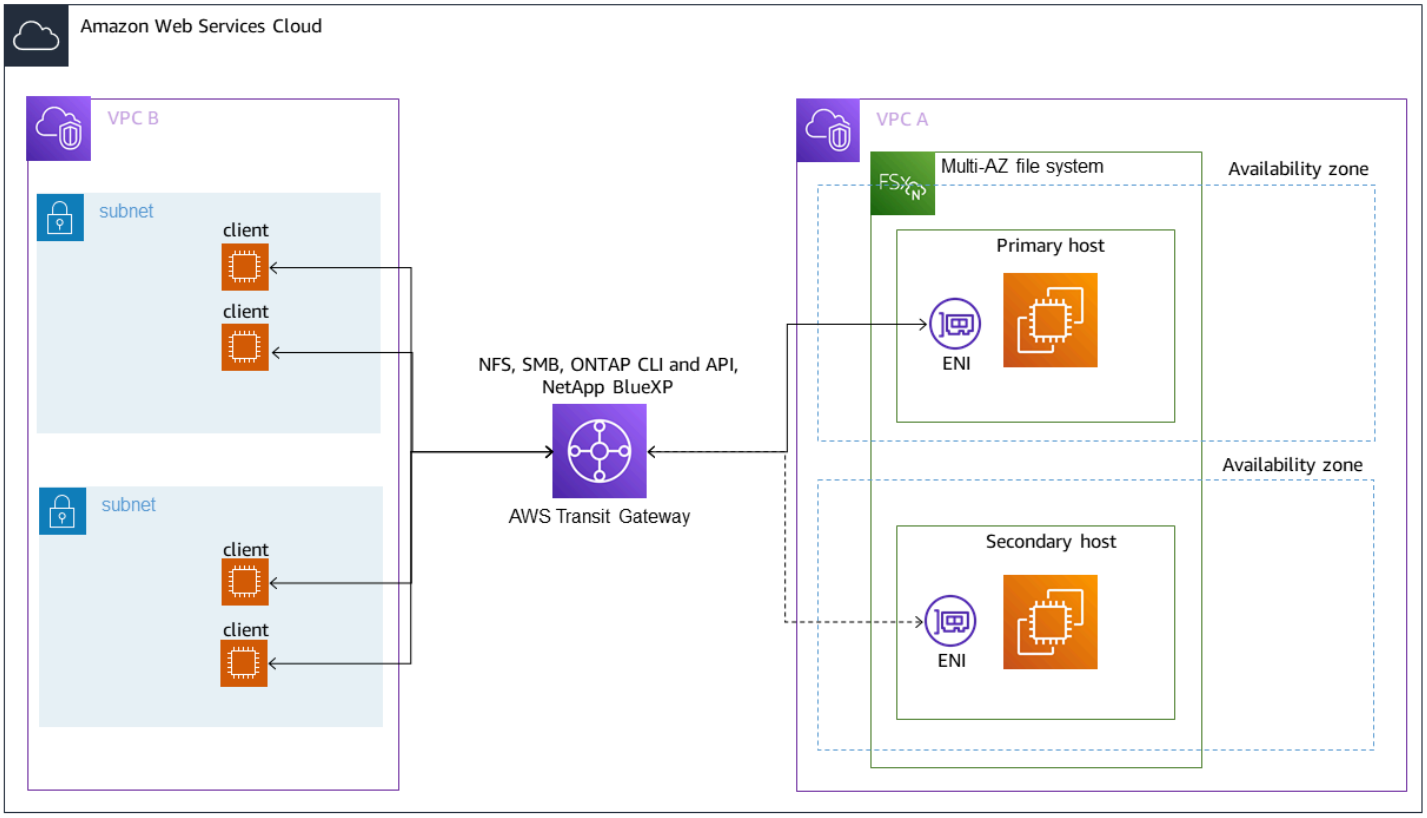
Los puntos finales de administración NFS, SMB y ONTAP de Amazon FSx NetApp para los sistemas de archivos Multi-AZ de ONTAP utilizan direcciones de protocolo de Internet (IP) flotantes para que los clientes conectados puedan realizar una transición fluida entre el servidor de archivos preferido y el servidor de archivos en espera durante un evento de conmutación por error. Para obtener más información acerca de las conmutaciones por error, consulte Proceso de conmutación por error para FSx para ONTAP.

Estas direcciones IP flotantes se crean en las tablas de enrutamiento de VPC que se asocian al sistema de archivos y se encuentran dentro de `EndpointIpAddressRange` de los sistemas de archivos que se pueden especificar durante la creación. `EndpointIpAddressRange` utiliza los siguientes rangos de direcciones, en función de cómo se cree el sistema de archivos:

- Los sistemas de archivos Multi-AZ creados con la consola de Amazon FSx utilizan las últimas 64 direcciones IP del rango de CIDR principal de la VPC para el sistema de archivos de forma predeterminada `EndpointIpAddressRange`.
- Los sistemas de archivos Multi-AZ creados con la AWS CLI API de Amazon FSx utilizan un rango de direcciones IP dentro `198.19.0.0/16` del bloque de direcciones de forma predeterminada`EndpointIpAddressRange`.

Solo AWS Transit Gateway admite el enrutamiento a direcciones IP flotantes, lo que también se conoce como emparejamiento transitivo. Emparejamiento de VPC y AWS VPN no admiten el emparejamiento transitivo. AWS Direct Connect Por lo tanto, debe utilizar una puerta de enlace de tránsito para acceder a estas interfaces desde redes que se encuentran fuera de la VPC de su sistema de archivos.

El siguiente diagrama ilustra el uso de una puerta de enlace de tránsito para NFS, SMB o acceso de administración a un sistema de archivos Multi-AZ que se encuentra en una VPC diferente a la de los clientes que acceden a él.



> **Note**
>
> Asegúrese de que todas las tablas de enrutamiento que utiliza estén asociadas a su sistema de archivos Multi-AZ. Esto ayuda a evitar la falta de disponibilidad durante una conmutación por error. Para obtener información sobre cómo asociar las tablas de enrutamiento de Amazon VPC a su sistema de archivos, consulte Actualización de un sistema de archivos.

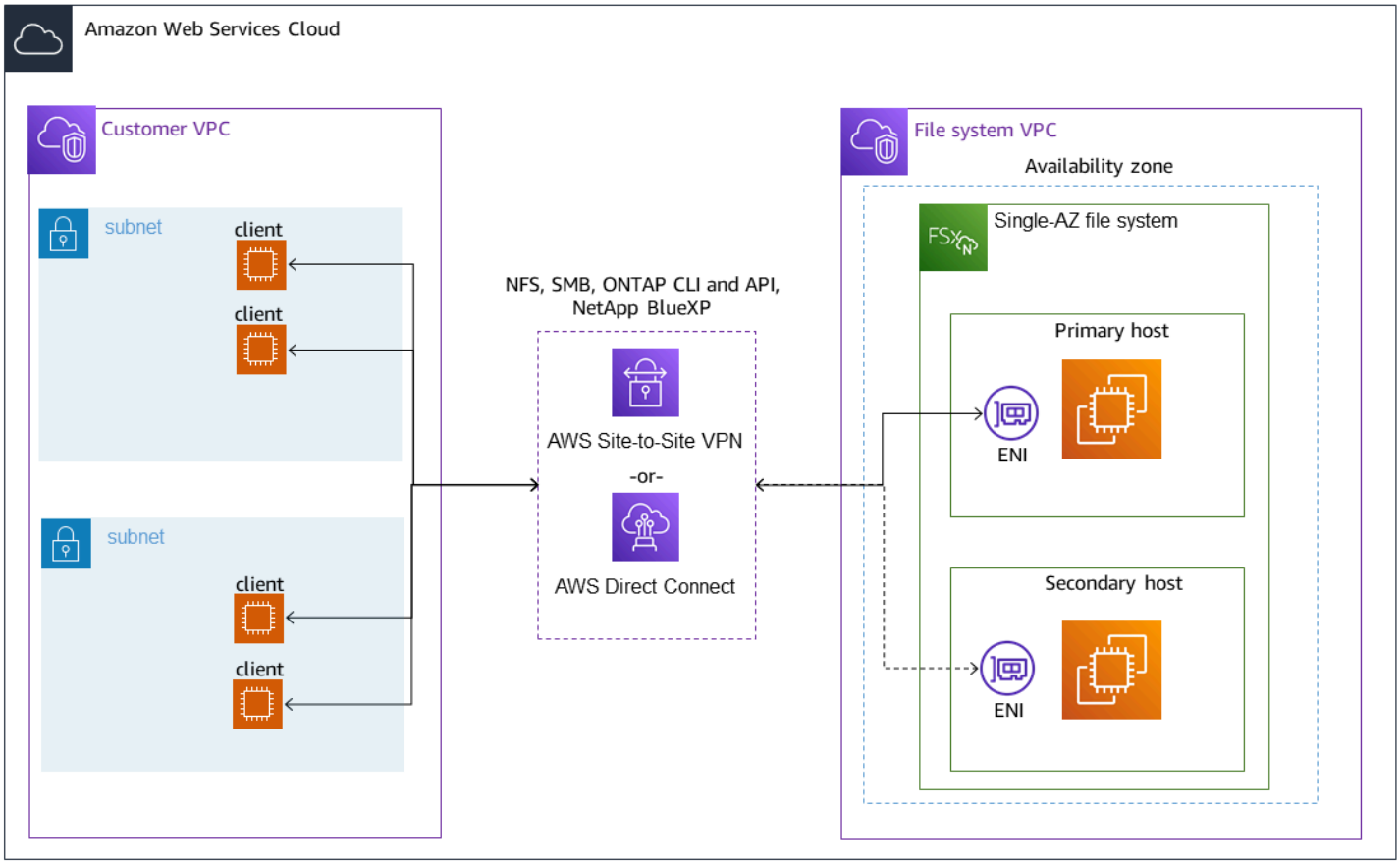
Para obtener información sobre cuándo debe utilizar una puerta de enlace de tránsito para acceder a su sistema de archivos de FSx para ONTAP, consulte ¿Cuándo se requiere una puerta de enlace de tránsito?.

Acceso a NFS, SMB o a la CLI y API de ONTAP para sistemas de archivos Single-AZ

Los puntos de conexión que se utilizan para acceder a los sistemas de archivos de FSx para ONTAP Single-AZ a través de NFS o SMB, y para administrar los sistemas de archivos mediante la CLI o la API de REST de ONTAP, son direcciones IP secundarias en el ENI del servidor de archivos activo. Las direcciones IP secundarias se encuentran dentro del rango CIDR de la VPC, por lo que

los clientes pueden acceder a los puertos de datos y administración mediante el emparejamiento de VPC o sin necesidad de hacerlo. AWS Direct Connect AWS VPN AWS Transit Gateway

En el siguiente diagrama, se muestra el uso AWS VPN o AWS Direct Connect el acceso de administración de NFS, SMB o de administración a un sistema de archivos Single-AZ que se encuentra en una VPC diferente a la de los clientes que acceden a él.



¿Cuándo se requiere una puerta de enlace de tránsito?

El hecho de que se requiera una puerta de enlace de tránsito para sus sistemas de archivos Multi-AZ depende del método que utilice para acceder a los datos del sistema de archivos. Los sistemas de archivos Single-AZ no requieren una puerta de enlace de tránsito. En la siguiente tabla se describe cuándo necesitará utilizar AWS Transit Gateway para acceder a los sistemas de archivos Multi-AZ.

Acceso a los datos	¿Necesita una puerta de enlace de tránsito?
Acceso a FSx a través de NFS, SMB o la API NetApp REST, CLI o BlueXP de ONTAP	Solo si:

Acceso a los datos	¿Necesita una puerta de enlace de tránsito?
	• Accede desde una red emparejada (en las instalaciones, por ejemplo) y • No está accediendo a FSx a través de una NetApp FlexCache instancia de Global File Cache
Acceso a los datos a través de iSCSI	No
Unión de una SVM a un Active Directory	No
SnapMirror	No
FlexCache Almacenamiento en caché	No
Caché de archivos global	No

Configuración del enrutamiento mediante AWS Transit Gateway

Si tiene un sistema de archivos Multi-AZ con un sistema `EndpointIPAddressRange` que se encuentra fuera del rango de CIDR de su VPC, debe configurar un enrutamiento adicional para acceder AWS Transit Gateway a su sistema de archivos desde redes interconectadas o locales.

Important

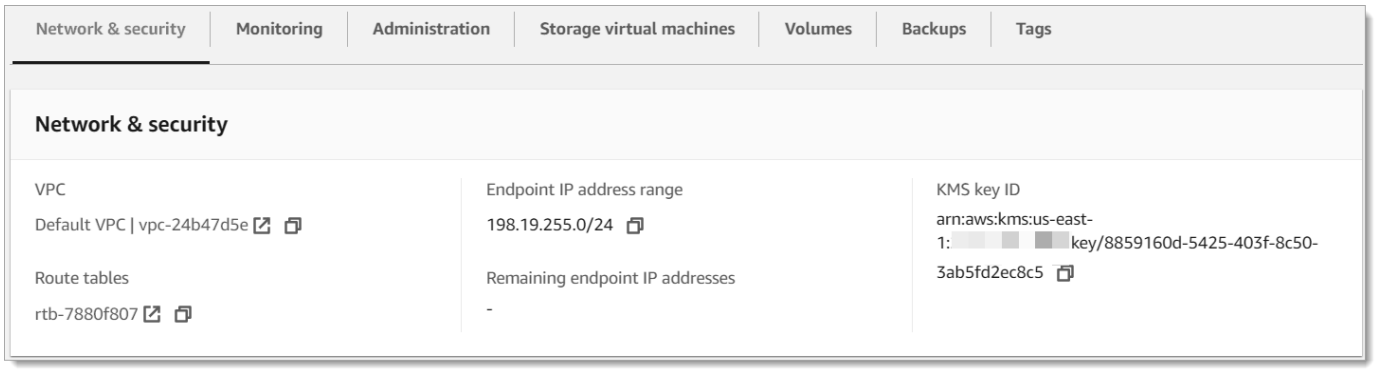
Para acceder a un sistema de archivos Multi-AZ mediante una puerta de enlace de tránsito, cada una de las conexiones de puerta de enlace de tránsito debe crearse en una subred cuya tabla de enrutamiento esté asociada a su sistema de archivos.

Note

No se requiere ninguna configuración adicional de puerta de enlace de tránsito para los sistemas de archivos Single-AZ o Multi-AZ con una `EndpointIPAddressRange` que se encuentre dentro del rango de direcciones IP de su VPC.

Para configurar el enrutamiento mediante AWS Transit Gateway

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Elija el sistema de archivos de FSx para ONTAP para el que está configurando el acceso desde una red emparejada.
3. En Red y seguridad, copie el rango de direcciones IP del punto de conexión.



4. Agregue una ruta a la puerta de enlace de tránsito que dirija el tráfico destinado a este rango de direcciones IP a la VPC de su sistema de archivos. Para obtener más información, consulte Uso de las puertas de enlace de tránsito en Puertas de enlace de tránsito de Amazon VPC.
5. Confirme que puede acceder a su sistema de archivos de FSx para ONTAP desde la red emparejada.

Para añadir la tabla de enrutamiento a su sistema de archivos, consulte Actualización de un sistema de archivos.

> **Note**
>
> Los registros de DNS de los puntos de conexión de administración, NFS y SMB solo se pueden resolver desde la misma VPC que el sistema de archivos. Para montar un volumen o conectarse a un puerto de administración desde otra red, debe usar la dirección IP del punto de conexión. Estas direcciones IP no cambian con el tiempo.

Acceso a puntos de conexión iSCSI o entre clústeres fuera de la VPC de implementación

Puede usar el emparejamiento de VPC o AWS Transit Gateway para acceder a los puntos finales iSCSI o entre clústeres del sistema de archivos desde fuera de la VPC de implementación del

sistema de archivos. Puede usar el emparejamiento de VPC para enrutar el tráfico iSCSI y entre clústeres entre las VPC. Una conexión de emparejamiento de VPC es una conexión de redes entre dos VPC que permite direccionar el tráfico entre ellas mediante direcciones IPv4 privadas. Puede utilizar el emparejamiento de VPC para conectar VPC dentro de la misma Región de AWS o entre diferentes. Regiones de 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.

Acceso a los datos en las instalaciones

Puede acceder a sus sistemas de archivos de FSx para ONTAP en las instalaciones mediante AWS VPN y AWS Direct Connect; en las siguientes secciones, encontrará pautas de casos de uso más específicas. Además de los requisitos que se indican a continuación para acceder a diferentes recursos de FSx para ONTAP en las instalaciones, también debe asegurarse de que el grupo de seguridad de VPC de su sistema de archivos permita que los datos fluyan entre su sistema de archivos y los clientes; para obtener una lista de los puertos necesarios, consulte Grupos de seguridad de Amazon VPC.

Acceso a los puntos de conexión de NFS, SMB o CLI o API de REST de ONTAP en las instalaciones

En esta sección se describe cómo acceder a los puertos de administración NFS, SMB y ONTAP de FSx para los sistemas de archivos ONTAP desde redes en las instalaciones.

Acceso a sistemas de archivos Multi-AZ

Amazon FSx requiere que utilice AWS Transit Gateway o configure la caché NetApp global de archivos remota o que acceda NetApp FlexCache a sistemas de archivos Multi-AZ desde una red local. Para admitir la conmutación por error en AZ para sistemas de archivos Multi-AZ, Amazon FSx utiliza direcciones IP flotantes para las interfaces utilizadas para los puntos de conexión de administración de NFS, SMB y ONTAP. Dado que los puntos de enlace NFS, SMB y de administración utilizan direcciones IP flotantes, debe AWS Transit Gatewayutilizarlas junto con estas interfaces AWS Direct Connect o AWS VPN para acceder a ellas desde una red local. Las direcciones IP flotantes utilizadas para estas interfaces se encuentran dentro de las especificadas en `EndpointIpAddressRange` al crear el sistema de archivos Multi-AZ. Si crea su sistema de archivos desde la consola de Amazon FSx, Amazon FSx elige las últimas 64 direcciones IP de forma predeterminada del rango de CIDR principal de la VPC para usarlas como rango de direcciones IP de punto de conexión del sistema de archivos. Si crea su sistema de archivos a partir de la API

AWS CLI o de Amazon FSx, Amazon FSx elige de forma predeterminada un rango de direcciones IP dentro del `198.19.0.0/16` rango de direcciones IP. Las direcciones IP flotantes se utilizan para permitir una transición fluida de sus clientes al sistema de archivos en espera en caso de que sea necesaria una conmutación por error. Para obtener más información, consulte Proceso de conmutación por error para FSx para ONTAP.

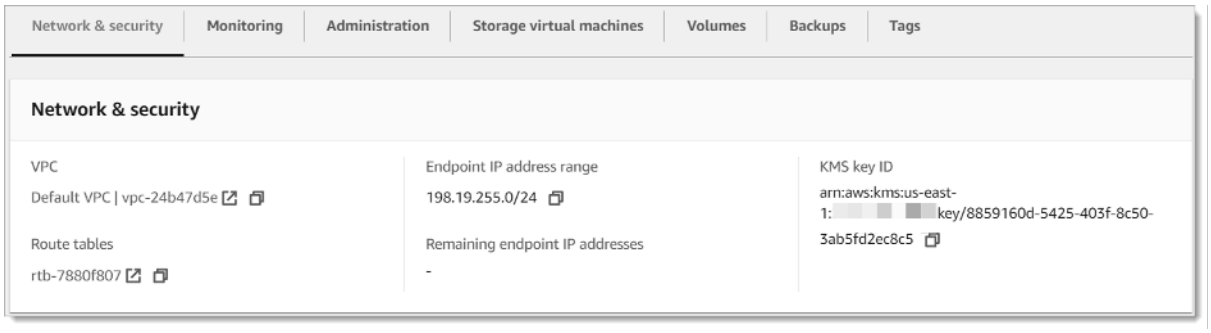
> **Important**
>
> Para acceder a un sistema de archivos Multi-AZ mediante una puerta de enlace de tránsito, cada una de las conexiones de puerta de enlace de tránsito debe crearse en una subred cuya tabla de enrutamiento esté asociada a su sistema de archivos.

AWS Transit Gateway Para configurar el acceso desde fuera de la VPC

Si tienes un sistema de archivos Multi-AZ con un sistema `EndpointIPAddressRange` que se encuentra fuera del rango de CIDR de tu VPC, debes configurar un enrutamiento adicional para acceder AWS Transit Gateway a tu sistema de archivos desde redes interconectadas o locales.

> **Note**
>
> No se requiere ninguna configuración adicional de puerta de enlace de tránsito para los sistemas de archivos Single-AZ o Multi-AZ con una `EndpointIPAddressRange` que se encuentre dentro del rango de direcciones IP de su VPC.

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Elija el sistema de archivos de FSx para ONTAP para el que está configurando el acceso desde una red emparejada.
3. En Red y seguridad, copie el rango de direcciones IP del punto de conexión.



4. Agregue una ruta a la puerta de enlace de tránsito que dirija el tráfico destinado a este rango de direcciones IP a la VPC de su sistema de archivos. Para obtener más información, consulte Uso de las puertas de enlace de tránsito en Guía del usuario de puertas de enlace de tránsito de Amazon VPC.
5. Confirme que puede acceder a su sistema de archivos de FSx para ONTAP desde la red emparejada.

> **Important**
>
> Para acceder a un sistema de archivos Multi-AZ mediante una puerta de enlace de tránsito, cada una de las conexiones de puerta de enlace de tránsito debe crearse en una subred cuya tabla de enrutamiento esté asociada a su sistema de archivos.

Para agregar una tabla de enrutamiento a su sistema de archivos, consulte Actualización de un sistema de archivos.

Acceso a sistemas de archivos Single-AZ

Los sistemas de archivos Single-AZ no tienen el requisito de AWS Transit Gateway utilizarlos para acceder a los datos desde una red local. Los sistemas de archivos Single-AZ se implementan en una sola subred y no se requiere una dirección IP flotante para proporcionar la conmutación por error entre los nodos. En cambio, las direcciones IP a las que accede en los sistemas de archivos Single-AZ se implementan como direcciones IP secundarias dentro del rango CIDR de VPC del sistema de archivos, lo que le permite acceder a sus datos desde otra red sin necesidad de requerir AWS Transit Gateway.

Acceso a los puntos de conexión entre clústeres en las instalaciones

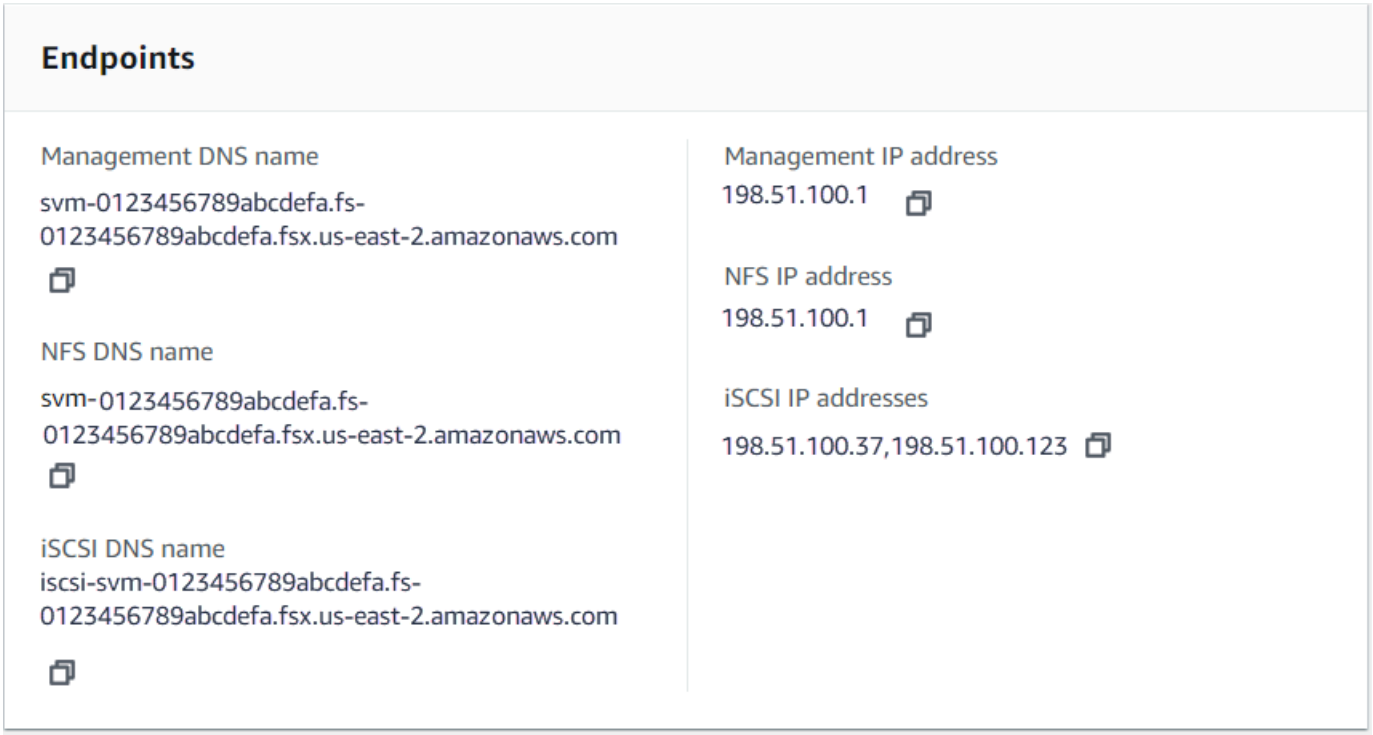
Los puntos finales entre clústeres de FSx para ONTAP están dedicados al tráfico de replicación entre los sistemas de archivos de NetApp ONTAP, incluso entre las implementaciones locales y FSx para ONTAP. NetApp El tráfico de replicación incluye SnapMirror y FlexClone las relaciones entre las máquinas virtuales de almacenamiento (SVM) y los volúmenes de distintos sistemas de archivos y la caché global de archivos. FlexCache NetApp Los puntos de conexión entre clústeres también se utilizan para el tráfico de Active Directory.

Dado que los puntos de conexión entre clústeres de un sistema de archivos utilizan direcciones IP que se encuentran dentro del rango CIDR de la VPC que proporciona al crear su sistema de archivos

de FSx para ONTAP, no es necesario que utilice una puerta de enlace de tránsito para enrutar el tráfico entre clústeres entre el sistema en las instalaciones y el Nube de AWS. Sin embargo, los clientes locales deben seguir utilizando AWS VPN o AWS Direct Connect establecer una conexión segura con su VPC.

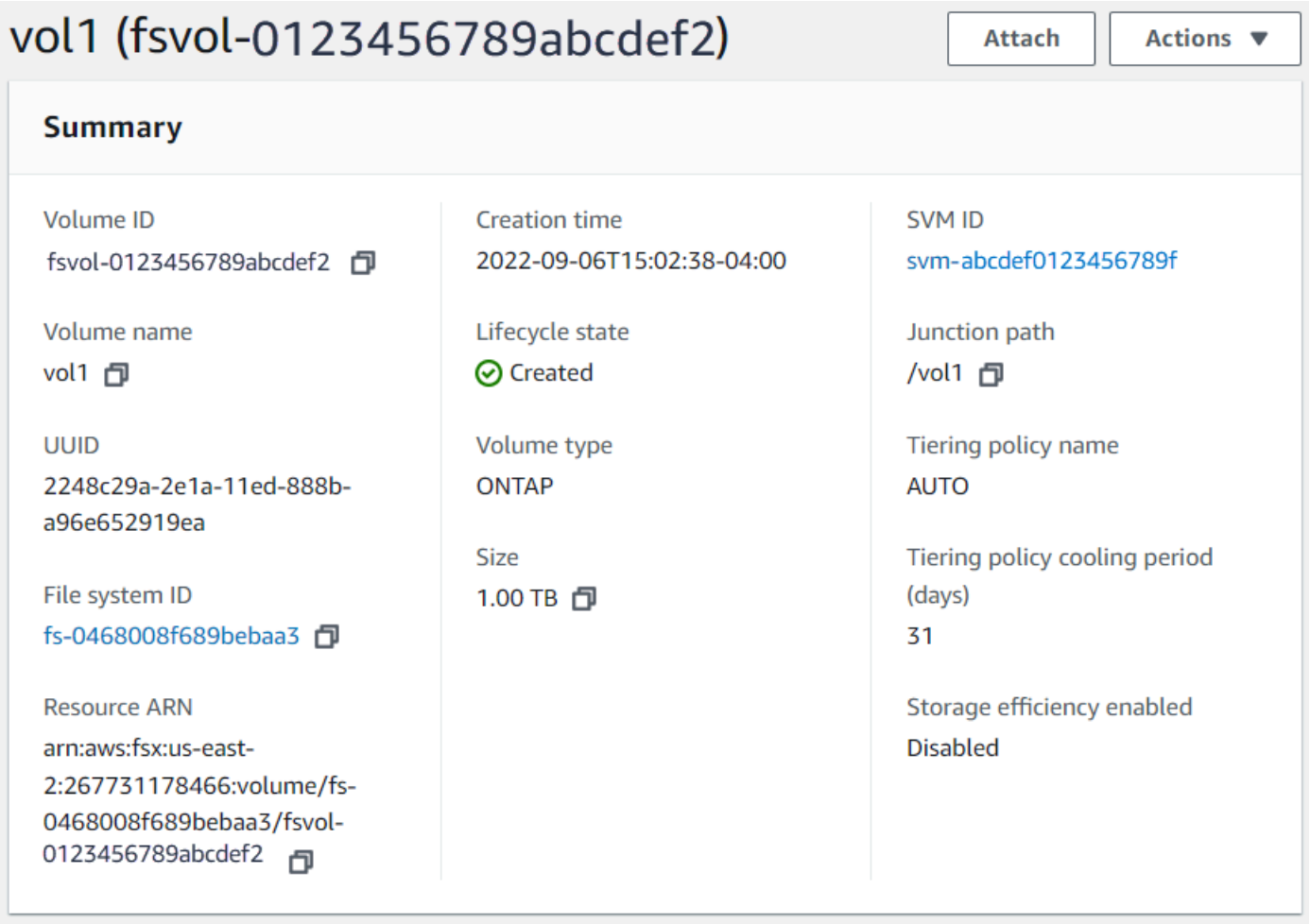
Volúmenes de montaje

Para acceder a los datos de FSx para ONTAP, debe montar un volumen en su cliente. Los comandos de esta sección utilizan el nombre de DNS o la dirección IP de la SVM en la que se ha creado el volumen para montar o adjuntar un volumen. Para encontrar el nombre de DNS y la dirección IP del SVM en la consola de Amazon FSx, seleccione ONTAP > Máquinas virtuales de almacenamiento o en la pestaña Máquina virtual de almacenamiento de la página de Detalles del sistema de archivos para el sistema de archivos, que se muestra en la siguiente imagen.



O bien, puede encontrarlos en la respuesta de la operación de la DescribeStorageVirtualMachinesAPI.

Puede encontrar la ruta de unión de un volumen en la consola de Amazon FSx, en el panel Resumen de la página de detalles del volumen, que se muestra en la siguiente imagen.



Temas

- Montaje en clientes Linux
- Montaje en clientes de Microsoft Windows
- Montaje en clientes macOS

Montaje en clientes Linux

Se recomienda que los volúmenes SVM a los que va a adjuntar los clientes Linux tengan una configuración de estilo de seguridad de `UNIX` o. `mixed` Para obtener más información, consulte Gestión de volúmenes FSx para ONTAP.

> **Note**
>
> De forma predeterminada, los montajes FSx para ONTAP NFS son montajes de `hard`. Para garantizar una conmutación por error fluida en caso de que se produzca, le recomendamos que utilice la opción de montaje de `hard` predeterminada.

Para montar un volumen de ONTAP en un cliente Linux

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Cree o seleccione una instancia de Amazon EC2 que ejecute Amazon Linux 2 y que esté en la misma VPC que el sistema de archivos.

   Para obtener más información sobre el lanzamiento de una instancia de Linux de EC2, consulte Paso 1: Lanzar una instancia en la Guía del usuario de Amazon EC2 para instancias Linux.
3. Conéctese a su instancia de Linux de Amazon EC2. Para obtener más información, consulte Conexión con la instancia de Linux en la Guía del usuario de Amazon EC2 para instancias de Linux.
4. Abra un terminal en su instancia de EC2 mediante un secure shell (SSH) e inicie sesión con las credenciales correspondientes.
5. Cree un directorio en la instancia EC2 para montar el volumen SVM de la siguiente manera:

   ```
   sudo mkdir /fsx
   ```
6. Monte el volumen en el directorio que acaba de crear utilizando el siguiente comando:

   ```
   sudo mount -t nfs svm-dns-name:/volume-junction-path /fsx
   ```

   En el ejemplo siguiente se usan valores de muestra.

   ```
   sudo mount -t nfs svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-
   east-1.amazonaws.com:/vol1 /fsx
   ```

   También puede utilizar la dirección IP SVM del SVM en lugar de su nombre DNS. Recomendamos usar el nombre DNS para montar los clientes en sistemas de archivos escalables, ya que ayuda a garantizar que los clientes estén equilibrados entre los pares de alta disponibilidad (HA) del sistema de archivos.

```
sudo mount -t nfs 198.51.100.1:/vol1 /fsx
```

> **Note**
>
> Para los sistemas de archivos escalables, el protocolo NFS paralelo (pNFS) está habilitado de forma predeterminada y se utiliza de forma predeterminada para cualquier cliente que monte volúmenes con NFS v4.1 o superior.

Usar /etc/fstab para montar automáticamente en el reinicio de la instancia

Para volver a montar automáticamente el volumen FSx para ONTAP cuando se reinicie una instancia de Linux de Amazon EC2, utilice el archivo `/etc/fstab`. El archivo `/etc/fstab` contiene información sobre los sistemas de archivos. El comando `mount -a`, que se ejecuta durante el arranque de la instancia, monta los sistemas de archivos enumerados en `/etc/fstab`.

> **Note**
>
> Los sistemas de archivos de FSx para ONTAP no admiten el montaje automático con `/etc/fstab` en instancias Mac de Amazon EC2.

> **Note**
>
> Antes de poder actualizar el archivo `/etc/fstab` de la instancia EC2, asegúrese de que ya haya creado su sistema de archivos de FSx para ONTAP. Para obtener más información, consulte Creación de FSx para sistemas de archivos ONTAP.

Para actualizar el archivo /etc/fstab en la instancia EC2

1. Conéctese a su instancia EC2:

   - Para conectarse a la instancia desde un equipo que ejecute macOS o Linux, especifique el archivo .pem para su comando SSH. Para ello, use la opción `-i` y la ruta a su clave privada.
   - Para conectarte a tu instancia desde un ordenador con Windows, puedes usar MindTerm o PuTTY. Para usar PuTTY, instálelo y convierta el archivo .pem en un archivo .ppk.

Para obtener más información, consulte los siguientes temas en la Guía del usuario de Amazon EC2 para instancias de Linux:

- Conexión a la instancia de Linux mediante SSH
- Conexión a la instancia Linux desde Windows utilizando PuTTY

2. Cree un directorio local que se utilizará para montar el volumen SVM.

```
sudo mkdir /fsx
```

3. Abra el archivo `/etc/fstab` con el editor que prefiera.
4. Añada la línea siguiente al archivo `/etc/fstab`. Inserte un carácter de tabulación entre cada parámetro. Debe aparecer como una línea sin saltos de línea.

```
svm-dns-name:volume-junction-path /fsx nfs nfsvers=version,defaults 0 0
```

También puede usar la dirección IP del SVM del volumen. Los tres últimos parámetros indican las opciones de NFS (que configuramos como predeterminadas), la descarga del sistema de archivos y la comprobación del sistema de archivos (normalmente no se utilizan, por lo que los configuramos en 0).

5. Guarde los cambios en el archivo.
6. Monte el sistema de recursos compartidos de archivos con el siguiente comando. La próxima vez que se inicie el sistema, la carpeta se montará automáticamente.

```
sudo mount /fsx
sudo mount svm-dns-name:volume-junction-path
```

La instancia EC2 está configurada ahora para montar el volumen de ONTAP cuando se reinicia.

Montaje en clientes de Microsoft Windows

En esta sección se describe cómo acceder a los datos del sistema de archivos de FSx para ONTAP con clientes que ejecutan el sistema operativo Microsoft Windows. Revise los siguientes requisitos, independientemente del tipo de cliente que utilice.

Este procedimiento supone que el cliente y el sistema de archivos están ubicados en la misma VPC y Cuenta de AWS. Si el cliente está ubicado en las instalaciones o en una VPC diferente Cuenta de

AWS, Región de AWS o bien, este procedimiento también supone que ha AWS Transit Gateway configurado una conexión de red dedicada AWS Direct Connect mediante o un túnel privado y seguro mediante. AWS Virtual Private Network Para obtener más información, consulte Acceso a los datos desde fuera de la VPC de implementación.

Se recomienda adjuntar los volúmenes a los clientes de Windows mediante el protocolo SMB.

Requisitos previos

Para acceder a un volumen de almacenamiento de ONTAP mediante un cliente de Microsoft Windows, debe cumplir los siguientes requisitos previos:

- El SVM del volumen que va a adjuntar debe estar unido al Active Directory de su organización o debe utilizar un grupo de trabajo. Para obtener más información sobre unir su SVM a un Active Directory, consulte Administración de FSx para máquinas virtuales de almacenamiento ONTAP. Para obtener más información sobre el uso de grupos de trabajo, consulte la descripción general de la configuración de un servidor SMB en un grupo de trabajo en el Centro de documentación. NetApp
- El volumen que va a adjuntar tiene una configuración de estilo de seguridad de `NTFS` o `mixed`. Para obtener más información, consulte Gestión de volúmenes FSx para ONTAP.

Para adjuntar un volumen de ONTAP a un cliente de Windows mediante SMB y Active Directory

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Cree o seleccione una instancia de Amazon EC2 que ejecute Microsoft Windows y que esté en la misma VPC que el sistema de archivos y unida al mismo Microsoft Active Directory que la SVM del volumen.

   Para obtener más información sobre el lanzamiento de una instancia, consulte Paso 1: Lanzar una instancia en la Guía del usuario de Amazon EC2 para instancias de Windows.

   Para obtener más información sobre unir una SVM a un Active Directory, consulte Administración de FSx para máquinas virtuales de almacenamiento ONTAP.
3. Conéctese a la instancia de Amazon EC2 de Windows. Para obtener más información, consulte Conexión con la instancia de Windows en la Guía del usuario de Amazon EC2 para instancias de Windows.
4. Abra un símbolo del sistema.
5. Ejecute el siguiente comando de la . Sustituya lo siguiente:

- Sustituya `Z:` por cualquier letra disponible a la unidad de disco.
- Sustituya `DNS_NAME` por el nombre de DNS o la dirección IP del punto de conexión de SMB para la SVM del volumen.
- `SHARE_NAME`Sustitúyalo por el nombre de un recurso compartido para pequeñas y medianas empresas. `C$`es el recurso compartido SMB predeterminado en la raíz del espacio de nombres del SVM, pero no debe montarlo, ya que expondría el almacenamiento al volumen raíz y podría provocar interrupciones en la seguridad y el servicio. Debe proporcionar un nombre de recurso compartido SMB para montarlo en lugar de. `C$` Para obtener más información acerca de la creación de SMB compartidos, consulte Gestión de recursos compartidos SMB.

```
net use Z: \\DNS_NAME\SHARE_NAME
```

En el ejemplo siguiente se usan valores de muestra.

```
net use Z: \\corp.example.com\group_share
```

También puede utilizar la dirección IP del SVM en lugar de su nombre de DNS. Recomendamos usar el nombre DNS para montar los clientes en sistemas de archivos escalables, ya que ayuda a garantizar que los clientes estén equilibrados entre los pares de alta disponibilidad (HA) del sistema de archivos.

```
net use Z: \\198.51.100.5\group_share
```

Montaje en clientes macOS

En esta sección se describe cómo acceder a los datos del sistema de archivos de FSx para ONTAP con clientes que ejecutan el sistema operativo macOS. Revise los siguientes requisitos, independientemente del tipo de cliente que utilice.

Este procedimiento supone que el cliente y el sistema de archivos están ubicados en la misma VPC y Cuenta de AWS. Si el cliente está ubicado en las instalaciones o en una VPC diferente Cuenta de AWS , Región de AWS o si ha AWS Transit Gateway configurado una conexión de red dedicada o un túnel privado y seguro AWS Direct Connect mediante. AWS Virtual Private Network Para obtener más información, consulte Acceso a los datos desde fuera de la VPC de implementación.

Se recomienda adjuntar los volúmenes a los clientes de Mac mediante el protocolo SMB.

Para montar un volumen ONTAP en un cliente de macOS mediante SMB

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Cree o seleccione una instancia de Amazon EC2 Mac que ejecute macOS y que esté en la misma VPC que el sistema de archivos.

   Para obtener más información sobre el lanzamiento de una instancia, consulte Paso 1: Lanzar una instancia en la Guía del usuario de Amazon EC2 para instancias Linux.
3. Conecte a su instancia de Amazon EC2 Mac. Para obtener más información, consulte Conexión con la instancia de Linux en la Guía del usuario de Amazon EC2 para instancias de Linux.
4. Abra un terminal en su instancia de EC2 mediante un secure shell (SSH) e inicie sesión con las credenciales correspondientes.
5. Cree un directorio en la instancia EC2 para montar el volumen de la siguiente manera:

   ```
   sudo mkdir /fsx
   ```
6. Monte el volumen con el siguiente comando.

   ```
   sudo mount -t smbfs filesystem-dns-name:/smb-share-name mount-point
   ```

   En el ejemplo siguiente se usan valores de muestra.

   ```
   sudo mount -t smbfs svm-01234567890abcde2.fs-01234567890abcde5.fsx.us-
   east-1.amazonaws.com:/C$ /fsx
   ```

   También puede utilizar la dirección IP del SVM en lugar de su nombre de DNS. Recomendamos usar el nombre DNS para montar los clientes en sistemas de archivos escalables, ya que ayuda a garantizar que los clientes estén equilibrados entre los pares de alta disponibilidad (HA) del sistema de archivos.

   ```
   sudo mount -t smbfs 198.51.100.10:/C$ /fsx
   ```

   `C$` es el recurso compartido SMB predeterminado que puede montar para ver la raíz del espacio de nombres del SVM. Si ha creado algún bloque de mensajes de servidor (SMB) compartido en su SVM, proporcione los nombres del recurso compartido SMB en lugar de `C$`. Para obtener

más información acerca de la creación de SMB compartidos, consulte Gestión de recursos compartidos SMB.

Para montar un volumen ONTAP en un cliente de macOS mediante NFS

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Cree o seleccione una instancia de Amazon EC2 que ejecute Amazon Linux 2 y que esté en la misma VPC que el sistema de archivos.

   Para obtener más información sobre el lanzamiento de una instancia de Linux de EC2, consulte Paso 1: Lanzar una instancia en la Guía del usuario de Amazon EC2 para instancias Linux.
3. Conéctese a su instancia de Linux de Amazon EC2. Para obtener más información, consulte Conexión con la instancia de Linux en la Guía del usuario de Amazon EC2 para instancias de Linux.
4. Monte su volumen FSx para ONTAP en la instancia EC2 de Linux mediante un script de datos de usuario durante el lanzamiento de la instancia o ejecutando los siguientes comandos:

   ```
   sudo mount -t nfs -o nfsvers=NFS_version svm-dns-name:/volume-junction-path /mount-point
   ```

   En el ejemplo siguiente se usan valores de muestra.

   ```
   sudo mount -t nfs -o nfsvers=4.1
    svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /
   fsxontap
   ```

   También puede utilizar la dirección IP SVM del SVM en lugar de su nombre DNS. Recomendamos usar el nombre DNS para montar los clientes en sistemas de archivos escalables, ya que ayuda a garantizar que los clientes estén equilibrados entre los pares de alta disponibilidad del sistema de archivos.

   ```
   sudo mount -t nfs -o nfsvers=4.1 198.51.100.1:/vol1 /fsxontap
   ```
5. Monte el volumen en el directorio que acaba de crear utilizando el siguiente comando.

   ```
   sudo mount -t nfs svm-dns-name:/volume-junction-path /fsx
   ```

En el ejemplo siguiente se usan valores de muestra.

```
sudo mount -t nfs svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-
east-1.amazonaws.com:/vol1 /fsx
```

También puede utilizar la dirección IP SVM del SVM en lugar de su nombre DNS. Recomendamos usar el nombre DNS para montar los clientes en sistemas de archivos escalables, ya que ayuda a garantizar que los clientes estén equilibrados entre los pares de alta disponibilidad (HA) del sistema de archivos.

```
sudo mount -t nfs 198.51.100.1:/vol1 /fsx
```

Montaje de LUNs iSCSI

Amazon FSx para NetApp ONTAP ofrece soporte de almacenamiento en bloque compartido a través del protocolo iSCSI (Interfaz de sistemas informáticos pequeños de Internet). Puede habilitar el almacenamiento iSCSI mediante el aprovisionamiento de LUNs (número de unidad lógica) y su asignación a grupos de iniciadores (igrupos), exponiendo el almacenamiento en bloque a sus hosts Linux y Windows.

> **Note**
>
> El protocolo iSCSI no es compatible con FSx para los sistemas de archivos escalables de ONTAP, que son sistemas de archivos con más de un par de servidores de archivos de alta disponibilidad (HA).

Temas

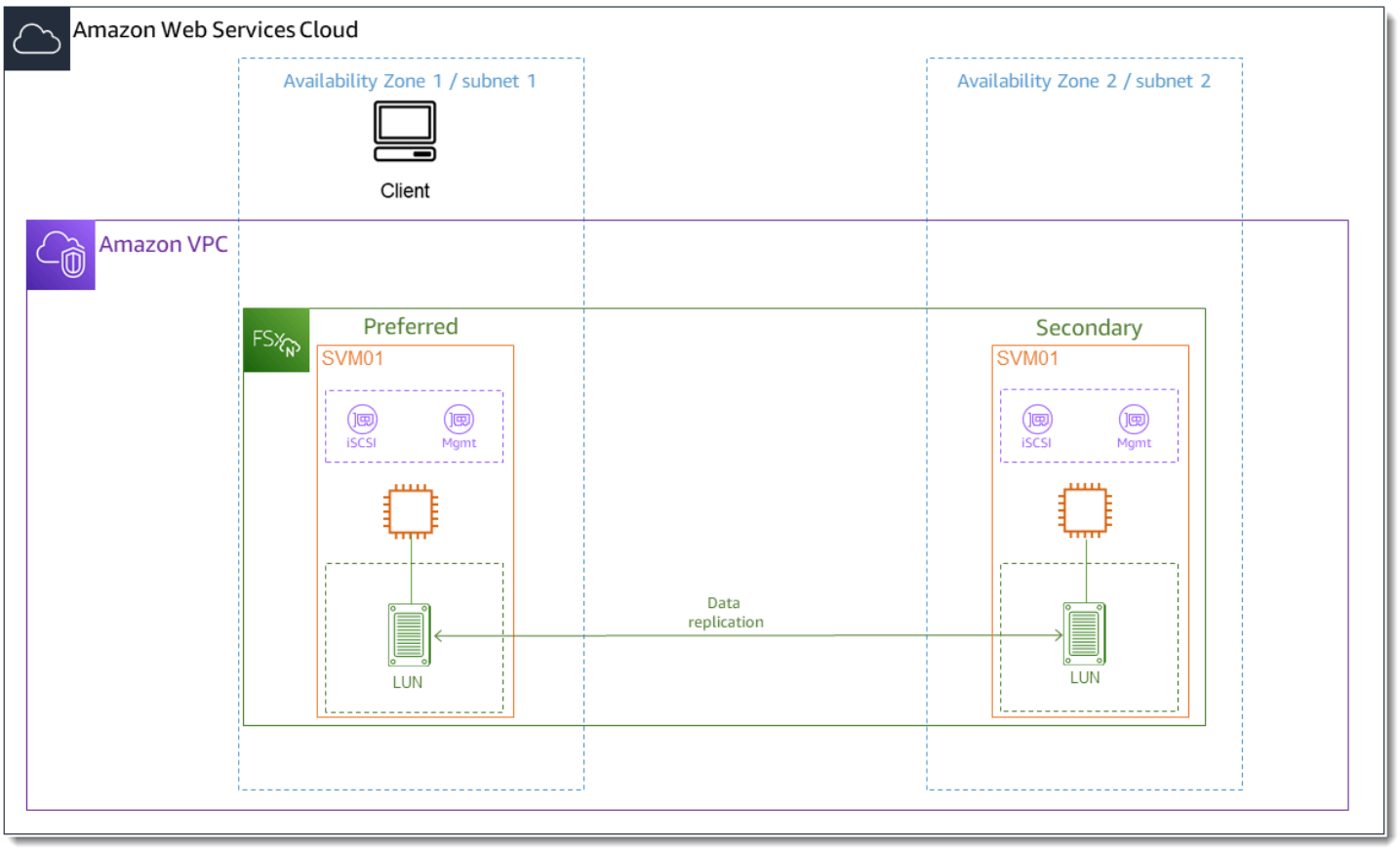
Montaje de LUNs iSCSI en un cliente Linux

Los ejemplos que se presentan en estos procedimientos utilizan la siguiente configuración:

- El LUN iSCSI que se va a montar en el host Linux ya está creado. Para obtener más información, consulte Creación de un iSCSI LUN.
- El host de Linux que está montando el LUN iSCSI es una instancia de Amazon EC2 que se ejecuta en la Imagen de máquina de Amazon (AMI) de Amazon Linux 2. Cuenta con grupos de seguridad de VPC configurados para permitir el tráfico entrante y saliente, tal y como se describe en Control de acceso al sistema de archivos con Amazon VPC.
- El host Linux y el sistema de archivos de FSx para ONTAP están ubicados en la misma VPC y Cuenta de AWS. Si el host está ubicado en otra VPC, puede utilizar el emparejamiento de VPC o conceder AWS Transit Gateway a otras VPC el acceso a los puntos finales iSCSI del volumen. Para obtener más información, consulte Acceso a los datos desde fuera de la VPC de implementación.

  Si utiliza una instancia EC2 que ejecuta una AMI de Linux diferente, es posible que algunas de las utilidades que se instalan en el host estén preinstaladas y que utilice comandos diferentes para instalar los paquetes necesarios. Además de instalar los paquetes, los comandos utilizados en esta sección son válidos para otras AMI Linux de EC2.

  Se recomienda que la instancia EC2 se encuentre en la misma zona de disponibilidad que la subred preferida del sistema de archivos, como se muestra en el siguiente gráfico.



Temas

- Instalar y configurar iSCSI en el cliente Linux
- Configuración de iSCSI en el sistema de archivos de FSx para ONTAP
- Monte un LUN iSCSI en su cliente Linux

Instalar y configurar iSCSI en el cliente Linux

Para instalar el cliente iSCSI

1. Confirme que `iscsi-initiator-utils` y `device-mapper-multipath` están instalados en su dispositivo Linux. Conexión a la instancia de Linux mediante un cliente SSH. Para más información, consulte Conectarse a su instancia Linux mediante SSH.
2. Instale `multipath` el cliente iSCSI mediante el siguiente comando. La instalación de `multipath` es necesaria si desea realizar una conmutación por error automática entre los servidores de archivos.

```
~$ sudo yum install -y device-mapper-multipath iscsi-initiator-utils
```

3. Para facilitar una respuesta más rápida al conmutar automáticamente entre servidores de archivos cuando se utiliza `multipath`, establezca el valor de tiempo de espera de sustitución en el archivo `/etc/iscsi/iscsid.conf` en un valor de `5` en lugar de utilizar el valor predeterminado de `120`.

```
~$ sudo sed -i 's/node.session.timeo.replacement_timeout = .*/
node.session.timeo.replacement_timeout = 5/' /etc/iscsi/iscsid.conf; sudo cat /etc/
iscsi/iscsid.conf | grep node.session.timeo.replacement_timeout
```

4. Inicie el servicio iSCSI.

```
~$ sudo service iscsid start
```

Tenga en cuenta que, según su versión de Linux, puede que tenga que usar este comando en su lugar:

```
~$ sudo systemctl start iscsid
```

5. Confirme que el servicio se está ejecutando mediante el siguiente comando.

```
~$ sudo systemctl status iscsid.service
```

El sistema responde con el siguiente resultado:

```
iscsid.service - Open-iSCSI
    Loaded: loaded (/usr/lib/systemd/system/iscsid.service; disabled; vendor
 preset: disabled)
    Active: active (running) since Fri 2021-09-02 00:00:00 UTC; 1min ago
    Docs: man:iscsid(8)
    man:iscsiadm(8)
    Process: 14658 ExecStart=/usr/sbin/iscsid (code=exited, status=0/SUCCESS)
    Main PID: 14660 (iscsid)
    CGroup: /system.slice/iscsid.service
    ##14659 /usr/sbin/iscsid
    ##14660 /usr/sbin/iscsid
```

Para configurar iSCSI en su cliente Linux

1. Para permitir que sus clientes realicen la conmutación por error automática entre sus servidores de archivos, debe configurar la multiruta. Utilice el siguiente comando:

```
~$ sudo mpathconf --enable --with_multipathd y
```

2. Determine el nombre del iniciador de su host de Linux con el siguiente comando. La ubicación del nombre del iniciador depende de la utilidad iSCSI. Si está utilizando `iscsi-initiator-utils`, el nombre del iniciador se encuentra en el archivo `/etc/iscsi/initiatorname.iscsi`.

```
~$ sudo cat /etc/iscsi/initiatorname.iscsi
```

El sistema responde con el nombre del iniciador.

```
InitiatorName=iqn.1994-05.com.redhat:abcdef12345
```

Configuración de iSCSI en el sistema de archivos de FSx para ONTAP

1. Conéctese a la CLI de NetApp ONTAP del sistema de archivos FSx para ONTAP en el que creó el LUN iSCSI mediante el siguiente comando. Para obtener más información, consulte Uso de la NetApp ONTAP CLI.

```
~$ ssh fsxadmin@your_management_endpoint_ip
```

2. Cree el grupo iniciador (`igroup`) mediante el comando NetApp lun igroup createCLI de ONTAP. Un grupo de iniciadores se asigna a los LUNs iSCSI y controla qué iniciadores (clientes) tienen acceso a los LUNs. Reemplace `host_initiator_name` con el nombre del iniciador de su host Linux que recuperó en el procedimiento anterior.

```
::> lun igroup create -vserver svm_name -igroup igroup_name -
initiator host_initiator_name -protocol iscsi -ostype linux
```

Si desea que los LUNs asignados a este igroup estén disponibles para varios hosts, puede especificar varios nombres de iniciadores separados por una coma. Para obtener más información, consulte lun igroup create en el Centro de documentación de ONTAP. NetApp

3. Confirme que existe `igroup` con el comando: lun igroup show

```
::> lun igroup show
```

El sistema responde con el siguiente resultado:

```
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
svm_name  igroup_name  iscsi    linux    iqn.1994-05.com.redhat:abcdef12345
```

4. Este paso supone que ya ha creado un iSCSI LUN. Si no lo ha hecho, consulte step-by-step las instrucciones Creación de un iSCSI LUN para hacerlo.

Cree un mapeo desde el LUN que creó hasta el igroup que creó, utilizando lun mapping create y especificando los siguientes atributos:

- *svm_name*: el nombre de la máquina virtual de almacenamiento que proporciona el destino iSCSI. El host usa este valor para llegar al LUN.
- *vol_name*: el nombre del volumen que aloja el LUN.
- *lun_name*: El nombre que ha asignado al servicio.
- *igroup_name*: el nombre del grupo iniciador.
- *lun_id*: el número entero del ID del LUN es específico de la asignación, no del propio LUN. Los iniciadores del igroup lo utilizan como número de unidad lógica. Utilice este valor para el iniciador al acceder al almacenamiento.

```
::> lun mapping create -vserver svm_name -path /vol/vol_name/lun_name -
igroup igroup_name -lun-id lun_id
```

5. Use el comando `lun show -path` para confirmar que el LUN está creado, en línea y mapeado.

```
::> lun show -path /vol/vol_name/lun_name -fields state,mapped,serial-hex
```

El sistema responde con el siguiente resultado:

```
 Vserver    Path                            serial-hex              state    mapped
 --------- ------------------------------- ----------------------- --------
 --------
```

```
 svm_name  /vol/vol_name/lun_name          6c5742314e5d52766e796150 online   mapped
```

Guarde el valor `serial_hex` (en este ejemplo, es `6c5742314e5d52766e796150`) y lo usará en un paso posterior para crear un nombre descriptivo para el dispositivo de bloques.

6. Utilice el comando `network interface show -vserver` para recuperar las direcciones del `iscsi_1` y las interfaces `iscsi_2` de la SVM en la que creó el LUN iSCSI.

```
::> network interface show -vserver svm_name
```

El sistema responde con el siguiente resultado:

```
            Logical               Status     Network            Current
        Current Is
Vserver     Interface             Admin/Oper Address/Mask       Node
        Port    Home
----------- ----------            ---------- ------------------ -------------
        ------- ----
svm_name
            iscsi_1               up/up      172.31.0.143/20
 FSxId0123456789abcdef8-01  e0e     true
            iscsi_2               up/up      172.31.21.81/20
 FSxId0123456789abcdef8-02  e0e     true
            nfs_smb_management_1
                                  up/up      198.19.250.177/20
 FSxId0123456789abcdef8-01  e0e     true
3 entries were displayed.
```

En este ejemplo, la dirección IP de `iscsi_1` es `172.31.0.143` y `iscsi_2` es`172.31.21.81`.

Monte un LUN iSCSI en su cliente Linux

1. En su cliente Linux, utilice el siguiente comando para detectar los nodos iSCSI de destino con la dirección IP de `iscsi_1` *iSCSI_1_IP*.

```
~$ sudo iscsiadm --mode discovery --op update --type sendtargets --
portal iscsi_1_IP
```

```
172.31.0.143:3260,1029
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3
```

```
172.31.21.81:3260,1028
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3
```

En este ejemplo, `iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3` corresponde al `target_initiator` para LUN iSCSI de la zona de disponibilidad preferida.

2. (Opcional) Puede establecer sesiones adicionales con `target_initiator`. Amazon EC2 tiene un límite de ancho de banda de 5 Gb/s (~625 MB/s) para el tráfico de flujo único, pero puede crear varias sesiones para impulsar niveles más altos de rendimiento en su sistema de archivos desde un solo cliente. Para obtener más información, consulte Ancho de banda de la red de instancias de Amazon EC2 en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux.

   El siguiente comando establece 8 sesiones por iniciador por nodo ONTAP en cada zona de disponibilidad, lo que permite al cliente transferir hasta 40 Gb/s (5000 MB/s) de rendimiento total al LUN iSCSI.

   ```
   ~$ sudo iscsiadm --mode node -T target_initiator --op update -n
    node.session.nr_sessions -v 8
   ```

3. Inicie sesión en los iniciadores de destino. Los LUNs iSCSI se presentan como discos disponibles.

   ```
   ~$ sudo iscsiadm --mode node -T target_initiator --login
   ```

   ```
   Logging in to [iface: default, target:
    iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3, portal:
    172.31.14.66,3260] (multiple)
   Login to [iface: default, target:
    iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3, portal:
    172.31.14.66,3260] successful.
   ```

   El resultado anterior está truncado; debería ver una respuesta `Logging in` y `Login successful` una para cada sesión en cada servidor de archivos. En el caso de 4 sesiones por nodo, habrá 8 `Logging in` y 8 respuestas `Login successful`.

4. Utilice el siguiente comando para comprobar que `dm-multipath` ha identificado y fusionado las sesiones iSCSI mostrando un único LUN con varias políticas. Debe haber un número igual de dispositivos listados como `active` y de aquellos listados como `enabled`.

```
~$ sudo multipath -ll
```

En la salida, el nombre del disco se formatea como `dm-xyz`, donde `xyz` es un número entero. Si no hay otros discos de rutas múltiples, este valor es `dm-0`.

```
3600a09806c5742314e5d52766e79614f dm-xyz NETAPP  ,LUN C-Mode
size=10G features='4 queue_if_no_path pg_init_retries 50 retain_attached_hw_handle'
 hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| |- 0:0:0:1 sda     8:0   active ready running
| |- 1:0:0:1 sdc     8:32  active ready running
| |- 3:0:0:1 sdg     8:96  active ready running
| `- 4:0:0:1 sdh     8:112 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- 2:0:0:1 sdb     8:16  active ready running
  |- 7:0:0:1 sdf     8:80  active ready running
  |- 6:0:0:1 sde     8:64  active ready running
  `- 5:0:0:1 sdd     8:48  active ready running
```

Su dispositivo de bloques ahora está conectado a su cliente Linux. Se encuentra debajo de la ruta `/dev/dm-xyz`. No debe usar esta ruta con fines administrativos; en su lugar, utilice el enlace simbólico que se encuentra debajo de la ruta `/dev/mapper/wwid`, donde *`wwid`* es un identificador único para su LUN que sea coherente en todos los dispositivos. En el siguiente paso, proporcionará un nombre descriptivo para el *`wwid`* para que pueda distinguirlo de otros discos con múltiples rutas.

Para asignar un nombre descriptivo al dispositivo de bloques

1. Para darle a su dispositivo un nombre descriptivo, cree un alias en el archivo `/etc/multipath.conf`. Para ello, agregue la siguiente entrada al archivo utilizando el editor de texto que prefiera y sustituya los siguientes marcadores:

   - Reemplace `serial_hex` por el valor que guardó en el procedimiento Configuración de iSCSI en el sistema de archivos de FSx para ONTAP.
   - Añada el prefijo `3600a0980` al valor `serial_hex`, tal y como se muestra en el ejemplo. Este es un preámbulo exclusivo de la distribución NetApp ONTAP que utiliza Amazon FSx for ONTAP. NetApp

- Reemplace `device_name` por el nombre descriptivo que desee utilizar para su dispositivo.

```
multipaths {
    multipath {
        wwid 3600a0980serial_hex
        alias device_name
    }
}
```

Como alternativa, puede copiar y guardar el siguiente script como un archivo bash, por ejemplo `multipath_alias.sh`. Puede ejecutar el script con los privilegios de sudo, reemplace *`serial_hex`* (sin el prefijo 3600a0980) y *`device_name`* por su número de serie respectivo y con el nombre descriptivo que desee. Este script busca una sección `multipaths` no comentada en el archivo `/etc/multipath.conf`. Si existe, añade una entrada `multipath` a esa sección; de lo contrario, creará una nueva sección `multipaths` con una entrada `multipath` para el dispositivo de bloques.

```
#!/bin/bash
SN=serial_hex
ALIAS=device_name
CONF=/etc/multipath.conf
grep -q '^multipaths {' $CONF
UNCOMMENTED=$?
if [ $UNCOMMENTED -eq 0 ]
then
        sed -i '/^multipaths {/a\\tmultipath {\n\t\twwid 3600a0980'"${SN}"'\n\t
\talias '"${ALIAS}"'\n\t}\n' $CONF
else
        printf "multipaths {\n\tmultipath {\n\t\twwid 3600a0980$SN\n\t\talias
 $ALIAS\n\t}\n}" >> $CONF
fi
```

2. Reinicie el servicio `multipathd` para que los cambios `/etc/multipathd.conf` surtan efecto.

```
~$ systemctl restart multipathd.service
```

Para particionar el LUN

El siguiente paso es formatear y particionar el LUN con `fdisk`.

1. Utilice el siguiente comando para verificar que la ruta a su `device_name` está presente.

```
~$ ls /dev/mapper/device_name
```

```
/dev/device_name
```

2. Particione el disco usando `fdisk`. Ingresará un mensaje interactivo. Ingrese las opciones en el orden que se muestra. Tenga en cuenta que el valor `Last sector` variará según el tamaño del LUN iSCSI (10 GB en este ejemplo). Puede crear varias particiones utilizando un valor menor que el último sector (`20971519` en este ejemplo).

```
~$ sudo fdisk /dev/mapper/device_name
```

Se inicia el mensaje interactivo `fsdisk`.

```
Welcome to fdisk (util-linux 2.30.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0x66595cb0.

Command (m for help): n
Partition type
   p primary (0 primary, 0 extended, 4 free)
   e extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-20971519, default 2048): 2048
Last sector, +sectors or +size{K,M,G,T,P} (2048-20971519, default
 20971519): 20971519

Created a new partition 1 of type 'Linux' and of size 512 B.
Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.
```

Tras ingresar `w`, la nueva partición `/dev/mapper/`*`partition_name`* estará disponible. El *`partition_name`* tiene el formato *`<device_name><partition_number>`*. 1 se utilizó como el número de partición utilizado en el `fdisk` comando en el paso anterior.

3. Cree su sistema de archivos con `/dev/mapper/`*`partition_name`* como ruta.

```
~$ sudo mkfs.ext4 /dev/mapper/partition_name
```

El sistema responde con el siguiente resultado:

```
mke2fs 1.42.9 (28-Dec-2013)
Discarding device blocks: done
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=16 blocks
655360 inodes, 2621184 blocks
131059 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677952
80 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
     32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632
Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

Para montar el LUN en el cliente Linux

1. Cree un directorio *`directory_path`* como punto de montaje para su sistema de archivos.

```
~$ sudo mkdir /directory_path/mount_point
```

2. Monte el sistema de archivos utilizando el siguiente comando.

```
~$ sudo mount -t ext4 /dev/mapper/partition_name /directory_path/mount_point
```

3. (Opcional) Puede cambiar la propiedad del directorio de montaje a su usuario. Reemplace *username* por su nombre de usuario.

```
~$ sudo chown username:username /directory_path/mount_point
```

4. (Opcional) Compruebe que puede leer y escribir datos en el sistema de archivos.

```
~$ echo "Hello world!" > /directory_path/mount_point/HelloWorld.txt
~$ cat directory_path/HelloWorld.txt
Hello world!
```

Ha creado y montado correctamente un LUN iSCSI en su cliente Linux.

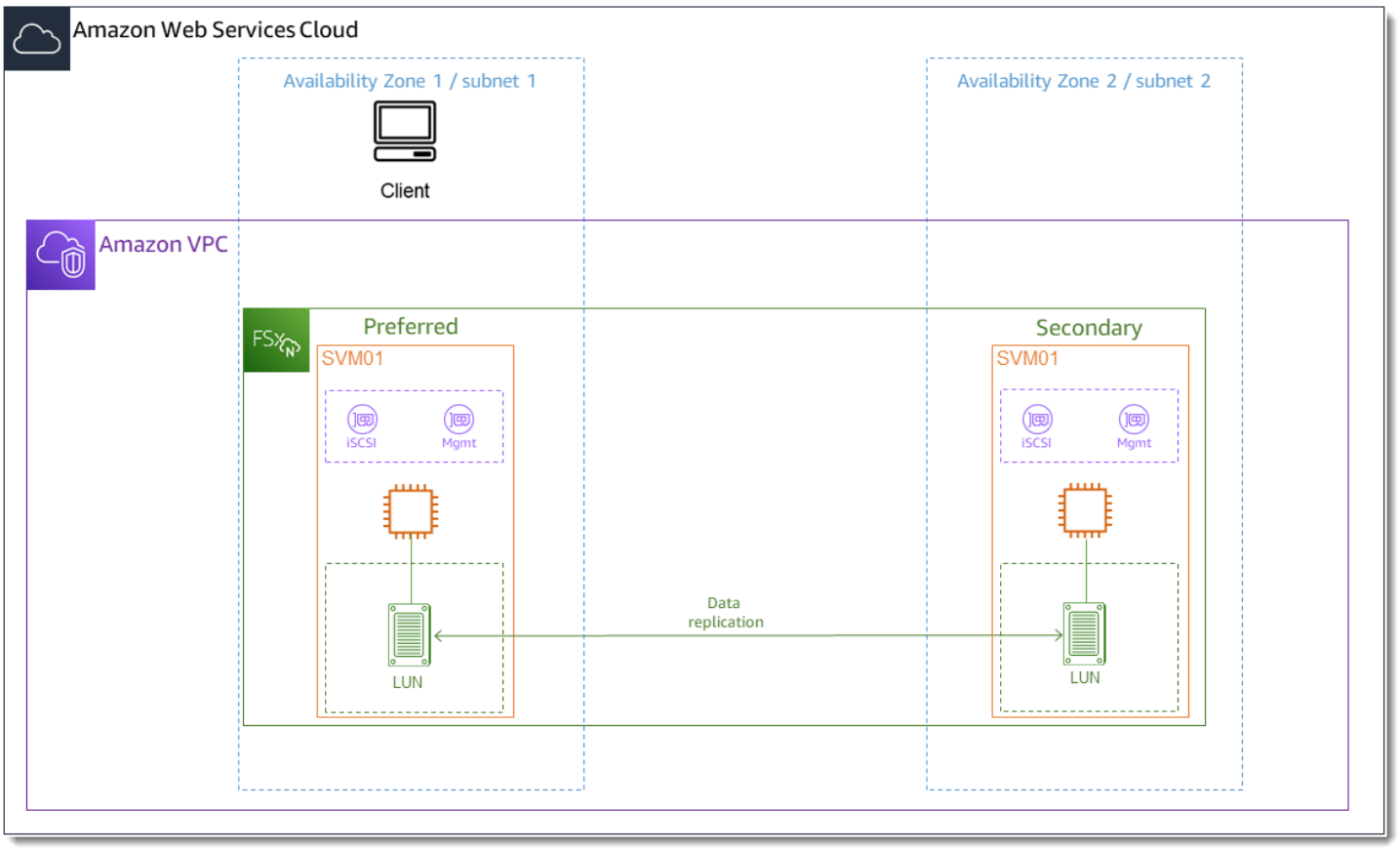
Montaje de LUNs iSCSI en un cliente de Windows

Los ejemplos que se presentan en estos procedimientos utilizan la siguiente configuración:

- El LUN iSCSI que se va a montar en un host de Windows ya está creado. Para obtener más información, consulte Creación de un iSCSI LUN.
- El host de Microsoft Windows que monta el LUN iSCSI es una instancia de Amazon EC2 que ejecuta una Imagen de máquina de Amazon (AMI) de Microsoft Windows Server 2019. Cuenta con grupos de seguridad de VPC configurados para permitir el tráfico entrante y saliente, tal y como se describe en Control de acceso al sistema de archivos con Amazon VPC.

  Puede que esté utilizando una AMI de Microsoft Windows diferente en su configuración.
- El cliente y el sistema de archivos están ubicados en la misma VPC y Cuenta de AWS. Si el cliente está ubicado en otra VPC, puede utilizar el emparejamiento de VPC o conceder AWS Transit Gateway a otras VPC el acceso a los puntos finales iSCSI. Para obtener más información, consulte Acceso a los datos desde fuera de la VPC de implementación.

  Recomendamos que la instancia EC2 esté en la misma zona de disponibilidad que la subred preferida del sistema de archivos, como se muestra en el siguiente gráfico.



Temas

- Configurar iSCSI en el cliente de Windows
- Configuración de iSCSI en el sistema de archivos de FSx para ONTAP
- Montar un LUN iSCSI en el cliente de Windows

Configurar iSCSI en el cliente de Windows

1. Utilice el escritorio remoto de Windows para conectarse al cliente de Windows en el que desee montar el LUN iSCSI. Para obtener más información, consulte Conectarse a su instancia de Windows con RDP en la Guía del usuario de Amazon Elastic Compute Cloud.
2. Abra una ventana de Windows como administrador. PowerShell Use los siguientes comandos para habilitar iSCSI en la instancia de Windows y configurar el servicio iSCSI para que se inicie automáticamente.

```
PS C:\> Start-Service MSiSCSI
PS C:\> Set-Service -Name msiscsi -StartupType Automatic
```

3. Recupera el nombre del iniciador de la instancia de Windows. Utilizará este valor para configurar iSCSI en el sistema de archivos FSx para ONTAP mediante la CLI de ONTAP. NetApp

```
PS C:\> (Get-InitiatorPort).NodeAddress
```

El sistema responde con el puerto iniciador:

```
iqn.1991-05.com.microsoft:ec2amaz-abc123d
```

4. Para permitir que sus clientes realicen automáticamente la conmutación por error entre sus servidores de archivos, necesita instalar `Multipath-IO` (MPIO) en su instancia de Windows. Utilice el siguiente comando:

```
PS C:\> Install-WindowsFeature Multipath-IO
```

5. Reinicia la instancia de Windows una vez finalizada la instalación de `Multipath-IO`. Mantenga abierta la instancia de Windows para realizar los pasos de montaje del LUN iSCSI que se describen en la siguiente sección.

Configuración de iSCSI en el sistema de archivos de FSx para ONTAP

1. Conéctese a la CLI de NetApp ONTAP del sistema de archivos FSx para ONTAP en el que creó el LUN iSCSI mediante el siguiente comando. Para obtener más información, consulte Uso de la NetApp ONTAP CLI.

```
~$ ssh fsxadmin@your_management_endpoint_ip
```

2. Mediante la CLI de NetApp ONTAP lun igroup create, cree el grupo de iniciadores o. `igroup` Un grupo de iniciadores se asigna a los LUNs iSCSI y controla qué iniciadores (clientes) tienen acceso a los LUNs. Reemplace `host_initiator_name` por el nombre del iniciador del host de Windows que recuperaste en el procedimiento anterior.

```
::> lun igroup create -vserver svm_name -igroup igroup_name -
initiator host_initiator_name -protocol iscsi -ostype windows
```

Si desea que los LUNs asignados al `igroup` estén disponibles para varios hosts, puede especificar varios nombres de iniciadores separados por comas. Para obtener más información, consulte el Centro `lun igroup create`de documentación de NetApp ONTAP.

3. Confirme que `igroup` se ha creado correctamente utilizando el siguiente comando:

```
::> lun igroup show
```

El sistema responde con el siguiente resultado:

```
Vserver    Igroup        Protocol OS Type  Initiators
---------  ------------  -------- -------- ------------------------------------
svm_name   igroup_name   iscsi    windows  iqn.1994-05.com.windows:abcdef12345
```

Una vez creado el `igroup`, está listo para crear LUNs y asignarlos al `igroup`.

4. Este paso supone que ya ha creado un iSCSI LUN. Si no lo ha hecho, consulte step-by-step las instrucciones Creación de un iSCSI LUN para hacerlo.

Cree un mapeo de LUN desde el LUN al nuevo `igroup`.

```
::> lun mapping create -vserver svm_name -path /vol/vol_name/lun_name -
igroup igroup_name -lun-id lun_id
```

5. Confirme que el LUN está creado, en línea y mapeado con el siguiente comando:

```
::> lun show -path /vol/vol_name/lun_name
Vserver     Path                            State   Mapped   Type     Size
---------   ------------------------------- ------- -------- -------- --------
svm_name    /vol/vol_name/lun_name          online  mapped   windows  10GB
```

Ahora está listo para añadir el destino iSCSI a su instancia de Windows.

6. Recupere las direcciones IP de las interfaces `iscsi_1` y `iscsi_2` de la SVM mediante el siguiente comando:

```
::> network interface show -vserver svm_name
```

```
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
svm_name
            iscsi_1    up/up      172.31.0.143/20    FSxId0123456789abcdef8-01
                                                                   e0e     true
            iscsi_2    up/up      172.31.21.81/20    FSxId0123456789abcdef8-02
```

```
                                                                    e0e     true
            nfs_smb_management_1
                       up/up      198.19.250.177/20  FSxId0123456789abcdef8-01
                                                                    e0e     true
3 entries were displayed.
```

En este ejemplo, la dirección IP de `iscsi_1` es `172.31.0.143` y `iscsi_2` es `172.31.21.81`.

Montar un LUN iSCSI en el cliente de Windows

1. En su instancia de Windows, abra un PowerShell terminal como administrador.
2. Creará un script `.ps1` que hace lo siguiente:

   - Se conecta a cada una de las interfaces iSCSI del sistema de archivos.
   - Agrega y configura MPIO para iSCSI.
   - Establece 8 sesiones para cada conexión iSCSI, lo que permite al cliente impulsar hasta 40 Gb/s (5000 MB/s) de rendimiento total al LUN iSCSI. Tener 8 sesiones garantiza que un solo cliente pueda impulsar la capacidad de rendimiento total de 4000 MB/s para obtener la capacidad de rendimiento de FSx for ONTAP del más alto nivel. Opcionalmente, puede cambiar el número de sesiones a un número superior o inferior (cada sesión proporciona hasta 625 MB/s de rendimiento) modificando el bucle for del script en el paso `#Establish iSCSI connection` de `1..8` a otro límite superior. Para obtener más información, consulte Ancho de banda de la red de instancias de Amazon EC2 en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Windows.

   Copie el siguiente conjunto de comandos en un archivo para crear el script `.psl`.

   - Reemplace `iscsi_1` y `iscsi_2` por las direcciones IP recuperadas en el paso anterior.
   - Reemplace `ec2_ip` por la dirección IP pública de la instancia de Windows.

```
#iSCSI IP addresses for Preferred and Standby subnets
$TargetPortalAddresses = @("iscsi_1","iscsi_2")

#iSCSI Initator IP Address (Local node IP address)
$LocaliSCSIAddress = "ec2_ip"
```

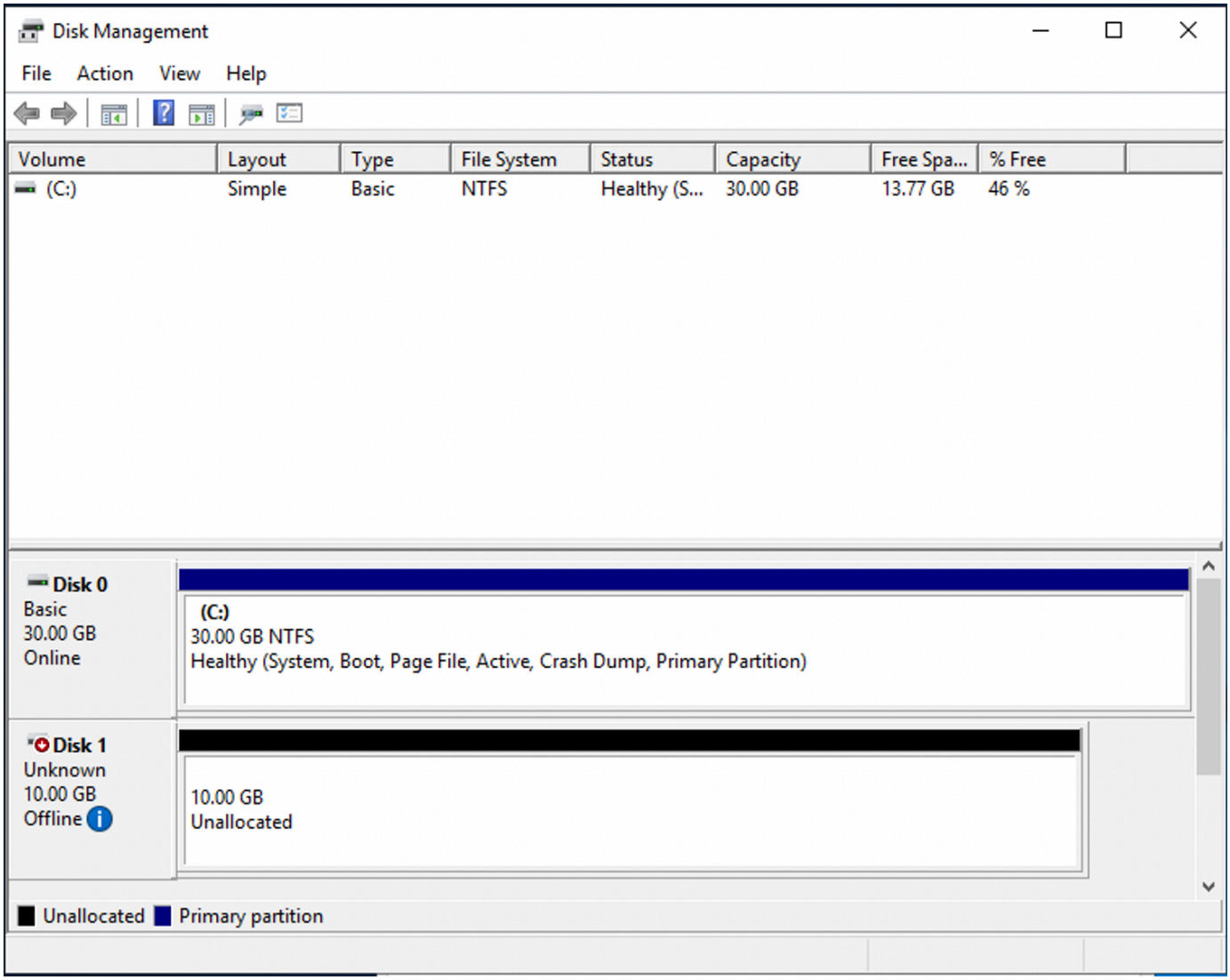
```
#Connect to FSx for NetApp ONTAP file system
Foreach ($TargetPortalAddress in $TargetPortalAddresses) {
New-IscsiTargetPortal -TargetPortalAddress $TargetPortalAddress -
TargetPortalPortNumber 3260 -InitiatorPortalAddress $LocaliSCSIAddress
}

#Add MPIO support for iSCSI
New-MSDSMSupportedHW -VendorId MSFT2005 -ProductId iSCSIBusType_0x9

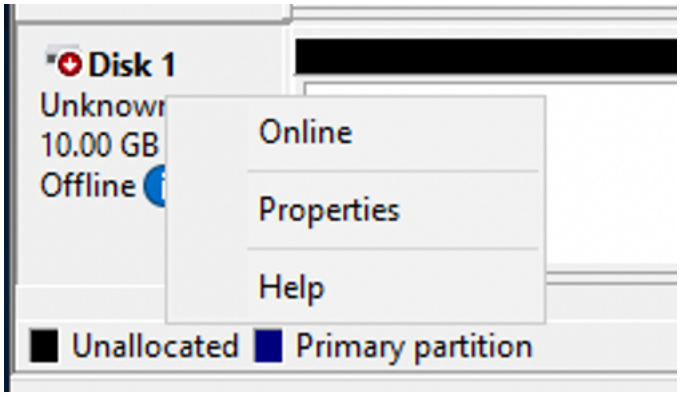
#Establish iSCSI connection
1..8 | %{Foreach($TargetPortalAddress in $TargetPortalAddresses)
{Get-IscsiTarget | Connect-IscsiTarget -IsMultipathEnabled $true -
TargetPortalAddress $TargetPortalAddress -InitiatorPortalAddress $LocaliSCSIAddress
 -IsPersistent $true}}

#Set the MPIO Policy to Round Robin
Set-MSDSMGlobalDefaultLoadBalancePolicy -Policy RR
```

3. Inicie la aplicación de administración de discos de Windows. Abra el cuadro de diálogo Ejecutar de Windows, ingrese `diskmgmt.msc` y pulse Entrar. Se abre la aplicación Administración de discos.



4. Localice el disco no asignado. Este es el LUN iSCSI. En el ejemplo, el disco 1 es el disco iSCSI. Está fuera de línea.



Coloque el volumen en línea colocando el cursor sobre el disco 1, haga clic con el botón derecho y, a continuación, seleccione En línea.

> **Note**
>
> Puede modificar la política de la red de área de almacenamiento (SAN) para que los nuevos volúmenes se pongan en línea automáticamente. Para obtener más información, consulte las Políticas de SAN en la Referencia de comandos de Microsoft Windows Server.

5. Para inicializar el disco, coloque el cursor sobre el Disco 1, haga clic con el botón derecho y seleccione Inicializar. Aparecerá el cuadro de diálogo de inicialización. Seleccione Aceptar para inicializar el disco.
6. Formatee el disco como lo haría normalmente. Una vez finalizado el formateo, la unidad iSCSI aparece como unidad utilizable en el cliente Windows.

Uso de FSx para ONTAP con otros servicios de AWS

Además de Amazon EC2, puede utilizar otros AWS servicios con sus volúmenes para acceder a sus datos.

Temas

- Uso de Amazon WorkSpaces con FSx para ONTAP
- Uso de Amazon Elastic Container Service con FSx para ONTAP
- Uso de VMware Cloud con FSx para ONTAP

Uso de Amazon WorkSpaces con FSx para ONTAP

FSx for ONTAP se puede utilizar con Amazon para proporcionar almacenamiento compartido conectado WorkSpaces a la red (NAS) o para almacenar perfiles de itinerancia para las cuentas de Amazon. WorkSpaces Tras conectarse a un recurso compartido de archivos SMB con una WorkSpaces instancia, el usuario puede crear y editar archivos en el recurso compartido de archivos.

Los siguientes procedimientos muestran cómo usar Amazon FSx con Amazon WorkSpaces para proporcionar una experiencia uniforme de acceso a perfiles móviles y carpetas de inicio y proporcionar una carpeta de equipo compartida para los usuarios de Windows y Linux WorkSpaces . Si eres nuevo en Amazon WorkSpaces, puedes crear tu primer WorkSpaces entorno de Amazon

siguiendo las instrucciones de Comenzar con la configuración WorkSpaces rápida de la Guía de WorkSpaces administración de Amazon.

Temas

Proporcione soporte para perfiles itinerantes

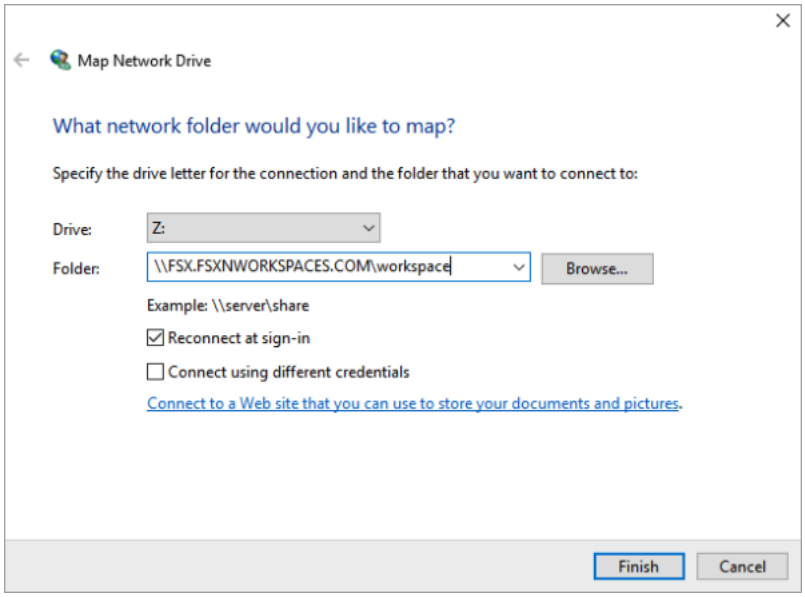
Puede usar Amazon FSx para proporcionar soporte para perfiles itinerantes a los usuarios de su organización. El usuario tendrá permisos para acceder únicamente a su perfil de itinerancia. La carpeta se conectará automáticamente mediante las políticas de grupo de Active Directory. Con un perfil itinerante, los datos y la configuración del escritorio de los usuarios se guardan cuando cierran sesión en un recurso compartido de archivos de Amazon FSx, lo que permite compartir documentos y configuraciones entre distintas WorkSpaces instancias, y se realiza una copia de seguridad automática mediante las copias de seguridad automáticas diarias de Amazon FSx.

Paso 1: Crear una ubicación de carpeta de perfil para los usuarios del dominio mediante Amazon FSx

1. Cree un sistema de archivos de FSx para ONTAP mediante la Amazon FSx. Para más información, consulte Para crear un sistema de archivos (consola).

> **Important**
>
> Cada sistema de archivos FSx para ONTAP tiene un rango de direcciones IP de punto de conexión a partir del cual se crean los puntos de conexión asociados al sistema de archivos. Para los sistemas de archivos Multi-AZ, FSx para ONTAP elige un rango de direcciones IP no utilizadas predeterminado de 198.19.0.0/16 como rango de direcciones IP de punto de conexión. Este rango de direcciones IP también lo usa WorkSpaces para administrar el rango de tráfico, tal y como se describe en los requisitos de direcciones IP y puertos de WorkSpaces la Guía de WorkSpaces administración de Amazon. Por lo tanto, para acceder a su sistema de archivos FSx Multi-AZ para ONTAP WorkSpaces desde, debe seleccionar un rango de direcciones IP de punto final que no se superponga con 198.19.0.0/16.

2. Si no tiene una máquina virtual de almacenamiento (SVM) unida a Active Directory, cree una. Por ejemplo, puede aprovisionar una SVM con el nombre `fsx` y establecer el estilo de seguridad en NTFS. Para más información, consulte Para crear una máquina virtual de almacenamiento (consola).
3. Cree un volumen para su SVM. Por ejemplo, puede crear un volumen con un nombre `fsx-vol` que herede el estilo de seguridad del volumen raíz de su SVM. Para más información, consulte Para crear un volumen (consola) FlexVol.
4. Cree un recurso compartido para pequeñas y medianas empresas en su volumen. Por ejemplo, puede crear un recurso compartido llamado `workspace` en su volumen denominado `fsx-vol`, en el que puede crear una carpeta con el nombre `profiles`. Para más información, consulte Gestión de recursos compartidos SMB.
5. Acceda a su SVM de Amazon FSx desde una instancia de Amazon EC2 que ejecute Windows Server o desde un. WorkSpace Para más información, consulte Acceso a datos.
6. Usted asigna su recurso compartido a una instancia `Z:\` de Windows: WorkSpaces



Paso 2: Vincular el recurso compartido de archivos FSx para ONTAP a las cuentas de usuario

1. En la del usuario de prueba WorkSpace, seleccione Windows > Sistema > Configuración avanzada del sistema.
2. En Propiedades del sistema, seleccione la pestaña Avanzadas y pulse el botón Configuración en la sección Perfiles de usuario. El usuario que haya iniciado sesión tendrá un tipo de perfil de `Local`.

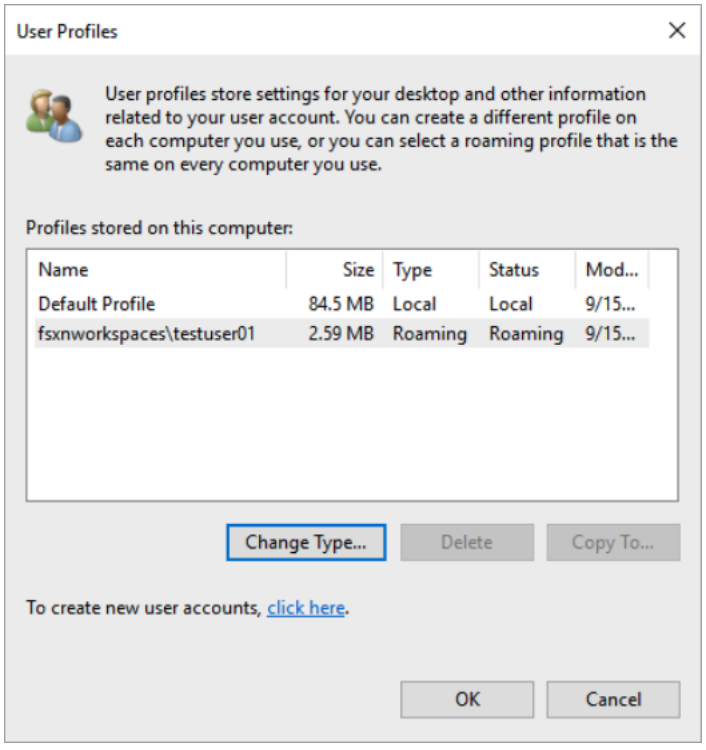
3. Cierre la sesión del usuario de prueba en WorkSpace.
4. Configure el usuario de prueba para que tenga un perfil de itinerancia ubicado en su sistema de archivos Amazon FSx. En el administrador WorkSpaces, abra una PowerShell consola y utilice un comando similar al siguiente ejemplo (que utiliza la `profiles` carpeta que creó anteriormente en el paso 1):

```
Set-ADUser username -ProfilePath \\filesystem-dns-
name\sharename\foldername\username
```

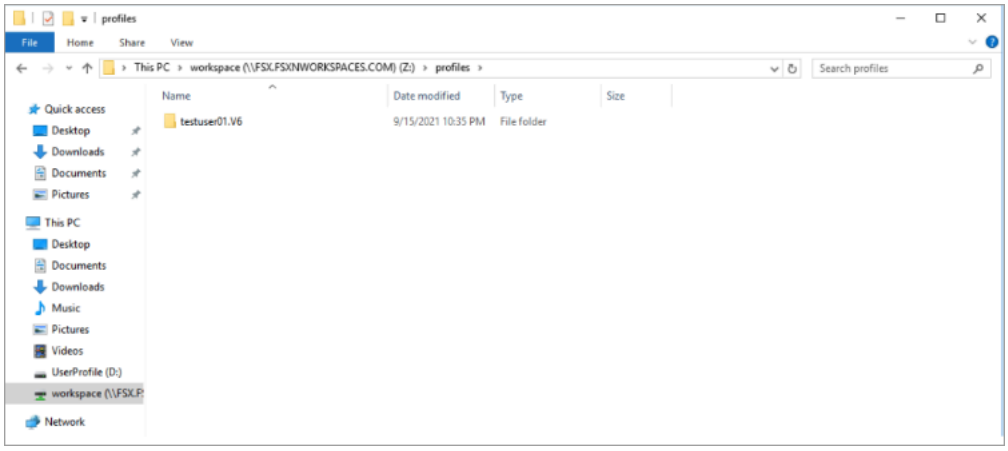
   Por ejemplo:

```
Set-ADUser testuser01 -ProfilePath \\fsx.fsxnworkspaces.com\workspace\profiles
\testuser01
```

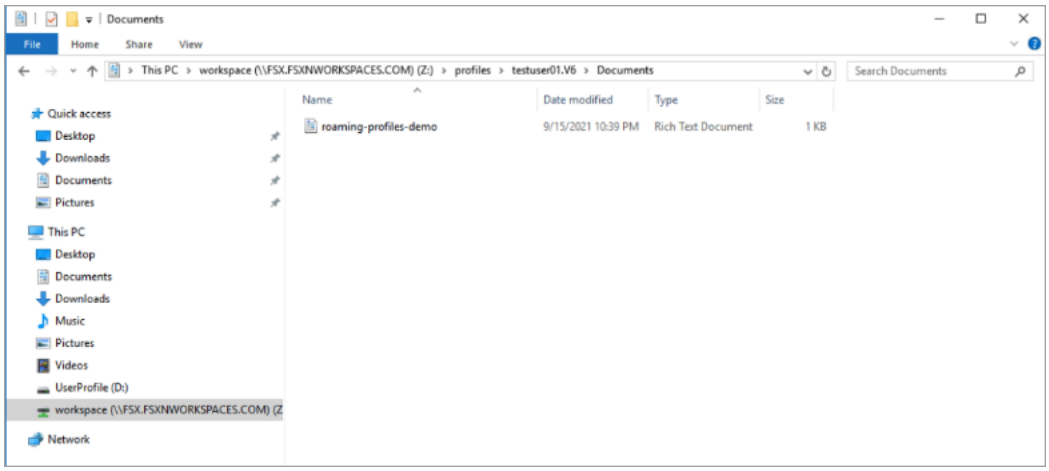
5. Inicie sesión con el usuario de prueba WorkSpace.
6. En Propiedades del sistema, seleccione la pestaña Avanzadas y pulse el botón Configuración en la sección Perfiles de usuario. El usuario que haya iniciado sesión tendrá un tipo de perfil de `Roaming`.



7. Busque en FSx la carpeta compartida ONTAP. En la carpeta `profiles`, verá una carpeta para el usuario.



8. Cree un documento en la carpeta `Documents` del usuario de prueba
9. Cierre la sesión del usuario de prueba de su WorkSpace.
10. Si vuelve a iniciar sesión como usuario de prueba y navega hasta su almacén de perfiles, verá el documento que creó.



Proporcione una carpeta compartida para acceder a los archivos comunes

Puede usar Amazon FSx para proporcionar una carpeta compartida a los usuarios de la organización. Puede utilizar una carpeta compartida para almacenar los archivos que utilice su comunidad de usuarios, como archivos de demostración, ejemplos de código y manuales de instrucciones que necesiten todos los usuarios. Por lo general, las unidades se asignan a carpetas compartidas; sin embargo, dado que las unidades mapeadas utilizan letras, hay un límite en la cantidad de recursos compartidos que se pueden compartir. Este procedimiento crea una carpeta compartida de Amazon FSx que está disponible sin una carta de unidad, lo que le proporciona una mayor flexibilidad a la hora de asignar recursos compartidos a los equipos.

Montar una carpeta compartida para el acceso multiplataforma desde Linux y Windows WorkSpaces

1. En la Barra de tareas, seleccione Lugares > Conectar al servidor.

   a. En Servidor, introduzca *`file-system-dns-name`*.

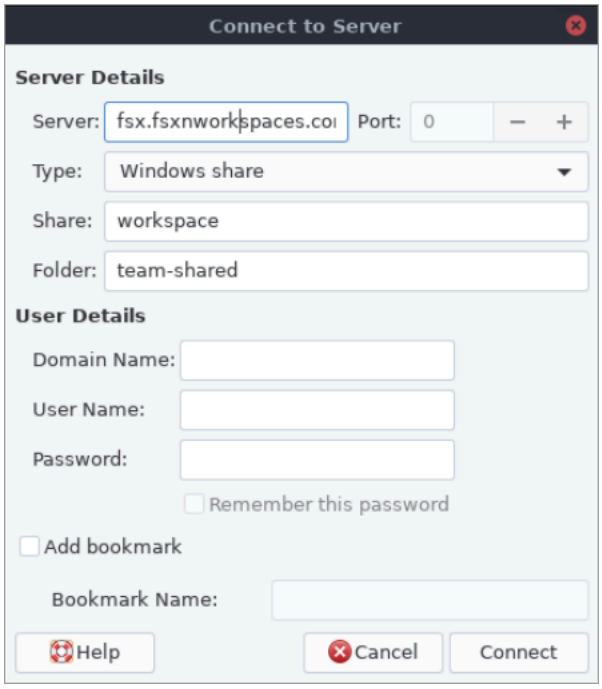
   b. Defina Tipo en `Windows share`.

   c. Defina Compartir con el nombre del recurso compartido SMB, como `workspace`.

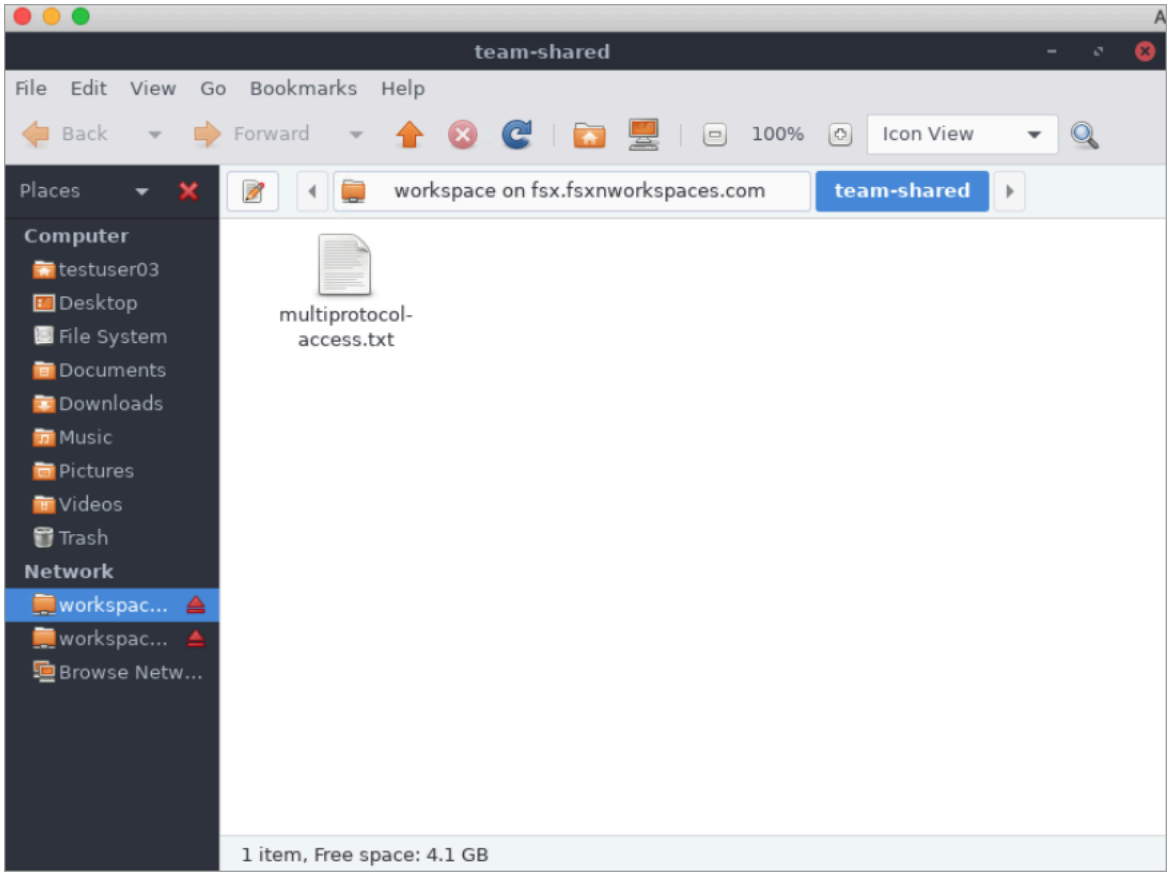
   d. Puede dejar Carpeta como `/` o configurarla en una carpeta, como una carpeta con el nombre `team-shared`.

   e. En el caso de Linux WorkSpace, no es necesario que introduzcas tus datos de usuario si tu Linux WorkSpace se encuentra en el mismo dominio que el recurso compartido de Amazon FSx.

   f. Elija Conectar.



2. Una vez realizada la conexión, podrá ver la carpeta compartida (nombrada `team-shared` en este ejemplo) en el recurso compartido SMB denominado `workspace`.



Uso de Amazon Elastic Container Service con FSx para ONTAP

Puede acceder a sus sistemas de archivos Amazon FSx for NetApp ONTAP desde un contenedor Docker de Amazon Elastic Container Service (Amazon ECS) en una instancia de Amazon EC2 para Linux o Windows.

Montaje en un contenedor de Amazon ECS Linux

1. Cree un clúster ECS con la plantilla de clúster EC2 Linux + Networking para sus contenedores de Linux. Para obtener más información, consulte Creación de un clúster en la Guía para desarrolladores de Amazon Elastic Container Service.
2. Cree un directorio en la instancia EC2 para montar el volumen SVM de la siguiente manera:

```
sudo mkdir /fsxontap
```

3. Monte su volumen FSx para ONTAP en la instancia EC2 de Linux mediante un script de datos de usuario durante el lanzamiento de la instancia o ejecutando los siguientes comandos:

```
sudo mount -t nfs svm-ip-address:/vol1 /fsxontap
```

4. Monte el volumen con el siguiente comando:

```
sudo mount -t nfs -o nfsvers=NFS_version svm-dns-name:/volume-junction-path /
fsxontap
```

En el ejemplo siguiente se usan valores de muestra.

```
sudo mount -t nfs -o nfsvers=4.1
 svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /
fsxontap
```

También puede utilizar la dirección IP del SVM en lugar de su nombre de DNS.

```
sudo mount -t nfs -o nfsvers=4.1 198.51.100.1:/vol1 /fsxontap
```

5. Al crear las definiciones de sus tareas de Amazon ECS, añada las siguientes propiedades de contenedor `volumes` y `mountPoints` en la definición de contenedor de JSON. Sustituya `sourcePath` por el punto de montaje y el directorio de su sistema de archivos de FSx para ONTAP.

```
{
    "volumes": [
        {
            "name": "ontap-volume",
            "host": {
                "sourcePath": "mountpoint"
            }
        }
    ],
    "mountPoints": [
        {
            "containerPath": "containermountpoint",
            "sourceVolume": "ontap-volume"
        }
    ],
    .
    .
    .
```

```
}
```

Montaje en un contenedor de Amazon ECS Windows

1. Cree un clúster ECS con la plantilla de clúster EC2 Windows + Networking para sus contenedores de Windows. Para obtener más información, consulte Creación de un clúster en la Guía para desarrolladores de Amazon Elastic Container Service.
2. Agregue una instancia EC2 de Windows unida a un dominio al clúster de Windows de ECS y asigne un recurso compartido SMB.

   Inicie una instancia EC2 de Windows optimizada para ECS que esté unida a su dominio de Active Directory e inicialice el agente de ECS ejecutando el siguiente comando.

   ```
   PS C:\Users\user> Initialize-ECSAgent -Cluster windows-fsx-cluster -
   EnableTaskIAMRole
   ```

   También puede pasar la información de un script al campo de texto de datos del usuario de la siguiente manera.

   ```
   <powershell>
   Initialize-ECSAgent -Cluster windows-fsx-cluster -EnableTaskIAMRole
   </powershell>
   ```
3. Cree un mapeo global de SMB en la instancia de EC2 para poder asignar su recurso compartido SMB a una unidad. Sustituya los valores que aparecen debajo del nombre netbios o DNS del sistema de archivos de FSx y del nombre del recurso compartido. El volumen NFS vol1 que se montó en la instancia EC2 de Linux está configurado como un archivo compartido CIFS fsxontap en el sistema de archivos de FSx.

   ```
   vserver cifs share show -vserver svm08 -share-name fsxontap


                                   Vserver: svm08
                                     Share: fsxontap
                   CIFS Server NetBIOS Name: FSXONTAPDEMO
                                     Path: /vol1
                           Share Properties: oplocks
                                             browsable
                                             changenotify
   ```

```
                                            show-previous-versions
                         Symlink Properties: symlinks
                    File Mode Creation Mask: -
                Directory Mode Creation Mask: -
                               Share Comment: -
                                   Share ACL: Everyone / Full Control
            File Attribute Cache Lifetime: -
                                 Volume Name: vol1
                               Offline Files: manual
            Vscan File-Operations Profile: standard
          Maximum Tree Connections on Share: 4294967295
                 UNIX Group for File Create: -
```

4. Cree la asignación global de SMB en la instancia de EC2 mediante el siguiente comando:

```
New-SmbGlobalMapping -RemotePath \\fsxontapdemo.fsxontap.com\fsxontap -LocalPath Z:
```

5. Al crear las definiciones de sus tareas de Amazon ECS, añada las siguientes propiedades de contenedor `volumes` y `mountPoints` en la definición de contenedor de JSON. Sustituya `sourcePath` por el punto de montaje y el directorio de su sistema de archivos de FSx para ONTAP.

```
{
    "volumes": [
        {
            "name": "ontap-volume",
            "host": {
                "sourcePath": "mountpoint"
            }
        }
    ],
    "mountPoints": [
        {
            "containerPath": "containermountpoint",
            "sourceVolume": "ontap-volume"
        }
    ],
    .
    .
    .
}
```

Uso de VMware Cloud con FSx para ONTAP

Puede usar FSx for ONTAP como almacén de datos externo para VMware Cloud on AWS Software-Defined Data Centers (SDDC). Para obtener más información, consulte Configurar Amazon FSx para NetApp ONTAP como almacenamiento externo y la guía de implementación de VMware Cloud on with AWS Amazon FSx para ONTAP. NetApp

Disponibilidad y durabilidad

Amazon FSx para NetApp ONTAP utiliza dos tipos de implementación, Single-AZ y Multi-AZ, que ofrecen distintos niveles de disponibilidad y durabilidad. En este tema se describen las características de disponibilidad y durabilidad de cada tipo de implementación para ayudarle a elegir la que mejor se adapte a sus cargas de trabajo. Para obtener información sobre el ANS (Acuerdo de Nivel de Servicio) de disponibilidad del servicio, consulte el acuerdo de nivel de servicio de Amazon FSx.

Temas

Selección de un tipo de implementación del sistema de archivos

Las características de disponibilidad y durabilidad de los tipos de implementación de sistemas de archivos Single-AZ y Multi-AZ se describen en las siguientes secciones.

Tipo de implementación Single-AZ

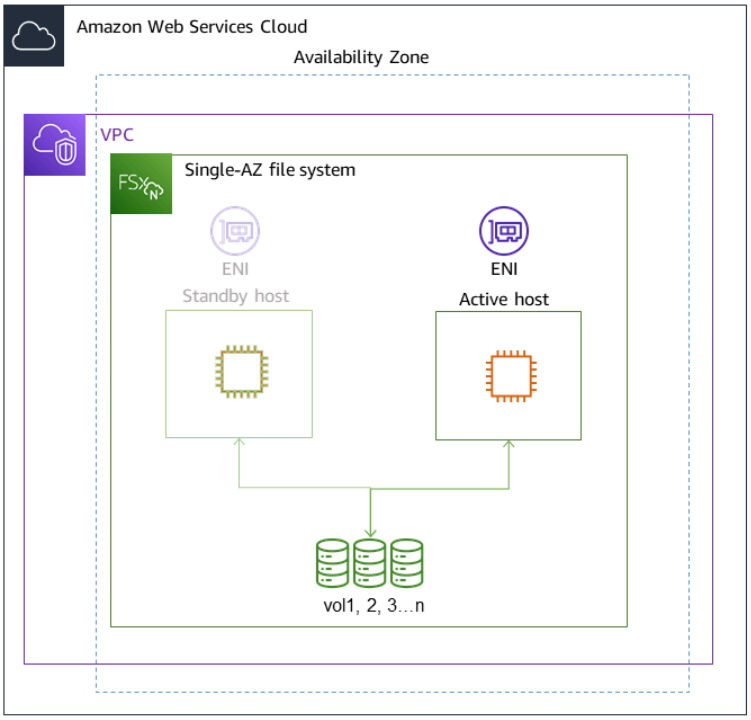
Al crear un sistema de archivos Single-AZ, Amazon FSx aprovisiona automáticamente de uno a doce pares de servidores de archivos en una configuración activo-en espera, con los servidores de archivos activos y en espera de cada par ubicados en dominios de errores separados dentro de una única zona de disponibilidad en el. Región de AWS Durante el mantenimiento planificado del sistema de archivos o una interrupción imprevista del servicio de cualquier servidor de archivos activo, Amazon FSx transfiere por error de forma automática e independiente ese par de alta disponibilidad (HA) al servidor de archivos en espera, normalmente en unos segundos. Durante una conmutación por error, seguirá teniendo acceso a sus datos sin intervención manual.

Para garantizar una alta disponibilidad, Amazon FSx monitorea continuamente los fallos de hardware y reemplaza automáticamente los componentes de la infraestructura en caso de que se produzca un fallo. Para lograr una alta durabilidad, Amazon FSx replica automáticamente sus datos dentro de una Zona de Disponibilidad para protegerlos de fallos de componentes. Además, tiene la opción de configurar copias de seguridad diarias automáticas de los datos de su sistema de archivos. Estas copias de seguridad se almacenan en varias zonas de disponibilidad para proporcionar una

capacidad de recuperación en zonas de disponibilidad múltiples para todos los datos de las copias de seguridad.

Los sistemas de archivos Single-AZ están diseñados para casos de uso que no requieren el modelo de resistencia de datos de un sistema de archivos Multi-AZ. Proporcionan una solución rentable para casos de uso como entornos de desarrollo y pruebas, o para almacenar copias secundarias de datos que ya están almacenados en las instalaciones o en otros entornos Regiones de AWS, al replicar únicamente los datos dentro de una única zona de disponibilidad.

El siguiente diagrama ilustra la arquitectura de un sistema de archivos de FSx para ONTAP Single-AZ.

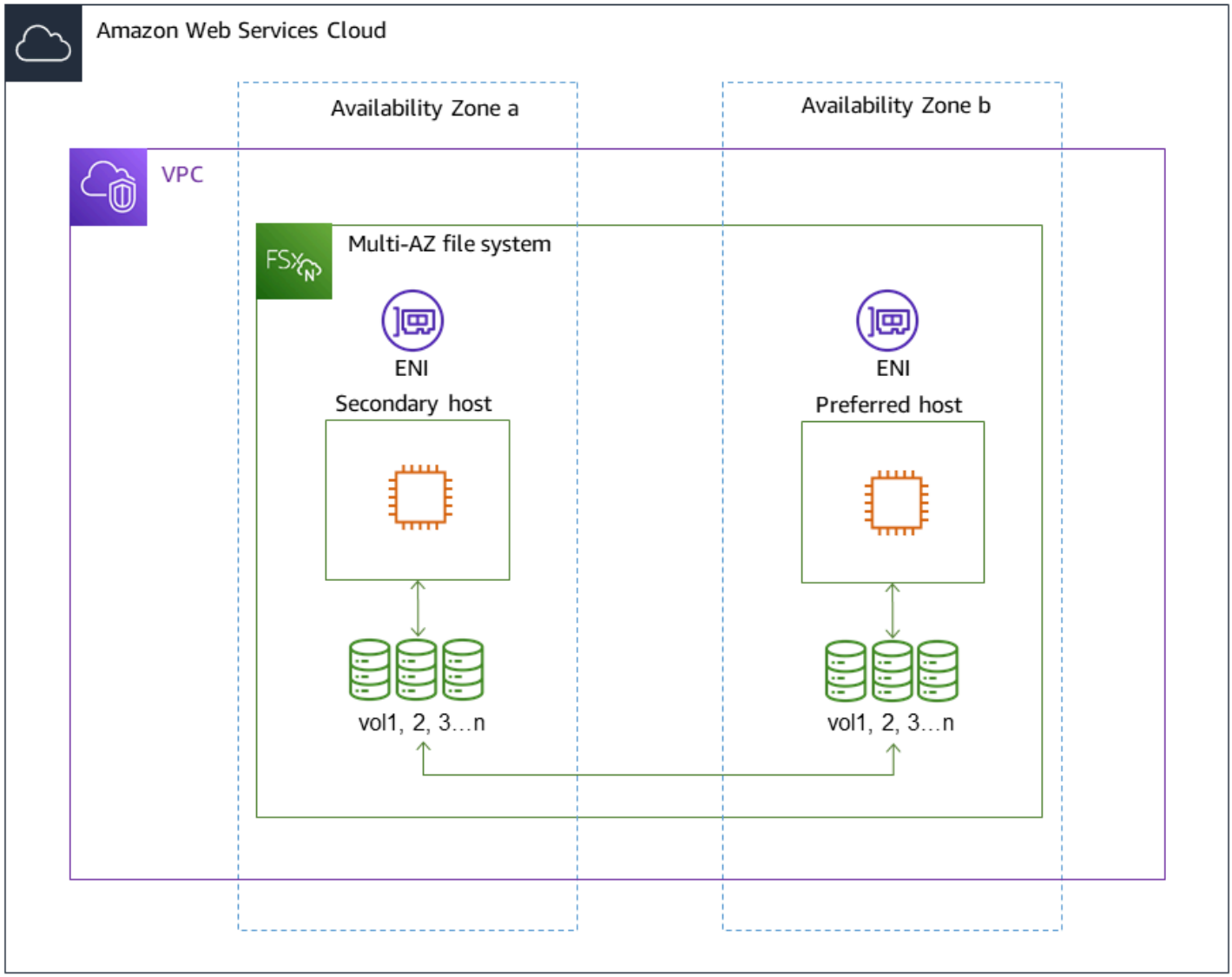


Tipo de implementación Multi-AZ

Los sistemas de archivos Multi-AZ admiten todas las características de disponibilidad y durabilidad de los sistemas de archivos Single-AZ. Además, están diseñados para proporcionar una disponibilidad continua de los datos incluso cuando una zona de disponibilidad no esté disponible. Las implementaciones Multi-AZ tienen un único par de servidores de archivos de alta disponibilidad; el servidor de archivos en espera se implementa en una zona de disponibilidad diferente a la del servidor de archivos activo en la misma zona. Región de AWS Los cambios que se escriban en el

sistema de archivos se replican sincrónicamente en las zonas de disponibilidad para el sistema de espera.

Los sistemas de archivos Multi-AZ están diseñados para casos de uso, como las cargas de trabajo de producción críticas para la empresa que requieren una alta disponibilidad de los datos de archivos compartidos de ONTAP y necesitan almacenamiento con replicación integrada en todas las zonas de disponibilidad. El siguiente diagrama ilustra la arquitectura de un sistema de archivos de FSx para ONTAP Multi-AZ.



Proceso de conmutación por error para FSx para ONTAP

Los sistemas de archivos Single-AZ y Multi-AZ conmutan automáticamente por error un par HA determinado del servidor de archivos preferido o activo al servidor de archivos en espera si se produce alguna de las siguientes condiciones:

- El servidor de archivos preferido o activo deja de estar disponible
- Se ha modificado la capacidad de rendimiento del sistema de archivos
- El servidor de archivos preferido o activo se somete a un mantenimiento planificado
- Se produce una interrupción en la zona de disponibilidad (sólo en sistemas de archivos Multi-AZ)

> **Note**
>
> En el caso de los sistemas de archivos ampliables, el comportamiento de conmutación por error de cada par HA es independiente. Si el servidor de archivos preferido para un par de HA no está disponible, solo ese par de HA realizará la conmutación por error a su servidor de archivos en espera.

Al pasar por error de un servidor de archivos a otro, el nuevo servidor de archivos activo comienza automáticamente a atender todas las solicitudes de lectura y escritura del sistema de archivos a ese par HA. En el caso de los sistemas de archivos Multi-AZ, cuando el servidor de archivos preferido se recupera por completo y está disponible, Amazon FSx falla automáticamente hacia él, y la conmutación por recuperación suele completarse en menos de 60 segundos. En el caso de los sistemas de archivos Single-AZ y Multi-AZ, la conmutación por error suele completarse en menos de 60 segundos, desde que se detecta el fallo en el servidor de archivos activo hasta que el servidor de archivos en espera pasa al estado activo. Como la dirección IP del punto de conexión que los clientes utilizan para acceder a los datos a través de NFS o SMB sigue siendo la misma, las conmutaciones por error son transparentes para las aplicaciones de Linux, Windows y macOS, que reanudan las operaciones del sistema de archivos sin intervención manual.

Para garantizar que las conmutaciones por error sean transparentes para los clientes conectados a su FSx para los sistemas de archivos ONTAP Single-AZ y Multi-AZ, consulte Acceder a los datos desde dentro AWS.

Probar la conmutación por error en un sistema de archivos

Puede probar la conmutación por error en su sistema de archivos escalable modificando su capacidad de rendimiento. Al modificar la capacidad de rendimiento del sistema de archivos, Amazon FSx desactiva los servidores de archivos del sistema de archivos en serie. Los sistemas de archivos conmutan automáticamente por error al servidor secundario, mientras que Amazon FSx sustituye primero al servidor de archivos preferido. Una vez actualizado, el sistema de archivos devuelve automáticamente al nuevo servidor principal y Amazon FSx sustituye al servidor de archivos secundario.

Puede supervisar el progreso de la solicitud de actualización de la capacidad de rendimiento en la consola Amazon FSx, la CLI y la API. Para obtener más información sobre la modificación de la capacidad de rendimiento del sistema de archivos y el monitoreo del progreso de la solicitud, consulte Administración de la capacidad de rendimiento.

Recursos de red

En esta sección, se describen los recursos de red que consumen los sistemas de archivos Single-AZ y Multi-AZ.

Subredes

Al crear un sistema de archivos Single-AZ, se especifica una única subred para el sistema de archivos. La subred que elija define la zona de disponibilidad en la que se crea el sistema de archivos. Al crear un sistema de archivos Multi-AZ, especifica dos subredes, una para el servidor de archivos preferido y otra para el estándar. Las dos subredes que elija deben estar en Zonas de Disponibilidad diferentes dentro de la misma Región de AWS. Para obtener más información sobre Amazon VPC, consulte ¿Qué es Amazon VPC? en la Guía del usuario de Amazon Virtual Private Cloud.

> **Note**
>
> Independientemente de la subred que especifique, puede acceder al sistema de archivos desde cualquier subred de la VPC del sistema de archivos.

Interfaces de red elástica del sistema de archivos

Para los sistemas de archivos Single-AZ, Amazon FSx aprovisiona dos interfaces de red elásticas (ENI) en la subred que usted asocia a su sistema de archivos. Para los sistemas de archivos Multi-AZ, Amazon FSx también aprovisiona dos ENI, uno en cada una de las subredes que asocie a su sistema de archivos. Los clientes se comunican con su sistema de archivos Amazon FSx mediante la interface de red elástica. Las interfaces de red se consideran dentro del ámbito de servicio de Amazon FSx, a pesar de formar parte de la VPC de su cuenta. Los sistemas de archivos Multi-AZ utilizan direcciones de protocolo de Internet (IP) flotantes para que los clientes conectados puedan realizar una transición fluida entre el servidor de archivos preferido y el servidor de archivos en espera durante una conmutación por error.

Warning

- No debe modificar ni eliminar las interfaces de red elásticas asociadas al sistema de archivos. Si modifica o elimina la interfaz de red, puede perder permanentemente la conexión entre su VPC y su sistema de archivos.
- Las rutas de las interfaces de red elásticas asociadas al sistema de archivos se crearán automáticamente y se agregarán a las tablas de enrutamiento de subred y VPC predeterminadas. La modificación o eliminación de estas rutas puede provocar una pérdida temporal o permanente de la conectividad de los clientes del sistema de archivos.

La siguiente tabla resume los recursos de subred, interfaz de red elástica y dirección IP para cada uno de los tipos de implementación de sistemas de archivos de FSx para ONTAP:

	Single-AZ (escalable)	Single-AZ (escalado horizontal)	Multi-AZ (ampliación)
Número de subredes	1	1	2
Número de interfaces de red elásticas	2	2 por par de HA	2

	Single-AZ (escalable)	Single-AZ (escalado horizontal)	Multi-AZ (ampliación)
Número de direcciones IP por ENI	1 + el número de SVM en el sistema de archivos	Recuento de pares HA + recuento de pares HA multiplicado por el número de SVM en el sistema de archivos	1 + el número de SVM en el sistema de archivos
Número de rutas de VPC de tabla de enrutamiento	N/A	N/A	1 + el número de SVM en el sistema de archivos

Una vez creado un sistema de archivos o SVM, sus direcciones IP no cambian hasta que se elimina el sistema de archivos.

> **Important**
>
> Amazon FSx no admite el acceso a los sistemas de archivos ni la exposición de los sistemas de archivos a la Internet pública. Amazon FSx separa automáticamente cualquier dirección IP elástica, que sea una dirección IP pública a la que se pueda acceder desde Internet, que se adjunta a la interfaz de red elástica de un sistema de archivos.

Administración de la capacidad de almacenamiento

Amazon FSx para NetApp ONTAP ofrece una serie de funciones relacionadas con el almacenamiento que puede utilizar para gestionar la capacidad de almacenamiento de su sistema de archivos.

Temas

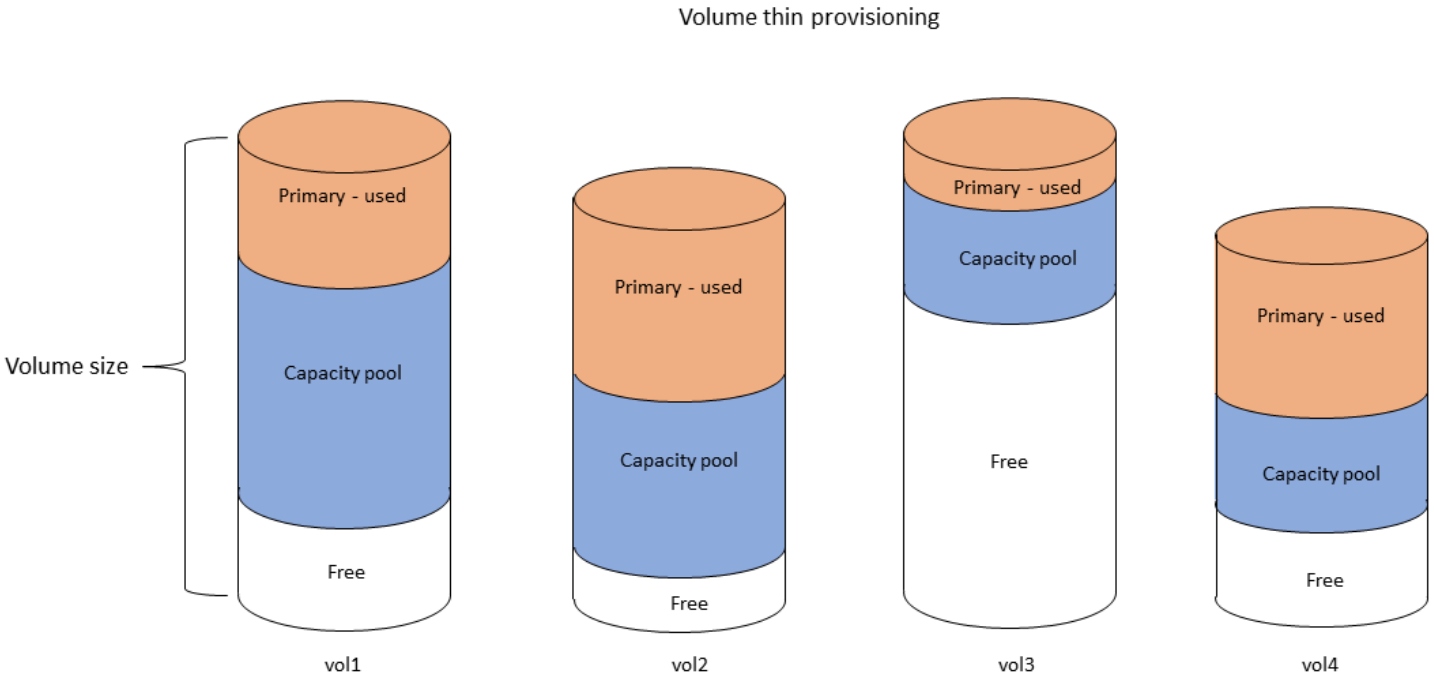
Niveles de almacenamiento de FSx para ONTAP

Los niveles de almacenamiento son los medios de almacenamiento físico de un sistema de archivos Amazon FSx for NetApp ONTAP. FSx para ONTAP ofrece los siguientes niveles de almacenamiento:

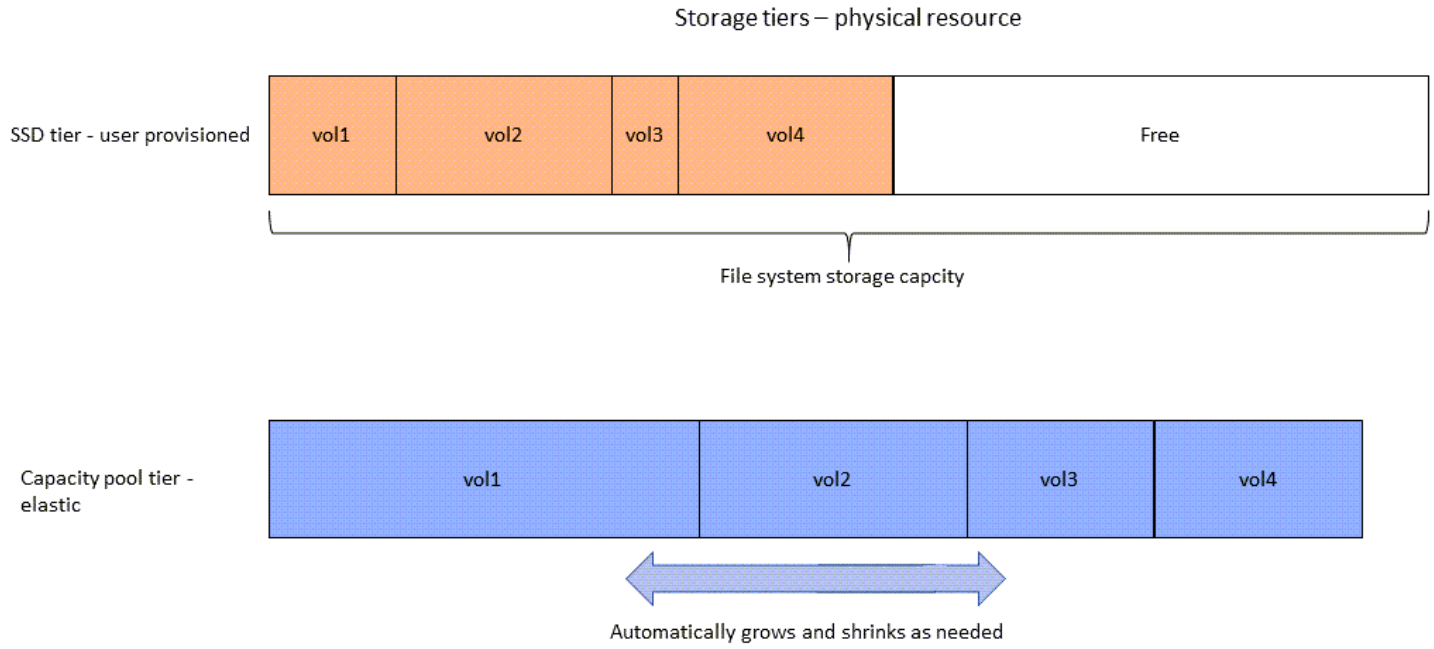
- Nivel SSD: almacenamiento en unidad de estado sólido (SSD) de alto rendimiento, aprovisionado por el usuario y diseñado específicamente para la parte activa del conjunto de datos.
- Nivel de reserva de capacidad: almacenamiento totalmente elástico que escala automáticamente a petabytes de tamaño y tiene un coste optimizado para los datos a los que se accede con poca frecuencia.

Un volumen FSx para ONTAP es un recurso virtual que, al igual que las carpetas, no consume capacidad de almacenamiento. Los datos que se almacenan (y que consumen almacenamiento físico) se encuentran dentro de los volúmenes. Al crear un volumen, se especifica su tamaño, que se puede modificar una vez creado. Los volúmenes de FSx para ONTAP tienen aprovisionamiento ligero y el almacenamiento del sistema de archivos no se reserva por adelantado. En su lugar, el almacenamiento en SSD y en conjunto de capacidades se asignan de forma dinámica, según sea necesario. Una política de niveles, que se configura a nivel de volumen, determina si y cuándo los datos almacenados en el nivel SSD pasan al nivel de pool de capacidad.

El siguiente diagrama ilustra un ejemplo de datos distribuidos en varios FSx para volúmenes ONTAP de un sistema de archivos.



El siguiente diagrama ilustra cómo consumen los datos de los cuatro volúmenes del diagrama anterior la capacidad de almacenamiento físico del sistema de archivos.



Puede reducir sus costos de almacenamiento si elige la política de niveles que mejor se adapte a los requisitos de cada volumen de su sistema de archivos. Para obtener más información, consulte Organización de datos de volumen en niveles.

Elegir la cantidad correcta de almacenamiento en SSD del sistema de archivos

Al elegir la cantidad de capacidad de almacenamiento en SSD para su sistema de archivos de FSx para ONTAP, debe tener en cuenta los siguientes factores que afectan a la cantidad de almacenamiento en SSD disponible para almacenar sus datos:

- Capacidad de almacenamiento reservada para la sobrecarga del software NetApp ONTAP.
- Metadatos de archivos
- Datos escritos recientemente
- Archivos que pretende almacenar en un almacenamiento SSD, ya sean datos que no han alcanzado su período de enfriamiento o datos que leyó recientemente y que se recuperaron en un SSD.

Cómo se usa el almacenamiento SSD

El almacenamiento SSD de su sistema de archivos se utiliza para una combinación del software NetApp ONTAP (sobrecarga), los metadatos de los archivos y sus datos.

NetApp Gastos generales del software ONTAP

Al igual que otros sistemas de archivos de NetApp ONTAP, hasta un 16% de la capacidad de almacenamiento en SSD de un sistema de archivos se reserva para la sobrecarga de ONTAP, lo que significa que no está disponible para almacenar sus archivos. La sobrecarga de ONTAP se distribuye de la siguiente manera:

- El 11% está reservado para el software NetApp ONTAP. Para los sistemas de archivos con más de 30 tebibytes (TiB) de capacidad de almacenamiento SSD, se reserva el 6%.
- El 5% se reserva para las instantáneas agregadas, que son necesarias para sincronizar los datos entre los dos servidores de archivos de un sistema de archivos.

Metadatos de archivos

Los metadatos de los archivos suelen consumir entre el 3 y el 7% de la capacidad de almacenamiento que consumen los archivos. Este porcentaje depende del tamaño medio del archivo

(un tamaño medio de archivo más pequeño requiere más metadatos) y de la cantidad de ahorro en eficiencia de almacenamiento que se logre con los archivos. Tenga en cuenta que los metadatos de los archivos no se benefician del ahorro en la eficiencia del almacenamiento. Puede utilizar las siguientes pautas para estimar la cantidad de almacenamiento SSD que se utiliza para los metadatos en su sistema de archivos.

Tamaño de archivo promedio	Tamaño de los metadatos como porcentaje de los datos del archivo
4 KB	7%
8 KB	3,5%
32 KB o mayor	1-3%

Al dimensionar la cantidad de capacidad de almacenamiento SSD que necesita para los metadatos de los archivos que planea almacenar en el nivel del pool de capacidad, le recomendamos usar una proporción conservadora de 1 GiB de almacenamiento SSD por cada 10 GiB de datos que planea almacenar en el nivel del pool de capacidad.

Datos de archivos almacenados en el nivel de SSD

Además del conjunto de datos activo y de todos los metadatos de los archivos, todos los datos que se escriben en el sistema de archivos se escriben inicialmente en el nivel de SSD antes de transferirse por niveles al almacenamiento del pool de capacidad. Esto es cierto independientemente de la política de organización en niveles del volumen, con la excepción de la transferencia de datos SnapMirror a un volumen configurado con una política de organización en niveles de todos los datos.

Las lecturas aleatorias del nivel del pool de capacidad se almacenan en caché en el nivel de SSD, siempre que el nivel de SSD se utilice por debajo del 90%. Para obtener más información, consulte Organización de datos de volumen en niveles.

Utilización recomendada de la capacidad del SSD

Le recomendamos que no utilice más del 80% de su nivel de almacenamiento SSD de forma continua. En el caso de los sistemas de archivos ampliables, también le recomendamos que no utilice más del 80% de ninguno de los agregados del sistema de archivos de forma continua. Estas recomendaciones son coherentes con la recomendación NetApp de ONTAP. Como el nivel de SSD

del sistema de archivos también se utiliza para organizar las escrituras y las lecturas aleatorias desde el nivel del conjunto de capacidades, cualquier cambio repentino en los patrones de acceso puede provocar un aumento rápido de la utilización del nivel de SSD.

Con un uso del SSD del 90%, los datos leídos desde el nivel del pool de capacidad ya no se almacenan en caché en el nivel SSD, de modo que la capacidad restante del SSD se conserva para cualquier dato nuevo que se escriba en el sistema de archivos. Esto provoca que las lecturas repetidas de los mismos datos del nivel del pool de capacidad se lean desde el almacenamiento del pool de capacidad en lugar de almacenarlos en caché y leerse desde el nivel SSD, lo que puede afectar a la capacidad de rendimiento del sistema de archivos.

Todas las funciones de niveles se detienen cuando el nivel de SSD tiene una utilización igual o superior al 98%. Para obtener más información, consulte Umbrales de niveles.

FSx para la eficiencia de almacenamiento de ONTAP

NetApp ONTAP ofrece funciones de eficiencia de almacenamiento a nivel de bloques, como la compresión, la compactación y la deduplicación, que pueden ahorrarle hasta un 65% de la capacidad de almacenamiento al compartir archivos en general, sin sacrificar el rendimiento.

Amazon FSx para NetApp ONTAP también es compatible con otras funciones de ONTAP que le permiten ahorrar espacio, como las instantáneas, el aprovisionamiento ligero y los volúmenes. FlexClone

Las características de eficiencia de almacenamiento no están habilitadas de forma predeterminada. Puede habilitarlos de la siguiente manera:

- En el volumen raíz de un SVM al crear un sistema de archivos.
- Al crear un volumen nuevo.
- Al modificar un volumen existente.

Para ver el ahorro de almacenamiento en un sistema de archivos con la eficiencia de almacenamiento habilitada, consulte. Visualización de los ahorros en eficiencia de almacenamiento

Calcular los ahorros en la eficiencia del almacenamiento

Puede utilizar las métricas del sistema de CloudWatch archivos `LogicalDataStored` y `StorageUsed` FSx for ONTAP para calcular los ahorros de almacenamiento derivados de la

compresión, la deduplicación, la compactación, las instantáneas y. FlexClones Estas métricas tienen una única dimensión, `FileSystemId`. Para obtener más información, consulte Métricas del sistema de archivos.

- Para calcular el ahorro de eficiencia de almacenamiento en bytes, tome la media de `StorageUsed` durante un periodo determinado y réstela del valor medio de `LogicalDataStored` durante el mismo periodo.
- Para calcular los ahorros en la eficiencia del almacenamiento como un porcentaje del tamaño total de los datos lógicos, tome el valor `Average` de `StorageUsed` durante un período determinado y reste `Average` del `LogicalDataStored` mismo período. A continuación, divida la diferencia entre `Average` de `LogicalDataStored` durante el mismo período.

Ejemplo de tamaño de SSD

Supongamos que desea almacenar 100 TiB de datos para una aplicación en la que el 80% de los datos se consultan con poca frecuencia. En este escenario, el 80% (80 TB) de los datos se agrupan automáticamente en el nivel del pool de capacidad y el 20% restante (20 TB) permanece en un almacenamiento SSD. Basado en el ahorro típico de eficiencia de almacenamiento del 65% para las cargas de trabajo de uso general de uso compartido de archivos, lo que equivale a 7 TiB de datos. Para mantener una tasa de utilización de SSD del 80%, necesita 8,75 TiB de capacidad de almacenamiento SSD para los 20 TiB de datos a los que se accede activamente. La cantidad de almacenamiento en SSD que aprovisione también debe representar la sobrecarga de almacenamiento del software de ONTAP, que es del 16%, como se muestra en el siguiente cálculo.

```
ssdNeeded = ssdProvisioned * (1 - 0.16)
8.75 TiB / 0.84 = ssdProvisioned
10.42 TiB = ssdProvisioned
```

Por lo tanto, en este ejemplo, debe aprovisionar al menos 10,42 TiB de almacenamiento SSD. También utilizará 28 TiB de almacenamiento agrupado de capacidad para los 80 TiB restantes de datos a los que se accede con poca frecuencia.

Capacidad de almacenamiento e IOPS del sistema de archivos

Al crear un sistema de archivos de FSx para ONTAP, debe especificar la capacidad de almacenamiento del nivel SSD. En el caso de los sistemas de archivos ampliables, la capacidad de almacenamiento que especifique se distribuye de manera uniforme entre los grupos de

almacenamiento de cada par de alta disponibilidad (HA); estos grupos de almacenamiento se denominan agregados.

Por cada GiB de almacenamiento SSD que aprovisione, Amazon FSx aprovisiona automáticamente 3 operaciones de entrada/salida por segundo (IOPS) de SSD para el sistema de archivos, hasta un máximo de 160 000 IOPS de SSD por sistema de archivos. En el caso de los sistemas de archivos ampliables, las IOPS de las SSD se distribuyen de forma uniforme entre cada uno de los agregados del sistema de archivos. Tiene la opción de especificar un nivel de IOPS de SSD aprovisionadas superior a las 3 IOPS de SSD automáticas por GiB. Para obtener más información sobre la cantidad máxima de IOPS de SSD que puede aprovisionar para su sistema de archivos de FSx para ONTAP, consulte Impacto de la capacidad de rendimiento en el rendimiento.

Temas

Actualización del sistema de archivos, el almacenamiento SSD y las IOPS

Cuando necesite almacenamiento adicional para la parte activa de su conjunto de datos, puede aumentar la capacidad de almacenamiento en SSD de su sistema de archivos Amazon FSx for NetApp ONTAP. Utilice la consola Amazon FSx, la API Amazon FSx o AWS Command Line Interface (AWS CLI) para aumentar la capacidad de almacenamiento de la SSD. Para obtener más información, consulte Modificación de la capacidad de almacenamiento de la SSD y las IOPS aprovisionadas.

Cuando aumenta la capacidad de almacenamiento SSD de su sistema de archivos Amazon FSx, la nueva capacidad suele estar disponible para su uso en cuestión de minutos. Se le facturará la nueva capacidad de almacenamiento en SSD una vez que esté disponible para usted. Para obtener más información sobre los precios, consulte los precios de Amazon FSx for NetApp ONTAP.

Tras aumentar la capacidad de almacenamiento, Amazon FSx ejecuta un proceso de optimización del almacenamiento en segundo plano para reequilibrar los datos. En la mayoría de los sistemas de

archivos, la optimización del almacenamiento tarda unas horas y el impacto en el rendimiento de la carga de trabajo es mínimo y perceptible.

Puede realizar un seguimiento del progreso del proceso de optimización del almacenamiento en cualquier momento mediante la consola, la CLI y la API de Amazon FSx. Para obtener más información, consulte Monitoreo de la capacidad de almacenamiento y las actualizaciones de IOPS.

Consideraciones

Estos son algunos aspectos importantes que se deben tener en cuenta al modificar la capacidad de almacenamiento en SSD y las IOPS aprovisionadas de un sistema de archivos:

- Sólo aumento de la capacidad de almacenamiento: sólo puede aumentar la cantidad de capacidad de almacenamiento en SSD de un sistema de archivos; no puede disminuir la capacidad de almacenamiento.
- Aumento mínimo de la capacidad de almacenamiento: cada aumento de la capacidad de almacenamiento en SSD debe representar como mínimo el 10 por ciento de la capacidad de almacenamiento en SSD actual del sistema de archivos, hasta alcanzar la capacidad máxima de almacenamiento en SSD para la configuración del sistema de archivos.
- Distribución de la capacidad de almacenamiento (solo con capacidad de ampliación horizontal): la nueva capacidad de almacenamiento o IOPS de SSD que seleccione para su sistema de archivos se distribuye de manera uniforme entre cada uno de los agregados del sistema de archivos.
- Tiempo entre incrementos: después de modificar la capacidad de almacenamiento de la SSD, las IOPS aprovisionadas o la capacidad de rendimiento de un sistema de archivos, debe esperar al menos seis horas antes de volver a modificar cualquiera de estas configuraciones en el mismo sistema de archivos. Esto es lo que a veces se denomina periodo de recuperación.
- Modos de IOPS aprovisionadas: para cambiar las IOPS aprovisionadas, debe especificar uno de los dos modos de IOPS aprovisionadas:
  - Modo automático: Amazon FSx escala automáticamente las IOPS de SSD para mantener 3 IOPS de SSD aprovisionadas por GiB de capacidad de almacenamiento de SSD, hasta el máximo de IOPS de SSD para la configuración de su sistema de archivos.

> **Note**
>
> Para obtener más información sobre la cantidad máxima de IOPS de SSD que puede aprovisionar para su sistema de archivos de FSx para ONTAP, consulte Impacto de la capacidad de rendimiento en el rendimiento.

- Modo aprovisionado por el usuario: especifique la cantidad de IOPS de SSD, que debe ser mayor o igual a 3 IOPS por GiB de capacidad de almacenamiento de SSD. Si opta por aprovisionar un nivel superior de IOPS, paga por el promedio de IOPS aprovisionadas por encima de la tarifa incluida del mes, medida en IOPS por mes.

Para obtener más información sobre los precios, consulte los precios de Amazon FSx for NetApp ONTAP.

¿Cuándo aumentar la capacidad de almacenamiento de la SSD

Si se está agotando el almacenamiento en niveles SSD disponible, le recomendamos que aumente la capacidad de almacenamiento de su sistema de archivos. Quedarse sin almacenamiento indica que su nivel SSD es insuficiente para la parte activa de su conjunto de datos.

Para monitorizar la cantidad de almacenamiento gratuito disponible en el sistema de archivos, usa las métricas de `StorageCapacity` `StorageUsed` Amazon CloudWatch y a nivel del sistema de archivos. Puedes crear una CloudWatch alarma en una métrica y recibir una notificación cuando caiga por debajo de un umbral específico. Para obtener más información, consulte Monitorización con Amazon CloudWatch.

> **Note**
>
> Le recomendamos que no utilice más del 80% de la capacidad de almacenamiento de la SSD para garantizar que la organización de los datos en niveles, el escalado del rendimiento y otras actividades de mantenimiento funcionen correctamente, y que haya capacidad disponible para datos adicionales. En el caso de los sistemas de archivos escalables, esta recomendación se aplica tanto a la utilización media de todos los agregados del sistema de archivos como a cada agregado individual.

Para obtener más información sobre cómo se usa el almacenamiento SSD de un sistema de archivos y cuánto almacenamiento SSD se reserva para los metadatos de los archivos y el software operativo, consulte Elegir la cantidad correcta de almacenamiento en SSD del sistema de archivos.

Supervisión del uso del almacenamiento SSD

Puede supervisar el uso de la capacidad de almacenamiento SSD de su sistema de archivos mediante una variedad AWS de NetApp herramientas. Con Amazon CloudWatch puedes monitorizar

la utilización de la capacidad de almacenamiento y configurar alarmas que te avisen cuando la utilización de la capacidad de almacenamiento alcance un umbral personalizable.

> **Note**
>
> Le recomendamos que no supere el 80% de utilización de la capacidad de almacenamiento de su nivel de almacenamiento SSD. Esto garantiza que la organización en niveles funcione correctamente y supone una sobrecarga para los datos nuevos. Si su nivel de almacenamiento SSD utiliza constantemente la capacidad de almacenamiento por encima del 80%, puede aumentar la capacidad de su nivel de almacenamiento SSD. Para obtener más información, consulte Actualización del sistema de archivos, el almacenamiento SSD y las IOPS.

Puede ver el almacenamiento SSD disponible de un sistema de archivos y la distribución general del almacenamiento en la consola Amazon FSx. El gráfico de Capacidad de almacenamiento en SSD disponible muestra la cantidad de capacidad de almacenamiento basada en SSD disponible en un sistema de archivos a lo largo del tiempo. El gráfico de Distribución del almacenamiento muestra cómo la capacidad de almacenamiento total de un sistema de archivos se distribuye actualmente en tres categorías:

- Nivel del pool de capacidad
- Nivel SSD: disponible
- Nivel SSD: usado

Puede monitorizar el uso de la capacidad de almacenamiento SSD de su sistema de archivos en el AWS Management Console sistema de archivos mediante el siguiente procedimiento.

Para supervisar la capacidad de almacenamiento disponible en el nivel SSD del sistema de archivos (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Seleccione Sistemas de archivos en la columna de navegación de la izquierda y, a continuación, elija el sistema de ONTAP archivos del que desee ver la información sobre la capacidad de almacenamiento. Aparece la página de detalles del sistema de archivos.

3. En el segundo panel, selecciona la pestaña Supervisión y rendimiento y, a continuación, selecciona Almacenamiento. Se muestran los gráficos de capacidad de almacenamiento principal disponible y de utilización de la capacidad de almacenamiento por agregado.

Configuración de una alarma de utilización del almacenamiento

Le recomendamos que no supere el 80% de utilización media de la capacidad de almacenamiento de la SSD de forma continua. Se aceptan picos ocasionales de utilización del almacenamiento SSD superiores al 80%. Mantener una utilización media inferior al 80% le proporciona la capacidad suficiente para aumentar el almacenamiento sin problemas. El siguiente procedimiento muestra cómo crear una CloudWatch alarma que le avise cuando la utilización del almacenamiento SSD del sistema de archivos se acerca al 80%.

Para crear una CloudWatch alarma de uso del almacenamiento principal

Para calcular la utilización media de la capacidad de almacenamiento de las SSD, utilice la métrica `StorageUsed`. Divida por el máximo StorageCapacity durante el mismo período, con la StorageTier dimensión igual a SSD.

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación, elija File systems (Sistemas de archivos) y elija el sistema de archivos para el que desee crear la alarma.
3. En la página de Summary (Resumen), seleccione Monitoring (Monitoreo).
4. Selecciona Crear CloudWatch alarma. Se le redirigirá a la página Alarmas > Crear alarma > Especificar métricas y condiciones de la CloudWatch consola.
5. Elija Seleccionar métrica.
6. En la sección de Métricas, elija FSx.
7. Elija la categoría Métricas detalladas del sistema de archivos.
8. Para mostrar solo las métricas disponibles para el sistema de archivos para el que está creando la alarma, introduzca el ID del sistema de archivos en el campo de búsqueda.
9. Para el sistema de archivos para el que desee configurar la alarma, elija las siguientes métricas:

Nombre de métrica	StorageTier	DataType
StorageUsed	SSD	Todos

Nombre de métrica	StorageTier	DataType
StorageCapacity	SSD	Todos

10. Seleccione la pestaña Métricas diagramadas. Para cada una de las métricas que agregó anteriormente, realice las siguientes acciones:

    - Establezca el valor de la columna Estadística para cada una de las métricas en Promedio.
    - Establezca el valor del Periodo en uno de los períodos de evaluación predefinidos.

11. Elija el menú desplegable Add math (Agregar expresión matemática) y, a continuación, seleccione Start with an empty expression (Comenzar con una expresión vacía) de la lista de expresiones matemáticas de métricas predefinidas.

    Después de elegir Start with an empty expression (Comenzar con una expresión vacía), aparecerá un cuadro de expresión matemática en el que podrá aplicar o editar expresiones matemáticas.

12. En el campo Edit math expression (Editar expresión matemática), ingrese la expresión para dividir la métrica `StorageUsed` entre la métrica `StorageCapacity`, de la siguiente manera:

    - Ingrese la etiqueta de la métrica `StorageUsed`, por ejemplo, m1.
    - Ingrese el carácter de barra diagonal, /, para la operación de división.
    - Ingrese la etiqueta de la métrica `StorageCapacity`.

    Seleccione Aplicar.

13. Desactive las casillas de verificación situadas a la izquierda de las métricas de la página. Solo debe seleccionarse la casilla de verificación situada junto a la expresión que se va a utilizar para la alarma. La expresión que elija para la alarma debe producir una serie temporal única y mostrar solo una línea en el gráfico. A continuación, elija Select metric (Seleccionar métrica).

    Aparece la página Specify metric and conditions (Especificar métrica y condiciones), en la que se muestra un gráfico y otra información acerca de la expresión matemática que ha seleccionado.

14. Para Whenever *`expression`* is (Siempre que la expresión sea), especifique que la expresión debe ser mayor, menor o igual que el umbral. En than... (que...), especifique el valor de umbral.

Para crear una alarma que le avise cuando la capacidad de almacenamiento de la SSD se acerca al umbral del 80%, configure Whenever *`expression`* is (Siempre que la expresión sea) igual al umbral y especifique un valor de umbral del 80%.

15. Elija Configuración adicional. Para Puntos de datos para alarma, especifique el número de periodos de evaluación (puntos de datos) que deben tener el estado `ALARM` para que se active la alarma. Si estos dos valores coinciden, creerá una alarma que pasará al estado `ALARM` si se infringen muchos periodos consecutivos.

    Para crear una alarma M de N, especifique un número menor para el primer valor que el especificado para el segundo valor. Para obtener más información, consulta Cómo evaluar una alarma en la Guía del CloudWatch usuario de Amazon.

16. En Missing data treatment (Tratamiento de datos que faltan), elija cómo debe comportarse la alarma cuando falten algunos puntos de datos. 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, consulta Cómo CloudWatch las alarmas tratan los datos faltantes en la Guía del CloudWatch usuario de Amazon.

    > **Note**
    >
    > Es posible que las métricas no se publiquen durante el mantenimiento del sistema de archivos.

17. Elija Siguiente.

18. En Notification (Notificación), seleccione el tema de SNS al que desee enviar la notificación cuando la alarma tenga el estado `ALARM`, `OK` o `INSUFFICIENT_DATA`.

    Si elige Create topic (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.

    > **Note**
    >
    > 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.

Para que la alarma envíe varias notificaciones para el mismo estado de alarma o para estados de alarma diferentes, seleccione Add notificación (Añadir notificación).

Para que la alarma no envíe notificaciones, elija Remove (Eliminar).

Si CloudWatch quieres enviarte un correo electrónico o una notificación de Amazon SNS cuando el estado de alarma inicie la acción, selecciona un estado de alarma para Whenever this alarm state is.

19. Cuando haya terminado, elija Next (Siguiente).
20. Escriba un nombre y la descripción de la alarma. El nombre solo debe contener caracteres ASCII. A continuación, elija Siguiente.
21. Previsualice la alarma que va a crear en la página Preview and create (Previsualizar y crear) y, a continuación, seleccione Create alarm (Crear alarma).

Visualización de los ahorros en eficiencia de almacenamiento

Cuando está habilitada, puede ver cuánta capacidad de almacenamiento está ahorrando en la consola Amazon FSx, la CloudWatch consola Amazon y la CLI de ONTAP.

Para ver los ahorros en eficiencia de almacenamiento (consola)

Los ahorros en eficiencia de almacenamiento que se muestran en la consola Amazon FSx para un sistema de archivos fSx para ONTAP incluyen los ahorros de y. FlexClones SnapShots

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Seleccione el sistema de archivos de FSx para ONTAP para el que desea ver el ahorro de eficiencia de almacenamiento de la lista de Sistemas de archivos.
3. Seleccione Resumen en la pestaña Supervisión y rendimiento del segundo panel de la página de detalles del sistema de archivos.
4. El gráfico de Ahorro en eficiencia de almacenamiento muestra cuánto espacio se ahorra como porcentaje del tamaño lógico de los datos y en bytes físicos.

Para ver los ahorros en eficiencia del almacenamiento (ONTAPCLI)

Puede obtener ahorros en la eficiencia del almacenamiento solo con la compactación, la compresión y la deduplicación, sin los efectos de las instantáneas, al ejecutar el `storage aggregate show-efficiency` comando mediante la CLI. FlexClones ONTAP Para obtener más información, consulte Storage Aggregate show-efficiency en el Centro de documentación. NetApp ONTAP

1. Para acceder a la CLI de NetApp ONTAP, ejecute el siguiente comando para establecer una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP. Reemplace *`management_endpoint_ip`* con la dirección IP del puerto de gestión del sistema de archivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obtener más información, consulte Administración de sistemas de archivos con la ONTAP CLI.
2. El storage aggregate show-efficiency comando muestra información sobre la eficiencia de almacenamiento de todos los agregados. La eficiencia del almacenamiento se muestra en cuatro niveles diferentes:

   - Total
   - Agregado
   - Volumen
   - Instantánea y FlexClone volumen

   ```
   ::*> aggr show-efficiency

   Aggregate: aggr1
        Node: node1

   Total Data Reduction Efficiency Ratio:  3.29:1
   Total Storage Efficiency Ratio:         4.29:1
   Aggregate: aggr2
        Node: node1

   Total Data Reduction Efficiency Ratio:  4.50:1
   Total Storage Efficiency Ratio:         5.49:1
   ```

```
cluster::*> aggr show-efficiency -details

Aggregate: aggr1
     Node: node1

Total Data Reduction Ratio:                    2.39:1
Total Storage Efficiency Ratio:                4.29:1

Aggregate level Storage Efficiency
(Aggregate Deduplication and Data Compaction): 1.00:1
Volume Deduplication Efficiency:               5.03:1
Compression Efficiency:                        1.00:1

Snapshot Volume Storage Efficiency:            8.81:1
FlexClone Volume Storage Efficiency:           1.00:1
Number of Efficiency Disabled Volumes:         1

Aggregate: aggr2
     Node: node1
Total Data Reduction Ratio:                    2.39:1
Total Storage Efficiency Ratio:                4.29:1

Aggregate level Storage Efficiency
(Aggregate Deduplication and Data Compaction): 1.00:1
Volume Deduplication Efficiency:               5.03:1
Compression Efficiency:                        1.00:1

Snapshot Volume Storage Efficiency:            8.81:1
FlexClone Volume Storage Efficiency:           1.00:1
Number of Efficiency Disabled Volumes:         1
```

Modificación de la capacidad de almacenamiento de la SSD y las IOPS aprovisionadas

Puede aumentar el almacenamiento basado en SSD de un sistema de archivos y aumentar o disminuir la cantidad de IOPS de SSD aprovisionadas mediante la consola Amazon FSx, la y la API. AWS CLI

Para actualizar la capacidad de almacenamiento de la SSD o las IOPS aprovisionadas para 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 File systems (Sistemas de archivos). En la lista de File systems (Sistemas de archivos), seleccione el sistema de archivos de FSx para ONTAP en el que desee actualizar la capacidad de almacenamiento de la SSD y las IOPS de la SSD.
3. En Actions (Acciones), seleccione Update storage capcity (Actualizar capacidad de almacenamiento). O bien, en la sección Summary (Resumen), seleccione Upade (Actualizar) junto al valor de la Capacidad de almacenamiento en SSD del sistema de archivos.

   Aparece el cuadro de diálogo Update SSD storage capacity and IOPS (Actualizar la capacidad de almacenamiento de la SSD y las IOPS).

Update SSD storage capacity and IOPS

File system ID

fs-01234567890abcdef

Current configuration

SSD storage capacity: 4096 GiB
IOPS mode: Automatic (3 IOPS per GiB of SSD storage)
SSD IOPS: 12288

SSD storage capacity

☑ Modify storage capacity

Input type

◉ Percentage
○ Absolute

Desired % increase

10 %

Minimum 4506 GiB (10% above current); Maximum 1048576 GiB.

Provisioned SSD IOPS

◉ Automatic (3 IOPS per GiB of SSD storage)
○ User-provisioned

Configuration preview

Attribute	Current configuration	New configuration
SSD storage capacity	4,096 GiB (2,048 GiB per HA pair)	4,506 GiB (2,253 GiB per HA pair)
	Mode: Automatic	Mode: Automatic

4. Para aumentar la capacidad de almacenamiento de la SSD, seleccione Modify storage capacity (Modificar la capacidad de almacenamiento).
5. En Input type (Tipo de motor), seleccione una de las siguientes:
   - Para introducir la nueva capacidad de almacenamiento de la SSD como un cambio porcentual con respecto al valor actual, seleccione Percentage (Porcentaje).
   - Para introducir el nuevo valor en GiB, elija Absolute (Absoluto).
6. Según el tipo de entrada, ingrese un valor para % de aumento deseado.
   - En Percentage (Porcentaje), ingrese el valor de aumento porcentual. Este valor debe ser al menos un 10% superior al valor actual.
   - Para Absolute (Absoluto), ingrese el nuevo valor en GiB, hasta el valor máximo permitido de 196 608 GiB.
7. En Provisioned SSD IOPS (IOPS de SSD provisionadas), tiene dos opciones para aprovisionar la cantidad de IOPS para su sistema de archivos:
   - Si desea que Amazon FSx escale automáticamente las IOPS de su SSD para mantener 3 IOPS de SSD aprovisionadas por GiB de capacidad de almacenamiento SSD (hasta un máximo de 160 000), elija Automatic (Automático).
   - Si desea especificar la cantidad de IOPS de SSD, elija User-provisioned (Aprovisionadas por el usuario). Ingrese un número absoluto de IOPS que sea al menos tres veces la cantidad de GiB de su nivel de almacenamiento SSD e inferior o igual a 160 000.

> **Note**
>
> Para obtener más información sobre la cantidad máxima de IOPS de SSD que puede aprovisionar para su sistema de archivos de FSx para ONTAP, consulte Impacto de la capacidad de rendimiento en el rendimiento.

8. Elija Actualizar.

> **Note**
>
> En la parte inferior del mensaje, se muestra una vista previa de la configuración de la nueva capacidad de almacenamiento de la SSD y de las IOPS de la SSD. En el caso de los sistemas de archivos ampliables, también se muestra el valor por par HA.

Para actualizar la capacidad de almacenamiento SSD y las IOPS aprovisionadas para un sistema de archivos (CLI)

Para actualizar la capacidad de almacenamiento SSD y las IOPS aprovisionadas para un sistema de archivos FSx for ONTAP, utilice el AWS CLI comando update-file-systemo la acción de API equivalente. UpdateFileSystem Defina los siguientes parámetros con sus valores:

- Establezca `--file-system-id` en el ID del sistema de archivos que va a actualizar.
- Para aumentar la capacidad de almacenamiento de su SSD, `--storage-capacity` establézcalo en el valor de capacidad de almacenamiento objetivo, que debe ser al menos un 10 por ciento superior al valor actual.
- Para modificar las IOPS de SSD aprovisionadas, utilice la propiedad `--ontap-configuration DiskIopsConfiguration`. Esta propiedad tiene dos parámetros, `Iops` y `Mode`:
  - Si desea especificar el número de IOPS aprovisionadas, utilice `Iops=`*`number_of_IOPS`* (hasta un máximo de 160 000) y `Mode=USER_PROVISIONED`. El valor de IOPS debe ser mayor o igual a tres veces la capacidad de almacenamiento SSD solicitado. Si no va a aumentar la capacidad de almacenamiento, el valor de las IOPS debe ser superior o igual a tres veces la capacidad de almacenamiento de la SSD actual.
  - Si quiere que Amazon FSx aumente automáticamente las IOPS de su SSD, utilice `Mode=AUTOMATIC` y no utilice el parámetro. `Iops` Amazon FSx mantendrá automáticamente 3 IOPS de SSD por GiB de la capacidad de almacenamiento SSD aprovisionada (hasta un máximo de 160 000).

> **Note**
>
> Para obtener más información sobre la cantidad máxima de IOPS de SSD que puede aprovisionar para su sistema de archivos de FSx para ONTAP, consulte Impacto de la capacidad de rendimiento en el rendimiento.

El siguiente ejemplo aumenta el almacenamiento en SSD del sistema de archivos a 2000 GiB y establece la cantidad de IOPS de SSD aprovisionadas por el usuario en 7000.

```
aws fsx update-file-system \
--file-system-id fs-0123456789abcdef0 \
--storage-capacity 2000 \
--ontap-configuration 'DiskIopsConfiguration={Iops=7000,Mode=USER_PROVISIONED}'
```

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

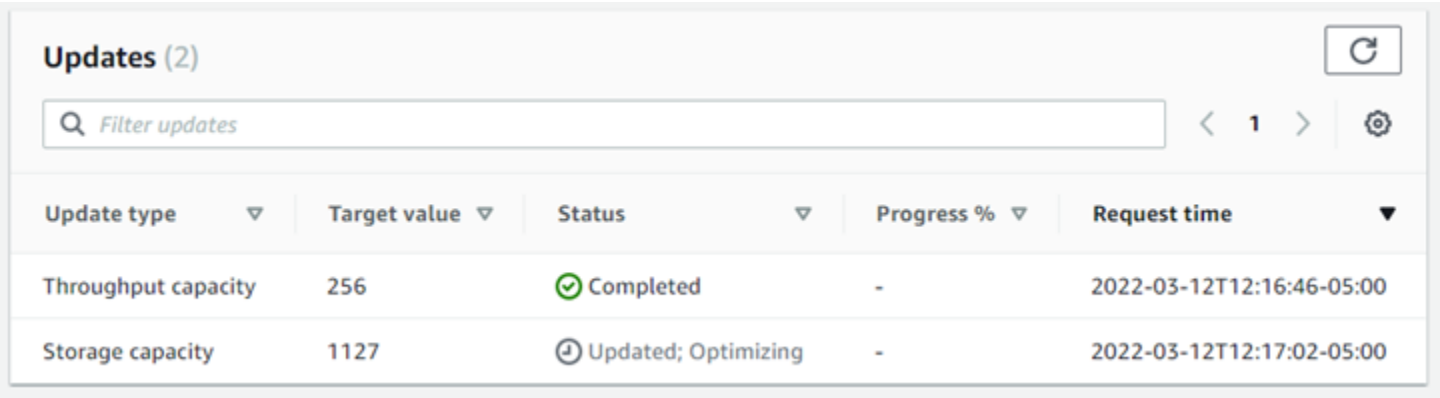
Para obtener más información, consulte la AdministrativeActionreferencia de la API Amazon FSx for NetApp ONTAP.

Monitoreo de la capacidad de almacenamiento y las actualizaciones de IOPS

Puede supervisar el progreso de una actualización de la capacidad de almacenamiento SSD y de las IOPS mediante la consola, la CLI y la API de Amazon FSx.

Para supervisar el almacenamiento y las actualizaciones de IOPS (consola)

En la pestaña Updates (Actualizaciones) de la ventana de Información del sistema de archivos, puede ver las 10 actualizaciones más recientes de cada tipo de actualización.



Para ver la capacidad de almacenamiento de la SSD y las actualizaciones de IOPS, puede consultar la siguiente información:

Tipo de actualización

Los tipos admitidos son la Capacidad de almacenamiento, el Modo y las IOPS. Los valores de Modo e IOPS aparecen en una lista para todas las solicitudes de escalado de la capacidad de almacenamiento y las IOPS.

Valor de destino

El valor al que especificó para actualizar la capacidad de almacenamiento SSD o las IOPS del sistema de archivos.

Status

Estado actual de la actualización. Los valores posibles son los siguientes:

- Pendiente: Amazon FSx recibió la solicitud de actualización, pero no ha empezado a procesarla.
- En curso: Amazon FSx está procesando la solicitud de actualización.
- Actualizado y optimizado: Amazon FSx aumentó la capacidad de almacenamiento en SSD del sistema de archivos. El proceso de optimización del almacenamiento ahora está reequilibrando los datos en segundo plano.
- Completada: la actualización finalizó correctamente.
- Error: la solicitud de actualización falló. Elija el signo de interrogación (?) para ver la información.

% de progreso

Muestra el progreso del proceso de optimización del almacenamiento como porcentaje completado.

Tiempo de solicitud

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

Para supervisar el almacenamiento y las actualizaciones de IOPS (CLI)

Puede ver y monitorear la capacidad de almacenamiento SSD del sistema de archivos y aumentar las solicitudes mediante el describe-file-systems AWS CLI comando y la operación de la DescribeFileSystemsAPI. La matriz de `AdministrativeActions` enumera las 10 acciones de actualización más recientes para cada tipo de acción administrativa. Al aumentar la capacidad de almacenamiento en SSD de un sistema de archivos, se generan dos acciones `AdministrativeActions`: una acción `FILE_SYSTEM_UPDATE` y una `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 acción administrativa pendiente para aumentar la capacidad de almacenamiento de la SSD a 2000 GiB y las IOPS de las SSD aprovisionadas a 7000.

```
"AdministrativeActions": [
    {
```

```
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586797629.095,
        "Status": "PENDING",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
             }
        }
    },
    {
        "AdministrativeActionType": "STORAGE_OPTIMIZATION",
        "RequestTime": 1586797629.095,
        "Status": "PENDING"
    }
]
```

Amazon FSx procesa primero la acción de `FILE_SYSTEM_UPDATE` y añade los discos de almacenamiento nuevos y de mayor tamaño 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`. Este comportamiento se muestra en el siguiente extracto de la respuesta de un comando 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 se haya completado correctamente, el estado de la `FILE_SYSTEM_UPDATE` acción cambia a `COMPLETED` y la acción `STORAGE_OPTIMIZATION` deja de aparecer.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586799169.445,
        "Status": "UPDATED_OPTIMIZING",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
```

```
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
            }
        }
    },
    {
        "AdministrativeActionType": "STORAGE_OPTIMIZATION",
        "ProgressPercent": 41,
        "RequestTime": 1586799169.445,
        "Status": "IN_PROGRESS"
    }
]
```

Si se produce un error en la solicitud de actualización de la capacidad de almacenamiento o de las IOPS, 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": 1586373915.697,
        "Status": "FAILED",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
            }
        },
        "FailureDetails": {
            "Message": "failure-message"
        }
    }
]
```

Aumento dinámico de la capacidad de almacenamiento SSD

Puede utilizar la siguiente solución para aumentar dinámicamente la capacidad de almacenamiento SSD de un sistema de archivos de FSx para ONTAP cuando la cantidad de capacidad de

almacenamiento SSD utilizada supere un umbral que especifique. Esta AWS CloudFormation plantilla implementa automáticamente todos los componentes necesarios para definir el umbral de capacidad de almacenamiento, la CloudWatch alarma de Amazon basada en este umbral y la AWS Lambda función que aumenta la capacidad de almacenamiento del sistema de archivos.

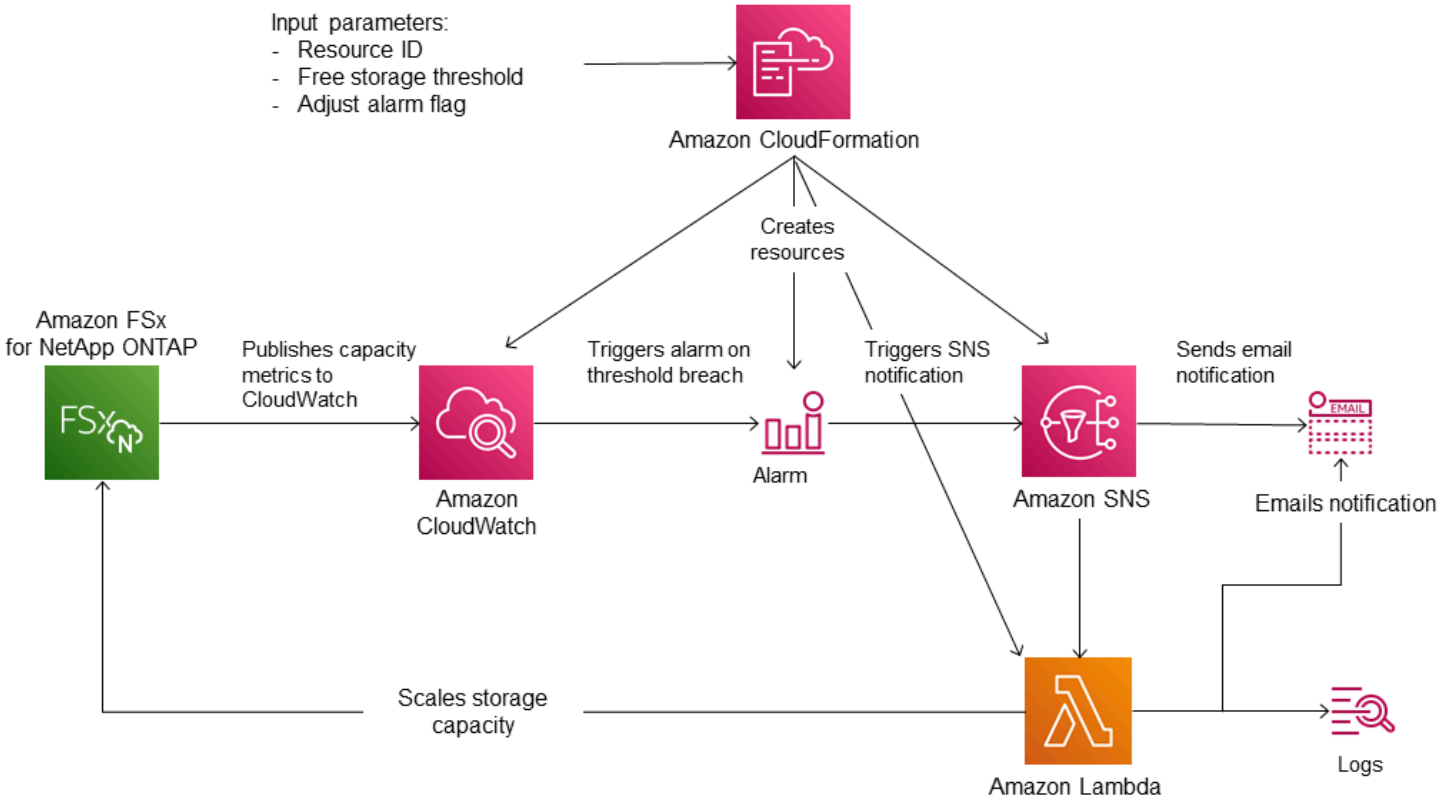
La solución implementa automáticamente todos los componentes necesarios y utiliza los siguientes parámetros:

- El ID de su sistema de archivos de FSx para ONTAP.
- El umbral de capacidad de almacenamiento de la SSD utilizada (valor numérico). Este es el porcentaje en el que se activará la CloudWatch alarma.
- El porcentaje en el que se va a aumentar la capacidad de almacenamiento (%).
- La dirección de correo electrónico utilizada para recibir las notificaciones de escalado.

Temas

Información general de la arquitectura

La implementación de esta solución crea los siguientes recursos en Nube de AWS.



El siguiente diagrama muestra los siguientes pasos:

1. La AWS CloudFormation plantilla despliega una CloudWatch alarma, una AWS Lambda función, una cola de Amazon Simple Notification Service (Amazon SNS) y todas las funciones obligatorias (IAM). AWS Identity and Access Management El rol de IAM otorga a la función de Lambda permiso para invocar las operaciones de la API de Amazon FSx.
2. CloudWatch activa una alarma cuando la capacidad de almacenamiento utilizada del sistema de archivos supera el umbral especificado y envía un mensaje a la cola de Amazon SNS. Sólo se activa una alarma cuando la capacidad utilizada del sistema de archivos supera el umbral de forma continua durante un período de 5 minutos.
3. A continuación, la solución activa la función de Lambda que está suscrita a este tema de Amazon SNS.
4. La función de Lambda calcula la nueva capacidad de almacenamiento del sistema de archivos en función del valor porcentual de aumento especificado y establece la nueva capacidad de almacenamiento del sistema de archivos.
5. El estado de CloudWatch alarma original y los resultados de las operaciones de la función Lambda se envían a la cola de Amazon SNS.

Para recibir notificaciones sobre las acciones que se realizan en respuesta a la CloudWatch alarma, debe confirmar la suscripción al tema de Amazon SNS siguiendo el enlace que se proporciona en el correo electrónico de confirmación de la suscripción.

AWS CloudFormation plantilla

Esta solución se utiliza AWS CloudFormation para automatizar la implementación de los componentes que se utilizan para aumentar automáticamente la capacidad de almacenamiento de un sistema de archivos FSx para ONTAP. Para usar esta solución, descargue la plantilla F. SxOntapDynamicStorageScaling AWS CloudFormation

La plantilla utiliza los Parámetros que se describen a continuación. Revise los parámetros de la plantilla y los valores predeterminados, y modifíquelos según las necesidades del sistema de archivos.

FileSystemId

Sin valor predeterminado. El ID del sistema de archivos cuya capacidad de almacenamiento desea aumentar de forma automática.

LowFreeDataStorageCapacityThreshold

Sin valor predeterminado. Especifica el umbral de capacidad de almacenamiento utilizado para activar una alarma y aumentar automáticamente la capacidad de almacenamiento del sistema de archivos, especificado en porcentaje (%) de la capacidad de almacenamiento actual del sistema de archivos. Se considera que el sistema de archivos tiene una capacidad de almacenamiento libre baja cuando el almacenamiento utilizado supera este umbral.

EmailAddress

Sin valor predeterminado. Especifica la dirección de correo electrónico que se va a utilizar para la suscripción a SNS y recibe las alertas sobre el umbral de capacidad de almacenamiento.

PercentIncrease

El valor predeterminado es 20%. Especifica la cantidad en la que se va a aumentar la capacidad de almacenamiento, expresada como porcentaje de la capacidad de almacenamiento actual.

> **Note**
>
> El escalado del almacenamiento se intenta escalar una vez cada vez que la CloudWatch alarma entra en `ALARM` estado. Si el uso de la capacidad de almacenamiento de la

SSD permanece por encima del umbral después de intentar realizar una operación de escalado del almacenamiento, la operación de escalado del almacenamiento no se volverá a intentar.

MaxF B SxSizeinGi

El valor predeterminado es 196608. Especifica la capacidad de almacenamiento máxima admitida para el almacenamiento SSD.

Despliegue automatizado con AWS CloudFormation

El siguiente procedimiento configura e implementa una AWS CloudFormation pila para aumentar automáticamente la capacidad de almacenamiento de un sistema de archivos FSx para ONTAP. La aplicación tarda unos minutos en implementarse. Para obtener más información sobre la creación de una CloudFormation pila, consulte Creación de una pila en la AWS CloudFormation consola en la Guía del usuario.AWS CloudFormation

> **Note**
>
> La implementación de esta solución implica la facturación de los AWS servicios asociados. Para más información, consulte las páginas de precios de estos servicios.

Antes de empezar, debe tener el ID del sistema de archivos Amazon FSx que se ejecuta en la Amazon Virtual Private Cloud (Amazon VPC) en su. Cuenta de AWS Para obtener más información sobre cómo crear los recursos de Amazon FSx, consulte Introducción a Amazon FSx para ONTAP NetApp .

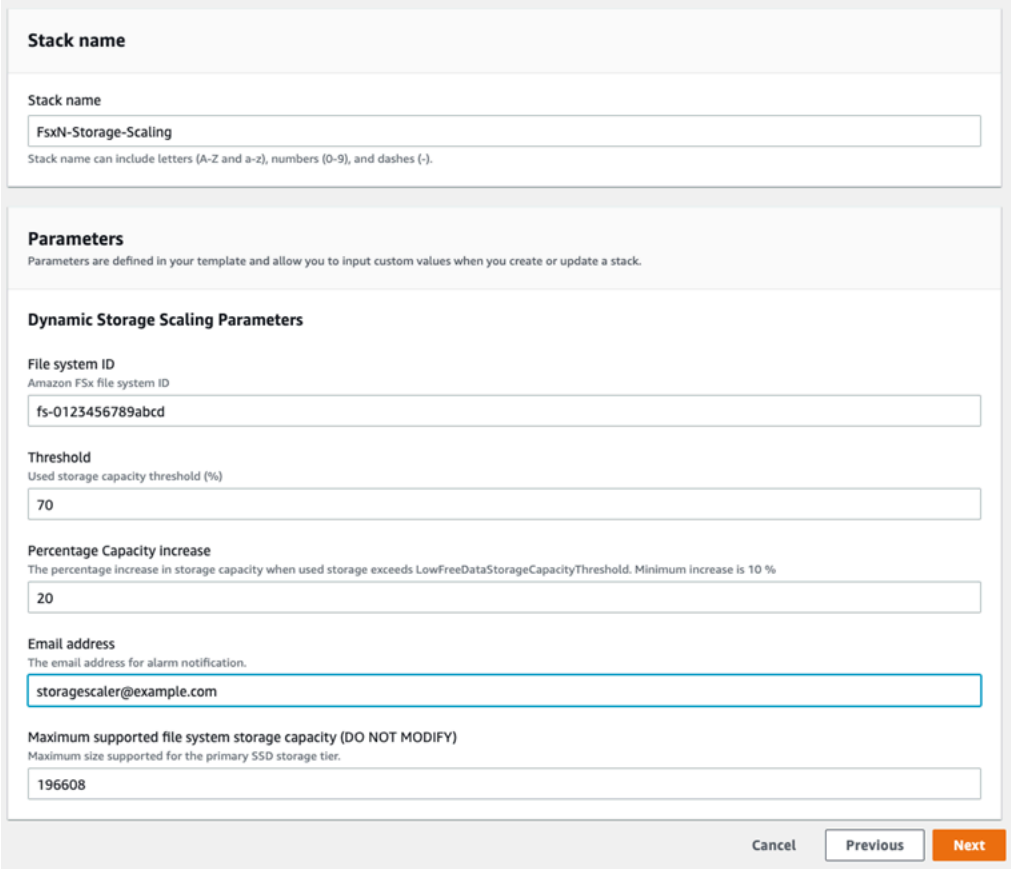
Para iniciar la pila de soluciones para el aumento de la capacidad de almacenamiento automático

1. Descargue la plantilla F. SxOntapDynamicStorageScaling AWS CloudFormation

> **Note**
>
> Actualmente, Amazon FSx solo está disponible en regiones específicas AWS . Debe lanzar esta solución en una AWS región en la que Amazon FSx esté disponible. Para

obtener más información, consulte Puntos de conexión de Amazon FSx y cuotas en Referencia general de AWS.

2. En la AWS CloudFormation consola, seleccione Crear pila > Con nuevos recursos.
3. Selecciona La plantilla está lista. En la sección Specify template (Especificar plantilla), seleccione Update a template file (Cargar un archivo de plantilla) y cargue la plantilla que descargó.
4. En Specify stack details (Especificar los detalles de la pila), ingrese los valores de la solución de aumento automático de la capacidad de almacenamiento.



5. Establezca un Nombre de pila.
6. En el caso de los Parámetros, revise los parámetros de la plantilla y modifíquelos para adaptarlos a las necesidades de su sistema de archivos. A continuación, elija Siguiente.

> **Note**
>
> Para recibir notificaciones por correo electrónico cuando esta CloudFormation plantilla intente escalar, confirme el correo electrónico de suscripción a SNS que recibe después de implementar la plantilla.

7. Ingrese la configuración de Opciones que desee para su solución personalizada y, a continuación, seleccione Next (Siguiente).
8. En Review, revise y confirme la configuración. Debe seleccionar la casilla para aceptar que la plantilla crea recursos de IAM.
9. Elija Crear para implementar la pila.

Puede ver el estado de la pila en la AWS CloudFormation consola, en la columna Estado. Debería ver el estado CREATE_COMPLETE en unos minutos.

Actualización la pila

Una vez creada la pila, puede actualizarla con la misma plantilla y proporcionando nuevos valores para los parámetros. Para obtener más información, consulte la Actualización de pilas directamente en la Guía del usuario de AWS CloudFormation .

Capacidad de almacenamiento de volumen

Los volúmenes FSx para ONTAP son recursos virtuales que se utilizan para agrupar datos, determinar cómo se almacenan los datos y determinar el tipo de acceso a los datos. Los volúmenes, como las carpetas, no consumen por sí mismos la capacidad de almacenamiento del sistema de archivos. Sólo los datos que se almacenan en un volumen consumen el almacenamiento SSD y, según la Política por niveles del volumen, el almacenamiento acumulado de capacidad. El tamaño de un volumen se establece al crearlo y se puede cambiar posteriormente. Puede supervisar y gestionar la capacidad de almacenamiento de sus FSx para los volúmenes de ONTAP mediante la API AWS Management Console, AWS CLI y la CLI de ONTAP.

Temas

- Organización de datos de volumen en niveles
- Capacidad de almacenamiento de instantáneas y volumen

- Capacidad de archivos de volumen
- Actualización de la capacidad de almacenamiento de un volumen
- Habilitar el ajuste automático del tamaño del volumen
- Supervisión de la capacidad de almacenamiento por volumen
- Establecer la política de niveles de un volumen
- Establecer los días mínimos de enfriamiento
- Establecer la política de recuperación de un volumen en la nube
- Visualización de la capacidad de archivos de un volumen
- Aumentar el número máximo de archivos en un volumen
- Habilitar el modo de escritura en la nube de un volumen

Organización de datos de volumen en niveles

Un sistema de archivos Amazon FSx para NetApp ONTAP tiene dos niveles de almacenamiento: almacenamiento principal y almacenamiento agrupado de capacidad. El almacenamiento principal es un almacenamiento SSD aprovisionado, escalable y de alto rendimiento diseñado específicamente para la parte activa del conjunto de datos. El almacenamiento agrupado con capacidad es un nivel de almacenamiento totalmente elástico que puede escalar hasta petabytes y tiene un coste optimizado para los datos a los que se accede con poca frecuencia.

Los datos de cada volumen se agrupan automáticamente en el nivel de almacenamiento del grupo de capacidad en función de la política de estratificación del volumen, el período de enfriamiento y la configuración de los umbrales. En las siguientes secciones se describen las políticas de estratificación del ONTAP volumen y los umbrales que se utilizan para determinar cuándo se agrupan los datos en niveles en el grupo de capacidad.

Políticas de estratificación de volúmenes

Para determinar cómo utilizar los FSx para los niveles de almacenamiento del sistema de archivos ONTAP, debe elegir la política de estratificación de cada volumen del sistema de archivos. Usted elige la política de organización en niveles al crear un volumen y puede modificarla en cualquier momento con la consola de Amazon FSx AWS CLI, la API o NetApp mediante herramientas de administración. Puede elegir una de las siguientes políticas que determinan qué datos, si los hay, se agrupan en niveles en el pool de capacidad de almacenamiento.

> **Note**
>
> La organización en niveles puede mover los datos de los archivos y los datos de las instantáneas al nivel del pool de capacidad. Sin embargo, los metadatos de los archivos siempre permanecen en el nivel SSD. Para obtener más información, consulte Cómo se usa el almacenamiento SSD.

- Auto: esta política traslada todos los datos inactivos (datos de usuario e instantáneas) al nivel del pool de capacidad. La velocidad de enfriamiento de los datos viene determinada por el período de enfriamiento de la política, que de forma predeterminada es de 31 días, y se puede configurar en valores entre 2 y 183 días. Cuando los bloques de datos inactivos subyacentes se leen de forma aleatoria (como en un acceso a archivos normal), se calientan y se escriben en el nivel de almacenamiento principal. Cuando los bloques de datos inactivos se leen secuencialmente (por ejemplo, mediante un análisis antivirus), permanecen fríos y permanecen en el nivel de almacenamiento del pool de capacidad. Esta es la política predeterminada al crear un volumen con la consola Amazon FSx.
- Sólo instantáneas: esta política mueve solo datos de instantáneas al nivel de almacenamiento del pool de capacidad. La velocidad a la que las instantáneas se agrupan en niveles en el pool de capacidad viene determinada por el período de enfriamiento de la política, que de forma predeterminada se establece en 2 días y se puede configurar en valores entre 2 y 183 días. Cuando se leen datos de instantáneas inactivas, se calientan y se escriben en el nivel de almacenamiento principal. Esta es la política predeterminada al crear un volumen mediante la AWS CLI API Amazon FSx o la CLI de NetApp ONTAP.
- Todos: esta política marca todos los datos de los usuarios y los datos de las instantáneas como inactivos y los almacena en el nivel del pool de capacidad. Cuando se leen los bloques de datos, permanecen inactivos y no se escriben en el nivel de almacenamiento principal. Cuando los datos se escriben en un volumen con la política de Todos los niveles, se siguen escribiendo inicialmente en el nivel de almacenamiento SSD y se agrupan en niveles en el conjunto de capacidades mediante un proceso en segundo plano. Tenga en cuenta que los metadatos de los archivos siempre permanecen en el nivel SSD.
- Ninguna: esta política mantiene todos los datos del volumen en el nivel de almacenamiento principal e impide que se trasladen al almacenamiento del pool de capacidad. Si establece un volumen en esta política después de haber utilizado cualquier otra política, los datos existentes en el volumen que se encontraban en el almacenamiento del pool de capacidad se mueven al almacenamiento SSD mediante un proceso en segundo plano, siempre y cuando la utilización del

SSD sea inferior al 90%. Este proceso en segundo plano se puede acelerar leyendo los datos de forma intencionada o modificando la política de recuperación en la nube del volumen. Para obtener más información, consulte Políticas de recuperación en la nube.

Como práctica recomendada, al migrar los datos que planea almacenar a largo plazo en un pool de almacenamiento, le recomendamos que utilice la política de niveles Automática en su volumen. Con la asignación de niveles Automática, los datos se almacenan en el nivel de almacenamiento SSD durante un mínimo de 2 días (en función del periodo de refrigeración del volumen) antes de pasar al nivel del pool de capacidad. Al conservar los datos en el almacenamiento SSD durante al menos 2 días, ONTAP puede ahorrar en la compresión y la deduplicación posteriores al proceso de los datos, que se conservan cuando los datos se agrupan en niveles según el conjunto de capacidad. ONTAP sólo ejecuta la compresión y la deduplicación posteriores al proceso para los datos del almacenamiento SSD, por lo que seleccionar esta política puede ayudarle a maximizar sus ahorros de almacenamiento a largo plazo. También puede maximizar las velocidades de transferencia de las primeras copias de seguridad que cree de sus volúmenes, ya que los datos de los que se está haciendo la copia de seguridad se encuentran en un almacenamiento SSD.

Para obtener más información sobre cómo configurar o modificar la política de organización por niveles de un volumen, consulte Establecer la política de niveles de un volumen.

Periodo de enfriamiento de organización en niveles

El periodo de enfriamiento por niveles de un volumen establece la cantidad de tiempo que tardan los datos del nivel de SSD en marcarse como fríos. El periodo de enfriamiento se aplica a las políticas de niveles `Auto` y `Snapshot-only`. Puede establecer el período de refrigeración en un valor comprendido entre 2 y 183 días. Para obtener más información sobre la configuración del periodo de enfriamiento, consulte Establecer los días mínimos de enfriamiento.

Los datos se agrupan entre 24 y 48 horas después de que finalice su periodo de enfriamiento. La organización en niveles es un proceso en segundo plano que consume recursos de la red y tiene una prioridad inferior a la de las solicitudes dirigidas a los clientes. Las actividades de organización por niveles se limitan cuando hay solicitudes continuas dirigidas a los clientes.

Políticas de recuperación en la nube

La política de recuperación en la nube de un volumen establece las condiciones que especifican cuándo se permite que los datos leídos del nivel del pool de capacidad pasen al nivel de SSD. Si la política de recuperación en la nube se establece de forma distinta a `Default`, esta política anula el

comportamiento de recuperación de la política de organización por niveles del volumen. Un volumen puede tener una de las siguientes políticas de recuperación de la nube:

- Predeterminada: esta política recupera datos por niveles basándose en la política de niveles subyacente del volumen. Esta es la política de recuperación en la nube predeterminada para todos los volúmenes.
- Nunca: esta política nunca recupera datos por niveles, independientemente de si las lecturas son secuenciales o aleatorias. Esto es similar a configurar la política de organización por niveles de su volumen en Todos, con la diferencia de que puede utilizarla con otras políticas (Automática o Sólo instantáneas) para clasificar los datos según el período mínimo de enfriamiento en lugar de hacerlo de forma inmediata.
- Durante la lectura: esta política recupera datos por niveles para todas las lecturas de datos dirigidas por el cliente. Esta política no tiene efecto cuando se utiliza la política Todos los niveles.
- Promocionar: esta política marca todos los datos de un volumen que se encuentran en el pool de capacidad para su recuperación en el nivel SSD. Los datos se marcarán la próxima vez que se ejecute el escáner diario de organización en niveles en segundo plano. Esta política es beneficiosa para las aplicaciones que tienen cargas de trabajo cíclicas que se ejecutan con poca frecuencia, pero que requieren el rendimiento del nivel SSD cuando se ejecutan. Esta política no tiene efecto cuando se utiliza la política Todos los niveles.

Para obtener información sobre cómo configurar la política de recuperación de un volumen en la nube, consulte Establecer la política de recuperación de un volumen en la nube.

Umbrales de niveles

La utilización de la capacidad de almacenamiento SSD de un sistema de archivos determina la forma en que ONTAP gestiona el comportamiento de organización en niveles de todos los volúmenes. En función del uso de la capacidad de almacenamiento SSD de un sistema de archivos, los siguientes umbrales establecen el comportamiento de organización en niveles tal como se describe. Para obtener información sobre cómo monitorizar la utilización de la capacidad del nivel de almacenamiento SSD de un volumen, consulte Supervisión de la capacidad de almacenamiento por volumen.

> **Note**
>
> Le recomendamos que no supere el 80% de utilización de la capacidad de almacenamiento de su nivel de almacenamiento SSD. En el caso de los sistemas de archivos escalables,

esta recomendación se aplica tanto a la utilización media total de todos los agregados del sistema de archivos como a la utilización de cada agregado individual. Esto garantiza que la organización en niveles funcione correctamente y supone una sobrecarga para los datos nuevos. Si su nivel de almacenamiento SSD utiliza constantemente la capacidad de almacenamiento por encima del 80%, puede aumentar la capacidad de su nivel de almacenamiento SSD. Para obtener más información, consulte Actualización del sistema de archivos, el almacenamiento SSD y las IOPS.

FSx para ONTAP utiliza los siguientes umbrales de capacidad de almacenamiento para gestionar la organización en niveles de los volúmenes:

- Utilización del nivel de almacenamiento SSD inferior al 50%: en este umbral, se considera que el nivel de almacenamiento SSD está infrautilizado, y sólo los volúmenes que están utilizando la política Todos los niveles tienen datos escalonados en el almacenamiento del pool de capacidad. Los volúmenes con políticas Auto y Sólo instantáneas no clasifican los datos en este umbral.
- Utilización de los niveles de almacenamiento SSD superior al 50%: los volúmenes con políticas de niveles Auto y Sólo instantáneas los datos según la configuración de estratificación mínima de días de enfriamiento. El valor predeterminado es de 31 días.
- Utilización del nivel de almacenamiento SSD superior al 90%: en este umbral, Amazon FSx prioriza la conservación del espacio en el nivel de almacenamiento SSD. Los datos fríos del nivel del pool de capacidad ya no se mueven al nivel de almacenamiento SSD cuando se leen para volúmenes que utilizan las políticas Auto y Sólo instantáneas.
- Utilización del nivel de almacenamiento SSD superior al 98%: todas las funciones de organización en niveles se detienen cuando el nivel de almacenamiento SSD tiene un uso igual o superior al 98%. Puede seguir leyendo desde los niveles de almacenamiento, pero no puede escribir en ellos.

Capacidad de almacenamiento de instantáneas y volumen

Una instantánea es una imagen de solo lectura de un volumen de Amazon FSx for NetApp ONTAP en un momento dado. Las copias instantáneas ofrecen protección contra la eliminación o modificación accidental de los archivos de sus volúmenes por parte de los usuarios finales. Con las instantáneas, los usuarios pueden ver y restaurar fácilmente archivos o carpetas individuales a partir de una instantánea anterior.

Las instantáneas se almacenan junto con los datos del sistema de archivos y consumen la capacidad de almacenamiento del sistema de archivos. Sin embargo, las instantáneas consumen capacidad de

almacenamiento solo para las partes de los archivos que han cambiado desde la última instantánea. Las instantáneas no se incluyen en las copias de seguridad de los volúmenes del sistema de archivos.

Las instantáneas están habilitadas de forma predeterminada en sus volúmenes, mediante la política de instantáneas predeterminada. Las instantáneas se almacenan en el directorio `.snapshot` de la raíz de un volumen. Puede administrar la capacidad de almacenamiento por volumen de instantáneas de las siguientes maneras:

- Políticas de instantáneas: seleccione una política de instantáneas integrada o elija una política personalizada que se haya creado en la CLI de ONTAP o la API de REST.
- Eliminar las instantáneas manualmente: recupere la capacidad de almacenamiento eliminando las instantáneas manualmente.
- Crear una política de eliminación automática de instantáneas: cree una política que elimine más instantáneas que la política de instantáneas predeterminada.
- Desactivar las instantáneas automáticas: conserve la capacidad de almacenamiento desactivando las instantáneas automáticas.

Para obtener más información, consulte Uso de instantáneas.

Capacidad de archivos de volumen

Los volúmenes de Amazon FSx para NetApp ONTAP tienen punteros de archivos que se utilizan para almacenar los metadatos de los archivos, como el nombre del archivo, la hora del último acceso, los permisos y el tamaño, y para servir como punteros a los bloques de datos. Estos punteros de archivos se denominan inodos y cada volumen tiene una capacidad finita para el número de inodos, lo que se denomina capacidad de archivos de volumen. Cuando un volumen se agota o se agotan los archivos disponibles (inodos), no se pueden escribir datos adicionales en ese volumen.

La cantidad de objetos del sistema de archivos (archivos, directorios, copias instantáneas) que puede contener un volumen viene determinada por el número de inodos que tenga. El número de inodos de un volumen aumenta proporcionalmente a la capacidad de almacenamiento del volumen (y al número de componentes del volumen). FlexGroup De forma predeterminada, los FlexVol volúmenes (o FlexGroup componentes) con una capacidad de almacenamiento de 648 GiB o más tienen todos el mismo número de inodos: 21 251 126. Si crea un volumen superior a 648 GiB y desea que tenga más de 21 251 126 inodos, debe aumentar el número máximo de inodos (archivos) manualmente.

Para obtener más información sobre la visualización del número máximo de archivos de un volumen, consulte. Visualización de la capacidad de archivos de un volumen

El número predeterminado de inodos en un volumen es 1 inodo por cada 32 KiB de capacidad de almacenamiento de volumen, hasta un tamaño de volumen de 648 GiB. Para un volumen de 1 GiB:

Tamaño del volumen en bytes × (1 archivo ÷ inode_size_in_bytes) = maximum_number_of_files

1 073 741 824 bytes × (1 archivo ÷ 32 768 bytes) = 32 768 archivos

Puede aumentar el número máximo de inodos que puede contener un volumen, hasta un máximo de 1 inodo por cada 4 KiB de capacidad de almacenamiento. Para un volumen de 1 GiB, esto aumenta el número máximo de inodos o archivos de 32.768 a 262.144:

1 073 741 824 bytes × (1 archivo ÷ 4096 bytes) = 262 144 archivos

Un volumen de FSx para ONTAP puede tener un máximo de 2 mil millones de inodos.

Para obtener información sobre cómo cambiar el número máximo de archivos que puede almacenar un volumen, consulteAumentar el número máximo de archivos en un volumen.

Actualización de la capacidad de almacenamiento de un volumen

Puede gestionar la capacidad de almacenamiento por volumen aumentando o disminuyendo manualmente el tamaño del volumen mediante la AWS Management Console API AWS CLI y la CLI de ONTAP. También puede activar el ajuste automático del tamaño del volumen para que el tamaño del volumen aumente o disminuya automáticamente cuando alcance determinados umbrales de capacidad de almacenamiento utilizada. Utilice la CLI de ONTAP para gestionar el tamaño automático del volumen.

Para cambiar la capacidad de almacenamiento de un volumen (consola)

- Puede aumentar o reducir la capacidad de almacenamiento de un volumen mediante la consola y la API de Amazon FSx. AWS CLI Para obtener más información, consulte Actualización de un volumen.

También puede usar la ONTAP CLI para modificar la capacidad de almacenamiento de un volumen mediante el `volume modify`comando.

Para modificar el tamaño de un volumen (ONTAP CLI)

1. Para acceder a la CLI de NetApp ONTAP, ejecute el siguiente comando para establecer una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP. Reemplace *management_endpoint_ip* con la dirección IP del puerto de gestión del sistema de archivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obtener más información, consulte Administración de sistemas de archivos con la ONTAP CLI.
2. Utilice el comando CLI volume modify ONTAP para modificar la capacidad de almacenamiento de un volumen. Ejecute el siguiente comando, utilizando sus datos en lugar de los valores siguientes:

   - Reemplace *svm_name* con el nombre de la máquina virtual de almacenamiento (SVM) en el que se crea el volumen.
   - *vol_name*Sustitúyalo por el nombre del volumen cuyo tamaño desee cambiar.
   - Reemplace *vol_size* con el nuevo tamaño del volumen en el formato *integer*`[KB|MB|GB|TB|PB]`; por ejemplo, `100GB` para aumentar el tamaño del volumen a 100 gigabytes.

   ```
   ::> volume modify -vserver svm_name -volume vol_name -size vol_size
   ```

Habilitar el ajuste automático del tamaño del volumen

Ajuste automático del tamaño del volumen para que el volumen crezca automáticamente hasta un tamaño específico cuando alcance el umbral de espacio utilizado. Puede hacerlo para los tipos de FlexVol volumen (el tipo de volumen predeterminado para FSx para ONTAP) mediante el comando CLI de ONTAP `volume autosize`.

Para habilitar el ajuste automático del tamaño del volumen (ONTAP CLI)

1. Para acceder a la CLI de NetApp ONTAP, ejecute el siguiente comando para establecer una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP. Reemplace *management_endpoint_ip* con la dirección IP del puerto de gestión del sistema de archivos.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Para obtener más información, consulte Administración de sistemas de archivos con la ONTAP CLI.

2. Utilice el comando `volume autosize` como se muestra; para ello, reemplace los siguientes valores:

   - Reemplace *svm_name* con el nombre de la SVM en la que se creó el volumen.
   - Reemplace *vol_name* con el nombre del volumen cuyo tamaño desee cambiar.
   - Reemplace *grow_threshold* con un valor porcentual de espacio usado (por ejemplo, 90) en el que el volumen aumentará automáticamente de tamaño (hasta el valor *max_size*).
   - Reemplace *max_size* con el tamaño máximo al que pueda crecer el volumen. Utilice el formato *integer*[KB|MB|GB|TB|PB]; por ejemplo, 300TB. El tamaño máximo es 300 TB. El valor predeterminado es el 120% del tamaño del volumen.
   - Reemplace *min_size* con el tamaño mínimo al que se reducirá el volumen. Utilice el mismo formato que para *max_size*.
   - Reemplace *shrink_threshold* con el porcentaje de espacio utilizado en el que el volumen se reducirá automáticamente de tamaño.

```
::> volume autosize -vserver svm_name -volume vol_name -mode grow_shrink -
grow-threshold-percent grow_threshold -maximum-size max_size -shrink-threshold-
percent shrink_threshold -minimum-size min_size
```

Supervisión de la capacidad de almacenamiento por volumen

Puede ver el almacenamiento disponible de un volumen y su distribución de almacenamiento en AWS Management Console AWS CLI, y en la CLI de NetApp ONTAP.

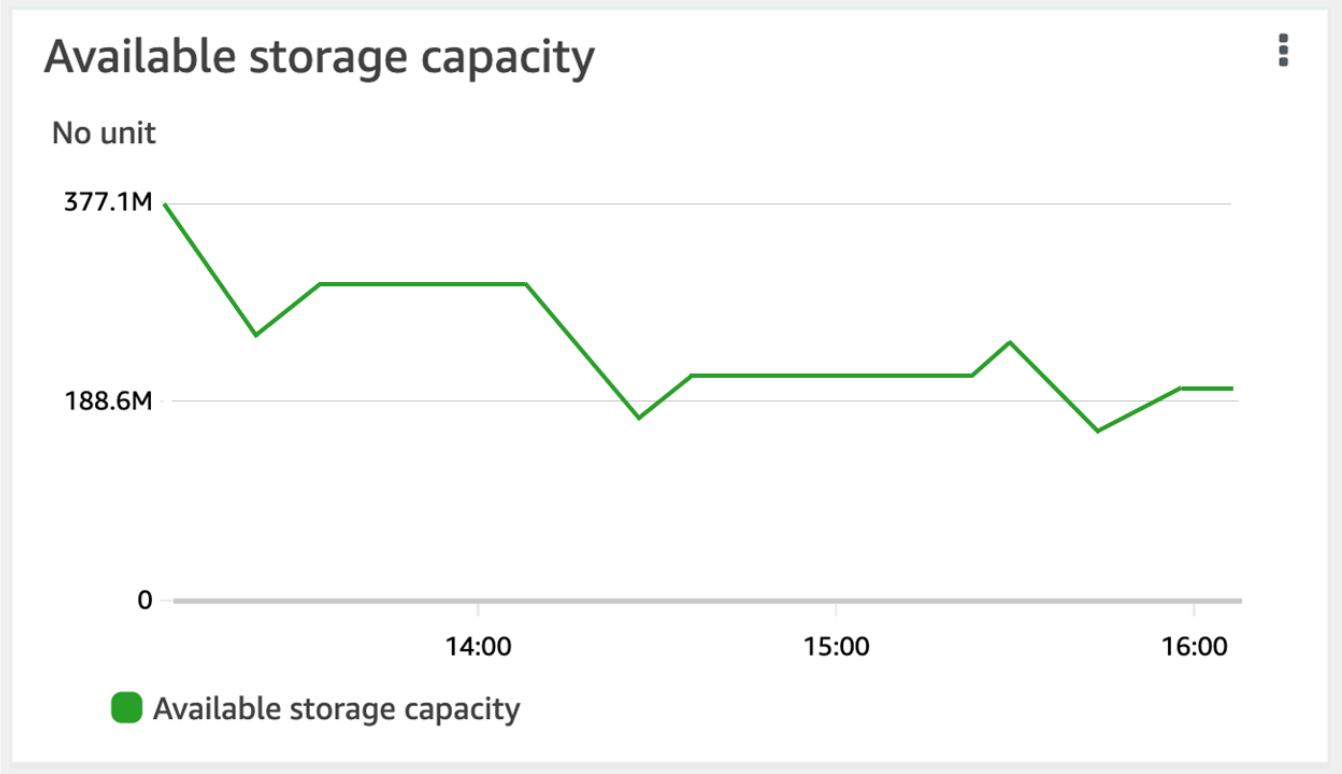
Para supervisar la capacidad de almacenamiento de un volumen (consola)

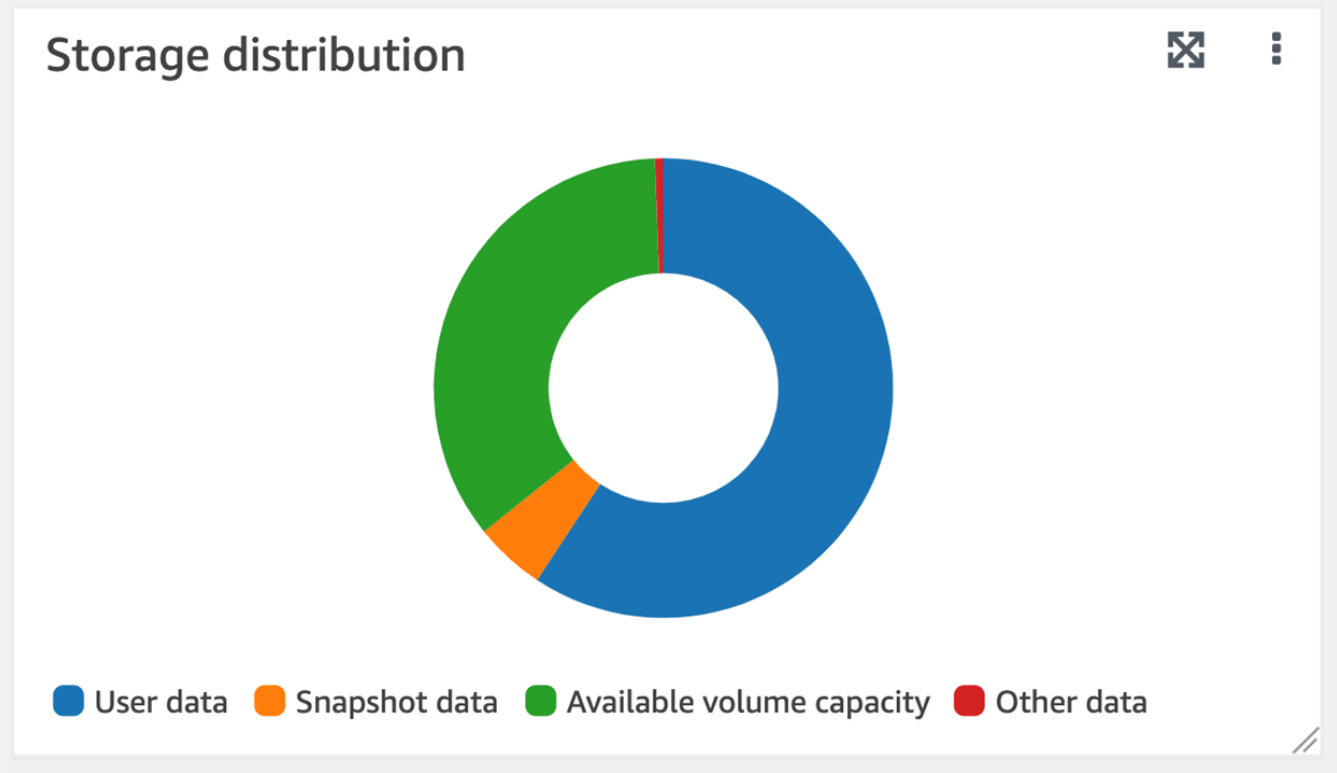
El gráfico de Almacenamiento disponible muestra la cantidad de capacidad de almacenamiento libre de un volumen a lo largo del tiempo. El gráfico Distribución del almacenamiento muestra cómo se distribuye actualmente la capacidad de almacenamiento de un volumen en 4 categorías:

- Datos de usuario

- Datos instantáneos
- Capacidad de volumen disponible
- Otros datos

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Seleccione Volumes (Volúmenes) en la columna de navegación de la izquierda y, a continuación, elija el volumen de ONTAP del que desee ver la información sobre la capacidad de almacenamiento. Aparece la página de detalles del volumen.
3. En el segundo panel, elija la pestaña Monitoring (Monitoreo). Aparecen los gráficos Almacenamiento disponible y Distribución del almacenamiento, junto con otros gráficos.





Para monitorear la capacidad de almacenamiento (ONTAPCLI) de un volumen

Puede supervisar el consumo de la capacidad de almacenamiento del volumen mediante el comando `volume show-space` ONTAP CLI. Para obtener más información, consulte `volume show-space`el Centro de NetApp ONTAP documentación.

1. Para acceder a la CLI de NetApp ONTAP, ejecute el siguiente comando para establecer una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP. Reemplace *`management_endpoint_ip`* con la dirección IP del puerto de gestión del sistema de archivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obtener más información, consulte Administración de sistemas de archivos con la ONTAP CLI.

2. Vea el uso de la capacidad de almacenamiento de un volumen emitiendo el siguiente comando, reemplazando los siguientes valores:

   - Reemplace *`svm_name`* con el nombre de la SVM en la que se creó el volumen.

- Reemplace *vol_name* con el nombre del volumen para el que está configurando la política de división en niveles de datos.

```
::> volume show-space -vserver svm_name -volume vol_name
```

Si el comando se ejecuta correctamente, verá una salida similar a la siguiente:

```
Vserver : svm_name
Volume  : vol_name
Feature                                     Used      Used%
--------------------------------     ----------     ------
User Data                                  140KB         0%
Filesystem Metadata                      164.4MB         1%
Inodes                                   10.28MB         0%
Snapshot Reserve                         563.2MB         5%
Deduplication                               12KB         0%
Snapshot Spill                            9.31GB        85%
Performance Metadata                        668KB         0%

Total Used                               10.03GB        91%

Total Physical Used                      10.03GB        91%
```

El resultado de este comando muestra la cantidad de espacio físico que ocupan los distintos tipos de datos en este volumen. También muestra el porcentaje de la capacidad total del volumen que consume cada tipo de datos. En este ejemplo, `Snapshot Spill` y `Snapshot Reserve` consumen un 90 por ciento combinado de la capacidad del volumen.

`Snapshot Reserve` muestra la cantidad de espacio en disco reservado para almacenar las copias instantáneas. Si el almacenamiento de copias instantáneas supera el espacio de reserva, se derrama en el sistema de archivos y esta cantidad se muestra en `Snapshot Spill`.

Para aumentar la cantidad de espacio disponible, puede aumentar el tamaño del volumen o eliminar las instantáneas que no esté utilizando, como se muestra en los procedimientos siguientes.

Para los tipos de FlexVol volumen (el tipo de volumen predeterminado para FSx para los volúmenes ONTAP), también puede activar el tamaño automático de los volúmenes. Al activar el tamaño automático, el tamaño del volumen aumenta automáticamente cuando alcanza determinados

umbrales. También existe la posibilidad de desactivar las instantáneas automáticas. Ambas funciones se explican en las siguientes secciones.

Establecer la política de niveles de un volumen

Puede modificar la política de organización en niveles de un volumen mediante la AWS Management Console API AWS CLI y y la CLI de ONTAP.

Para modificar la política de organización de datos en niveles de un volumen (consola)

Utilice el procedimiento siguiente para modificar la política de organización de datos de un volumen con AWS Management Console.

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Seleccione Volumes (Volúmenes) en el panel de navegación izquierdo y, a continuación, seleccione el volumen ONTAP para el que desea modificar la política de niveles de datos.
3. Seleccione Update volume (Actualizar volumen) en el menú desplegable Actions (Acciones). Aparece la ventana Update volume (Actualizar volumen).
4. En la Política de niveles del pool de capacidades, elija la nueva política para el volumen. Para obtener más información, consulte Políticas de estratificación de volúmenes.
5. Seleccione Update (Actualizar) para aplicar la nueva política al volumen.

Para establecer una política de organización por niveles (CLI) de un volumen

- Modifique la política de estratificación de un volumen mediante el comando CLI update-volume UpdateVolume(es la acción equivalente de la API Amazon FSx). El siguiente ejemplo de comando de la CLI establece la política de niveles de datos de un volumen en `SNAPSHOT_ONLY`.

```
aws fsx update-volume \
    --volume-id fsxvol-abcde0123456789f
    --ontap-configuration TieringPolicy={Name=SNAPSHOT_ONLY}
```

El sistema responde con la descripción del volumen para una solicitud correcta.

```
{
    "Volume": {
        "CreationTime": "2021-10-05T14:27:44.332000-04:00",
        "FileSystemId": "fs-abcde0123456789f",
```

```
        "Lifecycle": "CREATED",
        "Name": "vol1",
        "OntapConfiguration": {
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "UNIX",
            "SizeInMegabytes": 1048576,
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abc0123de456789f",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "CoolingPeriod": 2,
                "Name": "SNAPSHOT_ONLY"
            },
            "UUID": "aaaa1111-bb22-cc33-dd44-abcde01234f5",
            "OntapVolumeType": "RW"
        },
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcde0123456789f/fsvol-abc012def3456789a",
        "VolumeId": "fsvol-abc012def3456789a",
        "VolumeType": "ONTAP"
    }
}
```


Para modificar la política de niveles de un volumen (ONTAP CLI)

El comando `volume modify` CLI de ONTAP se utiliza para establecer la política de niveles de un volumen. Para obtener más información, consulte el Centro de documentación de `volume modify`ONTAP NetApp .

1. Para acceder a la CLI de NetApp ONTAP, ejecute el siguiente comando para establecer una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP. Reemplace *`management_endpoint_ip`* con la dirección IP del puerto de gestión del sistema de archivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obtener más información, consulte Administración de sistemas de archivos con la ONTAP CLI.

2. Acceda al modo avanzado de la CLI de ONTAP con el siguiente comando.

```
FSx::> set adv

Warning: These advanced commands are potentially dangerous; use them only when
     directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y
```

3. Utilice el siguiente comando para modificar la política de organización de datos de volumen en niveles; para ello, reemplace los siguientes valores:

   - Reemplace *svm_name* con el nombre de la SVM en la que se creó el volumen.
   - Reemplace *vol_name* con el nombre del volumen para el que está configurando la política de división en niveles de datos.
   - Reemplace *tiering_policy* con la política deseada. Los valores válidos son `snapshot-only`, `auto`, `all` o `none`. Para obtener más información, consulte Políticas de estratificación de volúmenes.

```
FSx::> volume modify -vserver svm_name -volume vol_name -tiering-
policy tiering_policy
```

Establecer los días mínimos de enfriamiento

Los días de enfriamiento mínimos para un volumen establecen el umbral que se utiliza para determinar qué datos están calientes y cuáles están fríos. Puede establecer los días de refrigeración mínimos de un volumen mediante una API AWS CLI y la CLI de ONTAP.

Para establecer el número mínimo de días de refrigeración (CLI) de un volumen

- Modifique la configuración de un volumen mediante el comando CLI update-volume (UpdateVolumees la acción equivalente de la API Amazon FSx). El siguiente ejemplo de comando CLI establece un volumen `CoolingPeriod` en 104 días.

```
aws fsx update-volume \
    --volume-id fsxvol-abcde0123456789f
    --ontap-configuration TieringPolicy={Name=SNAPSHOT_ONLY}
aws fsx update-volume --volume-id fsvol-006530558c14224ac --ontap-configuration
 TieringPolicy={CoolingPeriod=104}
```

El sistema responde con la descripción del volumen si la solicitud se ha realizado correctamente.


```
{
    "Volume": {
        "CreationTime": "2021-10-05T14:27:44.332000-04:00",
        "FileSystemId": "fs-abcde0123456789f",
        "Lifecycle": "CREATED",
        "Name": "vol1",
        "OntapConfiguration": {
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "UNIX",
            "SizeInMegabytes": 1048576,
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abc0123de456789f",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "CoolingPeriod": 104,
                "Name": "SNAPSHOT_ONLY"
            },
            "UUID": "aaaa1111-bb22-cc33-dd44-abcde01234f5",
            "OntapVolumeType": "RW"
        },
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcde0123456789f/fsvol-abc012def3456789a",
        "VolumeId": "fsvol-abc012def3456789a",
        "VolumeType": "ONTAP"
    }
}
```


Para establecer los días de refrigeración mínimos de un volumen (ONTAP CLI)

Utilice el comando `volume modify` CLI ONTAP para establecer el número mínimo de días de enfriamiento para un volumen existente. Para obtener más información, consulte el Centro de documentación `volume modify`de NetApp ONTAP.

1. Para acceder a la CLI de NetApp ONTAP, ejecute el siguiente comando para establecer una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP. Reemplace *`management_endpoint_ip`* con la dirección IP del puerto de gestión del sistema de archivos.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Para obtener más información, consulte Administración de sistemas de archivos con la ONTAP CLI.

2. Acceda al modo avanzado de la CLI de ONTAP con el siguiente comando.

```
FSx::> set adv

Warning: These advanced commands are potentially dangerous; use them only when
     directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y
```

3. Utilice el siguiente comando para cambiar el número mínimo de días de refrigeración de su volumen; para ello, reemplace los siguientes valores:

   - Reemplace *svm_name* con el nombre de la SVM en la que se creó el volumen.
   - Reemplace *vol_name* con el nombre del volumen para el que está configurando los días de enfriamiento.
   - Reemplace *cooling_days* por el número deseado, un número entero entre 2 y 183.

```
FSx::> volume modify -vserver svm_name -volume vol_name -tiering-minimum-cooling-
days cooling_days
```

El sistema responde de la siguiente manera si la solicitud se ha realizado correctamente.

```
Volume modify successful on volume vol_name of Vserver svm_name.
```

Establecer la política de recuperación de un volumen en la nube

Utilice el comando `volume modify` CLI de ONTAP para configurar la política de recuperación en la nube para un volumen existente. Para obtener más información, consulte el Centro `volume modify`de documentación de NetApp ONTAP.

Para configurar la política de recuperación en la nube de un volumen (ONTAP CLI)

1. Para acceder a la CLI de NetApp ONTAP, ejecute el siguiente comando para establecer una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP. Reemplace *management_endpoint_ip* con la dirección IP del puerto de gestión del sistema de archivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obtener más información, consulte Administración de sistemas de archivos con la ONTAP CLI.

2. Acceda al modo avanzado de la CLI de ONTAP con el siguiente comando.

   ```
   FSx::> set adv

   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

3. Utilice el siguiente comando para establecer la política de recuperación de nubes del volumen; para ello, reemplace los siguientes valores:

   - Reemplace *svm_name* con el nombre de la SVM en la que se creó el volumen.
   - Reemplace *vol_name* con el nombre del volumen para el que está configurando la política de recuperación en la nube.
   - Reemplace *retrieval_policy* con el valor deseado, ya sea `default`on-read,`never`, o`promote`.

   ```
   FSx::> volume modify -vserver svm_name -volume vol_name -cloud-retrieval-
   policy retrieval_policy
   ```

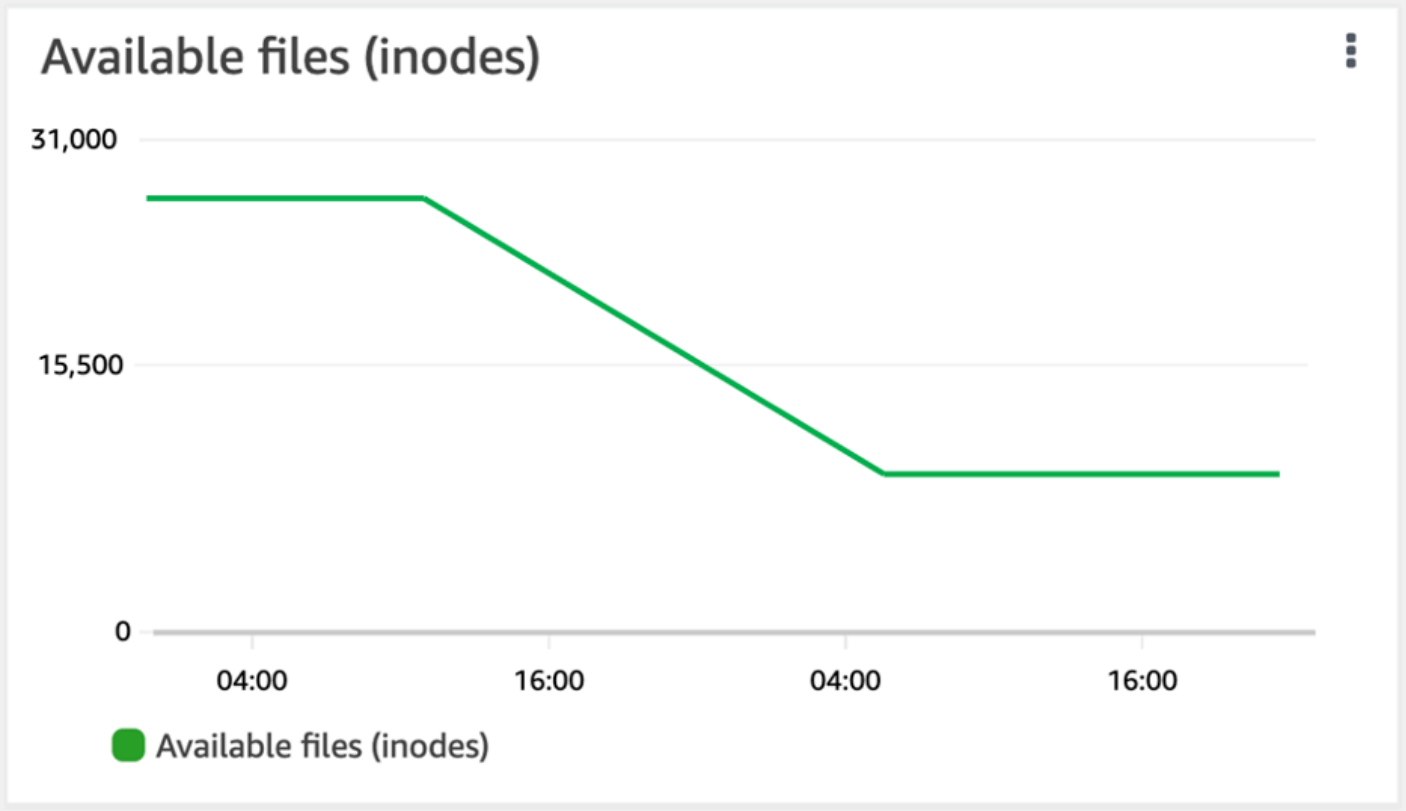
   El sistema responde de la siguiente manera si la solicitud se ha realizado correctamente.

   ```
   Volume modify successful on volume vol_name of Vserver svm_name.
   ```

Visualización de la capacidad de archivos de un volumen

Puede utilizar cualquiera de los métodos siguientes para ver el número máximo de archivos permitidos y el número de archivos que ya se utilizan en un volumen.

- Las CloudWatch métricas de volumen y. `FilesCapacity` `FilesUsed`
- En la consola de Amazon FSx, navegue hasta el gráfico de Archivos disponibles (inodos) en la pestaña Monitoring (Monitoreo) del volumen. La siguiente imagen muestra los archivos disponibles (inodos) en un volumen que disminuye con el tiempo.



Aumentar el número máximo de archivos en un volumen

Los volúmenes de FSx para ONTAP pueden quedarse sin capacidad de archivo cuando se agota el número de inodos o punteros de archivo disponibles.

Para aumentar el número máximo de archivos en un volumen (ONTAPCLI)

El comando `volume modify` ONTAP CLI se utiliza para aumentar el número máximo de archivos de un volumen. Para obtener más información, consulte `volume modify`en el Centro de NetApp ONTAP documentación.

1. Para acceder a la CLI de NetApp ONTAP, ejecute el siguiente comando para establecer una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP. Reemplace *`management_endpoint_ip`* con la dirección IP del puerto de gestión del sistema de archivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obtener más información, consulte Administración de sistemas de archivos con la ONTAP CLI.
2. Realice una de las siguientes acciones en función de su caso de uso. Reemplace *`svm_name`* y *`vol_name`* con sus valores.

   - Para configurar un volumen de manera que siempre tenga el número máximo de archivos (inodos) disponibles, lleve a cabo lo siguiente:

     1. Acceda al modo avanzado en la CLI de ONTAP mediante el siguiente comando.

        ```
        ::> set adv
        ```

     2. Después de ejecutar este comando, verá el resultado. Ingrese y para continuar.

        ```
        Warning: These advanced commands are potentially dangerous; use them only
         when
        directed to do so by NetApp personnel.
        Do you want to continue? {y|n}: y
        ```

     3. Ingrese el siguiente comando para utilizar siempre el número máximo de archivos del volumen:

        ```
        ::> volume modify -vserver svm_name -volume vol_name -files-set-maximum true
        ```

   - Para especificar manualmente el número total de archivos permitidos en el volumen, con *`max_number_files`* `= (current_size_of_volume) × (1 file ÷ 4 KiB)`, hasta un valor máximo posible de 2000 millones, utilice el siguiente comando:

```
::> volume modify -vserver svm_name -volume vol_name -files max_number_files
```

Habilitar el modo de escritura en la nube de un volumen

Utilice el comando CLI de `volume modify` ONTAP para activar o desactivar el modo de escritura en la nube para un volumen existente. Para obtener más información, consulte el Centro `volume modify`de documentación de NetApp ONTAP.

Los requisitos previos para configurar el modo de escritura en la nube son:

- El volumen debe ser un volumen existente. Solo puede activar la función en un volumen existente.
- El volumen debe ser de lectura y escritura (RW).
- El volumen debe tener la política de todos los niveles. Para obtener más información sobre la modificación de la política de estratificación de un volumen, consulte. Establecer la política de niveles de un volumen

El modo de escritura en la nube resulta útil para casos como las migraciones, por ejemplo, en los que se transfieren grandes cantidades de datos a un sistema de archivos mediante el protocolo NFS.

Para configurar el modo de escritura en la nube de un volumen (ONTAP CLI)

1. Para acceder a la CLI de NetApp ONTAP, ejecute el siguiente comando para establecer una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP. Reemplace *management_endpoint_ip* con la dirección IP del puerto de gestión del sistema de archivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obtener más información, consulte Administración de sistemas de archivos con la ONTAP CLI.
2. Acceda al modo avanzado de la CLI de ONTAP con el siguiente comando.

   ```
   FSx::> set -privilege advanced
   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

3. Utilice el siguiente comando para configurar el modo de escritura en la nube del volumen y sustituya los valores siguientes:

   - Reemplace *svm_name* con el nombre de la SVM en la que se creó el volumen.
   - *vol_name*Sustitúyalo por el nombre del volumen para el que está configurando el modo de escritura en la nube.
   - *vol_cw_mode*Sustitúyalo `true` por uno para activar el modo de escritura en la nube en el volumen o `false` para desactivarlo.

```
FSx::> volume modify -vserver svm_name -volume vol_name -is-cloud-write-
enabled vol_cw_mode
```

   El sistema responde de la siguiente manera si la solicitud se ha realizado correctamente.

```
Volume modify successful on volume vol_name of Vserver svm_name.
```

Protección de datos

Además de replicar automáticamente los datos de su sistema de archivos para garantizar una alta durabilidad, Amazon FSx le ofrece las siguientes opciones para proteger aún más los datos almacenados en sus sistemas de archivos:

- Las copias de seguridad nativas de Amazon FSx respaldan sus necesidades de retención y conformidad de copias de seguridad en Amazon FSx. También puede utilizarlo AWS Backup para gestionar, automatizar y proteger sus copias de seguridad de forma centralizada Servicios de AWS en la nube.
- Las instantáneas permiten a los usuarios deshacer fácilmente los cambios en los archivos y comparar las versiones de los archivos restaurando los archivos de versiones anteriores.
- Replicación de su sistema de archivos Amazon FSx en un segundo sistema de archivos para proporcionar protección y recuperación de datos. La replicación, cuando está habilitada, se produce de forma automática y programada.
- SnapLock puede proteger sus archivos al pasarlos a un estado de escritura única y lectura múltiple (WORM), lo que impide su modificación o eliminación durante un período de retención específico.

Temas

Trabajo con copias de seguridad

Con FSx para ONTAP, puede realizar copias de seguridad automáticas diarias y copias de seguridad iniciadas por el usuario de los volúmenes de su sistema de archivos. Las copias de seguridad de FSx para ONTAP se realizan por volumen, por lo que cada copia de seguridad contiene solo los datos de un volumen concreto. Las copias de seguridad de Amazon FSx son muy duraderas e incrementales.

Todas las copias de seguridad de Amazon FSx (copias de seguridad diarias automáticas y copias de seguridad iniciadas por el usuario) son incrementales. Esto significa que solo se guardan los datos del volumen que han cambiado luego de la copia de seguridad más reciente. Esto minimiza

el tiempo necesario para crear la copia de seguridad y el almacenamiento necesario para la copia de seguridad, lo que permite ahorrar costes de almacenamiento al no duplicar los datos. 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 Amazon FSx contiene toda la información necesaria para crear un nuevo volumen a partir de la copia de seguridad y restaurar de forma efectiva una point-in-time instantánea del volumen del sistema de archivos.

Crear copias de seguridad periódicas para sus volúmenes es una práctica recomendada que le ayuda a satisfacer sus necesidades de retención de datos y de conformidad. Trabajar con copias de seguridad de Amazon FSx es fácil, ya sea para crear copias de seguridad, restaurar a partir de una copia de seguridad o eliminar una copia de seguridad.

Amazon FSx admite copias de seguridad de ONTAP FlexVol volúmenes (en todos los sistemas de archivos) y FlexGroup volúmenes con un `OntapVolumeType` de `RW` (lectura-escritura).

> **Note**
>
> Amazon FSx no admite copias de seguridad de volúmenes de protección de datos (DP), volúmenes de carga compartida (LS) ni volúmenes de destino. FlexCache

Hay límites en cuanto al número de copias de seguridad que puede almacenar por sistema de archivos y por volumen. Para obtener más información, consulte Cuotas que puede aumentar y Cuotas de recursos para cada sistema de archivos.

Temas

- Crear una copia de seguridad iniciada por el usuario
- Restaurar una copia de seguridad en un volumen nuevo
- Eliminación de una copia de seguridad

Cómo funcionan las copias de seguridad

Las copias de seguridad de Amazon FSx utilizan instantáneas (point-in-timeimágenes de solo lectura de sus volúmenes) para mantener la incrementalidad entre las copias de seguridad. Cada vez que se realiza una copia de seguridad, Amazon FSx primero toma una instantánea del volumen. La instantánea de la copia de seguridad se almacena en el volumen y ocupa espacio en el nivel de almacenamiento de la SSD. A continuación, Amazon FSx compara esta instantánea con la instantánea de la copia de seguridad anterior (si existe) y copia solo los datos modificados en la copia de seguridad.

Si no existe ninguna instantánea de respaldo anterior, todo el contenido de la instantánea de respaldo más reciente se copia en su copia de seguridad. Una vez realizada correctamente la última instantánea de la copia de seguridad, Amazon FSx elimina la instantánea de la copia de seguridad anterior. La instantánea utilizada para la última copia de seguridad permanece en el volumen hasta que se realice la siguiente copia de seguridad, cuando el proceso se repite. Para optimizar los costos de almacenamiento de copias de seguridad, ONTAP preserva la eficiencia de almacenamiento de un volumen y ahorra en sus copias de seguridad.

Amazon FSx no puede realizar copias de seguridad de volúmenes que están fuera de línea.

Requisitos de almacenamiento

Para poder realizar copias de seguridad de sus volúmenes, tanto el volumen como el sistema de archivos deben tener suficiente capacidad de almacenamiento en SSD disponible para almacenar una instantánea de respaldo. Al realizar una copia de seguridad, la capacidad de almacenamiento adicional que consume la instantánea no puede provocar que el volumen supere el 98% de utilización del almacenamiento SSD. Si esto ocurre, la copia de seguridad fallará. Puedes aumentar el almacenamiento en SSD de un volumen o sistema de archivos en cualquier momento para asegurarte de que tus copias de seguridad no se interrumpan.

Trabajo con copias de seguridad diarias automáticas

Las copias de seguridad diarias automáticas de los volúmenes del sistema de archivos están habilitadas de forma predeterminada al crear un sistema de archivos. Puede activar o desactivar

las copias de seguridad diarias automáticas de un sistema de archivos en cualquier momento. Las copias de seguridad diarias automáticas se producen durante el período de copias de seguridad diarias, que se establece automáticamente al crear un sistema de archivos. Puede modificar la ventana de copia de seguridad diaria en cualquier momento. Le recomendamos que elija una hora del día para realizar la copia de seguridad diaria que esté fuera del horario normal de funcionamiento de las aplicaciones que utilizan sus volúmenes a fin de mejorar el rendimiento de la copia de seguridad. Para obtener más información, consulte Rendimiento de backup y restauración.

Puede configurar el período de retención de las copias de seguridad diarias automáticas entre 1 y 90 días en la consola al crear un sistema de archivos o en cualquier momento. El período de retención diario automático predeterminado de las copias de seguridad es de 30 días. El servicio elimina una copia de seguridad diaria automática una vez que vence su período de retención. Con la CLI o la API, puede establecer el período de retención entre 0 y 90 días; si lo establece en 0, se desactivan las copias de seguridad diarias automáticas.

El período de copia de seguridad diario y el período de retención de la copia de seguridad son configuraciones a nivel del sistema de archivos que se aplican a todos los volúmenes del sistema de archivos. Puede utilizar la consola Amazon FSx, la o la API para cambiar la AWS CLI ventana y el período de retención de las copias de seguridad de sus sistemas de archivos, así como para activar o desactivar las copias de seguridad diarias automáticas. Para obtener más información, consulte Actualización de un sistema de archivos.

No puede crear una copia de seguridad por volumen si el volumen está desconectado. Para obtener más información, consulte Copias de seguridad y volúmenes sin conexión.

> **Note**
>
> Las copias de seguridad diarias automáticas tienen un período de retención máximo de 90 días, pero las copias de seguridad iniciadas por el usuario que usted cree, incluidas las copias de seguridad creadas con ella AWS Backup, se conservan para siempre, a menos que usted o el AWS Backup servicio las eliminen.

Puede eliminar manualmente una copia de seguridad diaria automática mediante la consola, la CLI y la API. Al eliminar un volumen, también se eliminan las copias de seguridad diarias automáticas de ese volumen. Amazon FSx ofrece la opción de crear una copia de seguridad final de un volumen antes de eliminarlo. La copia de seguridad final se conserva para siempre, a menos que la elimine. Para obtener más información, consulte. Eliminación de copias de seguridad

Trabajo con copias de seguridad iniciadas por el usuario

Con Amazon FSx, puede realizar copias de seguridad manuales de los volúmenes de su sistema de archivos en cualquier momento mediante la API AWS Management Console AWS CLI, y. Las copias de seguridad iniciadas por el usuario son incrementales en relación con otras copias de seguridad que se hayan creado para un volumen y se conservan para siempre, a menos que las elimine. Las copias de seguridad iniciadas por el usuario se conservan incluso después de eliminar el volumen o el sistema de archivos en el que se crearon las copias de seguridad. Solo puede eliminar las copias de seguridad iniciadas por el usuario con la consola de Amazon FSx, la API o la CLI. Amazon FSx nunca los elimina de manera automática. Para obtener más información, consulte Eliminación de copias de seguridad.

No puede crear una copia de seguridad de un volumen si el volumen está desconectado. Para obtener más información, consulte Copias de seguridad y volúmenes sin conexión.

Copiar etiquetas en copias de seguridad

Al crear o actualizar un volumen mediante la CLI o la API, puede `CopyTagsToBackups` habilitar la copia automática de cualquier etiqueta del volumen en sus copias de seguridad. Sin embargo, si agrega alguna etiqueta al crear una copia de seguridad iniciada por el usuario, incluida la asignación de un nombre a una copia de seguridad cuando utiliza la consola, el servicio no copia las etiquetas del volumen, aunque `CopyTagsToBackups` esté activado.

Rendimiento de backup y restauración

Diversos factores pueden influir en el rendimiento de las operaciones de respaldo y restauración. Las operaciones de backup y restauración son procesos en segundo plano, lo que significa que tienen una prioridad inferior en relación con las operaciones de E/S del cliente. Las operaciones de E/S del cliente incluyen lectura y escritura de datos NFS, CIFS e iSCSI. Todos los procesos en segundo plano, incluidas las operaciones de copia de seguridad y restauración, utilizan solo la parte no utilizada de la capacidad de procesamiento del sistema de archivos y pueden tardar entre unos minutos y unas horas en completarse, según el tamaño de la copia de seguridad y la cantidad de capacidad de rendimiento no utilizada del sistema de archivos.

Otros factores que afectan al rendimiento de las copias de seguridad y la restauración son el nivel de almacenamiento en el que se almacenan los datos y el perfil del conjunto de datos. Le recomendamos que cree las primeras copias de seguridad de sus volúmenes cuando la mayoría de los datos estén en un almacenamiento SSD. Los conjuntos de datos que contienen principalmente archivos pequeños suelen tener un rendimiento inferior en comparación con los conjuntos de datos

de tamaño similar que contienen principalmente archivos grandes. Esto se debe a que procesar grandes cantidades de archivos pequeños consume más ciclos de CPU y sobrecarga de red que procesar menos archivos grandes.

Por lo general, puede esperar las siguientes velocidades de copia de seguridad al realizar copias de seguridad de los datos almacenados en el nivel de almacenamiento SSD:

- 750 MBps en varias copias de seguridad simultáneas que contienen en su mayoría archivos de gran tamaño.
- 100 MBps en varias copias de seguridad simultáneas que contienen en su mayoría archivos pequeños.

Por lo general, puede esperar las siguientes tasas de restauración:

- 250 MBps en varias restauraciones simultáneas que contienen en su mayoría archivos de gran tamaño.
- 100 MBps en varias restauraciones simultáneas que contienen principalmente archivos pequeños.

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 sus Amazon FSx para los volúmenes de NetApp ONTAP. AWS Backup es un servicio de copias de seguridad unificado diseñado para simplificar la creación, 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.
- Supervisar toda la actividad reciente de copias de seguridad, copias y restauración.

AWS Backup utiliza la funcionalidad de copia de seguridad integrada de Amazon FSx. Las copias de seguridad creadas con la AWS Backup consola tienen el mismo nivel de coherencia y rendimiento

del sistema de archivos, son incrementales en relación con cualquier otra copia de seguridad de Amazon FSx que realice de su volumen (iniciada por el usuario o automática) y ofrecen las mismas opciones de restauración que las copias de seguridad realizadas a través de la consola de Amazon FSx. Si las utiliza AWS Backup para administrar estas copias de seguridad, obtiene funciones adicionales, como la posibilidad de crear copias de seguridad programadas con una frecuencia de hasta una hora. Puede añadir una capa de defensa adicional para proteger las copias de seguridad de eliminaciones inadvertidas o malintencionadas almacenándolas en una bóveda. AWS Backup

Las copias de seguridad creadas 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. Para obtener más información, consulte Cuotas que puede aumentar. Puede ver y restaurar las copias de seguridad creadas mediante AWS Backup la consola, la CLI y la API de Amazon FSx. Sin embargo, no puede eliminar las copias de seguridad creadas AWS Backup en la consola, la CLI o la API de Amazon FSx. Para obtener más información, consulte Primeros pasos AWS Backup en la Guía para AWS Backup desarrolladores.

AWS Backup no puede hacer copias de seguridad de los volúmenes que están fuera de línea.

Restaurar copias de seguridad en un volumen nuevo

Puede restaurar una copia de seguridad de un volumen en un volumen nuevo, restaurando de forma efectiva una point-in-time instantánea de un volumen mediante la consola, la CLI o la API.

Al restaurar una copia de seguridad, todos los datos se escriben primero en el nivel de almacenamiento SSD antes de que el servicio comience a organizarlos en niveles en el almacenamiento del pool de capacidad de acuerdo con la política de estratificación que haya establecido para el volumen restaurado. Al restaurar una copia de seguridad en un volumen con una política de estratificación de`All`, un proceso periódico en segundo plano coloca los datos en niveles en el conjunto de capacidad. Al restaurar una copia de seguridad en un volumen con una política de estratificación igual `Snapshot Only` o igual`Auto`, los datos se agrupan en niveles en el pool de capacidad si la utilización de la SSD en el sistema de archivos es superior al 50%, y la velocidad de enfriamiento viene determinada por el período de enfriamiento de la política de organización en niveles.

Al restaurar una copia de seguridad por FlexGroup volumen en un sistema de archivos que tiene un número de pares de alta disponibilidad (HA) diferente al del sistema de archivos original, Amazon FSx puede añadir volúmenes constitutivos adicionales para garantizar que los componentes se distribuyan uniformemente.

Para step-by-step obtener instrucciones sobre cómo restaurar una copia de seguridad en un volumen nuevo, consulte. Restaurar una copia de seguridad en un volumen nuevo

> **Note**
>
> Un volumen restaurado siempre tiene el mismo estilo de volumen que el volumen original. No puede cambiar el estilo del volumen al restaurarlo.

Eliminación de copias de seguridad

Puede eliminar las copias de seguridad diarias automáticas y las copias de seguridad iniciadas por el usuario de sus volúmenes. 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. Para obtener instrucciones que describen cómo eliminar las copias de seguridad, consulteEliminación de una copia de seguridad.

No puede eliminar las copias de seguridad creadas por AWS Backup, que tengan tipo AWS Backup, en la consola, CLI o API de Amazon FSx. Para obtener información sobre cómo eliminar las copias de seguridad creadas por AWS Backup, consulte Eliminar copias de seguridad en la Guía para AWS Backup desarrolladores.

No puede eliminar la copia de seguridad de un volumen si el volumen está desconectado. Para obtener más información, consulte Copias de seguridad y volúmenes sin conexión.

> **Important**
>
> No elimine la instantánea común del volumen porque se utiliza para mantener la incrementalidad entre las copias de seguridad. Si se elimina la instantánea común del volumen, la siguiente copia de seguridad será de todo el volumen y no solo de forma incremental.

Copias de seguridad y volúmenes sin conexión

No puede crear ni eliminar copias de seguridad de volúmenes si ese volumen está desconectado. Utilice el comando `volume show`ONTAPCLI para determinar el estado y el estado actuales de un volumen.

Para volver a poner en línea un volumen sin conexión, utilice el comando `volume online`ONTAPCLI como en el siguiente ejemplo:

```
::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

Crear una copia de seguridad iniciada por el usuario

El siguiente procedimiento describe cómo utilizar la consola Amazon FSx para crear una copia de seguridad de un volumen iniciada por el usuario.

No puede crear una copia de seguridad de un volumen si el volumen está desconectado. Para obtener más información, consulte Copias de seguridad y volúmenes sin conexión.

Para crear una copia de seguridad de un volumen (consola) iniciada por el usuario

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 ONTAP archivos del que desee hacer una copia de seguridad de un volumen.
3. Seleccione la pestaña Volúmenes.
4. Elija el volumen del que desea hacer una copia de seguridad.
5. En Acciones, elija Crear copia de seguridad.
6. 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 . + - = _ : /
7. Elija Create backup.

Ahora ha creado una copia de seguridad de uno de los volúmenes de su sistema de archivos. Para encontrar una tabla de todas las copias de seguridad en la consola de Amazon FSx, seleccione Copias de seguridad 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.

Cuando crea una copia de seguridad iniciada por el usuario como se describe en este procedimiento, esta tendrá el tipo `USER_INITIATED`, y el estado `CREATING`, hasta que se vuelva completamente disponible.

Restaurar una copia de seguridad en un volumen nuevo

Los siguientes procedimientos describen cómo restaurar una copia de seguridad de FSx for ONTAP en un volumen nuevo mediante y. AWS Management Console AWS CLI

Para restaurar una copia de seguridad de un volumen en un volumen nuevo (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación, seleccione Copias de seguridad y, a continuación, elija la copia de seguridad por volumen de FSx for ONTAP que desee restaurar.
3. En el menú de acciones superior derecho, selecciona Restaurar copia de seguridad. Aparece la página Crear volumen a partir de una copia de seguridad.
4. Elija la máquina virtual de almacenamiento y sistema de archivos FSx for ONTAP en la que desee restaurar la copia de seguridad en los menús desplegables.
5. En Detalles del volumen, hay varias selecciones. En primer lugar, introduzca el nombre del volumen. Puede utilizar un máximo de 203 caracteres alfanuméricos o de subrayado (_).
6. En Volume size, introduzca cualquier número entero en el rango de 20 a 314 572 800 para especificar el tamaño en mebibytes (MiB).
7. En el tipo de volumen, seleccione Lectura y escritura (RW) para crear un volumen que sea legible y grabable o Protección de datos (DP) para crear un volumen que sea de solo lectura y pueda usarse como destino de una relación o. NetApp SnapMirror SnapVault Para obtener más información, consulte Tipos de volúmenes.
8. En Ruta de unión, introduzca una ubicación dentro del sistema de archivos para montar el volumen. El nombre debe tener una barra delantera hacia adelante, por ejemplo `/vol3`.
9. En cuanto a la eficiencia del almacenamiento, elija Activado para activar las funciones de ONTAP eficiencia del almacenamiento (deduplicación, compresión y compactación). Para obtener más información, consulte FSx para la eficiencia de almacenamiento de ONTAP.
10. Para el Estilo de seguridad de los volúmenes, elija Unix (Linux), NTFS o Mixto. El estilo de seguridad de un volumen determina si se da preferencia a las ACL de NTFS o UNIX para el acceso multiprotocolo. El modo MIXTO no es necesario para el acceso multiprotocolo y solo se recomienda para usuarios avanzados.
11. Para la Política de instantáneas, elija una política de instantáneas para el volumen. Para obtener más información acerca de las políticas de instantáneas, consulte Políticas de instantáneas.

    Si elige Política personalizada, debe especificar el nombre de la política en el campo de política personalizada. La política personalizada ya debe existir en la SVM o en el sistema de archivos.

Puede crear una política de instantáneas personalizada con la ONTAP CLI o la API REST. Para obtener más información, consulte Crear una política de instantáneas en la documentación NetApp ONTAP del producto.

12. Para el Periodo de enfriamiento de la política de niveles, los valores válidos son de 2 a 183 días. El periodo de enfriamiento de la política de niveles de un volumen define el número de días que transcurren antes de que los datos a los que no se ha accedido se marquen como fríos y se trasladen al repositorio de capacidad. Esta configuración solo afecta a las políticas `Auto` y `Snapshot-only`.
13. En la sección Avanzada, para la SnapLockconfiguración, puede dejar la configuración predeterminada deshabilitada o seleccionar Habilitada para configurar un SnapLock volumen. Para obtener más información sobre la configuración de un SnapLock Compliance volumen o un SnapLock Enterprise volumen, consulte Crear un volumen de Conformidad de SnapLock yCreación de un volumen Empresarial de SnapLock. Para obtener más información acerca de SnapLock, consulte Proteja sus datos con SnapLock.
14. Seleccione Confirm (Confirmar) para crear el volumen.

Para restaurar una copia de seguridad de un volumen en un volumen nuevo (CLI)

Utilice el comando create-volume-from-backupCLI o el comando CreateVolumeFromBackupAPI equivalente para restaurar una copia de seguridad de un volumen en un volumen nuevo.

- ```
  $ aws fsx create-volume-from-backup --backup-id backup-08e6fc1133fff3532 \
        --name demo --ontap-configuration JunctionPath=/demo, SizeInMegabytes=100000,
   \
        StorageVirtualMachineId=svm-0f04a9c7c27e1908b, TieringPolicy={Name=ALL}
  ```

  La respuesta del sistema para una solicitud correcta:

  ```
  {
        "Volume": {
            "CreationTime": 1692721488.428,
            "FileSystemId": "fs-07ab735385276ed60",
            "Lifecycle": "CREATING",
            "Name": "demo",
            "OntapConfiguration": {
                "FlexCacheEndpointType": "NONE",
                "JunctionPath": "/demo",
                "SizeInMegabytes": 100000,
  ```
  ```

```
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-0f04a9c7c27e1908b",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "Name": "ALL"
            },
            "OntapVolumeType": "DP",
            "SnapshotPolicy": "default",
            "CopyTagsToBackups": false,
        },
        "ResourceARN": "arn:aws:fsx:us-east-1:752825163408:volume/
fs-07ab735385276ed60/fsvol-0b6ec764c9c5f654a",
        "VolumeId": "fsvol-0b6ec764c9c5f654a",
        "VolumeType": "ONTAP",

    }
}
```


Eliminación de una copia de seguridad

Puede eliminar las copias de seguridad diarias automáticas y las copias de seguridad iniciadas por el usuario mediante la consola, la CLI y la API de Amazon FSx, tal y como se describe en los siguientes procedimientos.

Para eliminar las copias de seguridad creadas con ella AWS Backup, consulte Eliminar copias de seguridad en la Guía AWS Backup para desarrolladores.

Para eliminar una copia de seguridad (consola)

1. Abra la consola de Amazon FSx 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 Eliminar copias de seguridad que se abre, confirme que el identificador de la copia de seguridad que se muestra es la copia de seguridad que desea eliminar.
5. Confirme que la casilla de la copia de seguridad que desea eliminar está marcada.
6. Elija Eliminar copias de seguridad.

La copia de seguridad y todos los datos incluidos se eliminarán ahora de forma permanente e irrecuperable.

Para eliminar una copia de seguridad (CLI)

- Utilice el comando CLI delete-backup o la acción de DeleteBackup API equivalente para eliminar un FSx para la copia de seguridad de volúmenes de ONTAP, como se muestra en el siguiente ejemplo.

  ```
  $ aws fsx delete-backup --backup-id backup-a0123456789abcdef
  ```

  La respuesta del sistema incluye el identificador de la copia de seguridad que se va a eliminar y el estado de su ciclo de vida, e `DELETED` indica que la solicitud se ha realizado correctamente.

  ```
  {
      "BackupId": "backup-a0123456789abcdef",
      "Lifecycle": "DELETED"
  }
  ```

Uso de instantáneas

Una instantánea es una imagen de solo lectura de un volumen de Amazon FSx for NetApp ONTAP en un momento dado. Las copias instantáneas ofrecen protección contra la eliminación o modificación accidental de los archivos de sus volúmenes por parte de los usuarios finales. Con las instantáneas, los usuarios pueden ver y restaurar fácilmente archivos o carpetas individuales a partir de una instantánea anterior. De este modo, los usuarios pueden deshacer los cambios y comparar las versiones de los archivos con facilidad.

Debido a que las instantáneas se almacenan junto con los datos del sistema de archivos, consumen la capacidad de almacenamiento del sistema de archivos. Sin embargo, las instantáneas consumen capacidad de almacenamiento solo para las partes de los archivos que han cambiado desde la última instantánea. Tenga en cuenta que las instantáneas no consumen capacidad en el momento de su creación. Las instantáneas almacenadas en su sistema de archivos no se incluyen en las copias de seguridad de los volúmenes del sistema de archivos.

Las instantáneas están habilitadas de forma predeterminada en sus volúmenes, mediante la política de instantáneas predeterminada. Su sistema de archivos FSx para ONTAP tiene tres políticas de instantáneas integradas entre las que puede elegir al crear o actualizar un volumen en la consola de

Amazon FSx, en la API de Amazon FSx o en AWS CLI la API de Amazon FSx. Además, puede crear una política de instantáneas personalizada o instantáneas a pedido mediante la CLI de ONTAP o la API de REST. Las instantáneas se almacenan en el directorio `.snapshot` de la raíz de un volumen. Puede almacenar hasta 1023 instantáneas por volumen en cualquier momento. Cuando alcance este límite, debe eliminar una instantánea existente antes de poder crear una nueva instantánea del volumen.

Temas

Políticas de instantáneas

La política de instantáneas define la forma en que el sistema crea las instantáneas de un volumen. La política especifica cuándo crear instantáneas, cuántas copias retener y cómo asignarles un nombre. Hay tres políticas de instantáneas integradas de FSx para ONTAP:

- `default`
- `default-1weekly`
- `none`

De forma predeterminada, cada volumen está asociado a la política de instantáneas `default` del sistema de archivos. Recomendamos usar esta política para la mayoría de las cargas de trabajo.

La política `default` crea automáticamente las instantáneas según el siguiente programa, y las copias más antiguas se eliminan para dejar espacio a las copias más recientes:

- Un máximo de seis instantáneas por horas tomadas cinco minutos después de la hora.

- Un máximo de dos instantáneas diarias tomadas de lunes a sábado 10 minutos después de medianoche.
- Un máximo de dos instantáneas semanales tomadas todos los domingos 15 minutos después de medianoche.

> **Note**
>
> Los tiempos de las instantáneas se basan en la zona horaria del sistema de archivos, que por defecto es Hora Universal Coordinada (UTC). Para obtener información sobre cómo cambiar la zona horaria, consulte Visualización y configuración de la zona horaria del sistema en la documentación de NetApp Support.

La política `default-1weekly` funciona de la misma forma que la política `default`, excepto que solo retiene una instantánea de la programación semanal.

La política `none` no toma ninguna instantánea. Puede asignar esta política a los volúmenes para evitar que se tomen instantáneas automáticas.

Puede crear una política de instantáneas personalizada con la CLI de ONTAP o la API de REST. Para obtener más información, consulte Creación de una política instantánea en la documentación del producto NetApp ONTAP. Puede elegir una política de instantáneas al crear o actualizar un volumen en la consola de Amazon FSx, en la API de Amazon FSx o en la AWS CLI API de Amazon FSx. Para obtener más información, consulte Creación de volúmenes y Actualización de un volumen.

Restauración de los archivos y las carpetas individuales

Con las instantáneas en el sistema de archivos de Amazon FSx, sus usuarios pueden restaurar rápidamente las versiones anteriores de archivos o carpetas individuales. Esto les permite recuperar los archivos borrados o modificados que están guardados en el sistema de archivos compartidos. Lo hacen de forma autoservicio directamente en su escritorio sin la ayuda del administrador. Este enfoque de autoservicio aumenta la productividad y reduce la carga de trabajo administrativa.

Los clientes de Linux y macOS pueden ver las instantáneas en el directorio `.snapshot` de la raíz de un volumen. Los clientes de Windows pueden ver las instantáneas en la pestaña `Previous Versions` del Explorador de Windows (al hacer clic derecho en un archivo o carpeta).

Restaure archivos a partir de instantáneas

Para restaurar un archivo a partir de una instantánea (clientes Linux y macOS)

1. Si el archivo original aún existe y no desea que el archivo de una instantánea lo sobrescriba, utilice su cliente Linux o macOS para cambiar el nombre del archivo original o moverlo a un directorio diferente.
2. En el directorio `.snapshot`, busque la instantánea que contiene la versión del archivo que desea restaurar.
3. Copie el archivo del directorio `.snapshot` al directorio en el que existía originalmente.

Para restaurar un archivo a partir de una instantánea (clientes de Windows)

Los usuarios en clientes de Windows pueden restaurar los archivos a versiones anteriores con la interfaz conocida del Explorador de archivos de Windows.

1. Para restaurar un archivo, los usuarios eligen el archivo que desean restaurar y, a continuación, eligen Restaurar versiones anteriores en el menú contextual (clic derecho).
2. A continuación, los usuarios pueden ver y restaurar una versión anterior desde la lista de Versiones anteriores.

Los datos de las instantáneas son de solo lectura. Si desea realizar modificaciones en los archivos y carpetas que aparecen en la pestaña Versiones anteriores, debe guardar una copia de los archivos y carpetas que desee modificar en una ubicación en la que se pueda escribir y realizar modificaciones en las copias.

Eliminación de instantáneas

Las instantáneas son imágenes de point-in-time solo lectura de un estado anterior del volumen y están habilitadas de forma predeterminada en todos los volúmenes FSx for ONTAP para proteger sus datos. Las instantáneas consumen capacidad de almacenamiento solo para las partes de los archivos que han cambiado desde la última instantánea. Por este motivo, si su carga de trabajo cambia los datos rápidamente, las instantáneas de datos antiguos pueden ocupar una parte importante de la capacidad del volumen.

Por ejemplo, el resultado del comando `volume show-space` proporcionado anteriormente muestra 140 KB de `User Data`. Sin embargo, el volumen tenía 9,8 GB de `User Data` antes de que se

eliminaran los datos del usuario. Incluso si has eliminado los archivos del volumen, es posible que una instantánea siga haciendo referencia a datos de usuario antiguos. Por este motivo, `Snapshot Reserve` y `Snapshot Spill` en el ejemplo anterior, ocupan un total de 9,8 GB de espacio, aunque prácticamente no haya datos de usuario en el volumen.

Para liberar espacio en los volúmenes, puede eliminar las instantáneas antiguas que ya no necesite. Para ello, puede crear una política de eliminación automática de instantáneas o eliminar las instantáneas manualmente. Al eliminar una instantánea, se eliminan los datos modificados almacenados en la instantánea.

Cree una política de borrado automático de instantáneas

Puede crear una política para eliminar automáticamente las instantáneas cuando se agote la cantidad de espacio disponible en el volumen. Para establecer una política de eliminación automática para un volumen, utilice el siguiente comando.

Antes de ejecutar este comando, reemplace los siguientes valores:

- Reemplace *`svm_name`* con el nombre de la SVM en la que se creó el volumen.
- Reemplace *`vol_name`* por el nombre del volumen.

En `-trigger`, asigne uno de los siguientes valores:

- `volume`: use `volume` si desea que el umbral en el que se eliminan las instantáneas se corresponda con el umbral de capacidad total del volumen utilizado. Los umbrales de capacidad del volumen utilizado que provocan la eliminación de las instantáneas vienen determinados por el tamaño del volumen, y el umbral escala del 85 al 98 por ciento de la capacidad utilizada. Los volúmenes más pequeños tienen un umbral más pequeño y los volúmenes más grandes, uno más grande.
- `snap_reserve`: use `snap_reserve` si desea que las instantáneas se eliminen en función de lo que pueda quedar en su reserva de instantáneas.

```
::> volume snapshot autodelete modify -vserver svm_name -volume vol_name -enabled true
 -trigger [volume|snap_reserve]
```

Para obtener más información, consulte el comando volume snapshot autodelete modify en el Centro de documentación de NetApp ONTAP.

Eliminación de instantáneas

Use el siguiente comando para eliminar una instantánea manualmente: Antes de ejecutar este comando, reemplace los siguientes valores:

- Reemplace *svm_name* con el nombre de la SVM en la que se creó el volumen.
- Reemplace *vol_name* por el nombre del volumen.
- Reemplace *snapshot_name* por el nombre de la instantánea. Este comando admite caracteres comodines (*) para *snapshot_name*. Por lo tanto, puede eliminar todas las instantáneas cada hora, por ejemplo, utilizando `hourly*`.

> **Important**
>
> Si tiene habilitadas las copias de seguridad de Amazon FSx, Amazon FSx retiene una instantánea de la copia de seguridad de Amazon FSx más reciente de cada volumen. Estas instantáneas se utilizan para mantener la incrementalidad entre las copias de seguridad y no se deben eliminar con este método.

```
FsxIdabcdef01234567892::> volume snapshot delete -vserver svm_name -volume vol_name -
snapshot snapshot_name
```

Para obtener más información sobre la eliminación manual de las instantáneas, consulte el volume snapshot deletecomando en el Centro de documentación de NetApp ONTAP.

Desactivación de las instantáneas automáticas

La política de instantáneas predeterminada habilita las instantáneas automáticas para los volúmenes del sistema de archivos FSx for ONTAP. Si no necesita instantáneas de sus datos (por ejemplo, si utiliza datos de prueba), puede deshabilitar las instantáneas configurando la política de instantáneas del volumen para que `none` utilice la API AWS Management Console, AWS CLI y la ONTAP CLI, tal y como se describe en los siguientes procedimientos.

Para deshabilitar las instantáneas automáticas ()AWS Management Console

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 ONTAP para el que desee actualizar un volumen.
3. Seleccione la pestaña Volúmenes.
4. Elija el volumen que desea actualizar.
5. En Acciones, seleccione Actualizar volumen.

   Aparece el cuadro de diálogo Actualizar volumen con la configuración actual del volumen.
6. Para la política de instantáneas, elija Ninguna.
7. Seleccione Actualizar para actualizar el volumen.

Para deshabilitar las instantáneas automáticas ()AWS CLI

- Utilice el comando CLI update-volume (o la operación de UpdateVolumeAPI equivalente) para establecer el `SnapshotPolicy` valor`none`, como se muestra en el siguiente ejemplo.

```
aws fsx update-volume \
    --volume-id fsvol-1234567890abcdefa \
    --name new_vol \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/new_vol, \
           SizeInMegabytes=2048,SnapshotPolicy=none, \
           StorageEfficiencyEnabled=true, \
           TieringPolicy=all
```

Para deshabilitar las instantáneas automáticas () ONTAP CLI

1. Para mostrar la política de `none`, use el siguiente comando.

```
::> snapshot policy show -policy none

Vserver: FsxIdabcdef01234567892
                         Number of Is
Policy Name              Schedules Enabled Comment
------------------------ --------- ------- ----------------------------------
none                              0 false   Policy for no automatic snapshots.
    Schedule               Count     Prefix                SnapMirror Label
    ---------------------- -----     ---------------------- ------------------
    -                          -     -                      -
```

2. Para deshabilitar las instantáneas automáticas, añada la política de none al volumen mediante el siguiente comando.

   - Reemplace *svm_name* por el nombre de SVM.
   - Reemplace *vol_name* por el nombre de su volumen.

   Cuando se le pida continuar, ingrese **y**.

```
::> volume modify -vserver svm_name -volume vol_name -snapshot-policy none

Warning: You are changing the Snapshot policy on volume "vol_name" to "none".
 Snapshot copies on this volume
         that do not match any of the prefixes of the new Snapshot policy will not
 be deleted. However, when
         the new Snapshot policy takes effect, depending on the new retention
 count, any existing Snapshot copies
         that continue to use the same prefixes might be deleted. See the 'volume
 modify' man page for more information.
Do you want to continue? {y|n}: y
Volume modify successful on volume vol_name of Vserver svm_name.
```

Reserva de instantáneas

La reserva de copias instantáneas establece un porcentaje específico del espacio en disco para almacenar las copias instantáneas. La reserva de copias instantáneas predeterminada se establece en el 5 por ciento del espacio en disco. Si las copias de instantáneas superan el espacio reservado, se distribuyen en el sistema de archivos activo y este proceso se denomina dispersión de instantáneas.

La reserva de copias instantáneas debe tener suficiente espacio asignado para las copias instantáneas, incluidas las copias de seguridad por volumen. Si las copias instantáneas superan el espacio reservado, debe eliminar las copias instantáneas existentes del sistema de archivos activo para recuperar el espacio y poder utilizarlas en el sistema de archivos. También puede modificar el porcentaje de espacio en disco que se asigna a las copias instantáneas.

Cuando las instantáneas consumen más del 100% de la reserva de instantáneas, comienzan a ocupar el espacio de almacenamiento principal de la SSD. Este proceso se denomina derrame de instantáneas. Si las instantáneas siguen ocupando el espacio activo del sistema de archivos, el

sistema corre el riesgo de llenarse. Si el sistema se llena debido a un derrame de instantáneas, solo podrá crear archivos después de eliminar suficientes instantáneas.

Cuando hay suficiente espacio en disco disponible para las instantáneas en la reserva de instantáneas, al eliminar los archivos del nivel de SSD principal se libera espacio en disco para nuevos archivos, mientras que las copias de instantáneas que hacen referencia a esos archivos consumen solo el espacio de la reserva de copias instantáneas.

Como no hay forma de evitar que las instantáneas consuman espacio en disco superior a la cantidad reservada para ellas (la reserva de instantáneas), es importante reservar suficiente espacio en disco para las instantáneas de modo que el nivel SSD principal siempre tenga espacio disponible para crear nuevos archivos o modificar los existentes.

Si se crea una instantánea cuando los discos están llenos, al eliminar archivos de la capa SSD principal no se crea espacio libre, ya que la instantánea recién creada también hace referencia a todos esos datos. Debe eliminar la instantánea antes para liberar espacio de almacenamiento y poder crear o actualizar cualquier archivo.

Puede modificar la cantidad de reserva de instantáneas en un volumen mediante la NetApp ONTAP CLI. Para obtener más información, consulte Actualización de la reserva de instantáneas del volumen.

Actualización de la reserva de instantáneas del volumen

Puede cambiar la cantidad de reserva de instantáneas en un volumen mediante la NetApp ONTAP CLI o la API, tal como se describe en el siguiente procedimiento.

1. Para acceder a la CLI de NetApp ONTAP, ejecute el siguiente comando para establecer una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP. Reemplace *`management_endpoint_ip`* con la dirección IP del puerto de gestión del sistema de archivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obtener más información, consulte Administración de sistemas de archivos con la ONTAP CLI.

2. Utilice el comando CLI de `snap reserve` ONTAP para cambiar el porcentaje de espacio en disco utilizado para la reserva de copias instantáneas. *`vol_name`*Sustitúyalo por el nombre del

volumen y *percent* with the percent of disk space you want to reserve for Snapshot copies.

```
::> snap reserve vol_name percent
```

En el siguiente ejemplo, se cambia la reserva de instantáneas del volumen 1 al 25% de la capacidad de almacenamiento del volumen.

```
::> snap reserve vol1 25
```

Replicación programada mediante NetApp SnapMirror

Se puede utilizar NetApp SnapMirror para programar la replicación periódica de su FSx para el sistema de archivos ONTAP hacia o desde un segundo sistema de archivos. Esta capacidad está disponible tanto para implementaciones dentro de la región como entre regiones.

NetApp SnapMirror replica los datos a altas velocidades, por lo que obtiene una alta disponibilidad de datos y una replicación de datos rápida en todos los sistemas ONTAP, ya sea que esté replicando entre dos sistemas de archivos de Amazon FSx dentro o desde las AWS instalaciones. AWS La replicación se puede programar con una frecuencia de hasta 5 minutos, aunque los intervalos se deben elegir cuidadosamente en función de los RPO (objetivos de punto de recuperación), los RTO (objetivos de tiempo de recuperación) y las consideraciones de rendimiento.

Al replicar los datos en los sistemas NetApp de almacenamiento y actualizar continuamente los datos secundarios, los datos se mantienen actualizados y están disponibles siempre que los necesite. No se requieren servidores de replicación externos. Para obtener más información sobre cómo NetApp SnapMirror replicar sus datos, consulte Más información sobre el servicio de replicación en la documentación de NetApp BlueXP.

Puede crear un volumen de destino de protección de datos (DP) para NetApp SnapMirror utilizar la consola Amazon FSx, la API Amazon FSx y la API de Amazon FSx AWS CLI, además de la NetApp CLI de ONTAP y la API REST. Para obtener información sobre la creación de un volumen de destino mediante la consola Amazon FSx AWS CLI, consulte. Creación de volúmenes

Puede utilizar NetApp BlueXP o la CLI de NetApp ONTAP para programar la replicación de su sistema de archivos.

> **Note**
>
> Existen dos tipos de replicación de SnapMirror: a nivel de volumen de SnapMirror y recuperación de desastres (SVMDR). FSx for ONTAP solo admite la replicación de SnapMirror a nivel de volumen.

Uso de NetApp BlueXP para programar la replicación

Puede usar NetApp BlueXP para configurar la replicación SnapMirror en su sistema de archivos FSx for ONTAP. Para obtener más información, consulte Replicación de datos entre sistemas en la documentación de BlueXP. NetApp

Uso de la CLI NetApp de ONTAP para programar la replicación

Puede utilizar la CLI de NetApp ONTAP para configurar la replicación de volúmenes programada. Para obtener más información, consulte Gestión de la replicación de SnapMirror volúmenes en el Centro de documentación de NetApp ONTAP.

Proteja sus datos con SnapLock

SnapLock es una característica que permite proteger los archivos mediante la transición a un estado de escritura única y lectura múltiple (WORM), lo que impide su modificación o eliminación durante un período de retención específico. Puede utilizar SnapLock para cumplir con las normativas, proteger los datos críticos para la empresa de los ataques de ransomware y proporcionar un nivel adicional de protección para sus datos contra su alteración o eliminación.

Amazon FSx para NetApp ONTAP admite los modos de retención empresarial y de conformidad con. SnapLock Para obtener más información, consulte Conformidad de SnapLock y Empresarial de SnapLock.

Puede crear volúmenes SnapLock en FSx para sistemas de archivos ONTAP creados a partir del 13 de julio de 2023. Los sistemas de archivos existentes recibirán soporte de SnapLock durante un próximo período de mantenimiento semanal.

Temas

- Cómo funciona SnapLock
- Conformidad de SnapLock

- Empresarial de SnapLock
- Trabajando con el período de retención en SnapLock.
- Pasar archivos a estado WORM
- Copia de seguridad de volúmenes SnapLock
- Eliminación de volúmenes SnapLock

Cómo funciona SnapLock

SnapLock puede ayudarlo a cumplir con los fines normativos y de gobierno al evitar que sus archivos se eliminen, cambien o cambien de nombre. Cuando creas un volumen SnapLock, compromete sus archivos a un almacenamiento de escritura única y lectura múltiple (WORM) y estableces periodos de retención para los datos. Los archivos se pueden almacenar en un estado que no se pueda borrar ni escribir durante un período determinado o de forma indefinida.

> **Important**
>
> Debe especificar si un volumen utilizará la configuración de SnapLock en el momento de su creación. Un volumen que no sea un volumen SnapLock no se puede convertir en un volumen SnapLock después de su creación.

Modos de retención

SnapLock tiene dos modos de retención: Conformidad y Empresarial. Amazon FSx para NetApp ONTAP es compatible con ambos. Tienen distintos casos de uso y algunas de sus características son diferentes, pero ambas protegen los datos contra la modificación o la eliminación mediante el modelo WORM. En la siguiente tabla se explican algunas de las similitudes y diferencias entre estos modos de retención.

Característica de SnapLock	Conformidad de SnapLock	Empresarial de SnapLock
Descripción	Los archivos que se hayan transferido a WORM en un volumen de Conformidad no se pueden eliminar hasta	Los usuarios autorizados pueden eliminar los archivos que hayan pasado a WORM en un volumen empresari al antes de que venzan

Característica de SnapLock	Conformidad de SnapLock	Empresarial de SnapLock
	que venzan sus períodos de retención.	sus períodos de retención mediante la eliminación privilegiada.
Casos de uso	• Para cumplir los mandatos gubernamentales o específicos del sector, como la Norma 17a-4(f) de la SEC, la Norma 4511 de la FINRA y el Reglamento 1.31 de la CFTC. • Para protegerse contra los ataques de ransomware.	• Para promover la integridad de los datos y la conformidad interna de una organización. • Para probar la configuración de retención antes de usar Conformidad de SnapLock.
Confirmación automática	Sí	Sí
Retención basada en eventos (EBR)*	Sí	Sí
Retención legal*	Sí	No
Eliminación privilegiada	No	Sí
Modo añadir volumen	Sí	Sí
Registros de auditoría SnapLock	Sí	Sí

* Las operaciones EBR y Legal Hold son compatibles con la CLI de ONTAP y la API de REST.

Administrador de SnapLock

Debe tener privilegios de administrador de SnapLock para realizar determinadas acciones en los volúmenes SnapLock. Los permisos de administrador SnapLock se definen en el rol `vsadmin-snaplock` de la CLI ONTAP. Debe ser administrador de clústeres para crear una cuenta de administrador de máquinas virtuales de almacenamiento (SVM) con la función de administrador SnapLock.

Puede realizar las siguientes acciones con el rol `vsadmin-snaplock` en la CLI ONTAP:

- Administre su propia cuenta de usuario, contraseña local e información clave
- Administre los volúmenes, excepto los volúmenes móviles
- Gestione las cuotas, los qtrees, las copias instantáneas y los archivos
- Realice acciones de SnapLock, como la eliminación privilegiada y la retención legal
- Configuración de los protocolos de Network File System (NFS) y Server Message Block (SMB)
- Configure los servicios del Sistema de nombres de dominio (DNS), el Protocolo ligero de acceso a directorios (LDAP) y el Servicio de información de red (NIS)
- Monitorear trabajos

El siguiente procedimiento detalla cómo crear un administrador SnapLock en la CLI ONTAP. Para realizar esta tarea, debe iniciar sesión como administrador del clúster en una conexión segura, como Secure Shell Protocol (SSH).

Para crear una cuenta de administrador de SVM con la función vsadmin-snaplock en la CLI ONTAP.

- Ejecute el siguiente comando de la . *`Sustituya SVM_name`* y *`SnapLockAdmin`*por su propia información.

```
cluster1::> security login create -vserver SVM_name -user-or-group-
name SnapLockAdmin -application ssh -authentication-method password -role vsadmin-
snaplock
```

Registros de auditoría SnapLock

Un volumen de registro de auditoría SnapLock contiene registros de auditoría SnapLock, que contienen marcas temporales de eventos, como cuándo se creó un administrador SnapLock, cuándo se ejecutaron operaciones de eliminación con privilegios o cuándo se impuso una retención legal a los archivos. El volumen del registro de auditoría SnapLock es un registro de eventos que no se puede borrar.

Debe crear un volumen de registro de auditoría SnapLock en la misma SVM que el volumen SnapLock para realizar las siguientes acciones:

- Para activar o desactivar la eliminación privilegiada en un volumen Empresarial de SnapLock .
- Aplicar una retención legal a un archivo de un volumen de Conformidad de SnapLock.

Warning

- El período mínimo de retención de un volumen de registro de auditoría SnapLock es de seis meses. Hasta que venza este período de retención, el volumen del registro de auditoría SnapLock y la SVM y el sistema de archivos asociados a él no se pueden eliminar aunque el volumen se haya creado en modo Empresarial SnapLock.
- Si un archivo se elimina mediante una eliminación privilegiada y su período de retención es superior al período de retención del volumen, el volumen del registro de auditoría hereda el período de retención del archivo. Por ejemplo, si un archivo que tiene un período de retención de 10 meses se elimina mediante una eliminación privilegiada y el período de retención del volumen del registro de auditoría es de seis meses, el período de retención del volumen del registro de auditoría se amplía a 10 meses.

Sólo puede tener un volumen de registro de auditoría SnapLock activo en una SVM, pero varios volúmenes SnapLock de la SVM pueden compartirlo. Para montar correctamente un volumen de registro de auditoría SnapLock, defina la ruta de unión en `/snaplock_audit_log`. Ningún otro volumen puede utilizar esta ruta de unión, incluidos los volúmenes que no son volúmenes de registro de auditoría.

Puede encontrar los registros de auditoría SnapLock en el directorio `/snaplock_log` debajo de la raíz del volumen del registro de auditoría. Las operaciones de eliminación con privilegios se registran en el subdirectorio `privdel_log`. Las operaciones de inicio y fin de retención legal se registran en `/snaplock_log/legal_hold_logs/`. Todos los demás registros se almacenan en el subdirectorio `system_log`.

Puede crear un volumen de registro de auditoría SnapLock con la consola de Amazon FSx, la AWS CLI, la API de Amazon FSx y la CLI ONTAP y la API de REST.

Note

Un volumen de protección de datos (DP) no se puede utilizar como volumen de registro de auditoría SnapLock.

En el siguiente procedimiento se explica cómo crear un volumen de registro de auditoría SnapLock en la consola de Amazon FSx.

Para crear un volumen de registro de auditoría SnapLock, la consola Amazon FSx

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Siga el procedimiento para crear un volumen nuevo en Creación de volúmenes.
3. En la sección Avanzadas, en SnapLock Configuración, elija Activado.

   Seleccione la casilla de verificación para confirmar la advertencia sobre la activación de SnapLock en el volumen.
4. En Audit log volume (Volumen de registro de auditoría), seleccione Enabled (Activado).

   Asegúrese de que la Ruta de unión está configurada como `/snaplock_audit_log`.
5. Siga el resto del procedimiento para crear un volumen nuevo en Creación de volúmenes.
6. Seleccione Confirm (Confirmar) para crear el volumen.

Para activar el volumen del registro de auditoría SnapLock con la API Amazon FSx, utilice `AuditLogVolume` en `CreateSnaplockConfiguration`.

Acceder a los datos de un volumen SnapLock

Puede utilizar protocolos de archivos abiertos, como NFS y SMB, para acceder a los datos de un volumen SnapLock. Escribir datos en un volumen SnapLock o leer datos protegidos por WORM no afecta al rendimiento.

Puede copiar archivos de un volumen SnapLock a otro con NFS y SMB, pero no conservarán sus propiedades WORM en el volumen SnapLock de destino. Debe volver a enviar los archivos copiados a WORM para evitar que se modifiquen o eliminen. Para obtener más información, consulte Pasar archivos a estado WORM.

También puede replicar datos SnapLock con SnapMirror, pero los volúmenes de origen y destino deben ser volúmenes SnapLock con el mismo modo de retención (por ejemplo, ambos deben ser Conformidad o Empresarial).

Conformidad de SnapLock

Amazon FSx para NetApp ONTAP admite SnapLock volúmenes de conformidad.

Uso de Conformidad de SnapLock

Esta sección describe casos de uso y consideraciones para el modo de retención de Conformidad.

Casos de uso de Conformidad de SnapLock

Puede elegir el modo de retención de Conformidad para los siguientes casos de uso.

- Puede utilizar la función de Conformidad SnapLock para cumplir los mandatos gubernamentales o específicos del sector, como la norma 17a-4(f) de la SEC, la norma 4511 de la FINRA y la norma 1.31 de la CFTC.SnapLock El cumplimiento de estos mandatos y reglamentos en Amazon FSx para NetApp ONTAP fue evaluado por. Cohasset Associates Para obtener más información, consulte el informe de evaluación de la conformidad de Amazon FSx para NetApp ONTAP.
- Puede utilizar Conformidad de SnapLock para complementar o mejorar una estrategia integral de protección de datos para combatir los ataques de ransomware.

Consideraciones para el Conformidad de SnapLock

Estos son algunos aspectos importantes que se deben tener en cuenta sobre el modo de retención de Conformidad.

- Una vez que un archivo pasa al estado de escritura única y lectura múltiple (WORM) en un volumen de Conformidad de SnapLock, ningún usuario puede eliminarlo antes de que expire su periodo de retención.
- Un volumen de Conformidad de SnapLock sólo se puede eliminar cuando los períodos de retención de todos los archivos WORM del volumen hayan expirado y los archivos WORM se hayan eliminado del volumen.
- No puedes renombrar un volumen de Conformidad de SnapLock después de su creación.
- Puede utilizarlos SnapMirror para replicar archivos WORM, pero el volumen de origen y el volumen de destino deben tener el mismo modo de retención (por ejemplo, ambos deben ser de conformidad).
- Un volumen de Conformidad de SnapLock no se puede convertir en un volumen Empresarial de SnapLock y viceversa.

Crear un volumen de Conformidad de SnapLock

Puede crear un volumen de Conformidad de SnapLock con la consola de Amazon FSx, la AWS CLI, la API de Amazon FSx y las CLI ONTAP y la API de REST.

Para crear un volumen de Conformidad de SnapLock con la API de Amazon FSx, utilice `SnaplockType` en `CreateSnaplockConfiguration`.

En el siguiente procedimiento se explica cómo crear un volumen de Conformidad de SnapLock en la consola de Amazon FSx.

Para crear un volumen de Conformidad de SnapLock en la consola de Amazon FSx

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Siga el procedimiento para crear un volumen nuevo en Creación de volúmenes.
3. En la sección Avanzada, en SnapLock Configuración, elija Activado.

   Seleccione la casilla de verificación para confirmar la advertencia sobre la activación de SnapLock en el volumen.
4. Para el Retention mode (Modo de retención), seleccione Compliance (Conformidad).
5. Para el Audit log volume (Volumen del registro de auditoría), elija entre Enabled (Activado) y Disabled (Desactivado).

   Si selecciona Enabled (Activado), asegúrese de que la Ruta de unión esté establecida en `/snaplock_audit_log`.

   Para obtener más información, consulte Registros de auditoría SnapLock.
6. Para el Período de retención, ingrese los valores de Retención predeterminada, Retención mínima y Retención máxima. A continuación, elija la Unidad correspondiente para cada uno.

   Para obtener más información, consulte Trabajando con el período de retención en SnapLock..
7. Para la Autocommit (Confirmación automática), elija entre Enabled (Activado) y Disabled (Desactivado).

   Si selecciona Enabled (Activado), para el Período de confirmación automática, ingrese un valor y elija la unidad de Confirmación automática correspondiente.

   Puede especificar un valor entre 5 minutos y 10 años.

   Para obtener más información, consulte Confirmación automática.
8. Para el Volume append mode (Modo añadir volumen), elija entre Enabled (Activado) y Disabled (Desactivado).

   Para obtener más información, consulte Modo añadir volumen.
9. Siga el resto del procedimiento para crear un volumen nuevo en Creación de volúmenes.
10. Seleccione Confirm (Confirmar) para crear el volumen.

Empresarial de SnapLock

Amazon FSx para NetApp ONTAP admite SnapLock volúmenes empresariales.

Uso de Empresarial de SnapLock

Esta sección describe casos de uso y consideraciones para el modo de retención de Empresarial.

Casos de uso para Empresarial de SnapLock

Puede elegir el modo de retención Empresarial para los siguientes casos de uso.

- Puede usar Empresarial de SnapLock para autorizar únicamente a usuarios específicos a eliminar archivos.
- Puede usar Empresarial de SnapLock para mejorar la integridad de los datos y el cumplimiento interno de su organización.
- Puede usar Empresarial de SnapLock para probar la configuración de retención antes de usar Conformidad de SnapLock.

Consideraciones sobre el uso de Empresarial de SnapLock

Estos son algunos aspectos importantes a tener en cuenta sobre el modo de retención Empresarial.

- Puede utilizar SnapMirror para replicar archivos WORM, pero el volumen de origen y el de destino deben tener el mismo modo de retención (por ejemplo, ambos deben ser Empresarial).
- No se puede convertir un volumen SnapLock de Empresarial a Conformidad ni de Conformidad a Empresarial.
- Empresarial de SnapLock no admite Retención legal.

Eliminación privilegiada

Una de las principales diferencias entre Empresarial de SnapLock y Conformidad de SnapLock es que un administrador SnapLock puede activar el borrado privilegiado en un volumen Empresarial SnapLock para permitir que un archivo sea borrado antes de que expire el periodo de retención del archivo. El administrador SnapLock es el único usuario que puede eliminar archivos de un volumen Empresarial de SnapLock que tenga políticas de retención activas. Para obtener más información, consulte Administrador de SnapLock.

Puede activar o desactivar la eliminación de privilegios con la consola de Amazon FSx, la AWS CLI, la API de Amazon FSx, CLI ONTAP y la API de REST. Para activar la eliminación con privilegios, primero debe crear un volumen de registro de auditoría SnapLock en la misma SVM que el volumen SnapLock. Para obtener más información, consulte Registros de auditoría SnapLock.

Para activar la eliminación con privilegios con la API de Amazon FSx, utilice `PrivilegedDelete` en `CreateSnaplockConfiguration`.

En el siguiente procedimiento se explica cómo activar la eliminación privilegiada en la consola de Amazon FSx.

Para activar la eliminación con privilegios en un volumen Empresarial de SnapLock de la consola Amazon FSx

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Siga el procedimiento para crear un volumen nuevo en Creación de volúmenes.
3. En la sección Avanzadas, en SnapLock Configuración, seleccione Activado.

   Seleccione la casilla de verificación para confirmar la advertencia sobre la activación de SnapLock en el volumen.
4. Para el Retention mode (Modo de retención), elija Empresarial.
5. Para Privileged Delete (Eliminación privilegiada), seleccione (Enabled) Activado.
6. Siga el resto del procedimiento para crear un volumen nuevo en Creación de volúmenes.
7. Seleccione Confirm (Confirmar) para crear el volumen.

> **Note**
>
> No se puede ejecutar un comando de eliminación privilegiado para eliminar un archivo de escritura única y lectura múltiple (WORM) que tiene un período de retención vencido. Puede ejecutar una operación de eliminación normal una vez transcurrido el período de retención.

Puede optar por desactivar la eliminación privilegiada de forma permanente, pero esta acción es irreversible. Si la eliminación con privilegios está desactivada permanentemente, no es necesario tener un volumen de registro de auditoría SnapLock asociado al volumen Empresarial de SnapLock.

Para desactivar permanentemente la eliminación privilegiada con la API de Amazon FSx, utilice `PrivilegedDelete` en `CreateSnaplockConfiguration`.

Para desactivar permanentemente la eliminación privilegiada en un volumen Empresarial de SnapLock de la consola Amazon FSx

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Siga el procedimiento para crear un volumen nuevo en Creación de volúmenes.
3. En la sección Avanzada, en SnapLock Configuración, elija Habilitado.

   Seleccione la casilla de verificación para confirmar la advertencia sobre la activación de SnapLock en el volumen.
4. Para el Retention mode (Modo de retención), elija Empresarial.
5. Para Eliminación privilegiada, seleccione Desactivada permanentemente.
6. Siga el resto del procedimiento para crear un volumen nuevo en Creación de volúmenes.
7. Seleccione Confirm (Confirmar) para crear el volumen.

Creación de un volumen Empresarial de SnapLock

Puede crear un volumen Empresarial de SnapLock con la consola de Amazon FSx, la AWS CLI, la API de Amazon FSx y las CLI ONTAP y la API de REST.

Para crear un volumen Empresarial de SnapLock con la API Amazon FSx, utilice `SnaplockType` en `CreateSnaplockConfiguration`.

Para crear un volumen Empresarial de SnapLock en la consola Amazon FSx

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Siga el procedimiento para crear un volumen nuevo en Creación de volúmenes.
3. En la sección Avanzada, en SnapLock Configuración, elija Habilitado.

   Seleccione la casilla de verificación para confirmar la advertencia sobre la activación de SnapLock en el volumen.
4. Para el Retention mode (Modo de retención), elija Empresarial.
5. Para el Audit log volume (Volumen del registro de auditoría), elija entre Enabled (Activado) y Disabled (Desactivado).

Si selecciona Enabled (Activado), asegúrese de que la Ruta de unión esté establecida en `/snaplock_audit_log`.

Para obtener más información, consulte Registros de auditoría SnapLock.

6. Para el Período de retención, ingrese los valores de Retención predeterminada, Retención mínima y Retención máxima. A continuación, elija la Unidad correspondiente para cada uno.

   Para obtener más información, consulte Trabajando con el período de retención en SnapLock..

7. Para la Autocommit (Confirmación automática), elija entre Enabled (Activado) y Disabled (Desactivado).

   Si selecciona Enabled (Activado), para el Período de confirmación automática, ingrese un valor y elija la unidad de Confirmación automática correspondiente.

   Puede especificar un valor entre 5 minutos y 10 años.

   Para obtener más información, consulte Confirmación automática.

8. Para Eliminación privilegiada, elija entre Activado, Desactivado y Desactivada permanentemente.

   Para obtener más información, consulte Eliminación privilegiada.

9. Para el Volume append mode (Modo añadir volumen), elija entre Enabled (Activado) y Disabled (Desactivado).

   Para obtener más información, consulte Modo añadir volumen.

10. Siga el resto del procedimiento para crear un volumen nuevo en Creación de volúmenes.
11. Seleccione Confirm (Confirmar) para crear el volumen.

Omitir el modo Empresarial

Si utiliza la consola Amazon FSx o la API de Amazon FSx, debe tener el permiso `fsx:BypassSnapLockEnterpriseRetention` de IAM para eliminar un volumen Empresarial SnapLock que contenga archivos WORM con políticas de retención activas.

Para obtener más información, consulte Eliminación de volúmenes SnapLock.

Trabajando con el período de retención en SnapLock.

Al crear un volumen SnapLock, puede establecer un período de retención predeterminado para el volumen o puede establecer el período de retención para archivos de escritura única y lectura múltiple (WORM) de forma explícita. Durante el período de retención, no puede eliminar ni modificar los archivos protegidos por WORM. El período de retención se utiliza para calcular el tiempo de retención. Por ejemplo, si hace la transición de un archivo a WORM el 14 de julio de 2023 a medianoche y establece el período de retención en cinco años, el tiempo de retención sería hasta el 14 de julio de 2028 a medianoche.

Para obtener más información acerca de WORM, consulte Pasar archivos a estado WORM.

Políticas de periodo de retención

El periodo de retención viene determinado por los valores que se asignan a los siguientes parámetros:

- Retención predeterminada: el periodo de retención predeterminado que se asigna a un archivo WORM si no se le proporciona un período de retención explícito.
- Retención mínima: el periodo de retención más corto que se puede asignar a un archivo WORM.
- Retención máxima: el periodo de retención más largo que se puede asignar a un archivo WORM.

> **Note**
>
> Incluso después de que venza el período de retención, no puede modificar un archivo WORM. Sólo puede eliminarlo o establecer un nuevo período de retención para volver a activar la protección WORM.

Puede especificar el período de retención mediante varias unidades de tiempo diferentes. La siguiente tabla enumera los rangos específicos que se admiten.

Tipo	Valor	Notas
Segundos	0 - 65.535	
Minutos	0 - 65.535	

Tipo	Valor	Notas
Horas	0 - 24	
Días	0 - 365	
Meses	0 -12	
Años	0 - 100	
Infinito	-	Conserva los archivos para siempre. Disponible para la Retención predeterminada, la Retención máxima y la Retención mínima.
Sin especificar*	-	Conserva los archivos hasta que establezca un período de retención. Disponible sólo para la Retención predeterminada.

* Cuando se transfieren archivos a WORM con un período de retención no especificado, se les asigna el período de retención mínimo configurado para el volumen SnapLock. Al hacer la transición de los archivos protegidos por WORM a un tiempo de retención absoluto, el nuevo período de retención debe ser superior al período mínimo establecido anteriormente en los archivos.

Periodo de retención caducado

Cuando caduque el período de retención de un archivo WORM, puede eliminarlo o establecer un nuevo período de retención para volver a activar la protección WORM. Los archivos WORM no se eliminan automáticamente una vez transcurrido su período de retención. Incluso después de que venza el período de retención, no puede modificar un archivo WORM.

Definición del periodo de retención de un volumen SnapLock

Puede establecer el periodo de retención de un volumen SnapLock con la consola de Amazon FSx, AWS CLI, la API de Amazon FSx y CLI ONTAP y la API de REST.

Para establecer el período de retención con la API de Amazon FSx, utilice la configuración `SnaplockRetentionPeriod`.

En el siguiente procedimiento se explica cómo configurar el período de retención en la consola de Amazon FSx.

Para configurar el período de retención de un volumen SnapLock en la consola Amazon FSx

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Siga el procedimiento para crear un volumen nuevo en Creación de volúmenes.
3. En la sección Avanzada, en SnapLock Configuración, elija Activado.

   Seleccione la casilla de verificación para confirmar la advertencia sobre la activación de SnapLock en el volumen.
4. Para el Período de retención, ingrese los valores de Retención predeterminada, Retención mínima y Retención máxima. A continuación, elija la Unidad correspondiente para cada uno.
5. Siga el resto del procedimiento para crear un volumen nuevo en Creación de volúmenes.
6. Seleccione Confirm (Confirmar) para crear el volumen.

Pasar archivos a estado WORM

En esta sección se explica cómo hacer la transición de los archivos a un estado de escritura única y lectura múltiple (WORM). También se describe el modo añadir volúmenes, que es una forma de escribir datos de forma incremental en archivos protegidos por WORM.

Confirmación automática

Puede usar la confirmación automática para realizar la transición de archivos a WORM si no se han modificado durante el período que usted especifique. Puede activar la confirmación automática con la consola de Amazon FSx, la AWS CLI, la API de Amazon FSx, CLI ONTAP y la API de REST.

Puede especificar un período de confirmación automática de entre cinco minutos y 10 años. La siguiente tabla enumera los rangos específicos que se admiten.

Unidad	Valor
Minutos	5 - 65.535
Horas	1 - 65.535
Días	1 - 3.650
Meses	1 - 120
Años	1 - 10

Para activar la confirmación automática con la API de Amazon FSx, utilice `AutocommitPeriod` en `CreateSnaplockConfiguration`.

El siguiente procedimiento explica cómo activar la confirmación automática en la consola de Amazon FSx.

Para activar la confirmación automática en la consola Amazon FSx

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Siga el procedimiento para crear un volumen nuevo en Creación de volúmenes.
3. En la sección Avanzada, en SnapLock Configuración, elija Activado.

   Seleccione la casilla de verificación para confirmar la advertencia sobre la activación de SnapLock en el volumen.
4. En Autocommit (Confirmación automática), seleccione Enabled (Activado).
5. En Autocommit period (Periodo de confirmación automática), ingrese un valor y seleccione la Autocommit unit (unidad de confirmación automática) correspondiente.

   Puede especificar un valor entre 5 minutos y 10 años.
6. Siga el resto del procedimiento para crear un volumen nuevo en Creación de volúmenes.
7. Seleccione Confirm (Confirmar) para crear el volumen.

Modo añadir volumen

No puede modificar los datos existentes en un archivo protegido por WORM. Sin embargo, SnapLock le permite mantener la protección de los datos existentes mediante archivos que se pueden añadir a WORM. Por ejemplo, puede generar archivos de registro o conservar los datos de transmisión de audio o vídeo y, al mismo tiempo, escribir los datos en ellos de forma incremental. Puede activar o desactivar el modo añadir volumen con la consola de Amazon FSx, la AWS CLI, la API de Amazon FSx, CLI ONTAP y la API de REST.

Requisitos para actualizar el modo añadir volúmenes

- El volumen SnapLock debe estar desmontado.
- El volumen SnapLock debe estar vacío de copias instantáneas y datos de usuario.

Para activar el modo añadir volumen con la API de Amazon FSx, utilice `VolumeAppendModeEnabled` en `CreateSnaplockConfiguration`.

El siguiente procedimiento explica cómo activar el modo añadir volumen en la consola de Amazon FSx.

Para activar el modo añadir volumen en la consola Amazon FSx

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Siga el procedimiento para crear un volumen nuevo en Creación de volúmenes.
3. En la sección Avanzada, en SnapLock Configuración, elija Habilitado.

   Seleccione la casilla de verificación para confirmar la advertencia sobre la activación de SnapLock en el volumen.
4. Para el Volume append mode (Modo añadir volumen), seleccione Enabled (Activado).
5. Siga el resto del procedimiento para crear un volumen nuevo en Creación de volúmenes.
6. Seleccione Confirm (Confirmar) para crear el volumen.

Retención basada en eventos (EBR)

Puede usar la retención basada en eventos (EBR) para crear políticas personalizadas con los periodos de retención asociados. Por ejemplo, puede hacer la transición de todos los archivos de una ruta específica a WORM y establecer el período de retención en un año con los comandos

`snaplock event-retention policy create` y `snaplock event-retention apply`. Cuando utilice EBR, debe especificar un volumen, directorio o archivo. El periodo de retención que seleccione al crear la política de EBR se aplica a todos los archivos de la ruta especificada.

EBR es compatible con la CLI ONTAP y la API de REST.

> **Note**
>
> ONTAPno admite EBR con FlexGroup volúmenes.

En los siguientes procedimientos se explica cómo crear, aplicar, modificar y eliminar una política de EBR. Debe ser administrador SnapLock (tener la el rol `vsadmin-snaplock`) para completar estas tareas en la CLI ONTAP. Para obtener más información, consulte Administrador de SnapLock.

Para crear una política EBR en la CLI ONTAP

Ejecute el siguiente comando de la . Reemplace *p1* y *"10 años"* con su propia información.

```
vs1::> snaplock event-retention policy create -name p1 -retention-period "10 years"
```

Para aplicar una política de EBR en la CLI ONTAP

Ejecute el siguiente comando de la . Reemplace *p1* y *slc* con su propia información. Puede agregar una ruta después de la barra diagonal (/) si desea especificar una ruta concreta para la política de EBR. De lo contrario, este comando aplica la política EBR a todos los archivos del volumen.

```
vs1::> snaplock event-retention apply -policy-name p1 -volume slc -path /
```

Para modificar una política de EBR en la CLI ONTAP

Ejecute el siguiente comando de la . Reemplace *p1* y *"5 años"* con su propia información.

```
vs1::> snaplock event-retention policy modify -name p1 -retention-period "5 years"
```

Para eliminar una política de EBR en la CLI ONTAP

Ejecute el siguiente comando de la . Reemplace *p1* con su propia información.

```
vs1::> snaplock event-retention policy delete -name p1
```

Comandos relacionados en el Centro de documentación NetApp:

- snaplock event-retention abort
- snaplock event-retention show-vservers
- snaplock event-retention show
- snaplock event-retention policy show

Retención legal

Puede retener archivos WORM durante un periodo de tiempo indefinido utilizando la Retención legal. Por lo general, la retención legal se utiliza con fines de litigio. Un archivo WORM que esté sujeto a una Retención legal no se puede eliminar hasta que se levante la Retención legal.

La CLI ONTAP y la API de REST admiten la Retención legal.

> **Note**
>
> ONTAPno admite la retención legal con FlexGroup volúmenes.

En los siguientes procedimientos se explica cómo iniciar y finalizar una Retención legal. Debe ser administrador SnapLock (tener la el rol `vsadmin-snaplock`) para completar estas tareas en la CLI ONTAP. Para obtener más información, consulte Administrador de SnapLock.

Para iniciar una Retención legal de un archivo de un volumen de Conformidad de SnapLock con la CLI ONTAP

Ejecute el siguiente comando de la . Reemplace *litigation1*, *slc_vol1* y *file1* por su propia información.

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

Para iniciar una Retención legal de todos los archivos de un volumen de Conformidad de SnapLock con la CLI ONTAP

Ejecute el siguiente comando de la . Reemplace *litigation1* y *slc_vol1* por su propia información.

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -path /
```

Para poner fin a una Retención legal de un archivo de un volumen de Conformidad de SnapLock con la CLI ONTAP

Ejecute el siguiente comando de la . Reemplace *litigation1*, *slc_vol1* y *file1* por su propia información.

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

Para poner fin a una Retención legal de todos los archivos de un volumen de Conformidad de SnapLock con la CLI ONTAP

Ejecute el siguiente comando de la . Reemplace *litigation1* y *slc_vol1* por su propia información.

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -path /
```

> **Note**
>
> Le recomendamos que supervise el `-operation-status` con el comando `snaplock legal-hold show` cuando emita una Retención legal para asegurarse de que no falla.

Comandos relacionados en el Centro de documentación NetApp:

- snaplock legal-hold abort
- snaplock legal-hold dump-files
- snaplock legal-hold dump-litigations
- snaplock legal-hold show

Copia de seguridad de volúmenes SnapLock

Puede hacer copias de seguridad de los volúmenes SnapLock para obtener una protección de datos adicional. Al restaurar un volumen SnapLock, se conservan los ajustes originales del volumen, como

la retención predeterminada, la retención mínima y la retención máxima. También se conservan la configuración de escritura única y lectura múltiple (WORM) y la Retención legal.

> **Note**
>
> No puedes hacer copias de seguridad de un SnapLock FlexGroup volumen.

Puede restaurar la copia de seguridad de un volumen SnapLock como volumen SnapLock o volumen no SnapLock. Sin embargo, no puede restaurar una copia de seguridad que no sea de un volumen SnapLock como un volumen SnapLock.

Para obtener más información sobre las copias de seguridad, consulte Trabajo con copias de seguridad.

Eliminación de volúmenes SnapLock

Puede eliminar un volumen de Conformidad de SnapLock, si han caducado los períodos de retención de todos los archivos de escritura única y lectura múltiple (WORM) que contiene.

> **Note**
>
> Si cierra una Cuenta de AWS que contiene volúmenes SnapLock Enterprise y Compliance, AWS FSx para ONTAP suspenden su cuenta durante 90 días con sus datos intactos. Si no vuelve a abrir su cuenta durante esos 90 días, AWS eliminará sus datos, incluidos los datos de los volúmenes SnapLock, independientemente de su configuración de retención.

Puede eliminar un volumen Empresarial SnapLock en cualquier momento si tiene los permisos adecuados. Debe ser administrador de Amazon FSx. Además, tanto si utiliza la consola Amazon FSx como la API de Amazon FSx, debe tener el permiso IAM de `fsx:BypassSnapLockEnterpriseRetention` IAM para eliminar un volumen Empresarial de SnapLock que contenga datos de WORM con una política de retención activa.

> **Warning**
>
> El período mínimo de retención de un volumen de registro de auditoría SnapLock es de seis meses. Hasta que finalice este periodo de retención, no podrá eliminar el volumen del registro de auditoría SnapLock, la máquina virtual de almacenamiento (SVM) ni el sistema

de archivos asociado a la SVM, incluso si el volumen se creó en modo Empresarial de SnapLock. Para obtener más información, consulte Registros de auditoría SnapLock.

Para eliminar un volumen Empresarial de SnapLock en la consola Amazon FSx

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación izquierdo, seleccione Volumes (Volúmenes).
3. Seleccione el volumen que desea eliminar.
4. En Actions (Acciones), seleccione Delete volume (Eliminar volumen).
5. En Bypass SnapLock Enterprise Retention, selecciona Sí.
6. En el cuadro de diálogo de confirmación, elija una de las siguientes opciones para (Create final backup) Crear copia de seguridad final:
   - Seleccione Yes (Sí) para realizar una copia de seguridad final del volumen. Se muestra el nombre de la copia de seguridad final.
   - Seleccione No si no desea realizar una copia de seguridad final del volumen. Se le pedirá que confirme que, una vez eliminado el volumen, las copias de seguridad automáticas dejarán de estar disponibles.
7. Confirme la eliminación del volumen ingresando **`delete`** en el campo Confirm delete (Confirmar eliminación).
8. Seleccione Delete volume(s) Eliminar volúmenes.

Uso de Microsoft Active Directory en FSx para ONTAP

Amazon FSx funciona con Microsoft Active Directory para integrarse con sus entornos existentes. Active Directory es el servicio de directorio de Microsoft para almacenar información de los objetos de la red y para facilitarles la búsqueda y el uso de dicha información a los administradores y usuarios. Estos objetos suelen incluir recursos compartidos, como servidores de archivos y cuentas de usuarios y ordenadores de la red.

Si lo desea, puede unir sus máquinas virtuales de almacenamiento (SVM) FSx for ONTAP a su dominio de Active Directory para proporcionar autenticación de usuario y control de acceso a nivel de archivos y carpetas. A continuación, los clientes del bloque de mensajes de servidor (SMB) pueden utilizar sus identidades de usuario existentes en Active Directory para autenticarse y acceder a los volúmenes de SVM. Los usuarios pueden usar sus identidades actuales para controlar el acceso a archivos y carpetas individuales. Además, puede migrar sus archivos y carpetas existentes y sus configuraciones de lista de control de acceso (ACL) de seguridad a Amazon FSx sin ninguna modificación.

Cuando une Amazon FSx for NetApp ONTAP a un Active Directory, une las SVM del sistema de archivos a Active Directory de forma independiente. Esto significa que puede tener un sistema de archivos con algunas SVM que estén unidas a un Active Directory y otras SVM que no lo estén.

Después de unir un SVM a un Active Directory, puede actualizar las siguientes propiedades de configuración de Active Directory:

- Dirección IP del servidor DNS
- Nombre de usuario y contraseña de la cuenta de servicio de Active Directory autogestionada

Temas

Requisitos previos para unir una SVM a un Microsoft AD autogestionado

Antes de unir una SVM de FSx para ONTAP a un dominio de Microsoft AD autogestionado, asegúrese de que Active Directory y su red cumplen los requisitos descritos en las siguientes secciones.

Temas

Requisitos de Active Directory en las instalaciones

Asegúrese de que ya dispone de un Microsoft AD en las instalaciones u otro AD autogestionado al que pueda unirse la SVM. Este Active Directory debe tener la siguiente configuración:

- El nivel funcional del dominio del controlador de dominio de Active Directory está en Windows Server 2000 o superior.
- Active Directory usa un nombre de dominio que no está en el formato de dominio de etiqueta única (SLD). Amazon FSx no admite dominios SLD.
- Si tiene sitios de Active Directory definidos, asegúrese de que las subredes de la VPC asociadas al sistema de archivos FSx for ONTAP estén definidas en los mismos sitios de Active Directory y de que no existan conflictos entre las subredes de la VPC y las subredes de los sitios de Active Directory.

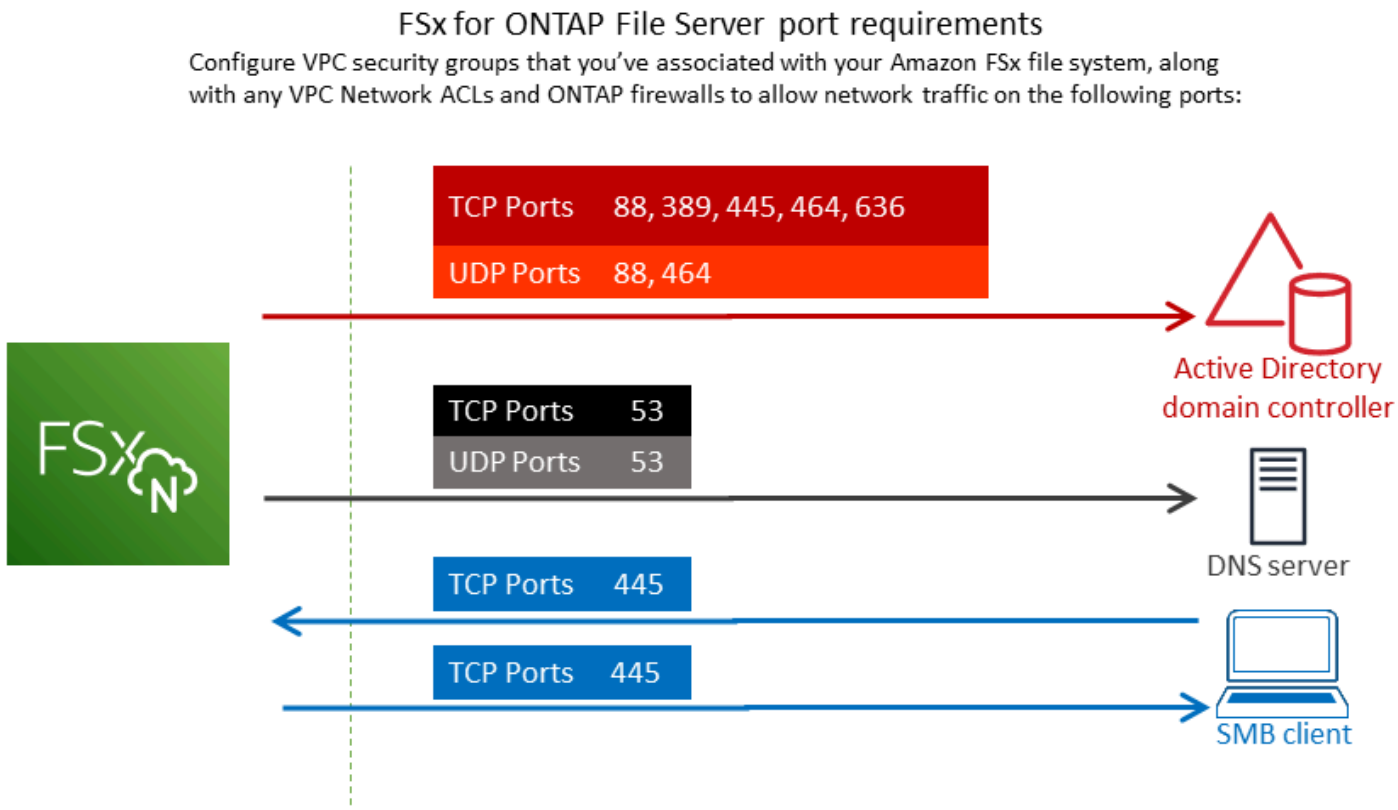
> **Note**
>
> Si lo utiliza AWS Directory Service, FSx para ONTAP no admite la unión de SVM al Active Directory simple.

Requisitos de configuración de la red

Asegúrese de tener las siguientes configuraciones de red y de disponer de la información asociada.

> **Important**
>
> Para que una SVM se una a Active Directory, debe asegurarse de que los puertos documentados en este tema permitan el tráfico entre todos los controladores de dominio de Active Directory y las dos direcciones IP iSCSI (interfaces lógicas (LIF) iscsi_1 e iscsi_2) en la SVM.

- Las direcciones IP del servidor DNS y del controlador de dominio de Active Directory.
- La conectividad debe estar configurada entre la Amazon VPC donde desea crear el sistema de archivos y el Active Directory autogestionado utilizando AWS Direct Connect, AWS VPN o AWS Transit Gateway.
- El grupo de seguridad y las ACL de red de la VPC para las subredes en las que está creando el sistema de archivos deben permitir el tráfico en los puertos y en las direcciones que se muestran en el siguiente diagrama.



El rol de cada puerto se describe en la tabla siguiente.

Protocolo	Puertos	Rol
TCP/UDP	53	Sistema de nombres de dominio (DNS)
TCP/UDP	88	Autenticación de Kerberos
TCP/UDP	389	Protocolo ligero de acceso a directori os (LDAP)
TCP	445	Uso compartido de archivos SMB de Directory Services
TCP/UDP	464	Cambiar/establecer contraseña
TCP	636	Protocolo ligero de acceso a directorios sobre TLS/SSL (LDAP)

- Estas reglas de tráfico también deben reflejarse en los firewalls que se aplican a cada uno de los controladores de dominio, servidores DNS, clientes de FSx y administradores de FSx de Active Directory.

> **Important**
>
> Si bien los grupos de seguridad de Amazon VPC requieren que los puertos se abran solo en la dirección en la que se inicia el tráfico de red, la mayoría de los firewalls de Windows y las ACL de red de VPC requieren que los puertos estén abiertos en ambas direcciones.

Requisitos de la cuenta de servicio de Active Directory

Asegúrese de que dispone de una cuenta de servicio en su Microsoft AD autogestionado que tenga permisos delegados para unir equipos al dominio. Una cuenta de servicio es una cuenta de usuario de su Active Directory autogestionado en la que se han delegado determinadas tareas.

Como mínimo, se deben delegar en la cuenta de servicio los siguientes permisos en la OU a la que se va a unir a la SVM:

- Capacidad de restablecer las contraseñas

- Capacidad de restringir la lectura y escritura de datos en las cuentas
- Posibilidad de establecer la `msDS-SupportedEncryptionTypes` propiedad en objetos de la computadora
- Capacidad validada para escribir en el nombre de host del DNS
- Capacidad validada para escribir en el nombre de entidad principal del servicio
- Capacidad para crear y eliminar objetos del equipo
- Capacidad validada para leer y escribir las restricciones de la cuenta

Estos representan el conjunto mínimo de permisos que se necesitan para unir objetos informáticos al Active Directory. Para obtener más información, consulte el tema Error de la documentación de Windows Server: se deniega el acceso cuando usuarios no administradores a los que se les ha delegado el control intentan unir equipos a un controlador de dominio.

Para obtener más información acerca de la creación de una cuenta de servicio con los permisos correctos, consulte Delegación de privilegios a la cuenta de servicio Amazon FSx.

> **Important**
>
> Amazon FSx requiere una cuenta de servicio válida durante toda la vida útil del sistema de archivos de Amazon FSx. Amazon FSx debe poder administrar completamente el sistema de archivos y realizar tareas que requieran que separe y vuelva a unir los recursos a su dominio de Active Directory. Estas tareas incluyen la sustitución de un sistema de archivos o SVM defectuoso o la aplicación de parches al software de ONTAP. NetApp Mantenga actualizada la información de configuración de Active Directory con Amazon FSx, incluidas las credenciales de la cuenta de servicio. Para obtener más información, consulte Mantener la configuración del Active Directory actualizada con Amazon FSx.

Si es la primera vez que utiliza AWS FSx para ONTAP, asegúrese de completar los pasos de configuración iniciales antes de iniciar la integración con Active Directory. Para obtener más información, consulte Configuración de FSx para ONTAP.

> **Important**
>
> No mueva los objetos informáticos que Amazon FSx crea en la unidad organizativa después de crear las SVM, ni elimine Active Directory mientras la SVM esté unida a ella. Si lo hace, las SVM se desconfigurarán.

Prácticas recomendadas para trabajar con Oracle

Estas son algunas sugerencias y directrices que debe tener en cuenta al incorporar Amazon FSx for NetApp ONTAP SVM a su Microsoft Active Directory autogestionado. Tenga en cuenta que se recomiendan como prácticas recomendadas, pero no son obligatorias.

Delegación de privilegios a la cuenta de servicio Amazon FSx

Asegúrese de configurar la cuenta de servicio que proporciona a Amazon FSx con los permisos mínimos requeridos. Además, separe la unidad organizativa (OU) de otras cuestiones relacionadas con el controlador de dominio.

Para unir las SVM de Amazon FSx a su dominio, asegúrese de que la cuenta de servicio tenga permisos delegados. Los miembros del grupo de Administradores de dominio tienen permisos suficientes para realizar esta tarea. Sin embargo, como práctica recomendada, utilice una cuenta de servicio que solo tenga los permisos mínimos necesarios para hacerlo. El siguiente procedimiento muestra cómo delegar solo los permisos necesarios para unir FSx for ONTAP SVM a su dominio.

Realice este procedimiento en un equipo que esté unido a su directorio y que tenga instalado el complemento MMC Usuarios y equipos de Active Directory.

Para crear una cuenta de servicio para su dominio de Microsoft Active Directory

1. Asegúrese de haber iniciado sesión como administrador de dominio de su dominio de Microsoft Active Directory.
2. Abra el complemento MMC Usuarios y equipos del Active Directory.
3. En el panel de tareas, expanda el nodo del dominio.
4. Busque y abra el menú contextual (botón derecho) de la unidad organizativa que quiera modificar y, a continuación, elija Delegar control.
5. En la página Delegation of Control Wizard (Asistente de delegación de control), elija Next (Siguiente).

6. Elija Add (Agregar) para agregar un usuario específico o un grupo específico para los usuarios y grupos seleccionados y, a continuación, elija Next (Siguiente).
7. En la página Tareas que se delegarán, elija Crear una tarea personalizada para delegar y luego elija Siguiente.
8. Elija Sólo los siguientes objetos en la carpeta y, a continuación, seleccione objetos informáticos.
9. Elija Crear los objetos seleccionados en esta carpeta y Eliminar los objetos seleccionados en esta carpeta. A continuación, elija Siguiente.
10. En Mostrar estos permisos, asegúrate de seleccionar General y Específico de propiedad.
11. Para los Permisos, elija lo siguiente:
    - Restablecer contraseña
    - Leer y escribir las restricciones de la cuenta
    - Escritura validada en el nombre de host DNS
    - Escritura validada en el nombre de entidad principal del servicio
    - Escribe MSDs- SupportedEncryptionTypes
12. Elija Siguiente y, a continuación, elija Finalizar.
13. Cierre el complemento MMC Usuarios y equipos del Active Directory.

> **Important**
>
> No mueva los objetos informáticos que Amazon FSx crea en la OU después de la creación de sus SVMs. Si lo hace, las SVM se desconfigurarán.

Mantener la configuración del Active Directory actualizada con Amazon FSx

Para una disponibilidad ininterrumpida de sus SVM de Amazon FSx, actualice la configuración de Active Directory (AD) autogestionada de una SVM cuando cambie la configuración de AD autogestionada.

Por ejemplo, suponga que su AD utiliza una política de restablecimiento de contraseñas basada en el tiempo. En este caso, tan pronto como se restablezca la contraseña, asegúrese de actualizar la contraseña de la cuenta de servicio con Amazon FSx. Para ello, utilice la consola Amazon FSx, la API de Amazon FSx o la AWS CLI. Del mismo modo, si las direcciones IP del servidor DNS cambian

para su dominio de Active Directory, en cuanto se produzca el cambio actualice las direcciones IP del servidor DNS con Amazon FSx.

Si hay un problema con la configuración AD autogestionada actualizada, el estado SVM cambia a Misconfigured (Desconfigurado). Este estado muestra un mensaje de error y una acción recomendada junto a la descripción de la SVM en la consola, la API y la CLI. Si se produce un problema con la configuración de AD de su SVM, asegúrese de tomar las medidas correctivas recomendadas para las propiedades de configuración. Si el problema se ha resuelto, compruebe que el estado de su SVM cambie a Created (Creado).

Para obtener más información, consulte Actualización de una configuración de SVM de Active Directory existente mediante las AWS Management Console API, y AWS CLI y Modificar una configuración de Active Directory mediante la CLI de ONTAP.

Uso de grupos de seguridad para limitar el tráfico dentro de la VPC

Para limitar el tráfico de red en la nube privada virtual (VPC), puede implementar el principio del privilegio mínimo en la VPC. En otras palabras, puedes limitar los permisos al mínimo necesario. Para ello, utilice las reglas de los grupos de seguridad. Para obtener más información, consulte Grupos de seguridad de Amazon VPC.

Crear reglas de grupos de seguridad salientes para la interfaz de red del sistema de archivos

Para mayor seguridad, considere la posibilidad de configurar un grupo de seguridad con reglas de tráfico saliente. Estas reglas deben permitir el tráfico saliente sólo a sus controladores de dominios AD autogestionados o dentro de la subred o grupo de seguridad. Aplique este grupo de seguridad a la VPC asociada con la interfaz de red elástica del sistema de archivos Amazon FSx. Para obtener más información, consulte Control de acceso al sistema de archivos con Amazon VPC.

Unir las SVM a Microsoft Active Directory

Su organización puede administrar las identidades y los dispositivos mediante un Active Directory, ya sea de forma local o en la nube. Con FSx para ONTAP, puede unir sus SVM directamente a su dominio de Active Directory existente de las siguientes maneras:

- Unir las nuevas SVM a un Active Directory en el momento de su creación:
  - Con la opción de creación estándar de la consola Amazon FSx para crear un nuevo sistema de archivos FSx para ONTAP, puede unir el SVM predeterminado a un Active Directory

autogestionado. Para obtener más información, consulte Para crear un sistema de archivos (consola).

- Uso de la consola de Amazon FSx o de la API de Amazon FSx para crear una nueva SVM en un sistema de archivos FSx para ONTAP existente. AWS CLI Para obtener más información, consulte Creación de una máquina virtual de almacenamiento.

- Unir las SVM existentes a un Active Directory:
  - Usar la API AWS Management Console AWS CLI, y para unir un SVM a un Active Directory y volver a intentar unir un SVM a un Active Directory si el intento inicial de unión falló. También puede actualizar algunas propiedades de configuración de Active Directory para las SVM que ya están unidas a un Active Directory. Para obtener más información, consulte Administrar las configuraciones de SVM Active Directory.
  - Uso de la CLI o la API REST de NetApp ONTAP para unir, volver a intentar unir y desunir las configuraciones de SVM Active Directory. Para obtener más información, consulte Administración de la configuración de SVM Active Directory mediante la CLI NetApp .

> ⚠ Important
>
> - Amazon FSx solo registra registros DNS para una SVM si utiliza Microsoft DNS como servicio DNS predeterminado. Si utiliza un DNS de terceros, deberá configurar las entradas DNS manualmente para sus SVM de Amazon FSx después de crearlas.
> - Si lo usa AWS Managed Microsoft AD, debe especificar un grupo como administradores AWS delegados de FSx AWS , administradores delegados o un grupo personalizado con permisos delegados para la OU.

Al unir un SVM de FSx for ONTAP directamente a un Active Directory autogestionado, el SVM reside en el mismo bosque de Active Directory (el contenedor lógico superior de una configuración de Active Directory que contiene dominios, usuarios y ordenadores) y en el mismo dominio de Active Directory que los usuarios y los recursos existentes, incluidos los servidores de archivos existentes.

Información necesaria para unir un SVM a un Active Directory

Debe proporcionar la siguiente información sobre su Active Directory al unir un SVM a un Active Directory, independientemente de la operación de API que elija:

- El nombre NetBIOS del objeto de equipo de Active Directory que se creará para la SVM. Es el nombre del SVM en Active Directory, que debe ser único en su Active Directory. No utilice el nombre NetBIOS del dominio principal. El nombre NetBIOS no puede superar los 15 caracteres.
- El fully qualified domain name (FQDN) de su Active Directory. El FQDN no puede superar los 255 caracteres.

> **Note**
>
> El FQDN no puede estar en el formato de dominio de etiqueta única (SLD). Amazon FSx no admite dominios SLD.

- Hasta tres direcciones IP de los servidores DNS o los hosts de dominio de su dominio.

  Las direcciones IP del servidor DNS y las direcciones IP del controlador de dominio de Active Directory pueden estar en cualquier rango de direcciones IP, excepto:

  - Las direcciones IP que entran en conflicto con las que son propiedad de Amazon Web Services en esa Región de AWS. Para obtener una lista de direcciones AWS IP por región, consulte los intervalos de direcciones AWS IP.
  - Direcciones IP en el siguiente rango de bloques de CIDR: 198.19.0.0/16
- Nombre de usuario y contraseña de una cuenta de servicio en su dominio de Active Directory para que Amazon FSx los utilice al unir la SVM al dominio de Active Directory. Para más información sobre los requisitos de las cuentas de servicio, consulte Requisitos de la cuenta de servicio de Active Directory.
- (Opcional) La unidad organizativa (OU) del dominio al que se une la SVM.

> **Note**
>
> Si une su SVM a un AWS Directory Service Active Directory, debe proporcionar una unidad organizativa que se encuentre dentro de la unidad organizativa predeterminada que se AWS Directory Service crea para los objetos de directorio con los que están relacionados. AWS Esto se debe a AWS Directory Service que no proporciona acceso a la `Computers` unidad organizativa predeterminada de Active Directory. Por ejemplo, si su dominio de Active Directory es`example.com`, puede especificar la siguiente OU:`OU=Computers,OU=example,DC=example,DC=com`.

- (Opcional) El grupo de dominios en el que quiere delegar la autoridad para realizar acciones administrativas en el sistema de archivos. Por ejemplo, este grupo de dominios puede administrar

los recursos compartidos de archivos SMB de Windows, tomar posesión de archivos y carpetas, etc. Si no especifica este grupo, Amazon FSx delega esta autoridad en el grupo de Administradores de dominio de su dominio del Active Directory de forma predeterminada.

Administrar las configuraciones de SVM Active Directory

En esta sección se describe cómo utilizar la AWS Management Console API fsX y la CLI de ONTAP para hacer lo siguiente: AWS CLI

- Unir un SVM existente a un Active Directory
- Modificación de una configuración de SVM de Active Directory existente
- Eliminar SVM de un Active Directory

Para eliminar un SVM de un Active Directory, debe usar la NetApp CLI de ONTAP.

Temas

- Unir un SVM a un Active Directory mediante la API y AWS Management ConsoleAWS CLI
- Actualización de una configuración de SVM de Active Directory existente mediante las AWS Management Console API, y AWS CLI
- Administración de la configuración de SVM Active Directory mediante la CLI NetApp

Unir un SVM a un Active Directory mediante la API y AWS Management ConsoleAWS CLI

Utilice el siguiente procedimiento para unir un SVM existente a un Active Directory. En este procedimiento, el SVM aún no está unido a un Active Directory.

Para unir un SVM a un Active Directory () AWS Management Console

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Elija la SVM que desee unir a un Active Directory:
   - En el panel de navegación izquierdo, elija File systems y, a continuación, elija el sistema de archivos de ONTAP con la SVM que desea actualizar.
   - Elija la pestaña Storage virtual machines.

–O bien –

- Para ver una lista de todas las SVM disponibles, en el panel de navegación izquierdo, expanda ONTAP y elija Storage virtual machines. Aparece una lista de todas las SVM de su cuenta. Región de AWS

Seleccione de la lista el SVM que desee unir a un Active Directory.

3. En la parte superior derecha del panel de Summary de la SVM, elija Actions > Join/Update Active Directory. Aparece la ventana Join SVM to an Active Directory.
4. Introduzca la siguiente información para el Active Directory al que se va a unir al SVM:

   - El nombre NetBIOS del objeto informático de Active Directory que se va a crear para la SVM. Es el nombre del SVM en Active Directory, que debe ser único en su Active Directory. No utilice el nombre NetBIOS del dominio principal. El nombre NetBIOS no puede superar los 15 caracteres.
   - El fully qualified domain name (FQDN) de su Active Directory. El nombre de dominio no puede superar los 255 caracteres.
   - DNS server IP addresses: las direcciones IPv4 de los servidores DNS de su dominio.
   - Service account username: el nombre de usuario de la cuenta de servicio de su Active Directory actual. No incluya un prefijo o sufijo de dominio. Por ejemplo, para `EXAMPLE\ADMIN`, utilice solo `ADMIN`.
   - Service account password: la contraseña de la cuenta de servicio.
   - Confirm password: la contraseña de la cuenta de servicio.
   - (Opcional) Organizational Unit (OU): el nombre de la ruta distintiva de la unidad organizativa a la que quiere unir la SVM.
   - Delegated file system administrators group: El nombre del grupo en su Active Directory que puede administrar su sistema de archivos.

     Si lo utiliza AWS Managed Microsoft AD, debe especificar un grupo como administradores AWS delegados de FSx AWS , administradores delegados o un grupo personalizado con permisos delegados para la OU.

     Si se va a unir a un Active Directory autoadministrado, utilice el nombre del grupo en su Active Directory. El grupo predeterminado es `Domain Admins`.

5. Elija Unirse a Active Directory para unir la SVM a Active Directory mediante la configuración que proporcionó.

Para unir un SVM a un Active Directory (AWS CLI)

- Para unir un SVM de FSx for ONTAP a un Active Directory, utilice el comando update-storage-virtual-machineCLI (o la operación UpdateStorageVirtualMachineAPI equivalente), como se muestra en el siguiente ejemplo.

```
aws fsx update-storage-virtual-machine \
  --storage-virtual-machine-id svm-abcdef0123456789a\
  --active-directory-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
    OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",
\
    FileSystemAdministratorsGroup="FSxAdmins",UserName="FSxService",\
    Password="password", \
    DnsIps=["10.0.1.18"]}',NetBiosName=amznfsx12345
```

Después de crear correctamente la máquina virtual de almacenamiento, Amazon FSx devuelve su descripción en formato JSON, como se muestra en el siguiente ejemplo.

```
{
  "StorageVirtualMachine": {
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
```

```
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATED",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef0123456789a",
    "StorageVirtualMachineId": "svm-abcdef0123456789a",
    "Subtype": "default",
    "Tags": [],

  }
}
```


Actualización de una configuración de SVM de Active Directory existente mediante las AWS Management Console API, y AWS CLI

Utilice el siguiente procedimiento para actualizar la configuración de Active Directory de un SVM que ya esté unido a un Active Directory.

Para actualizar una configuración de SVM de Active Directory () AWS Management Console

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Elija la SVM que desea actualizar de la siguiente manera:

   - En el panel de navegación izquierdo, elija File systems y, a continuación, elija el sistema de archivos de ONTAP con la SVM que desea actualizar.
   - Elija la pestaña Storage virtual machines.

   –O bien –

   - Para ver una lista de todas las SVM disponibles, en el panel de navegación izquierdo, expanda ONTAP y elija Storage virtual machines.

   Seleccione la SVM que desea unir a un AD de la lista.
3. En la parte superior derecha del panel de Summary de la SVM, elija Actions > Join/Update Active Directory. Aparece la ventana Update SVM Active Directory configuration.
4. Puede actualizar las siguientes propiedades de configuración de Active Directory en esta ventana.

   - DNS server IP addresses: las direcciones IPv4 de los servidores DNS de su dominio.
   - Service account username: el nombre de usuario de la cuenta de servicio de su Active Directory actual. No incluya un prefijo o sufijo de dominio. En `EXAMPLE\ADMIN`, utilice `ADMIN`.
   - Contraseña de la cuenta de servicio: la contraseña de la cuenta de servicio de Active Directory.
5. Una vez que haya introducido las actualizaciones, elija Update Active Directory para realizar los cambios.

Utilice el siguiente procedimiento para actualizar la configuración de Active Directory de un SVM que ya esté unido a un Active Directory.

Para actualizar una configuración de SVM de Active Directory () AWS CLI

- Para actualizar la configuración de Active Directory de una SVM con la AWS CLI o la API, utilice el comando update-storage-virtual-machineCLI (o la operación de UpdateStorageVirtualMachineAPI equivalente), como se muestra en el siguiente ejemplo.

```
aws fsx update-storage-virtual-machine \
    --storage-virtual-machine-id svm-abcdef0123456789a\
    --active-directory-configuration \
    SelfManagedActiveDirectoryConfiguration='{UserName="FSxService",\
    Password="password", \
    DnsIps=["10.0.1.18"]}'
```

Administración de la configuración de SVM Active Directory mediante la CLI NetApp

Puede usar la CLI de NetApp ONTAP para unir y desunir su SVM a un Active Directory y para modificar una configuración de SVM Active Directory existente.

Unir un SVM a un Active Directory mediante la CLI de ONTAP

Puede unir las SVM existentes a un Active Directory mediante la CLI de ONTAP, como se describe en el siguiente procedimiento. Puede hacerlo incluso si su SVM ya está unido a un Active Directory.

1. Para acceder a la CLI de NetApp ONTAP, ejecute el siguiente comando para establecer una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP. Reemplace *management_endpoint_ip* con la dirección IP del puerto de gestión del sistema de archivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obtener más información, consulte Administración de sistemas de archivos con la ONTAP CLI.
2. Cree una entrada de DNS para su Active Directory proporcionando el nombre DNS completo del directorio (`corp.example.com`) y al menos la dirección IP de un servidor DNS.

   ```
   ::>vserver services name-service dns create -vserver svm_name -
   domains corp.example.com -name-servers dns_ip_1, dns_ip_2
   ```

   Para comprobar la conexión a los servidores DNS, ejecute el siguiente comando. Reemplace *svm_name* con su propia información.

   ```
   FsxId0ae30e5b7f1a50b6a::>vserver services name-service dns check -vserver svm_name
   ```

```
                              Name Server
Vserver       Name Server     Status       Status Details
------------ -------------- ------------ -------------------------
svm_name      172.31.14.245   up           Response time (msec): 0
svm_name      172.31.25.207   up           Response time (msec): 1
2 entries were displayed.
```

3. Para unir la SVM a Active Directory, ejecute el siguiente comando. Tenga en cuenta que debe especificar un `computer_name` que no exista aún en su Active Directory y proporcionar el nombre DNS del directorio para `-domain`. Para `-OU`, introduzca las OU a las que desea que se una la SVM, así como el nombre completo del DNS en formato DC.

```
::>vserver cifs create -vserver svm_name -cifs-server computer_name -
domain corp.example.com -OU OU=Computers,OU=example,DC=corp,DC=example,DC=com
```

Para comprobar el estado de la conexión de Active Directory, ejecute el siguiente comando:

```
::>vserver cifs check -vserver svm_name

             Vserver : svm_name
                   Cifs NetBIOS Name : svm_netBIOS_name
                         Cifs Status : Running
                                Site : Default-First-Site-Name
Node Name       DC Server Name  DC Server IP    Status   Status Details
--------------- --------------  --------------- ------   --------------
FsxId0ae30e5b7f1a50b6a-01
                corp.example.com
                                172.31.14.245   up       Response time (msec): 5
FsxId0ae30e5b7f1a50b6a-02
                corp.example.com
                                172.31.14.245   up       Response time (msec): 20
2 entries were displayed.
```

4. Si no puede acceder a los recursos compartidos después de esta unión, determine si la cuenta que utiliza para acceder al recurso compartido tiene permisos. Por ejemplo, si utiliza la `Admin` cuenta predeterminada (un administrador delegado) con un Active Directory AWS administrado, deberá ejecutar el siguiente comando en ONTAP. El `netbios_domain` corresponde con el nombre de dominio de su Active Directory (para `corp.example.com`, el `netbios_domain` utilizado aquí es `example`).

```
FsxId0123456789a::>vserver cifs users-and-groups local-group add-members -vserver
 svm_name -group-name BUILTIN\Administrators -member-names netbios_domain\admin
```

Modificar una configuración de Active Directory mediante la CLI de ONTAP

Puede usar la CLI de ONTAP para modificar una configuración de Active Directory existente.

1. Para acceder a la CLI de NetApp ONTAP, ejecute el siguiente comando para establecer una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP. Reemplace *management_endpoint_ip* con la dirección IP del puerto de gestión del sistema de archivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obtener más información, consulte Administración de sistemas de archivos con la ONTAP CLI.
2. Ejecute el siguiente comando para desactivar temporalmente el servidor CIFS de las SVM:

   ```
   FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
   ```
3. Si necesita modificar las entradas de DNS de su Active Directory, ejecute el siguiente comando:

   ```
   ::>vserver services name-service dns modify -vserver svm_name -
   domains corp.example.com -name-servers dns_ip_1,dns_ip_2
   ```

   Puede validar el estado de la conexión con los servidores DNS de Active Directory mediante el `vserver services name-service dns check -vserver svm_name` comando.

   ```
   ::>vserver services name-service dns check -vserver svm_name
                               Name Server
   Vserver       Name Server     Status       Status Details
   ------------- --------------- ------------ --------------------------
   svmciad       dns_ip_1        up           Response time (msec): 1
   svmciad       dns_ip_2        up           Response time (msec): 1
   2 entries were displayed.
   ```
4. Si necesita modificar la configuración de Active Directory por sí misma, puede cambiar los campos existentes mediante el siguiente comando, sustituyendo:

- *computer_name*, si desea modificar el nombre de NetBIOS (cuenta de máquina) de la SVM.
- *domain_name*, si desea modificar el nombre del dominio. Debe corresponder a la entrada de dominio DNS indicada en el paso 3 de esta sección (`corp.example.com`).
- `organizational_unit`, si desea modificar la OU (`OU=Computers,OU=example,DC=corp,DC=example,DC=com`).

Deberá volver a introducir las credenciales de Active Directory que utilizó para unir este dispositivo a Active Directory.

```
::>vserver cifs modify -vserver svm_name -cifs-server computer_name -
domain domain_name -OU organizational_unit
```

Puede comprobar el estado de la conexión de Active Directory mediante el `vserver cifs check -vserver svm_name` comando.

5. Cuando termine de modificar la configuración de Active Directory y DNS, vuelva a activar el servidor CIFS ejecutando el siguiente comando:

```
::>vserver cifs modify -vserver svm_name -status-admin up
```

Separe un Active Directory de su SVM mediante la CLI de ONTAP NetApp

La CLI de NetApp ONTAP también se puede utilizar para desunir su SVM de un Active Directory siguiendo los pasos que se indican a continuación:

1. Para acceder a la CLI de NetApp ONTAP, ejecute el siguiente comando para establecer una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP. Reemplace *management_endpoint_ip* con la dirección IP del puerto de gestión del sistema de archivos.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Para obtener más información, consulte Administración de sistemas de archivos con la ONTAP CLI.

2. Elimine el servidor CIFS que desconectó su dispositivo de Active Directory ejecutando el siguiente comando. Para que ONTAP elimine la cuenta de máquina de su SVM, proporcione las credenciales que utilizó originalmente para unir la SVM a Active Directory.

```
FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
```

3. Si necesita modificar las entradas de DNS de su Active Directory, ejecute el siguiente comando:

```
FsxId0123456789a::vserver cifs delete -vserver svm_name

In order to delete an Active Directory machine account for the CIFS server, you
 must supply the name and password of a Windows account with
sufficient privileges to remove computers from the "CORP.ADEXAMPLE.COM" domain.

Enter the user name: user_name

Enter the password:

Warning: There are one or more shares associated with this CIFS server
         Do you really want to delete this CIFS server and all its shares? {y|n}: y
```

4. Elimine los servidores DNS de su Active Directory ejecutando el siguiente comando:

```
::vserver services name-service dns delete -vserver svm_name
```

Si ve una advertencia como la siguiente, que indica que `dns` debe eliminarse como tal, y no `ns-switch` tiene previsto volver a unir este dispositivo a un Active Directory, puede eliminar las entradas. `ns-switch`

```
Warning: "DNS" is present as one of the sources in one or more ns-switch databases
 but no valid DNS configuration was found for Vserver
         "svm_name". Remove "DNS" from ns-switch using the "vserver services name-
service ns-switch" command. Configuring "DNS" as a source
         in the ns-switch setting when there is no valid configuration can cause
 protocol access issues.
```

5. (Opcional) Elimine las entradas `ns-switch` del `dns` ejecutando el siguiente comando. Compruebe el orden de las fuentes y, a continuación, elimine la entrada `dns` de la base de datos de `hosts` modificando las `sources` para que solo contenga las demás fuentes de la lista. En este ejemplo, la única otra fuente es `files`.

```
::>vserver services name-service ns-switch show -vserver svm_name -database hosts

                    Vserver: svm_name
Name Service Switch Database: hosts
   Name Service Source Order: files, dns
```

```
::>vserver services name-service ns-switch modify -vserver svm_name -database hosts
 -sources files
```

6. (Opcional) Elimine la entrada `dns` modificando las `sources` para que el host de la base de datos solo incluya `files`.

```
::>vserver services name-service ns-switch modify -vserver svm_name -database hosts
 -sources files
```

Amazon FSx para NetApp el rendimiento de ONTAP

A continuación se ofrece una descripción general del rendimiento del sistema de archivos de Amazon FSx para NetApp ONTAP, con información sobre las opciones de rendimiento y rendimiento disponibles y consejos útiles sobre el rendimiento.

Temas

Cómo se mide el desempeño de FSx para sistemas de archivos ONTAP

El desempeño del sistema de archivos se mide en función de la latencia, el rendimiento y las operaciones de E/S por segundo (IOPS).

Latencia

Amazon FSx para NetApp ONTAP proporciona latencias de operación de archivos de menos de milisegundos con almacenamiento en unidades de estado sólido (SSD) y decenas de milisegundos de latencia para el almacenamiento de grupos de capacidad. Además, Amazon FSx tiene dos capas de almacenamiento en caché de lectura en cada servidor de archivos (unidades NVME (memoria express no volátil) y en memoria, para ofrecer latencias aún más bajas al acceder a los datos que lee con más frecuencia.

Rendimiento e IOPS

Cada sistema de archivos Amazon FSx proporciona hasta decenas de GB/s de rendimiento y millones de IOPS. La cantidad específica de rendimiento e IOPS que la carga de trabajo puede generar en el sistema de archivos depende de la capacidad de rendimiento total y de la configuración

de la capacidad de almacenamiento del sistema de archivos, así como de la naturaleza de la carga de trabajo, incluido el tamaño del conjunto de trabajo activo.

Soporte para SMB, multicanal y NFS nconnect

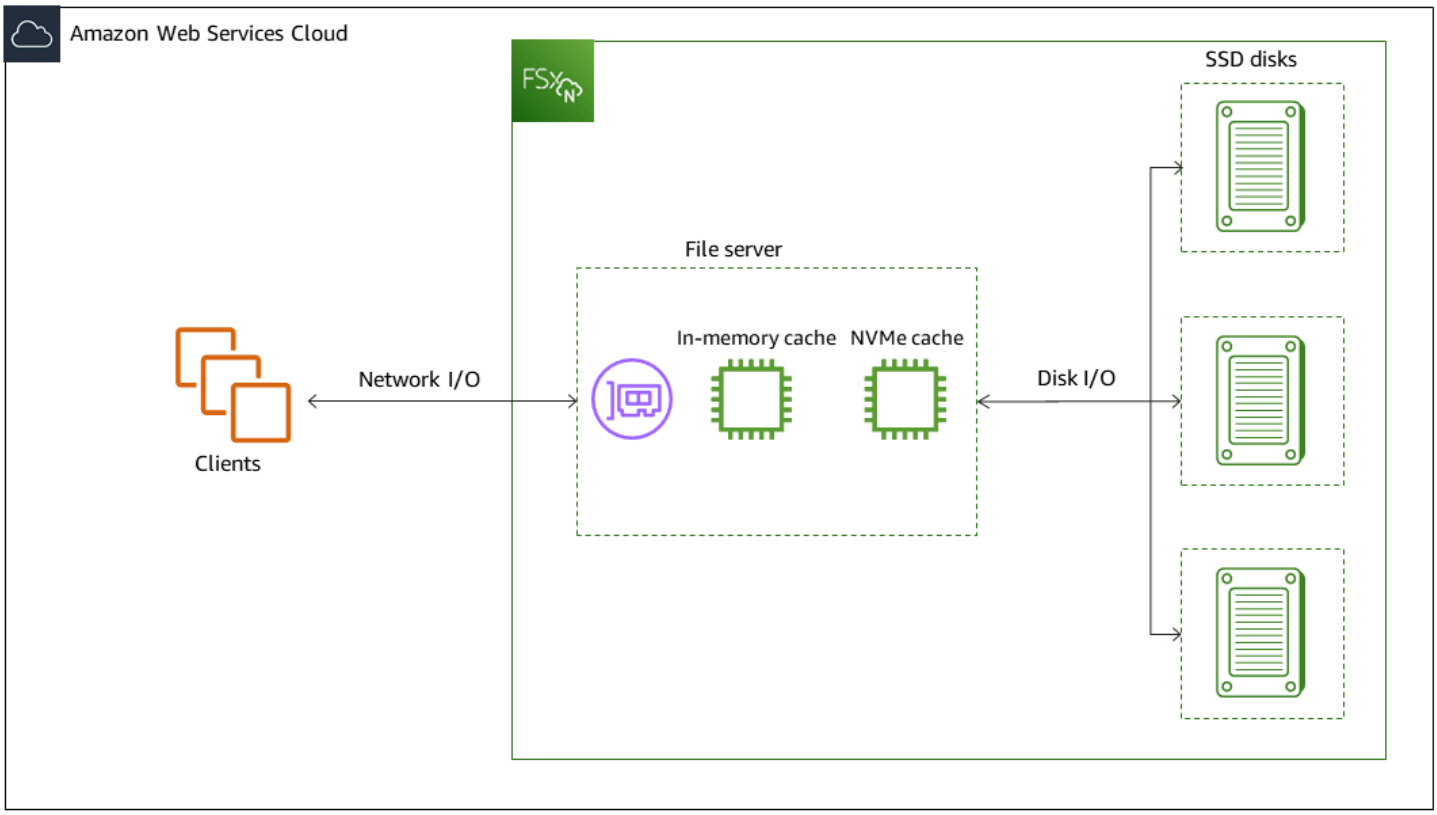
Con Amazon FSx, puede configurar SMB Multicanal para proporcionar múltiples conexiones entre ONTAP y los clientes en una sola sesión SMB. SMB Multicanal utiliza varias conexiones de red entre el cliente y el servidor de forma simultánea para agregar el ancho de banda de la red y maximizar su utilización. Para obtener información sobre el uso de la CLI de NetApp ONTAP para configurar la multicanal SMB, consulte Configuración de la multicanal SMB para mejorar el rendimiento y la redundancia.

Los clientes NFS pueden utilizar la opción de montaje `nconnect` para tener varias conexiones TCP (hasta 16) asociadas a un único montaje NFS. Un cliente NFS de este tipo multiplexa las operaciones de archivos en varias conexiones TCP de forma cíclica y, por lo tanto, obtiene un mayor rendimiento del ancho de banda de la red disponible. Compatible con NFSv3 y NFSv4.1+ `nconnect`. El ancho de banda de la red de la instancia de Amazon EC2 describe el límite de ancho de banda dúplex completo de 5 Gbps por flujo de red. Puede superar este límite mediante el uso de varios flujos de red con `nconnect` o multicanal SMB. Consulte la documentación del cliente NFS para confirmar si `nconnect` es compatible con su versión de cliente. Para obtener más información sobre la compatibilidad de ONTAP con NFSv4.1, consulte Compatibilidad de NetApp ONTAP con NFSv4.1`nconnect`.

Detalles de desempeño

Para comprender en detalle el modelo de rendimiento de Amazon FSx para NetApp ONTAP, puede examinar los componentes arquitectónicos de un sistema de archivos de Amazon FSx. Las instancias informáticas de sus clientes, ya sean internas AWS o locales, acceden a su sistema de archivos a través de una o varias interfaces de red elásticas (ENI). Estas interfaces de red residen en la Amazon VPC que asocie a su sistema de archivos. Detrás de cada sistema de archivos, el ENI hay un servidor de archivos NetApp ONTAP que envía datos a través de la red a los clientes que acceden al sistema de archivos. Amazon FSx proporciona una caché en memoria rápida y una caché NVMe en cada servidor de archivos para mejorar el rendimiento de los datos a los que se accede con más frecuencia. Los discos SSD que alojan los datos del sistema de archivos se adjuntan a cada servidor de archivos.

Estos componentes se ilustran en el siguiente diagrama.



Las principales características de rendimiento de un sistema de archivos Amazon FSx for NetApp ONTAP que determinan el rendimiento general y el rendimiento de las IOPS se corresponden con estos componentes arquitectónicos (interfaz de red, caché en memoria, caché NVMe y volúmenes de almacenamiento).

- Desempeño de E/S de la red: rendimiento/IOPS de las solicitudes entre los clientes y el servidor de archivos (en conjunto)
- Tamaño de la caché en memoria y NVMe en el servidor de archivos: tamaño del conjunto de trabajo activo que se puede almacenar en caché
- Desempeño de E/S del disco: rendimiento/IOPS de las solicitudes entre el servidor de archivos y los discos de almacenamiento

Hay dos factores que determinan estas características de rendimiento de su sistema de archivos: la cantidad total de IOPS del SSD y la capacidad de rendimiento que se configure para él. Las dos primeras características de rendimiento (el rendimiento de E/S de la red y el tamaño de la caché en memoria y NVMe) se determinan únicamente por la capacidad de rendimiento, mientras que la tercera (el rendimiento de E/S del disco) se determina mediante una combinación de la capacidad de rendimiento y las IOPS de los SSD.

Las cargas de trabajo basadas en archivos suelen tener picos de actividad y se caracterizan por períodos cortos e intensos de E/S elevadas y mucho tiempo de inactividad entre ráfagas. Para soportar cargas de trabajo con picos de actividad, además de las velocidades básicas que un sistema de archivos puede soportar las 24 horas del día, los 7 días de la semana, Amazon FSx ofrece la capacidad de alcanzar velocidades más altas durante períodos de tiempo tanto para las operaciones de E/S de red como de E/S de disco. Amazon FSx utiliza un mecanismo de créditos de E/S de red para asignar el rendimiento y las IOPS en función de la utilización media: los sistemas de archivos acumulan créditos cuando su rendimiento y su uso de IOPS están por debajo de sus límites de referencia, y pueden utilizar estos créditos cuando realizan operaciones de E/S.

Las operaciones de escritura utilizan el doble de ancho de banda de la red que las operaciones de lectura. Una operación de escritura debe replicarse en el servidor de archivos secundario, de modo que una sola operación de escritura supone el doble de rendimiento de la red.

Impacto del tipo de implementación en el rendimiento

Puede crear dos tipos de sistemas de archivos con FSx para ONTAP. Los sistemas de archivos con un único par de servidores de archivos de alta disponibilidad (HA) se denominan sistemas de archivos escalables. Los sistemas de archivos con varios pares de alta disponibilidad se denominan sistemas de archivos escalables. Para obtener más información, consulte Pares de alta disponibilidad (HA).

Los sistemas de archivos de FSx para ONTAP Multi-AZ y Single-AZ proporcionan latencias de operación de archivos consistentes de menos de un milisegundo con almacenamiento SSD y decenas de milisegundos de latencia con almacenamiento en pool de capacidad. Además, los sistemas de archivos que cumplen los siguientes requisitos proporcionan una caché de lectura NVMe para reducir las latencias de lectura y aumentar las IOPS para los datos que se leen con frecuencia:

- Sistemas de archivos Multi-AZ
- Sistemas de archivos escalables en zonas de disponibilidad única creados después del 28 de noviembre de 2022 con una capacidad de rendimiento de al menos 2 GBps

Las siguientes tablas muestran la cantidad de capacidad de rendimiento que los sistemas de archivos pueden ampliar en función de factores como la cantidad de pares de alta disponibilidad (HA) y la disponibilidad. Regiones de AWS

Scale-up

Estas especificaciones de rendimiento se aplican a los sistemas de archivos escalables.

Rendimiento máximo del almacenamiento SSD por par de HA para sistemas de archivos con capacidad de ampliación

	Región Este de EE. UU. (Ohio), Región Este de EE. UU. (Norte de Virginia), Región Oeste de EE. UU. (Oregón) y Europa (Irlanda).		Todos los demás Regiones de AWS lugares en los que FSx para ONTAP esté disponible	
	Rendimiento de lectura (MBps)	Rendimiento de escritura (MBps)	Rendimiento de lectura (MBps)	Rendimiento de escritura (MBps)
Single-AZ	4,096*	1,000	2,048	750
Multi-AZ	4,096*	1,800	2,048	1,300

> **Note**
>
> * Para aprovisionar una capacidad de rendimiento de 4 GBps, el sistema de archivos debe estar configurado con una capacidad mínima de almacenamiento SSD de 5.120 GiB y 160.000 IOPS de SSD.

Scale-out

Estas especificaciones de rendimiento se aplican a los sistemas de archivos escalables.

Rendimiento máximo del almacenamiento SSD por par de HA para sistemas de archivos con capacidad de ampliación

	Rendimiento de lectura (MBps)	Rendimiento de escritura (MBps)

Capacidad de ampliación en una sola zona de disponibilidad	6,144*	1,100*

> **Note**
>
> * Por par de HA (hasta 12). Para obtener más información, consulte Pares de alta disponibilidad (HA).

Impacto de la capacidad de almacenamiento en el rendimiento

El rendimiento máximo del disco y los niveles de IOPS que puede alcanzar su sistema de archivos son el menor de los siguientes:

- el nivel de rendimiento del disco que proporcionan sus servidores de archivos, en función de la capacidad de rendimiento que seleccione para su sistema de archivos
- el nivel de rendimiento del disco proporcionado por la cantidad de IOPS de SSD que aprovisiona para su sistema de archivos

De forma predeterminada, el almacenamiento SSD del sistema de archivos proporciona hasta los siguientes niveles de rendimiento de disco e IOPS:

- Rendimiento del disco (MBps por TiB de almacenamiento): 768
- IOPS de disco (IOPS por TiB de almacenamiento): 3072

Impacto de la capacidad de rendimiento en el rendimiento

Cada sistema de archivos de Amazon FSx tiene una capacidad de rendimiento que se configura cuando se crea el sistema de archivos. La capacidad de rendimiento del sistema de archivos determina el nivel de rendimiento de E/S de la red o la velocidad a la que cada uno de los servidores de archivos que alojan el sistema de archivos puede entregar los datos de archivos a través de la red a los clientes que acceden a ellos. Los niveles más altos de capacidad de rendimiento vienen acompañados de más memoria y almacenamiento exprés de memoria no volátil (NVMe) para

almacenar los datos en caché en cada servidor de archivos, y cada servidor de archivos admite niveles más altos de rendimiento de E/S de disco.

Si lo desea, puede aprovisionar un nivel superior de IOPS de SSD al crear su sistema de archivos. El nivel máximo de IOPS de SSD que puede alcanzar su sistema de archivos también depende de la capacidad de rendimiento del sistema de archivos, incluso al aprovisionar IOPS de SSD adicionales.

En las tablas siguientes se muestra el conjunto completo de especificaciones de la capacidad de rendimiento, junto con los niveles de referencia y de ráfaga, y la cantidad de memoria para almacenar en caché en el servidor de archivos, en las Regiones de AWS correspondientes.

Single-AZ (scale-up)

Estas especificaciones de rendimiento se aplican a los sistemas de archivos escalables Single-AZ creados después del 28 de noviembre de 2022, según se especifique. Regiones de AWS

Las especificaciones de rendimiento de los sistemas de archivos son las siguientes Regiones de AWS: EE.UU. Este (Norte de Virginia), EE.UU. Este (Ohio), EE.UU. Oeste (Oregón) y Europa (Irlanda)

Capacidad de rendimiento de FSx (MBps)	Capacidad de rendimiento de la red (MBps)		IOPS de red	Almacenamiento en caché en memoria (GB)	Almacenamiento en caché de lectura de NVMe (GB)	Rendimiento de disco (MBps)		IOPS de la unidad SSD *	
	Referencia	Ráfaga				Referencia	Ráfaga	Referencia	Ráfaga
128	188	1,500	Decenas de miles de referencia	16	–	128	1,250	6,000	40 000
256	375	1,500		32	–	256	1,250	12,000	40 000

Capacidad de rendimiento de FSx (MBps)	Capacidad de rendimiento de la red (MBps)		IOPS de red	Almacenamiento en caché en memoria (GB)	Almacenamiento en caché de lectura de NVMe (GB)	Rendimiento de disco (MBps)		IOPS de la unidad SSD *	
512	750	1,500	Cientos de miles de referencia	64	–	512	1,250	20,000	40,000
1 024	1,500	–		128	–	1,024	1,250	40,000	–
2048	3,125	–		256	1,900	2,048	–	80,000	–
4.096	6,250	–		512	5,400	4,096	–	160,000	–

> **Note**
>
> * Las IOPS de su SSD solo se utilizan cuando accede a datos que no están en caché en el caché en memoria del servidor de archivos o en la caché NVMe.

Estas especificaciones de rendimiento se aplican a los sistemas de archivos escalables Single-AZ en todos los demás lugares en los que Regiones de AWS fSx for ONTAP esté disponible.

Especificaciones de rendimiento para sistemas de archivos en [todos los demás sistemas en los Regiones de AWS que FSx para ONTAP](#) esté disponible

Capacidad de rendimiento de FSx (MBps)	Capacidad de rendimiento de la red (MBps)		IOPS de red	Almacenamiento en caché en memoria (GB)	Rendimiento de disco (MBps)		IOPS de la unidad SSD *	
	Referencia	Ráfaga			Referencia	Ráfaga	Referencia	Ráfaga
128	150	1,250	Decenas de miles de referencia	16	128	600	6,000	18 750
256	300	1,250		32	256	600	12,000	18 750
512	625	1,250	Cientos de miles de referencia	64	512	600	18,750	–
1 024	1,500	–		128	1,024	–	40,000	–
2048	3,125	–		256	2,048	–	80,000	–

> **Note**
>
> * Las IOPS de su SSD solo se utilizan cuando accede a datos que no están en caché en el caché en memoria del servidor de archivos o en la caché NVMe.

Single-AZ (scale-out)

Estas especificaciones de rendimiento se aplican a los sistemas de archivos escalables.

Especificaciones de rendimiento para sistemas de archivos escalables

Capacidad de rendimiento de FSx (MBps)	Capacidad de rendimiento de la red (MBps)		IOPS de red	Almacenamiento en caché en memoria (GB)	Rendimiento de disco (MBps)		IOPS de la unidad SSD *	
	Referencia	Ráfaga			Referencia	Ráfaga	Referencia	Ráfaga
3.072**	6,250	–	Cientos de miles de referencia	128	3,072	–	100,000	–
6.144**	12,500	–		256	6,144	–	200,000	–

> **Note**
>
> * Las IOPS de su SSD solo se utilizan cuando accede a datos que no están en caché en el caché en memoria del servidor de archivos o en la caché NVMe.
> ** Por par HA (hasta 12). Para obtener más información, consulte Pares de alta disponibilidad (HA).

Multi-AZ (scale-up)

Estas especificaciones de rendimiento se aplican a los sistemas de archivos ampliables Multi-AZ creados después del 28 de noviembre de 2022, según lo especificado. Regiones de AWS

Las especificaciones de rendimiento de los sistemas de archivos son las siguientes Regiones de AWS: EE.UU. Este (Norte de Virginia), EE.UU. Este (Ohio), EE.UU. Oeste (Oregón) y Europa (Irlanda)

Capacidad de rendimiento de FSx (MBps)	Capacidad de rendimiento de la red (MBps)		IOPS de red	Almacenamiento en caché en memoria (GB)	Almacenamiento en caché NVMe (GB)	Rendimiento de disco (MBps)		IOPS de la unidad SSD *	
	Referencia	Ráfaga				Referencia	Ráfaga	Referencia	Ráfaga
128	188	1,500	Decenas de miles de referencia	16	238	128	1,250	6,000	40 000
256	375	1,500		32	475	256	1,250	12,000	40 000
512	750	1,500	Cientos de miles de referencia	64	950	512	1,250	20,000	40,000
1 024	1,500	–		128	1,900	1,024	1250	40,000	–
2048	3,125	–		256	3,800	2,048	–	80,000	–
4.096	6,250	–		512	7,600	4,096	–	160,000	–

> **Note**
>
> * Las IOPS de su SSD solo se utilizan cuando accede a datos que no están en caché en el caché en memoria del servidor de archivos o en la caché NVMe.

Estas especificaciones de rendimiento se aplican a los sistemas de archivos escalables Multi-AZ en todos los demás lugares en los que Regiones de AWS FSx for ONTAP esté disponible.

Especificaciones de rendimiento para sistemas de archivos en [todos los demás sistemas en los Regiones de AWS que FSx para ONTAP](#) esté disponible

Capacidad de rendimiento de FSx (MBps)	Capacidad de rendimiento de la red (MBps)		IOPS de red	Almacenamiento en caché en memoria (GB)	Almacenamiento en caché NVMe (GB)	Rendimiento de disco (MBps)		IOPS de la unidad SSD *	
	Referencia	Ráfaga				Referencia	Ráfaga	Referencia	Ráfaga
128	150	1,250	Decenas de miles de referencia	16	150	128	600	6,000	18 750
256	300	1,250		32	300	256	600	12,000	18 750
512	625	1,250	Cientos de miles de referencia	64	600	512	600	18,750	–
1 024	1,500	–		128	1,200	1,024	–	40,000	–
2048	3,125	–		256	2,400	2,048	–	80,000	–

> **Note**
>
> * Las IOPS de su SSD solo se utilizan cuando accede a datos que no están en caché en el caché en memoria del servidor de archivos o en la caché NVMe.

Ejemplo: capacidad de almacenamiento y capacidad de rendimiento

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

Un sistema de archivos escalable que está configurado con 2 TiB de capacidad de almacenamiento SSD y 512 MBps de capacidad de rendimiento tiene los siguientes niveles de rendimiento:

- Rendimiento de red: 625 MBps de referencia y 1250 MBps de ráfaga (consulte la tabla de capacidad de rendimiento)
- Rendimiento de disco: 512 MBps de referencia y 600 MBps de ráfaga.

Por lo tanto, su carga de trabajo al acceder al sistema de archivos podrá generar un rendimiento de hasta 625 MBps de referencia y un rendimiento de ráfaga de 1250 MBps para las operaciones de archivos realizadas con datos a los que se accede activamente almacenados en caché en la caché en memoria del servidor de archivos y en la caché NVMe.

Administración de recursos FSx para ONTAP

Mediante la AWS Management Console CLI y la API de ONTAP, puede realizar las siguientes acciones administrativas para los recursos de FSx for ONTAP: AWS CLI

- Crear, enumerar, actualizar y eliminar sistemas de archivos, máquinas virtuales de almacenamiento (SVM), volúmenes, copias de seguridad y etiquetas.
- Administración del acceso, cuentas y contraseñas administrativas, requisitos de contraseñas, protocolos SMB e iSCSI, accesibilidad de la red para los destinos de montaje de los sistemas de archivos existentes

Temas

Gestión de FSx para sistemas de archivos ONTAP

Un sistema de archivos es el recurso principal de Amazon FSx, de forma análoga a un clúster ONTAP en las instalaciones. Debe especificar la capacidad de rendimiento y almacenamiento de la

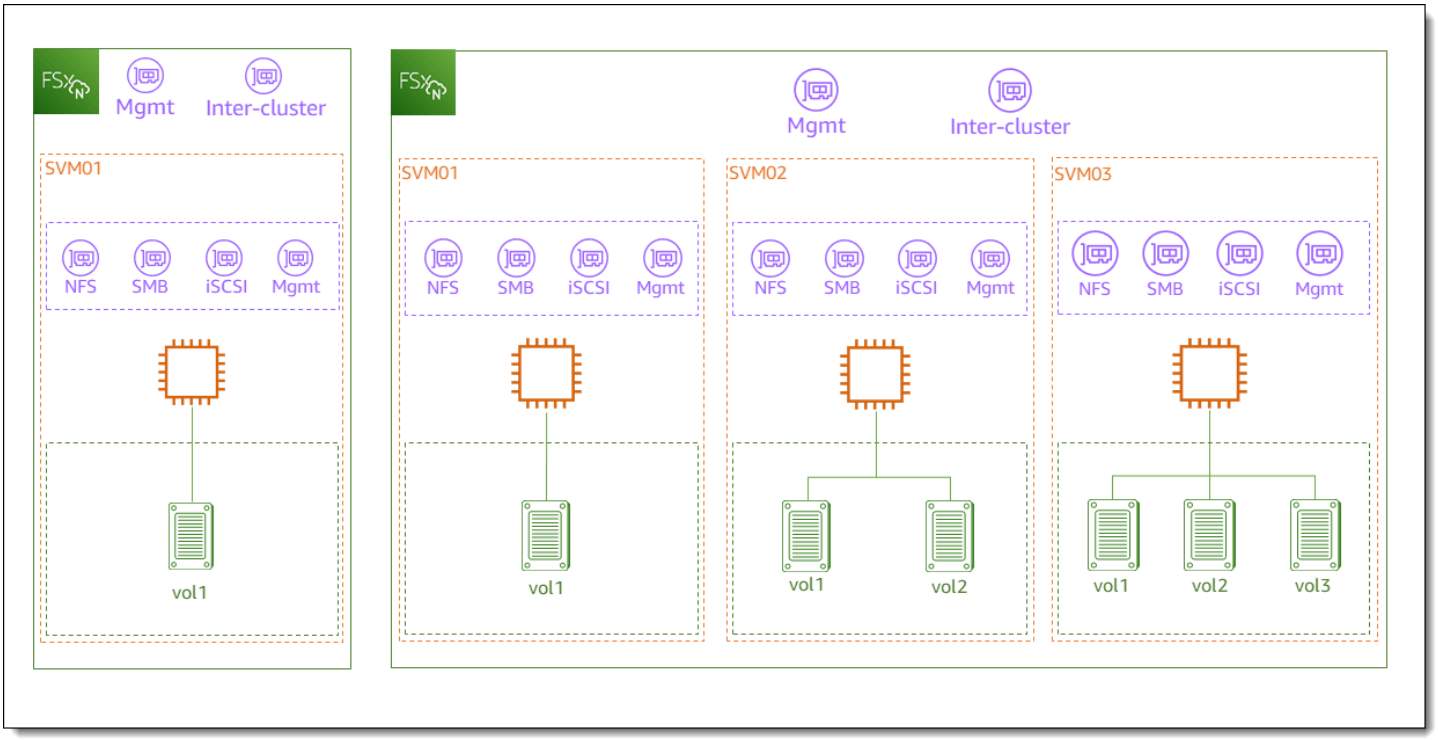
unidad de estado sólido (SSD) del sistema de archivos y elegir una nube privada virtual (VPC) en la que crear el sistema de archivos. Cada sistema de archivos tiene un punto final de administración que puede usar para administrar los recursos y los datos con la CLI de ONTAP o la API REST.

Recursos del sistema de archivos

Un sistema de archivos Amazon FSx para NetApp ONTAP se compone de los siguientes recursos principales:

- El hardware físico del propio sistema de archivos, que incluye los servidores de archivos y los medios de almacenamiento.
- Uno o más pares de servidores de archivos de alta disponibilidad (HA), que alojan sus máquinas virtuales de almacenamiento (SVM). Los sistemas de archivos escalables tienen un par de alta disponibilidad y los sistemas de archivos escalables tienen dos o más pares de alta disponibilidad. Cada par de alta disponibilidad tiene un grupo de almacenamiento denominado agregado. El conjunto de agregados de todos los pares de alta disponibilidad constituye el nivel de almacenamiento SSD.
- Una o más máquinas virtuales de almacenamiento (SVM) que aloja los volúmenes del sistema de archivos y con sus propias credenciales y gestión de acceso.
- Uno o más volúmenes que organizan virtualmente sus datos y que son montados por sus clientes.

La siguiente imagen ilustra la arquitectura de un FSx escalable para un sistema de archivos ONTAP con un par de alta disponibilidad y la relación entre sus recursos principales. El sistema de archivos de FSx para ONTAP de la izquierda es el sistema de archivos más simple, con una SVM y un volumen. El sistema de archivos de la derecha tiene varias SVM, y algunas SVM tienen varios volúmenes. Cada uno de los sistemas de archivos y las SVM tiene varios puntos finales de administración, y las SVM también tienen puntos finales de acceso a los datos.



Al crear un FSx para el sistema de archivos ONTAP, debe definir las siguientes propiedades:

- Tipo de implementación: el tipo de implementación del sistema de archivos (Multi-AZ o Single-AZ). Los sistemas de archivos Single-AZ replican sus datos y ofrecen una conmutación por error automática dentro de una única zona de disponibilidad, además de ofrecer sistemas de archivos escalables. Los sistemas de archivos Multi-AZ proporcionan una mayor resiliencia, ya que también replican los datos y admiten la conmutación por error en varias zonas de disponibilidad dentro de la misma Región de AWS.
- Capacidad de almacenamiento: es la cantidad de almacenamiento en SSD, hasta 192 tebibytes (TiB) para sistemas de archivos escalables y 1 pebibyte (PiB) para sistemas de archivos escalables.
- IOPS de SSD: de forma predeterminada, cada gigabyte de almacenamiento SSD incluye tres IOPS de SSD (hasta el máximo que admite la configuración del sistema de archivos). Si lo desea, puede aprovisionar IOPS SSD adicionales según sea necesario.
- Capacidad de rendimiento: velocidad constante a la que el servidor de archivos puede almacenar datos.
- Redes: la VPC y las subredes de los puntos de conexión de gestión y acceso a los datos que crea el sistema de archivos. Para un sistema de archivos Multi-AZ, también debe definir un rango de direcciones IP y tablas de enrutamiento.

- Cifrado: la clave AWS Key Management Service (AWS KMS) que se utiliza para cifrar los datos del sistema de archivos en reposo.
- Acceso administrativo: puede especificar la contraseña del usuario `fsxadmin`. Puede usar este usuario para administrar el sistema de archivos mediante la CLI de NetApp ONTAP y la API REST.

Puede gestionar FSx para los sistemas de archivos ONTAP mediante la NetApp CLI de ONTAP o la API REST. También puede configurar SnapMirror o establecer SnapVault relaciones entre un sistema de archivos Amazon FSx y otro despliegue de ONTAP (incluido otro sistema de archivos Amazon FSx). Cada sistema de archivos FSx for ONTAP tiene los siguientes puntos finales del sistema de archivos que proporcionan acceso a las aplicaciones: NetApp

- Administración: utilice este punto final para acceder a la CLI de NetApp ONTAP a través de Secure Shell (SSH) o para utilizar la API REST de NetApp ONTAP con su sistema de archivos.
- Interclúster: utilice este punto final al configurar la replicación mediante o el almacenamiento en caché mediante NetApp SnapMirror . NetApp FlexCache

Para obtener más información, consulte Gestión de los recursos de FSx para ONTAP mediante aplicaciones NetApp y Replicación programada mediante NetApp SnapMirror.

Pares de alta disponibilidad (HA)

Cada sistema de archivos FSx for ONTAP funciona con uno o varios pares de servidores de archivos de alta disponibilidad (HA) en una configuración activo-en espera. En esta configuración, hay un servidor de archivos preferido que atiende el tráfico de forma activa y un servidor de archivos secundario que asume el control si el servidor activo no está disponible. Los sistemas de archivos escalables FSx para ONTAP funcionan con un par HA, que ofrece una capacidad de rendimiento de hasta 4 GBps y 160 000 IOPS de SSD. Los sistemas de archivos escalables FSx para ONTAP funcionan con hasta 12 pares de alta disponibilidad, que pueden ofrecer hasta 72 GBps de capacidad de rendimiento y 2 400 000 IOPS de SSD (6 GBps de capacidad de rendimiento y 200 000 IOPS de SSD por par de HA).

Al crear el sistema de archivos desde la consola de Amazon FSx, Amazon FSx recomienda el número de pares de alta disponibilidad que debe utilizar en función del almacenamiento SSD que desee. También puede elegir manualmente el número de pares de alta disponibilidad en función de sus requisitos de carga de trabajo y rendimiento. Le recomendamos que utilice un solo par de alta disponibilidad si se cumplen los requisitos de su sistema de archivos, con una capacidad de

rendimiento de hasta 4 GBps y 160 000 IOPS de SSD, y varios pares de alta disponibilidad si sus cargas de trabajo necesitan niveles más altos de escalabilidad del rendimiento.

Cada par de alta disponibilidad tiene un agregado, que es un conjunto lógico de discos físicos.

> **Note**
>
> No puede añadir pares de alta disponibilidad a los sistemas de archivos existentes. En su lugar, puede migrar datos entre sistemas de archivos (con diferentes pares de alta disponibilidad) utilizando SnapMirror o restaurando los datos de una copia de seguridad a un nuevo sistema de archivos. AWS DataSync

Creación de FSx para sistemas de archivos ONTAP

En esta sección se describe cómo crear un sistema de archivos FSx para ONTAP mediante la consola Amazon FSx o AWS CLI la API de Amazon FSx. Puede crear un sistema de archivos en una nube privada virtual (VPC) de su propiedad o en una VPC que otra persona Cuenta de AWS haya compartido con usted. Hay que tener en cuenta al crear un sistema de archivos Multi-AZ en una VPC en la que participe. Estas consideraciones se explican en este tema.

De forma predeterminada, cuando crea un nuevo sistema de archivos desde la consola de Amazon FSx, Amazon FSx crea automáticamente un sistema de archivos con una sola máquina virtual de almacenamiento (SVM) y un volumen, lo que permite acceder rápidamente a los datos de las instancias de Linux a través del protocolo Network File System (NFS). Al crear el sistema de archivos, puede unir opcionalmente la SVM a un Active Directory para permitir el acceso desde los clientes de Windows y macOS a través del protocolo del bloque de mensajes del servidor (SMB). Una vez creado el sistema de archivos, puede crear SVM y volúmenes adicionales según sea necesario.

Para crear un sistema de archivos (consola)

Este procedimiento utiliza la opción de creación estándar para crear un sistema de archivos de FSx para ONTAP con una configuración que se personalice según sus necesidades. Para obtener información sobre el uso de la opción de creación rápida para crear rápidamente un sistema de archivos con un conjunto predeterminado de parámetros de configuración, consulte Paso 1: Crear un sistema de archivos Amazon FSx para NetApp ONTAP.

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

2. En el panel de control, elija Crear sistema de archivos.
3. En la página Seleccione el tipo de sistema de archivos, en Opciones del sistema de archivos, elija Amazon FSx para NetApp ONTAP y, a continuación, elija Siguiente.
4. En la sección Método de creación, elija Creación estándar.
5. En la sección Detalles del sistema de archivos, proporciona la siguiente información:

   - En File system name - optional, introduzca un nombre para su sistema de archivos. Es más fácil encontrar y gestionar sus sistemas de archivos cuando les asigna un nombre. Puede utilizar un máximo de 256 letras Unicode, espacios en blanco y números, además de los siguientes caracteres especiales: + - = . _ : /
   - En Deployment type, elija Multi-AZ o Single-AZ.
     - Los sistemas de archivos Multi-AZ replican sus datos y admiten la conmutación por error en varias zonas de disponibilidad de la misma Región de AWS.
     - Los sistemas de archivos Single-AZ replican sus datos y ofrecen una conmutación por error automática dentro de una única zona de disponibilidad.

     > **Note**
     >
     > Elija Single-AZ si desea tener la opción de crear un sistema de archivos con dos o más pares de alta disponibilidad (HA) (hasta 12). Para obtener más información, consulte Pares de alta disponibilidad (HA).

     Para obtener más información, consulte Disponibilidad y durabilidad.
   - En SSD storage capacity, introduzca la capacidad de almacenamiento del sistema de archivos, en gibibytes (GiB). Introduzca cualquier número entero en el rango de 1 024 a 1 048.576 GiB (hasta 1 pebibyte [PiB]).

     Puede aumentar la capacidad de almacenamiento según sea necesario en cualquier momento después de crear el sistema de archivos. Para obtener más información, consulte Administración de la capacidad de almacenamiento.
   - En Provisioned SSD IOPS, tiene dos opciones para aprovisionar la cantidad de IOPS para su sistema de archivos:
     - Elija Automatic (opción predeterminada) si desea que Amazon FSx aprovisione automáticamente 3 IOPS por GiB de almacenamiento SSD.

- Elija User-provisioned si desea especificar la cantidad de IOPS. Puede aprovisionar un máximo de 200 000 IOPS de SSD por sistema de archivos.

> **Note**
>
> Puede aumentar las IOPS SSD aprovisionadas después de crear el sistema de archivos. Tenga en cuenta que el nivel máximo de IOPS SSD que puede alcanzar su sistema de archivos también depende de la capacidad de rendimiento del sistema de archivos, incluso al aprovisionar IOPS SSD adicionales. Para obtener más información, consulte Impacto de la capacidad de rendimiento en el rendimiento y Administración de la capacidad de almacenamiento.

- En cuanto a la capacidad de rendimiento, tiene dos opciones para determinar su capacidad de rendimiento en megabytes por segundo (MBps):
  - Elija Capacidad de rendimiento recomendada si desea que Amazon FSx elija automáticamente la capacidad de rendimiento en función de la cantidad de capacidad de almacenamiento que haya elegido.
  - Elija Especificar la capacidad de rendimiento si desea especificar la cantidad de capacidad de rendimiento. Si elige esta opción, aparecerá un menú desplegable de capacidad de rendimiento que se rellenará en función del tipo de despliegue que haya elegido. También puede elegir el número de pares de alta disponibilidad (hasta 12). Para obtener más información, consulte Pares de alta disponibilidad (HA).

  Capacidad de rendimiento: velocidad constante a la que el servidor de archivos que aloja a su sistema de archivos puede servir datos. Para obtener más información, consulte Amazon FSx para NetApp el rendimiento de ONTAP.

6. En la sección Redes, proporcione la siguiente información:

- Para la nube privada virtual (VPC), elija la VPC que desea asociar con su sistema de archivos.
- En el caso de los grupos de seguridad de VPC, puede elegir un grupo de seguridad para asociarlo a la interfaz de red del sistema de archivos. Si no especifica ninguno, Amazon FSx asociará el grupo de seguridad predeterminado de la VPC a su sistema de archivos.
- Especifique una Subnet para su servidor de archivos. Si va a crear un sistema de archivos Multi-AZ, elija también una Standby subnet para el servidor de archivos en espera.
- (Solo Multi-AZ) Para VPC route tables, especifique las tablas de enrutamiento VPC para crear los puntos de conexión de su sistema de archivos. Seleccione todas las tablas de

enrutamiento de la VPC asociadas a las subredes en las que se encuentran sus clientes. De forma predeterminada, Amazon FSx selecciona la tabla de enrutamiento predeterminada de la VPC. Para obtener más información, consulte Acceso a los datos desde fuera de la VPC de implementación.

> **Note**
>
> Amazon FSx administra estas tablas de enrutamiento para sistemas de archivos Multi-AZ mediante la autenticación basada en etiquetas. Estas tablas de rutas están etiquetadas con. `Key: AmazonFSx; Value: ManagedByAmazonFSx` Al crear FSx para sistemas de archivos Multi-AZ de ONTAP con ellos, le AWS CloudFormation recomendamos que añada la etiqueta manualmente. `Key: AmazonFSx; Value: ManagedByAmazonFSx`

- (Solo Multi-AZ) punto de conexión IP address range especifica el rango de direcciones IP en el que se crearán los puntos de conexión para acceder al sistema de archivos.

  Tiene tres opciones para el rango de direcciones IP del punto de conexión:

  - Unallocated IP address range from your VPC: Amazon FSx elige las últimas 64 direcciones IP del rango de CIDR principal de la VPC para usarlas como rango de direcciones IP de punto de conexión del sistema de archivos. Este rango se comparte entre varios sistemas de archivos si elige esta opción varias veces.

    > **Note**
    >
    > Esta opción aparece atenuada si una subred utiliza alguna de las últimas 64 direcciones IP del rango CIDR principal de una VPC. En este caso, aún puede elegir un rango de direcciones en la VPC (es decir, un rango que no esté al final del rango CIDR principal o un rango que esté en un CIDR secundario de su VPC) al elegir la opción Enter an IP address range.

  - En Subred preferida, especifique una subred para su servidor de archivos. Si va a crear un sistema de archivos Multi-AZ, elija también una Standby subnet para el servidor de archivos en espera.
  - (Solo Multi-AZ) Para VPC route tables, especifique las tablas de enrutamiento VPC para crear los puntos de conexión de su sistema de archivos. Seleccione todas las tablas de enrutamiento de la VPC asociadas a las subredes en las que se encuentran sus clientes. De

forma predeterminada, Amazon FSx selecciona la tabla de enrutamiento predeterminada de la VPC.

- (Solo Multi-AZ) punto de conexión IP address range especifica el rango de direcciones IP en el que se crearán los puntos de conexión para acceder al sistema de archivos.

  Tiene tres opciones para el rango de direcciones IP del punto de conexión:

  - Unallocated IP address range from your VPC: Amazon FSx elige las últimas 64 direcciones IP del rango de CIDR principal de la VPC para usarlas como rango de direcciones IP de punto de conexión del sistema de archivos. Este rango se comparte entre varios sistemas de archivos si elige esta opción varias veces.

    > **Note**
    >
    > Esta opción aparece atenuada si una subred utiliza alguna de las últimas 64 direcciones IP del rango CIDR principal de una VPC. En este caso, aún puede elegir un rango de direcciones en la VPC (es decir, un rango que no esté al final del rango CIDR principal o un rango que esté en un CIDR secundario de su VPC) al elegir la opción Enter an IP address range.

  - Floating IP address range outside your VPC: Amazon FSx elige un rango de direcciones 198.19.x.0/24 que no esté ya utilizado por ningún otro sistema de archivos con la misma VPC y tablas de enrutamiento.
  - Enter an IP address range: Puede proporcionar un rango de CIDR de su elección. El rango de direcciones IP que elija puede estar dentro o fuera del rango de direcciones IP de la VPC, siempre que no se superponga con ninguna subred.

    > **Note**
    >
    > No elija ningún rango que se encuentre dentro de los siguientes rangos de CIDR, ya que son incompatibles con FSx para ONTAP:
    >
    > - 0.0.0.0/8
    > - 127,0,0,0/8
    > - 198,190,0/20
    > - 224,0.0.0/4
    > - 240.0.0.0/4

- 255,255,255,255/32

7. En la sección Security & encryption, en Encryption key, elija la clave de cifrado AWS Key Management Service (AWS KMS) que proteja los datos en reposo del sistema de archivos.
8. En File system administrative password, introduzca una contraseña segura para el usuario `fsxadmin`. Confirme la contraseña.

   Puede usar el usuario `fsxadmin` para administrar su sistema de archivos mediante la CLI y la API de REST de ONTAP. Para más información sobre el usuario `fsxadmin`, consulte Administración de sistemas de archivos con la ONTAP CLI.
9. En la sección Default storage virtual machine configuration, proporcione la siguiente información:

   - En el campo Storage virtual machine name, proporcione un nombre para la máquina virtual de almacenamiento. Puede utilizar un máximo de 47 caracteres alfanuméricos, además del carácter especial de guion bajo (_).
   - En SVM administrative password, si lo desea, puede elegir Specify a password y proporcionar una contraseña para el usuario `vsadmin` de la SVM. Puede usar el usuario `vsadmin` para administrar la SVM mediante la CLI y la API de REST de ONTAP. Para más información sobre el usuario `vsadmin`, consulte Administración de SVM con la CLI ONTAP.

     Si elige Don't specify a password (opción predeterminada), podrá seguir utilizando el usuario `fsxadmin` del sistema de archivos para gestionar el sistema de archivos mediante la CLI o la API de REST de ONTAP, pero no podrá utilizar el usuario `vsadmin` de su SVM para hacer lo mismo.
   - En la sección Active Directory, puede unir un Active Directory a la SVM. Para obtener más información, consulte Uso de Microsoft Active Directory en FSx para ONTAP.

     Si no desea unir su SVM a un Active Directory, elija Do not join an Active Directory.

     Si desea unir su SVM a un dominio de Active Directory autogestionado, elija Join an Active Directory y proporcione los siguientes detalles para su Active Directory:
     - El nombre NetBIOS del objeto de equipo de Active Directory que se creará para la SVM. El nombre NetBIOS no puede superar los 15 caracteres.
     - El nombre de dominio completo del dominio de Active Directory. El nombre de dominio no puede superar los 255 caracteres.
     - DNS server IP addresses: las direcciones IPv4 de los servidores del sistema de nombres de dominio (DNS) de su dominio.

- Service account username: el nombre de usuario de la cuenta de servicio de su Active Directory actual. No incluya un prefijo o sufijo de dominio.
- Service account password: la contraseña de la cuenta de servicio.
- Confirmar contraseña: la contraseña de la cuenta de servicio.
- (Opcional) Organizational Unit (OU): el nombre de la ruta distintiva de la unidad organizativa a la que quiere unir la SVM.
- Delegated file system administrators group: El nombre del grupo en su Active Directory que puede administrar su sistema de archivos.

  Si lo utiliza AWS Managed Microsoft AD, debe especificar un grupo, como administradores AWS delegados de FSx AWS , administradores delegados o un grupo personalizado con permisos delegados para la unidad organizativa.

  Si se va a unir a un AD autogestionado, utilice el nombre del grupo en su AD. El grupo predeterminado es `Domain Admins`.

10. En la sección de configuración del volumen predeterminado, proporcione la siguiente información para el volumen predeterminado que se crea con el sistema de archivos:

    - En el campo Volume name, introduzca un nombre para el volumen. Puede utilizar hasta 203 caracteres alfanuméricos o de subrayado (_).
    - (Solo sistemas de archivos ampliables) Para el estilo de volumen, elija una de las dos opciones. FlexVolFlexGroup FlexVollos volúmenes son volúmenes de uso general que pueden tener un tamaño de hasta 300 TiB. FlexGrouplos volúmenes están diseñados para cargas de trabajo de alto rendimiento y pueden tener un tamaño de hasta 20 GiB.
    - En Tamaño de volumen, introduzca cualquier número entero en el rango de 800 gibibytes (GiB) a 2000 pebibytes (PiB).
    - En el tipo de volumen, seleccione Lectura y escritura (RW) para crear un volumen que sea legible y grabable o Protección de datos (DP) para crear un volumen que sea de solo lectura y pueda usarse como destino de una relación o. NetApp SnapMirror SnapVault Para obtener más información, consulte Tipos de volúmenes.
    - En Ruta de unión, introduzca una ubicación dentro del sistema de archivos para montar el volumen. El nombre debe tener una barra delantera hacia adelante, por ejemplo `/vol3`.
    - En Eficiencia del almacenamiento, seleccione Enabled (Activado) para activar las características de eficiencia del almacenamiento de ONTAP (deduplicación, compresión

y compactación). Para obtener más información, consulte FSx para la eficiencia de almacenamiento de ONTAP.

- Para el estilo de seguridad del volumen, elija entre Unix (Linux), NTFS y Mixed para el volumen. Para obtener más información, consulte Estilo de seguridad del volumen.
- Para la política de instantáneas, elija una política de instantáneas para el volumen. Para obtener más información acerca de las políticas de instantáneas, consulte Políticas de instantáneas.

  Si elige Política personalizada, debe especificar el nombre de la política en el campo de política personalizada. La política personalizada ya debe existir en la SVM o en el sistema de archivos. Puede crear una política de instantáneas personalizada con la CLI de ONTAP o la API de REST. Para obtener más información, consulte Creación de una política de instantáneas en la documentación del producto NetApp ONTAP.

11. En la sección Default volume storage tiering, para Capacity pool tiering policy, elija la política de almacenamiento por niveles del grupo de almacenamiento para el volumen, que puede ser Auto (opción predeterminada), Snapshot Only, All o None. Para obtener más información sobre las políticas de niveles de los grupos de capacidad, consulte Políticas de estratificación de volúmenes.

    En Tiering policy cooling period, si ha establecido las políticas de niveles de almacenamiento en `Auto` y `Snapshot-only`, los valores válidos son de 2 a 183 días. El periodo de enfriamiento de la política de niveles de un volumen define el número de días que transcurren antes de que los datos a los que no se ha accedido se marquen como inactivos y se trasladen al repositorio de capacidad.

12. En Backup and maintenance - optional, puede configurar las siguientes opciones:

    - En Daily automatic backup, elija Enabled para realizar copias de seguridad diarias automáticas. Esta opción está habilitada de forma predeterminada.
    - En Daily automatic backup window, establezca la hora del día en tiempo universal coordinado (UTC) a la que desea que se inicie el período de copia de seguridad automática diaria. El período es de 30 minutos a partir de la hora establecida. Este período no se puede solapar con el período de copia de seguridad de mantenimiento semanal.
    - En Automatic backup retention period, establezca un período de 1 a 90 días en el que desee conservar las copias de seguridad automáticas.
    - En Weekly maintenance window, puede establecer la hora de la semana en la que desea que comience el período de mantenimiento. El día 1 es el lunes, el 2 es el martes, y así

sucesivamente. El período es de 30 minutos a partir de la hora establecida. Este período no se puede solapar con el de la copia de seguridad automática y diaria.

13. En Tags - optional, puede introducir una clave y un valor para añadir etiquetas a su sistema de archivos. Una etiqueta es un par clave-valor que distingue entre mayúsculas y minúsculas y que le ayuda a gestionar, filtrar y buscar en su sistema de archivos.

    Elija Next.

14. Revise la configuración del sistema de archivos que se muestra en la página Create File System. Para su referencia, anote qué configuración del sistema de archivos puede modificar después de crear el sistema de archivos.
15. Elija Create file system.

Para crear un sistema de archivos (CLI)

- Para crear un sistema de archivos FSx para ONTAP, utilice el comando create-file-systemCLI (o la operación CreateFileSystemAPI equivalente), como se muestra en el siguiente ejemplo.

```
aws fsx create-file-system \
    --file-system-type ONTAP \
    --storage-capacity 1024 \
    --storage-type SSD \
    --security-group-ids security-group-id \

    --subnet-ids subnet-abcdef1234567890b subnet-abcdef1234567890c \
    --ontap-configuration DeploymentType=MULTI_AZ_1,
        ThroughputCapacity=512,PreferredSubnetId=subnet-abcdef1234567890b
```

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

```
{
  "FileSystem": {
    "OwnerId": "111122223333",
    "CreationTime": 1625066825.306,
    "FileSystemId": "fs-0123456789abcdef0",
    "FileSystemType": "ONTAP",
    "Lifecycle": "CREATING",
    "StorageCapacity": 1024,
```

```
    "StorageType": "SSD",
    "VpcId": "vpc-11223344556677aab",
    "SubnetIds": [
      "subnet-abcdef1234567890b",
      "subnet-abcdef1234567890c"
    ],
    "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "ResourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/
fs-0123456789abcdef0",
    "Tags": [],
    "OntapConfiguration": {
      "DeploymentType": "MULTI_AZ_HA_1",
      "EndpointIpAddressRange": "198.19.0.0/24",
      "Endpoints": {
        "Management": {
          "DnsName": "management.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com"
        },
        "Intercluster": {
          "DnsName": "intercluster.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com"
        }
      },
      "DiskIopsConfiguration": {
                "Mode": "AUTOMATIC",
                "Iops": 3072
      },
      "PreferredSubnetId": "subnet-abcdef1234567890b",
      "RouteTableIds": [
        "rtb-abcdef1234567890e",
        "rtb-abcd1234ef567890b"
      ],
      "ThroughputCapacity": 512,
      "WeeklyMaintenanceStartTime": "4:10:00"
    }
  }
}
```

> **Note**
>
> A diferencia del proceso de creación de un sistema de archivos en la consola, el comando `create-file-system` CLI y la operación de la `CreateFileSystem` API no crean un SVM

o un volumen predeterminados. Para crear una SVM, consulte Creación de una máquina virtual de almacenamiento; para crear un volumen, consulte Creación de volúmenes.

Creación de FSx para sistemas de archivos ONTAP en subredes compartidas

El uso compartido de VPC permite Cuentas de AWS crear varios recursos en nubes privadas virtuales (VPC) compartidas y administradas de forma centralizada. En este modelo, la cuenta propietaria de la VPC (propietario) comparte una o más subredes con otras cuentas (participantes) que pertenecen a la misma organización de. AWS Organizations

Las cuentas de los participantes pueden crear FSx para los sistemas de archivos ONTAP Single-AZ y Multi-AZ en una subred de VPC que la cuenta propietaria haya compartido con ellos. Para que una cuenta de participante cree un sistema de archivos Multi-AZ, la cuenta del propietario también debe conceder permiso a Amazon FSx para modificar las tablas de enrutamiento de las subredes compartidas en nombre de la cuenta del participante. Para obtener más información, consulte Administración del soporte de VPC compartido para sistemas de archivos Multi-AZ.

> **Note**
>
> Es responsabilidad de la cuenta del participante coordinarse con el propietario de la VPC para evitar la creación de subredes de VPC posteriores que se superpongan con el CIDR integrado en la VPC de los sistemas de archivos del participante. Si las subredes se superponen, el tráfico al sistema de archivos puede interrumpirse.

Requisitos y consideraciones de la subred compartida

Al crear FSx para sistemas de archivos ONTAP en subredes compartidas, tenga en cuenta lo siguiente:

- El propietario de la subred de VPC debe compartir una subred con una cuenta de participante antes de que esa cuenta pueda crear un sistema de archivos FSx para ONTAP en ella.
- No puede lanzar recursos mediante el grupo de seguridad predeterminado de la VPC porque pertenece al propietario. Además, las cuentas de los participantes no pueden lanzar recursos mediante grupos de seguridad que sean propiedad de otros participantes o del propietario.

- En una subred compartida, el participante y el propietario controlan por separado los grupos de seguridad de cada cuenta respectiva. La cuenta de propietario puede ver los grupos de seguridad creados por los participantes, pero no puede realizar ninguna acción en ellos. Si la cuenta propietaria desea eliminar o modificar estos grupos de seguridad, el participante que creó el grupo de seguridad debe realizar la acción.
- Las cuentas de los participantes pueden ver, crear, modificar y eliminar los sistemas de archivos Single-AZ y sus recursos asociados en las subredes que la cuenta propietaria haya compartido con ellos.
- Las cuentas de los participantes pueden crear, ver, modificar y eliminar sistemas de archivos Multi-AZ y sus recursos asociados en las subredes que la cuenta propietaria haya compartido con ellos. Además, la cuenta del propietario también debe conceder al servicio Amazon FSx permisos para modificar las tablas de enrutamiento en las subredes compartidas en nombre de la cuenta del participante. Para más información, consulte Administración del soporte de VPC compartido para sistemas de archivos Multi-AZ
- El propietario de la VPC compartida no puede ver, modificar ni eliminar los recursos que un participante crea en la subred compartida. Esto se suma a los recursos de VPC a los que cada cuenta tiene un acceso diferente. Para obtener más información, consulte Responsabilidades y permisos para propietarios y participantes en la Guía del usuario de Amazon VPC.

Para obtener más información, consulte Compartir su VPC con otras cuentas en la Guía del usuario de Amazon VPC.

Al compartir una subred de VPC

Al compartir las subredes con las cuentas de los participantes que van a crear FSx para los sistemas de archivos de ONTAP en las subredes compartidas, tendrá que hacer lo siguiente:

- El propietario de la VPC debe AWS Resource Access Manager utilizarla para compartir de forma segura las VPC y las subredes con otros. Cuentas de AWS Para obtener más información, consulte Compartir sus AWS recursos en la Guía del AWS Resource Access Manager usuario.
- El propietario de la VPC debe compartir una o más VPC con una cuenta de participante. Para obtener más información, consulte Compartir su VPC con otras cuentas en la Guía del usuario de Amazon Virtual Private Cloud.
- Para que las cuentas de los participantes creen FSx para los sistemas de archivos Multi-AZ de ONTAP, el propietario de la VPC también debe conceder al servicio Amazon FSx permisos para crear y modificar tablas de enrutamiento en las subredes compartidas en nombre de las cuentas

de los participantes. Esto se debe a que los sistemas de archivos Multi-AZ de FSx para ONTAP utilizan direcciones IP flotantes para que los clientes conectados puedan realizar una transición fluida entre el servidor de archivos preferido y el servidor de archivos en espera durante un evento de conmutación por error. Cuando se produce un evento de conmutación por error, Amazon FSx actualiza todas las rutas de todas las tablas de rutas asociadas al sistema de archivos para que apunten al servidor de archivos actualmente activo.

Administración del soporte de VPC compartido para sistemas de archivos Multi-AZ

Las cuentas de propietario pueden gestionar si las cuentas de los participantes pueden o no crear FSx Multi-AZ para los sistemas de archivos de ONTAP en las subredes de VPC que el propietario haya compartido con los participantes mediante las API, y AWS CLI, tal y como se describe en AWS Management Console las siguientes secciones.

Para gestionar el uso compartido de VPC para sistemas de archivos Multi-AZ (consola)

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

1. En el panel de navegación, seleccione Configuración.
2. Localice la configuración de la VPC compartida Multi-AZ en la página de configuración.
   - Para habilitar el uso compartido de VPC para sistemas de archivos Multi-AZ en las subredes de VPC que comparte, elija Habilitar actualizaciones de tablas de enrutamiento desde las cuentas de los participantes.
   - Para deshabilitar el uso compartido de VPC para sistemas de archivos Multi-AZ en todas las VPC de su propiedad, elija Inhabilitar las actualizaciones de las tablas de enrutamiento de las cuentas de los participantes. Aparece la pantalla de confirmación.

   > **Important**
   >
   > Recomendamos encarecidamente que los sistemas de archivos Multi-AZ creados por los participantes en la VPC compartida se eliminen antes de deshabilitar esta función. Una vez desactivada la función, estos sistemas de archivos pasarán a un `MISCONFIGURED` estado y correrán el riesgo de dejar de estar disponibles.

3. Ingrese **`confirm`** y elija Confirmar para deshabilitar la función.

Para gestionar el uso compartido de VPC para sistemas de archivos Multi-AZ ()AWS CLI

1. Para ver la configuración actual del uso compartido de VPC en zonas de disponibilidad múltiples (Multi-AZ), describe-shared-vpc-configurationutilice el comando CLI o el comando API DescribeSharedVpcConfigurationequivalente, que se muestra a continuación:

   ```
   $ aws fsx describe-shared-vpc-configuration
   ```

   El servicio responde a una solicitud correcta de la siguiente manera:

   ```
   {
       "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
   }
   ```

2. Para administrar la configuración de la VPC compartida Multi-AZ, utilice el comando update-shared-vpc-configurationCLI o el comando API UpdateSharedVpcConfigurationequivalente. El siguiente ejemplo permite el uso compartido de VPC para sistemas de archivos Multi-AZ.

   ```
   $ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-participant-accounts true
   ```

   El servicio responde a una solicitud correcta de la siguiente manera:

   ```
   {
       "EnableFsxRouteTableUpdatesFromParticipantAccounts": "true"
   }
   ```

3. Para deshabilitar la función, `EnableFsxRouteTableUpdatesFromParticipantAccounts` configúrela en`false`, como se muestra en el siguiente ejemplo.

   ```
   $ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-participant-accounts false
   ```

   El servicio responde a una solicitud correcta de la siguiente manera:

   ```
   {
       "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
   }
   ```

Actualización de un sistema de archivos

En este tema se explican las propiedades de un sistema de archivos existente que se pueden actualizar y se proporcionan procedimientos para hacerlo mediante la consola y la CLI.

Puede actualizar los siguientes FSx para las propiedades del sistema de archivos ONTAP mediante la consola Amazon FSx, la API Amazon FSx y AWS CLI la API Amazon FSx:

- Copias de seguridad diarias automáticas. Activa o desactiva las copias de seguridad diarias automáticas, modifica el periodo de copia de seguridad y el periodo de retención de las copias de seguridad. Para obtener más información sobre las copias de seguridad, consulte Trabajo con copias de seguridad diarias automáticas.
- Período de mantenimiento semanal. Establece el día de la semana y la hora en que Amazon FSx realiza el mantenimiento y las actualizaciones del sistema de archivos. Para obtener más información sobre los períodos de mantenimiento, consulte Optimización del rendimiento con las ventanas de mantenimiento de Amazon FSx.
- Contraseña administrativa del sistema de archivos. Cambia la contraseña del usuario `fsxadmin` del sistema de archivos. Puede usar el usuario `fsxadmin` para administrar su sistema de archivos mediante la CLI y la API de REST de ONTAP. Para más información sobre el usuario `fsxadmin`, consulte Administración de sistemas de archivos con la ONTAP CLI.
- Tablas de enrutamiento de Amazon VPC. Con Multi-AZ FSx para sistemas de archivos ONTAP, los puntos de conexión que utilice para acceder a los datos a través de NFS o SMB y los puntos de conexión de gestión para acceder a la CLI, API y BlueXP de ONTAP utilizan direcciones IP flotantes en las tablas de enrutamiento de Amazon VPC que asocie a su sistema de archivos. Puede asociar las nuevas tablas de enrutamiento que cree con sus sistemas de archivos Multi-AZ existentes, lo que le permite configurar qué clientes pueden acceder a sus datos incluso a medida que la red evoluciona. También puede desasociar (eliminar) las tablas de enrutamiento existentes del sistema de archivos.

> **Note**
>
> Amazon FSx administra las tablas de enrutamiento de VPC para sistemas de archivos Multi-AZ mediante la autenticación basada en etiquetas. Estas tablas de rutas están etiquetadas con. `Key: AmazonFSx; Value: ManagedByAmazonFSx` Al crear o actualizar FSx para sistemas de archivos Multi-AZ de ONTAP, le AWS CloudFormation

recomendamos que añada la etiqueta manualmente. `Key: AmazonFSx; Value: ManagedByAmazonFSx`

Para actualizar un sistema de archivos (consola)

Los siguientes procedimientos proporcionan instrucciones sobre cómo realizar actualizaciones en un sistema de archivos FSx for ONTAP existente mediante el. AWS Management Console

Para actualizar las copias de seguridad diarias automáticas

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Para mostrar la página de detalles del sistema de archivos, en el panel de navegación izquierdo, elija File systems y, a continuación, elija el sistema de archivos de FSx para ONTAP que desee actualizar.
3. Elija la pestaña Backups en el segundo panel de la página.
4. Elija Update.
5. Modifique la configuración de las copias de seguridad diarias automáticas para este sistema de archivos.
6. Elija Save para guardar los cambios.

Para actualizar el período de mantenimiento semanal

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Para mostrar la página de detalles del sistema de archivos, en el panel de navegación izquierdo, elija File systems y, a continuación, elija el sistema de archivos de FSx para ONTAP que desee actualizar.
3. Elija la pestaña Administration en el segundo panel de la página.
4. En el panel Maintenance, elija Update.
5. Modifique cuándo se produce el período de mantenimiento semanal de este sistema de archivos.
6. Elija Guardar para guardar los cambios.

Para cambiar la contraseña administrativa del sistema de archivos

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Para mostrar la página de detalles del sistema de archivos, en el panel de navegación izquierdo, elija File systems y, a continuación, elija el sistema de archivos de FSx para ONTAP que desee actualizar.
3. Elija la pestaña Administration.
4. En el panel de ONTAP administration, elija Update en ONTAP administrator password.
5. En el cuadro de diálogo Update ONTAP administrator credentials, introduzca una nueva contraseña en el campo de ONTAP administrative password.
6. Utilice el campo Confirm password para confirmar la contraseña.
7. Elija Update credentials para guardar los cambios.

> **Note**
>
> Si recibe un error que indica que la nueva contraseña no cumple con los requisitos de contraseña, puede utilizar el comando `security login role config show`ONTAPCLI para ver la configuración de requisitos de contraseña en el sistema de archivos. Para obtener más información, incluidas las instrucciones sobre cómo cambiar la configuración de la contraseña, consulteNo se puede actualizar la contraseña de la `fsxadmin` cuenta.

Para actualizar las tablas de enrutamiento de VPC en sistemas de archivos Multi-AZ

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Para mostrar la página de detalles del sistema de archivos, en el panel de navegación izquierdo, elija File systems y, a continuación, elija el sistema de archivos de FSx para ONTAP que desee actualizar.
3. En Actions, elija Manage Route Tables. Esta opción solo está disponible para los sistemas de archivos Multi-AZ.
4. En el cuadro de diálogo Manage route tables, realice una de las acciones siguientes:
   - Para asociar una nueva tabla de enrutamiento de VPC, seleccione una tabla de enrutamiento de la lista desplegable Associate new route tables y, a continuación, elija Associate.

- Para desasociar una tabla de enrutamiento de VPC existente, seleccione una tabla de enrutamiento del panel Current route tables y, a continuación, elija Disassociate.

5. Elija Close.

Para actualizar un sistema de archivos (CLI)

El siguiente procedimiento ilustra cómo realizar actualizaciones en un sistema de archivos FSx for ONTAP existente mediante. AWS CLI

1. Para actualizar la configuración de un sistema de archivos FSx para ONTAP, utilice el comando update-file-systemCLI (o la operación UpdateFileSystemAPI equivalente), como se muestra en el siguiente ejemplo.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --ontap-configuration
 AutomaticBackupRetentionDays=30,DailyAutomaticBackupStartTime=01:00, \
      WeeklyMaintenanceStartTime=1:01:30,AddRouteTableIds=rtb-0123abcd, \
      FsxAdminPassword=new-fsx-admin-password
```

2. Para deshabilitar las copias de seguridad diarias automáticas, defina la `AutomaticBackupRetentionDays` propiedad en 0.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --ontap-configuration AutomaticBackupRetentionDays=0
```

Eliminación de un sistema de archivos

Puede eliminar un sistema de archivos FSx para ONTAP mediante la consola Amazon FSx, la API y AWS CLI los SDK de Amazon FSx.

Para eliminar un sistema de archivos:

- Usando la consola: siga el procedimiento descrito en Paso 3: Limpiar recursos.
- Mediante la CLI o la API: primero elimine todos los volúmenes y las SVM del sistema de archivos. A continuación, utilice el comando delete-file-systemCLI o la operación DeleteFileSystemAPI.

Visualización de los detalles del sistema de archivos

Puede ver información de configuración detallada de su sistema de archivos FSx para ONTAP mediante la consola Amazon FSx AWS CLI, la API y los SDK compatibles. AWS

Para ver información detallada del sistema de archivos:

- Uso de la consola: elija un sistema de archivos para visualizar la página de detalles del File systems. El panel de Summary muestra el identificador del sistema de archivos, el estado del ciclo de vida, el tipo de implementación, la capacidad de almacenamiento en SSD, la capacidad de rendimiento, las IOPS aprovisionadas, las zonas de disponibilidad y la hora de creación.

  Las siguientes pestañas proporcionan información detallada de configuración y edición de las propiedades que se pueden modificar:

  - Red y seguridad
  - Supervisión y rendimiento: muestra CloudWatch las alarmas que ha creado, así como las métricas y advertencias de las siguientes categorías:
    - Resumen: resumen de alto nivel de las métricas de actividad del sistema de archivos
    - Capacidad de almacenamiento del sistema de archivos
    - Rendimiento del disco y del servidor de archivos

    Para obtener más información, consulte Monitorización con Amazon CloudWatch.
  - Administración: muestra la siguiente información de administración del sistema de archivos:
    - Los DNS nombres y IP direcciones de los puntos finales de administración y entre clústeres del sistema de archivos.
    - El nombre de usuario del ONTAP administrador.
    - La opción de actualizar la contraseña ONTAP del administrador.
  - Lista de las SVM del sistema de archivos
  - Lista de los volúmenes del sistema de archivos
  - Configuración de copia de seguridad: cambie la configuración de copia de seguridad diaria automática del sistema de archivos.
  - Actualizaciones: muestra el estado de las actualizaciones iniciadas por el usuario en la configuración del sistema de archivos.
  - Etiquetas: ver, editar, añadir o eliminar los pares clave:valor de la etiqueta.

- Uso de la CLI o la API: utilice el comando describe-file-systemsCLI o la operación de DescribeFileSystemsAPI.

FSx para el estado del sistema de archivos ONTAP

Puede ver el estado de un sistema de archivos de Amazon FSx mediante la consola de Amazon FSx, el AWS CLI comando o la operación de la describe-file-systemsAPI. DescribeFileSystems

Estado del sistema de archivos	Descripción
DISPONIBLE	El sistema de archivos se ha creado correctamente y está disponible para su uso.
CREAR	Amazon FSx está creando un nuevo sistema de archivos.
ELIMINANDO	Amazon FSx está eliminando un sistema de archivos existente.
MAL CONFIGURADO	El sistema de archivos está mal configurado pero es recuperable.
ERROR	1. El sistema de archivos ha generado un error y Amazon FSx no puede recuperarlo. 2. Al crear un nuevo sistema de archivos, Amazon FSx no pudo crear uno nuevo.

Administración de FSx para máquinas virtuales de almacenamiento ONTAP

En FSx para ONTAP, los volúmenes se alojan en servidores de archivos virtuales denominados máquinas virtuales de almacenamiento (SVM). Un SVM es un servidor de archivos aislado con sus propias credenciales administrativas y puntos finales para administrar y acceder a los datos. Al acceder a los datos de FSx para ONTAP, sus clientes y estaciones de trabajo montan un volumen, un recurso compartido SMB o un LUN iSCSI alojado en una SVM mediante el punto de conexión de la SVM (dirección IP).

Amazon FSx crea automáticamente un SVM predeterminado en su sistema de archivos cuando crea un sistema de archivos con AWS Management Console. Puede crear SVM adicionales en su sistema de archivos en cualquier momento mediante la consola o la API AWS CLI y los SDK de Amazon FSx. No puede crear SVM mediante la CLI de ONTAP o la API de REST.

Puede unir sus SVM a un Active Directory de Microsoft para autenticar y autorizar el acceso a los archivos. Para obtener más información, consulte Uso de Microsoft Active Directory en FSx para ONTAP.

Número máximo de SVM por sistema de archivos

La siguiente tabla enumera la cantidad máxima de SVM que puede crear para un sistema de archivos. La cantidad máxima de SVM depende de la cantidad de capacidad de rendimiento aprovisionada en megabytes por segundo (MBps).

Tipo de implementación	Cantidad de capacidad de rendimiento (MBps)	Número máximo de SVM por sistema de archivos
Single-AZ (escalado hacia arriba) y Multi-AZ (escalado hacia arriba)	128	6
	256	6
	512	14
	1 024	14
	2048	24
	4.096	24
Zona de disponibilidad única (escalamiento horizontal)	Cualquiera	5

Temas

- Creación de una máquina virtual de almacenamiento
- Actualización de una máquina virtual de almacenamiento
- Eliminación de una máquina virtual de almacenamiento (SVM)
- Visualización de los detalles de configuración de la máquina virtual de almacenamiento

Creación de una máquina virtual de almacenamiento

Puede crear un FSx para ONTAP SVM mediante la API AWS Management Console, y AWS CLI.

El número máximo de SVM que puede crear para un sistema de archivos depende del tipo de despliegue del sistema de archivos y de la cantidad de capacidad de rendimiento aprovisionada. Para obtener más información, consulte Número máximo de SVM por sistema de archivos.

Propiedades de SVM

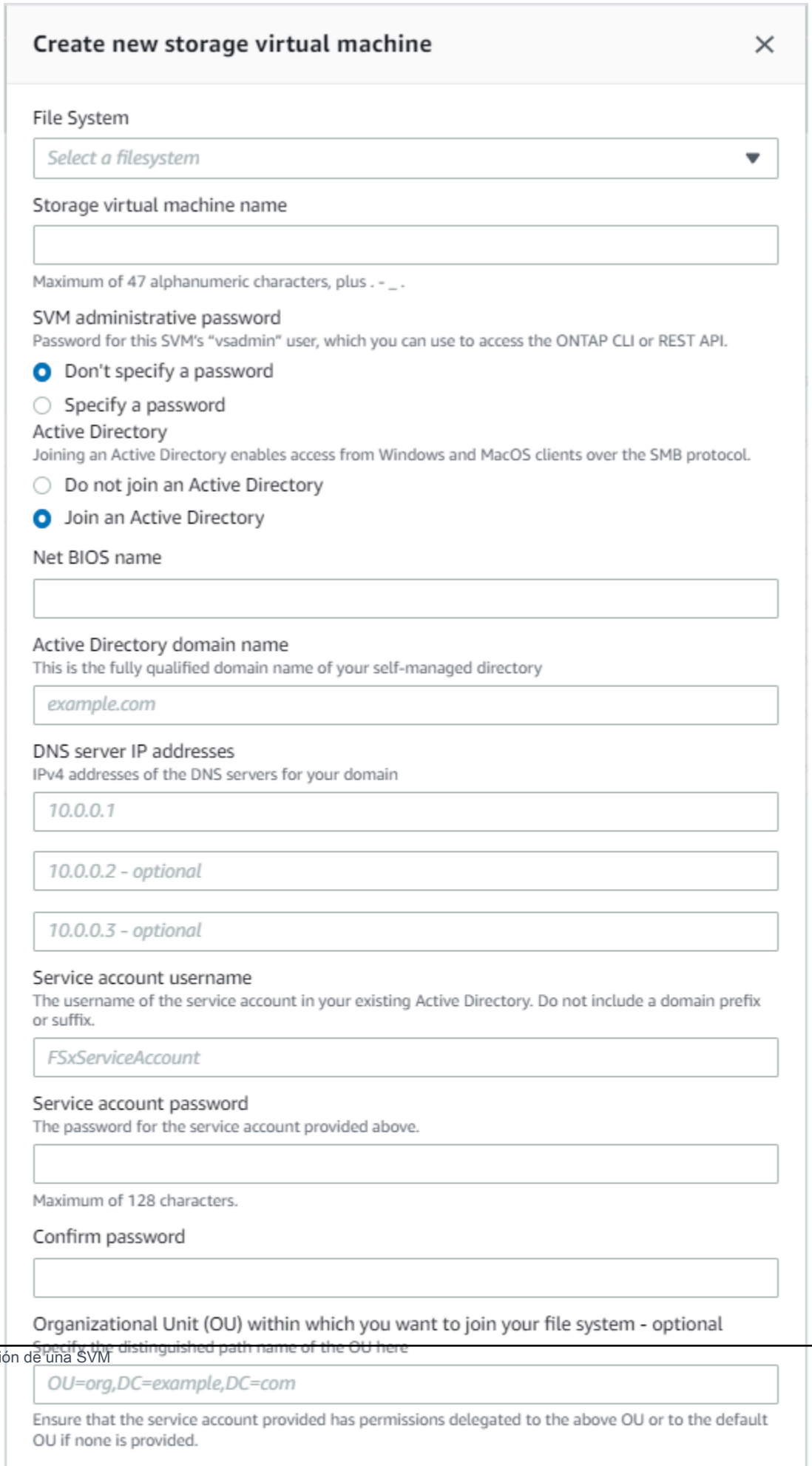
Al crear una SVM, se definen las siguientes propiedades:

- El sistema de archivos de FSx para ONTAP al que pertenece.
- La configuración de Microsoft Active Directory (AD): si lo desea, puede unir su SVM a un AD autogestionado para la autenticación y el control de acceso de los clientes de Windows y macOS. Para obtener más información, consulte Uso de Microsoft Active Directory en FSx para ONTAP.
- El estilo de seguridad del volumen raíz: defina el estilo de seguridad del volumen raíz (Unix, NTFS o mixto) para adaptarlo al tipo de clientes que utiliza para acceder a sus datos dentro del SVM. Para obtener más información, consulte Estilo de seguridad del volumen.
- La contraseña administrativa de la SVM: si lo desea, puede establecer la contraseña para el usuario `vsadmin` de la SVM. Para obtener más información, consulte Administración de SVM con la CLI ONTAP.

Para crear una máquina virtual de almacenamiento (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación izquierdo, seleccione Storage virtual machines (Máquinas virtuales de almacenamiento).
3. Seleccione Create new storage virtual machine (Crear una nueva máquina virtual de almacenamiento).

   Aparece el cuadro de diálogo Create new storage virtual machine (Crear nueva máquina virtual de almacenamiento).


Create new storage virtual machine
File System
Select a filesystem
Storage virtual machine name
Maximum of 47 alphanumeric characters, plus . - _ .
SVM administrative password
Password for this SVM's "vsadmin" user, which you can use to access the ONTAP CLI or REST API.
Don't specify a password
Specify a password
Active Directory
Joining an Active Directory enables access from Windows and MacOS clients over the SMB protocol.
Do not join an Active Directory
Join an Active Directory
Net BIOS name
Active Directory domain name
This is the fully qualified domain name of your self-managed directory
example.com
DNS server IP addresses
IPv4 addresses of the DNS servers for your domain
10.0.0.1
10.0.0.2 - optional
10.0.0.3 - optional
Service account username
The username of the service account in your existing Active Directory. Do not include a domain prefix or suffix.
FSxServiceAccount
Service account password
The password for the service account provided above.
Maximum of 128 characters.
Confirm password
Organizational Unit (OU) within which you want to join your file system - optional
Specify the distinguished path name of the OU here
OU=org,DC=example,DC=com
Ensure that the service account provided has permissions delegated to the above OU or to the default OU if none is provided.

4. En File system (Sistema de archivos), elija el sistema de archivos en el que se va a crear la máquina virtual de almacenamiento.
5. En el campo Storage virtual machine name (Nombre de la máquina virtual de almacenamiento), proporcione un nombre para la máquina virtual de almacenamiento. Puede utilizar un máximo de 47 caracteres alfanuméricos, además del carácter especial de guion bajo (_).
6. Para la contraseña administrativa de SVM, puede elegir opcionalmente Specify a password (Especificar una contraseña) y crear una contraseña para el usuario `vsadmin` de esta SVM. Puede usar el usuario `vsadmin` para administrar la SVM mediante la CLI y la API de REST de ONTAP. Para más información sobre el usuario `vsadmin`, consulte Administración de SVM con la CLI ONTAP.

   Si elige Don't specify a password (No especificar contraseña) (opción predeterminada), podrá seguir utilizando el usuario `fsxadmin` del sistema de archivos para gestionar el sistema de archivos mediante la CLI o la API de REST de ONTAP, pero no podrá utilizar el usuario `vsadmin` de su SVM para hacer lo mismo.
7. En el caso de Active Directory, tiene las siguientes opciones:

   - Si no va a unir su sistema de archivos a un Active Directory (AD), elija Do not join an Active Directory (No unirse a un Active Directory).
   - Si va a unir su SVM a un dominio de AD autogestionado, elija Join an Active Directory (Unirse a un Active Directory) y proporcione los siguientes detalles para su AD. Para obtener más información, consulte Requisitos previos para unir una SVM a un Microsoft AD autogestionado.
     - El nombre NetBIOS del objeto de equipo de Active Directory que se creará para la SVM. El nombre NetBIOS no puede superar los 15 caracteres. Este es el nombre de este SVM en Active Directory.
     - El nombre de dominio completo (FQDN) de su Active Directory. El FQDN no puede superar los 255 caracteres.
     - Direcciones IP del servidor DNS: las direcciones IPv4 de los servidores DNS de su dominio.
     - Nombre de usuario de la cuenta de servicio: el nombre de usuario de la cuenta de servicio de su Active Directory actual. No incluya un prefijo o sufijo de dominio. En `EXAMPLE\ADMIN`, utilice `ADMIN`.
     - Contraseña de la cuenta de servicio: la contraseña de la cuenta de servicio.
     - Confirmar contraseña: la contraseña de la cuenta de servicio.

- (Opcional) Unidad organizativa (OU): nombre de ruta distinguido de la unidad organizativa a la que quieres unir tu sistema de archivos.
- Grupo de administradores del sistema de archivos delegado: el nombre del grupo de su AD que puede administrar el sistema de archivos.

  Si lo utiliza AWS Managed Microsoft AD, debe especificar un grupo como administradores AWS delegados de FSx AWS , administradores delegados o un grupo personalizado con permisos delegados para la OU.

  Si se va a unir a un AD autogestionado, utilice el nombre del grupo en su AD. El grupo predeterminado es `Domain Admins`.

8. Para el SVM root volume security style (Estilo de seguridad del volumen raíz del SVM), elija el estilo de seguridad del SVM en función del tipo de clientes que accedan a sus datos. Elija Unix (Linux) si accede a sus datos principalmente mediante clientes Linux; elija NTFS si accede a sus datos principalmente mediante clientes de Windows. Para obtener más información, consulte Estilo de seguridad del volumen.
9. Elija Confirm (Confirmar) para crear la máquina virtual de almacenamiento.

Puede supervisar el progreso de la actualización en la página de detalles de los File systems (Sistemas de archivos), en la columna Status (Estado) del panel Storage virtual machines (Máquinas virtuales de almacenamiento). La máquina virtual de almacenamiento está lista para usarse cuando su estado es Created (Creado).

Para crear una máquina virtual de almacenamiento (CLI)

- Para crear una máquina virtual de almacenamiento (SVM) FSx para ONTAP, utilice el comando create-storage-virtual-machineCLI (o la operación CreateStorageVirtualMachineAPI equivalente), como se muestra en el siguiente ejemplo.

```
aws fsx create-storage-virtual-machine \
    --file-system-id fs-0123456789abcdef0 \
    --name svm1 \
    --svm-admin-password password \
    --active-directory-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",FileSystemAd
 \
UserName="FSxService",Password="password", \
```

```
    DnsIps=["10.0.1.18"]}',NetBiosName=amznfsx12345
```

Después de crear correctamente la máquina virtual de almacenamiento, Amazon FSx devuelve su descripción en formato JSON, como se muestra en el siguiente ejemplo.


```
{
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATING",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef0123456789a",
    "StorageVirtualMachineId": "svm-abcdef0123456789a",
    "Subtype": "default",
    "Tags": [],
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
```

```
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
  }
}
```

Actualización de una máquina virtual de almacenamiento

Puede actualizar las siguientes propiedades de configuración de la máquina virtual de almacenamiento (SVM) mediante la consola AWS CLI Amazon FSx y la API de Amazon FSx:

- Contraseña de la cuenta administradora de SVM.
- Configuración del Active Directory (AD) de la SVM - Puede unir una SVM a un AD, o modificar la configuración AD de una SVM ya unida a un AD. Para obtener más información, consulte Administrar las configuraciones de SVM Active Directory.

Para actualizar las credenciales de la cuenta de administrador de SVM (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Elija la SVM que desea actualizar de la siguiente manera:
   - En el panel de navegación, elija File systems (Sistemas de archivos) y, a continuación, elija el sistema de archivos de ONTAP para el que desea actualizar una SVM.
   - Elija la pestaña Storage virtual machines (Máquinas virtuales de almacenamiento).

     –O bien –

   - Para ver una lista de todas las máquinas virtuales disponibles en la actualidad Región de AWS, amplíe ONTAP y elija Máquinas virtuales de almacenamiento. Cuenta de AWS
3. Elija la máquina virtual de almacenamiento que desea actualizar.

4. Seleccione Actions > Update administrator password (Acciones > Actualizar la contraseña de administrador). Aparece la ventana Update SVM administrative credentials (Actualizar las credenciales administrativas de SVM).
5. Indique la nueva contraseña del usuario `vsadmin` y confírmela.
6. Seleccione Update credentials (Actualizar credenciales) para guardar la nueva contraseña.

Para actualizar las credenciales de la cuenta de administrador de SVM (CLI)

- Para actualizar la configuración de un FSx para ONTAP SVM, utilice el comando update-storage-virtual-machineCLI (o la operación UpdateStorageVirtualMachineAPI equivalente), como se muestra en el siguiente ejemplo.

```
aws fsx update-storage-virtual-machine \
--storage-virtual-machine-id svm-abcdef01234567890 \
--svm-admin-password new-svm-password \
```

Después de crear correctamente la máquina virtual de almacenamiento, Amazon FSx devuelve su descripción en formato JSON, como se muestra en el siguiente ejemplo.

```
{
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
```

```
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATING",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef01234567890",
    "StorageVirtualMachineId": "svm-abcdef01234567890",
    "Subtype": "default",
    "Tags": [],
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
  }
}
```

Eliminación de una máquina virtual de almacenamiento (SVM)

Solo puede eliminar un FSx para ONTAP SVM mediante la consola Amazon FSx, la y la API. AWS CLI Para poder eliminar una SVM, primero debe eliminar todos los volúmenes no raíz adjuntos a la SVM.

> **Important**
>
> No puede eliminar una SVM mediante la NetApp CLI o la API de ONTAP.

> **Note**
>
> Antes de eliminar una máquina virtual de almacenamiento, asegúrese de que ninguna aplicación acceda a los datos de la SVM y de que ha eliminado todos los volúmenes no raíz conectados a la SVM.

Para eliminar una máquina virtual de almacenamiento (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Elija la SVM que desea eliminar de la siguiente manera:

   - En el panel de navegación, elija File systems (Sistemas de archivos) y, a continuación, elija el sistema de archivos de ONTAP del que desea eliminar un SVM.
   - Elija la pestaña Storage virtual machines (Máquinas virtuales de almacenamiento).

     –O bien–

   - Para ver una lista de todas las máquinas virtuales disponibles, expanda ONTAP y seleccione Storage virtual machines (Almacenamiento de máquinas virtuales).

   Seleccione de la lista la SVM que desea eliminar.
3. En la pestaña Volumes (Volúmenes), consulte la lista de volúmenes adjuntos a la SVM. Si hay volúmenes no raíz adjuntos a la SVM, debe eliminarlos antes de poder eliminar la SVM. Para obtener más información, consulte Eliminación de un volumen.
4. Seleccione Delete storage virtual machine (Eliminar máquina virtual de almacenamiento) en el menú Actions (Acciones).
5. En el cuadro de diálogo de confirmación de eliminación, seleccione Delete storage virtual machine (Eliminar máquina virtual de almacenamiento).

Para eliminar una máquina virtual de almacenamiento (CLI)

- Para eliminar una máquina virtual de almacenamiento FSx para ONTAP, utilice el comando delete-storage-virtual-machineCLI (o la operación DeleteStorageVirtualMachineAPI equivalente), como se muestra en el siguiente ejemplo.

```
aws fsx delete-storage-virtual-machine --storage-virtual-machine-id svm-
abcdef0123456789d
```

Visualización de los detalles de configuración de la máquina virtual de almacenamiento

Puede ver las máquinas virtuales de almacenamiento FSx para ONTAP que se encuentran actualmente en su sistema de archivos mediante la consola Amazon FSx, la API Amazon FSx y AWS CLI la API Amazon FSx.

Para ver una máquina virtual de almacenamiento en su sistema de archivos:

- Uso de la consola: Seleccione un sistema de archivos para ver su página de detalles File systems (Sistemas de archivos). Para ver todas las máquinas virtuales de almacenamiento del sistema de archivos, seleccione la pestaña Storage virtual machines (Máquinas virtuales de almacenamiento) y, a continuación, elija la máquina virtual de almacenamiento que desee ver.
- Uso de la CLI o la API: utilice el comando describe-storage-virtual-machinesCLI o la operación de DescribeStorageVirtualMachinesAPI.

  La respuesta del sistema es una lista de descripciones completas de todas las SVM de su cuenta en esa Región de AWS.

Gestión de volúmenes FSx para ONTAP

Cada máquina virtual de almacenamiento (SVM) de un sistema de archivos de FSx para ONTAP puede tener uno o más volúmenes. Un volumen es un contenedor de datos aislado para archivos, directorios o unidades lógicas de almacenamiento (LUNs) iSCSI. Los volúmenes tienen aprovisionamiento ligero, lo que significa que consumen capacidad de almacenamiento únicamente para los datos almacenados en ellos.

Puede acceder a un volumen desde clientes Linux, Windows o macOS mediante el protocolo Network File System (NFS), el protocolo Server Message Block (SMB) o mediante el protocolo Internet Small Computer Systems Interface (iSCSI) mediante la creación de un LUN iSCSI (almacenamiento en bloque compartido). FSx para ONTAP también admite el acceso multiprotocolo (acceso simultáneo a NFS y SMB) al mismo volumen.

Puede crear volúmenes mediante la AWS Management Console API de Amazon FSx o NetApp BlueXP. AWS CLI También puede usar el punto final administrativo de su sistema de archivos o SVM para crear, actualizar y eliminar volúmenes mediante la NetApp CLI de ONTAP o la API REST.

Puede crear hasta 500 volúmenes por sistema de archivos escalable y 1000 volúmenes por sistema de archivos escalable.

Al crear un volumen, se definen las siguientes propiedades:

- Estilo de volumen: el estilo de volumen puede ser uno de los dos. FlexVol FlexGroup
- Nombre del volumen: el nombre del volumen.
- Tipo de volumen: el tipo de volumen puede ser de lectura y escritura (RW) o de protección de datos (DP). Los volúmenes DP son de solo lectura y se utilizan como destino en una relación NetApp SnapMirror oSnapVault.
- Tamaño del volumen: es la cantidad máxima de datos que el volumen puede almacenar, independientemente del nivel de almacenamiento.
- Ruta de unión: esta es la ubicación en el espacio de nombres de la SVM donde se monta el volumen.
- Eficiencia del almacenamiento: las funciones de eficiencia del almacenamiento, que incluyen la compactación, la compresión y la deduplicación de datos, proporcionan un ahorro de almacenamiento típico del 65% para las cargas de trabajo de uso general relacionadas con el uso compartido de archivos.
- Estilo de seguridad del volumen (Unix, NTFS o mixto): determina qué tipo de permisos se utilizan para el acceso a los datos del volumen al autorizar a los usuarios.
- Clasificación de datos por niveles: la política de organización por niveles define qué datos se almacenan en el rentable nivel del pool de capacidad.
- Periodo de enfriamiento de la política de estratificación: define cuándo los datos se marcan como inactivos y se trasladan al almacenamiento del grupo de capacidad.
- Política de instantáneas: las políticas de instantáneas definen cómo el sistema crea las instantáneas de un volumen. Puede elegir entre tres políticas predefinidas o utilizar una política personalizada que haya creado mediante la CLI de ONTAP o la API REST.
- Copiar etiquetas a las copias de seguridad: Amazon FSx copiará automáticamente cualquier etiqueta de sus volúmenes a las copias de seguridad mediante esta opción. Puede configurar esta opción mediante la API AWS CLI o Amazon FSx.

Temas

Estilos de volumen

FSx para ONTAP ofrece dos estilos de volúmenes que puede utilizar para distintos fines. Puede crear uno FlexVol o varios FlexGroup volúmenes mediante la consola de Amazon FSx, la API Amazon FSx y la AWS CLI API de Amazon FSx.

- FlexVolLos volúmenes ofrecen la experiencia más sencilla para los sistemas de archivos con un par de alta disponibilidad (HA) y son el estilo de volumen predeterminado para los sistemas de archivos escalables. El tamaño mínimo de un FlexVol volumen es de 20 mebibytes (MiB) y el tamaño máximo es de 314.572.800 MiB.
- FlexGroupLos volúmenes se componen de varios FlexVol volúmenes constitutivos, lo que les permite ofrecer un rendimiento y una escalabilidad de almacenamiento superiores a los volúmenes de sistemas de archivos con varios pares de FlexVol alta disponibilidad. FlexGrouplos volúmenes son el estilo de volumen predeterminado para los sistemas de archivos escalables. El tamaño mínimo de un FlexGroup volumen es de 100 gibibytes (GiB) por componente y el tamaño máximo es de 20 pebibytes (PiB).

Puede convertir un volumen con el FlexVol estilo en el FlexGroup estilo con la ONTAP CLI, lo que crea un FlexGroup con un solo componente. Sin embargo, le recomendamos que lo utilice AWS DataSync para mover los datos entre un FlexVol volumen y un FlexGroup volumen nuevo para garantizar que los datos se distribuyan uniformemente entre FlexGroup's los componentes. Para obtener más información, consulte FlexGroupelectores.

> **Note**
>
> Si desea utilizar la ONTAP CLI para convertir un FlexVol volumen en un FlexGroup volumen, asegúrese de eliminar todas las copias de seguridad del FlexVol volumen antes de convertirlas. ONTAPno reequilibra automáticamente los datos como parte de la conversión, por lo que es posible que los datos estén desequilibrados entre los FlexGroup componentes.

FlexGroupelectores

Un FlexGroup volumen se compone de componentes, que son FlexVol volúmenes. De forma predeterminada, FSx para ONTAP asigna ocho componentes a un FlexGroup volumen por par de HA.

Al crear el FlexGroup volumen, su tamaño se divide equitativamente entre sus componentes. Por ejemplo, si crea un FlexGroup volumen de 800 gigabytes (GB) con ocho componentes, cada componente tendrá un tamaño de 100 GB. Un FlexGroup volumen puede tener un tamaño de entre 100 GB y 20 PiB, pero el tamaño total depende del tamaño de los componentes. Cada componente tiene un tamaño mínimo de 100 GB y un tamaño máximo de 300 TiB. Por ejemplo, un FlexGroup volumen con ocho componentes tiene un tamaño mínimo de 800 GB y un tamaño máximo de 20 GiB.

ONTAP distribuye los datos a nivel de archivo entre los componentes. Puede almacenar hasta dos mil millones de archivos en cada componente de su volumen. FlexGroup

Al actualizar el tamaño del FlexGroup volumen, el nuevo tamaño se distribuye uniformemente entre los componentes existentes.

También puede agregar más componentes al FlexGroup volumen mediante la ONTAP CLI o la API REST. Sin embargo, le recomendamos que solo lo haga si necesita capacidad de almacenamiento adicional y todos sus componentes ya tienen su tamaño máximo (300 TiB por componente). La adición de componentes puede provocar un desequilibrio de datos y E/S entre los componentes. Hasta que los componentes estén equilibrados, es posible que el rendimiento de escritura sea entre un 5 y un 10% inferior al de un volumen balanceado. FlexGroup Cuando se escriben nuevos datos en el FlexGroup volumen, ONTAP prioriza su distribución entre los nuevos componentes hasta que éstos estén equilibrados. Si añade nuevos componentes, le recomendamos que elija un número par y que no exceda de ocho por agregado.

> **Note**
>
> Si agrega nuevos componentes, las instantáneas existentes se convierten en instantáneas parciales; por lo tanto, no se pueden usar para restaurar completamente el FlexGroup volumen a un estado anterior. Las instantáneas anteriores no ofrecen una point-in-time imagen completa del FlexGroup volumen porque los nuevos componentes aún no existían. Sin embargo, las instantáneas parciales se pueden usar para restaurar archivos y directorios individuales, para crear un volumen nuevo o para replicar con ellos. SnapMirror

Tipos de volúmenes

FSx for ONTAP ofrece dos tipos de volúmenes que puede crear mediante la consola Amazon FSx, la API Amazon FSx y AWS CLI la API de Amazon FSx.

- Los volúmenes de lectura y escritura (RW) se utilizan en la mayoría de los casos. Como su nombre indica, se pueden leer y escribir.
- Los volúmenes de protección de datos (DP) son volúmenes de solo lectura que se utilizan como destino de una relación o relación. NetApp SnapMirror SnapVault Debe utilizar los volúmenes DP cuando desee migrar o proteger los datos de un único volumen.

FlexVoly FlexGroup los volúmenes pueden ser RW o DP.

> **Note**
>
> No puede actualizar el tipo de volumen una vez creado el volumen.

Estilo de seguridad del volumen

FSx para ONTAP admite 3 estilos de seguridad de volumen diferentes: Unix, NTFS y mixto. Cada estilo de seguridad tiene un efecto diferente en la forma en que se gestionan los permisos de los datos. Debe comprender los diferentes efectos para asegurarse de seleccionar el estilo de seguridad adecuado para sus fines.

Es importante entender que los estilos de seguridad no determinan qué tipos de clientes pueden o no acceder a los datos. Los estilos de seguridad solo determinan el tipo de permisos que FSx

for ONTAP utiliza para controlar el acceso a los datos y qué tipo de cliente puede modificar estos permisos.

Los dos factores que se utilizan para determinar el estilo de seguridad de un volumen son el tipo de administradores que administran el sistema de archivos y el tipo de usuarios o servicios que acceden a los datos del volumen.

Al crear un volumen en la consola, la CLI y la API de Amazon FSx, el estilo de seguridad se establece automáticamente en el estilo de seguridad del volumen raíz. Puede modificar el estilo de seguridad de un volumen mediante la API AWS CLI o. Puede modificar esta configuración después de crear el volumen. Para obtener más información, consulte Actualización de un volumen.

Al configurar el estilo de seguridad de un volumen, tenga en cuenta las necesidades de su entorno para asegurarse de seleccionar el mejor estilo de seguridad a fin de evitar problemas con la administración de los permisos. Tenga en cuenta que el estilo de seguridad no determina qué tipos de clientes pueden acceder a los datos. El estilo de seguridad determina los permisos que se utilizan para permitir el acceso a los datos y los tipos de clientes que pueden modificar esos permisos. Las siguientes son consideraciones que pueden ayudarle a decidir qué estilo de seguridad elegir para un volumen:

- Unix (Linux): elija este estilo de seguridad si el sistema de archivos es gestionado por un administrador Unix, la mayoría de los usuarios son clientes NFS y una aplicación que accede a los datos utiliza un usuario Unix como cuenta de servicio. Sólo los clientes Linux pueden modificar los permisos con el estilo de seguridad Unix, y el tipo de permisos que se utilizan en archivos y directorios son los mode-bits o ACLs NFS v4.x.
- NTFS: elija este estilo de seguridad si el sistema de archivos está gestionado por un administrador de Windows, la mayoría de los usuarios son clientes SMB y una aplicación que accede a los datos utiliza un usuario de Windows como cuenta de servicio. Si se requiere el acceso de Windows a un volumen, le aconsejamos que utilice el estilo de seguridad de NTFS. Sólo los clientes de Windows pueden modificar los permisos con el estilo de seguridad NTFS, y los tipos de permisos utilizados en archivos y directorios es NTFS ACLs.
- Mixto: se trata de una configuración avanzada. Para obtener más información, consulte el tema Cuáles son los estilos de seguridad y sus efectos en el Centro de NetApp documentación.

Creación de volúmenes

Puede crear un FSx para ONTAP FlexVol o un FlexGroup volumen mediante la consola Amazon FSx, la API Amazon FSx, además de AWS CLI la interfaz de línea de NetApp comandos (CLI) de ONTAP y la API REST.

Para crear un volumen (consola) FlexVol

> **Note**
>
> El estilo de seguridad del volumen se establece automáticamente en el estilo de seguridad del volumen raíz.

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación izquierdo, seleccione Volumes (Volúmenes).
3. Seleccione Create volume (Crear volumen).
4. En Tipo de sistema de archivos, elija Amazon FSx para NetApp ONTAP.
5. En la sección de detalles del sistema de archivos, proporcione la siguiente información:
   - En Sistema de archivos, elija el sistema de archivos en el que se va a crear el volumen.
   - En Máquina virtual de almacenamiento, seleccione la máquina virtual de almacenamiento (SVM) en la que desea crear el volumen.
6. En la sección Estilo de volumen, elija FlexVol.
7. En la sección de detalles del volumen, proporciona la siguiente información:
   - En el campo Volume name, introduzca un nombre para el volumen. Puede utilizar hasta 203 caracteres alfanuméricos o de subrayado (_).
   - En Volume size, introduzca cualquier número entero en el rango de 20 a 314 572 800 para especificar el tamaño en mebibytes (MiB).
   - En el tipo de volumen, seleccione Lectura/Escritura (RW) para crear un volumen que se pueda leer y escribir o Protección de datos (DP) para crear un volumen que sea de solo lectura y pueda usarse como destino de una relación o. NetApp SnapMirror SnapVault Para obtener más información, consulte Tipos de volúmenes.
   - En Ruta de unión, introduzca una ubicación dentro del sistema de archivos para montar el volumen. El nombre debe tener una barra delantera hacia adelante, por ejemplo `/vol3`.

- En Eficiencia del almacenamiento, seleccione Enabled (Activado) para activar las características de eficiencia del almacenamiento de ONTAP (deduplicación, compresión y compactación). Para obtener más información, consulte FSx para la eficiencia de almacenamiento de ONTAP.
- Para el estilo de seguridad del volumen, elija entre Unix (Linux), NTFS y Mixed para el volumen. Para obtener más información, consulte Estilo de seguridad del volumen.
- Para la política de instantáneas, elija una política de instantáneas para el volumen. Para obtener más información acerca de las políticas de instantáneas, consulte Políticas de instantáneas.

  Si elige Política personalizada, debe especificar el nombre de la política en el campo de política personalizada. La política personalizada ya debe existir en la SVM o en el sistema de archivos. Puede crear una política de instantáneas personalizada con la CLI de ONTAP o la API de REST. Para obtener más información, consulte Creación de una política de instantáneas en la documentación del producto NetApp ONTAP.

8. En la sección sobre la organización del almacenamiento en niveles, proporcione la siguiente información:

   - Para la política de estratificación del pool de capacidad, elija la política de estratificación del pool de almacenamiento para el volumen, que puede ser Automática (la opción predeterminada), Solo instantáneas, Total o Ninguno. Para obtener más información, consulte Políticas de estratificación de volúmenes.
   - Si elige Automático o Solo instantáneas, puede configurar el período de enfriamiento de la política de organización por niveles para definir el número de días que deben transcurrir antes de que los datos a los que no se ha accedido se marquen como inactivos y se trasladen al almacenamiento del grupo de capacidad. Puede proporcionar un valor entre 2 y 183 días. El valor predeterminado es de 31 días.

9. En la sección Avanzada, en SnapLockConfiguración, elija entre Activado y Desactivado. Para obtener más información sobre la configuración de un volumen de SnapLock conformidad o un volumen SnapLock empresarial, consulte Crear un volumen de Conformidad de SnapLock yCreación de un volumen Empresarial de SnapLock. Para obtener más información acerca de SnapLock, consulte Proteja sus datos con SnapLock.
10. Seleccione Confirmar para crear el volumen.

Puede supervisar el progreso de la actualización en la página de detalles de los Sistemas de archivos, en la columna Estadodel panel Volúmenes. El volumen está listo para su uso cuando su estado es Creado.

Para crear un FlexGroup volumen (consola)

> **Note**
>
> Solo puede crear FlexGroup volúmenes para sistemas de archivos escalables mediante la consola Amazon FSx. Para crear FlexVol volúmenes para sus sistemas de archivos escalables, utilice la API AWS CLI Amazon FSx o las herramientas de administración. NetApp

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación izquierdo, seleccione Volumes (Volúmenes).
3. Seleccione Create volume (Crear volumen).
4. En Tipo de sistema de archivos, elija Amazon FSx para NetApp ONTAP.
5. En la sección de detalles del sistema de archivos, proporcione la siguiente información:
   - En Sistema de archivos, elija el sistema de archivos en el que se va a crear el volumen.
   - En Máquina virtual de almacenamiento, seleccione la máquina virtual de almacenamiento (SVM) en la que desea crear el volumen.
6. En la sección Estilo de volumen, elija FlexGroup.
7. En la sección de detalles del volumen, proporciona la siguiente información:
   - En el campo Volume name, introduzca un nombre para el volumen. Puede utilizar hasta 203 caracteres alfanuméricos o de subrayado (_).
   - En Tamaño de volumen, introduzca cualquier número entero en el rango de 800 gibibytes (GiB) a 2000 pebibytes (PiB).
   - En el tipo de volumen, seleccione Lectura y escritura (RW) para crear un volumen que sea legible y grabable o Protección de datos (DP) para crear un volumen que sea de solo lectura y pueda usarse como destino de una relación o. NetApp SnapMirror SnapVault Para obtener más información, consulte Tipos de volúmenes.
   - En Ruta de unión, introduzca una ubicación dentro del sistema de archivos para montar el volumen. El nombre debe tener una barra delantera hacia adelante, por ejemplo `/vol3`.

- En Eficiencia del almacenamiento, seleccione Enabled (Activado) para activar las características de eficiencia del almacenamiento de ONTAP (deduplicación, compresión y compactación). Para obtener más información, consulte FSx para la eficiencia de almacenamiento de ONTAP.
- Para el estilo de seguridad del volumen, elija entre Unix (Linux), NTFS y Mixed para el volumen. Para obtener más información, consulte Estilo de seguridad del volumen.

> **Note**
>
> El estilo de seguridad del volumen se establece automáticamente en el estilo de seguridad del volumen raíz.

- Para la política de instantáneas, elija una política de instantáneas para el volumen. Para obtener más información acerca de las políticas de instantáneas, consulte Políticas de instantáneas.

  Si elige Política personalizada, debe especificar el nombre de la política en el campo de política personalizada. La política personalizada ya debe existir en la SVM o en el sistema de archivos. Puede crear una política de instantáneas personalizada con la CLI de ONTAP o la API de REST. Para obtener más información, consulte Creación de una política de instantáneas en la documentación del producto NetApp ONTAP.

8. En la sección sobre la organización del almacenamiento en niveles, proporcione la siguiente información:

   - Para la política de estratificación del pool de capacidad, elija la política de estratificación del pool de almacenamiento para el volumen, que puede ser Automática (la opción predeterminada), Solo instantáneas, Total o Ninguno. Para obtener más información, consulte Políticas de estratificación de volúmenes.
   - Si elige Automático o Solo instantáneas, puede configurar el período de enfriamiento de la política de organización por niveles para definir el número de días que deben transcurrir antes de que los datos a los que no se ha accedido se marquen como inactivos y se trasladen al almacenamiento del grupo de capacidad. Puede proporcionar un valor de entre 2 y 183 días. El valor predeterminado es de 31 días.

9. En la sección Avanzada, en SnapLockConfiguración, elija entre Activado y Desactivado. Para obtener más información sobre la configuración de un volumen de SnapLock conformidad o un volumen SnapLock empresarial, consulte Crear un volumen de Conformidad de SnapLock

yCreación de un volumen Empresarial de SnapLock. Para obtener más información acerca de SnapLock, consulte Proteja sus datos con SnapLock.

10. Seleccione Confirmar para crear el volumen.

Puede supervisar el progreso de la actualización en la página de detalles de los Sistemas de archivos, en la columna Estadodel panel Volúmenes. El volumen está listo para su uso cuando su estado es Creado.

Para crear un volumen (CLI)

- Para crear un volumen FSx para ONTAP, utilice el comando CLI create-volume (o la operación CreateVolumeAPI equivalente), como se muestra en el siguiente ejemplo.

```
aws fsx create-volume \
    --volume-type ONTAP \
    --name vol1 \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/
vol1,SecurityStyle=NTFS, \
          SizeInMegabytes=1024,SnapshotPolicy=default, \
          StorageVirtualMachineId=svm-abcdef0123456789a,OntapVolumeType=RW, \
          StorageEfficiencyEnabled=true
```

Tras crear correctamente el volumen, Amazon FSx devuelve su descripción en formato JSON, como se muestra en el siguiente ejemplo.

```
{
    "Volume": {
        "CreationTime": "2022-08-12T13:03:37.625000-04:00",
        "FileSystemId": "fs-abcdef0123456789c",
        "Lifecycle": "CREATING",
        "Name": "vol1",
        "OntapConfiguration": {
            "CopyTagsToBackups": true,
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "NTFS",
            "SizeInMegabytes": 1024,
            "SnapshotPolicy": "default",
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abcdef0123456789a",
```

```
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "Name": "NONE"
            },
            "OntapVolumeType": "RW"
        },
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-abcdef0123456789c/
fsvol-abcdef0123456789b",
        "VolumeId": "fsvol-abcdef0123456789b",
        "VolumeType": "ONTAP"


    }
}
```

También puede crear un volumen nuevo restaurando una copia de seguridad de un volumen en un volumen nuevo. Para obtener más información, consulte Restaurar copias de seguridad en un volumen nuevo.

Actualización de un volumen

Puede actualizar la configuración de un volumen FSx para ONTAP mediante la consola Amazon FSx, la API Amazon FSx y la API Amazon FSx, además de AWS CLI la interfaz de línea de NetApp comandos (CLI) de ONTAP y la API REST. Puede modificar las siguientes propiedades de un volumen FSx para ONTAP existente:

- Nombre del volumen
- Ruta de unión
- Tamaño del volumen
- Eficacia de almacenamiento
- Política de niveles del pool de capacidad
- Estilo de seguridad del volumen
- Política de instantáneas
- Periodo de enfriamiento de la política de niveles
- Copiar etiquetas a copias de seguridad (mediante la AWS CLI API y Amazon FSx)

Para obtener más información, consulte Gestión de volúmenes FSx para ONTAP.

Para actualizar la configuración de un volumen (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 ONTAP para el que desee actualizar un volumen.
3. Seleccione la pestaña Volúmenes.
4. Elija el volumen que desea actualizar.
5. En Acciones, seleccione Actualizar volumen.

   Aparece el cuadro de diálogo Actualizar volumen con la configuración actual del volumen.
6. En Ruta de unión, introduzca una ubicación existente en el sistema de archivos para montar el volumen. El nombre debe tener una barra delantera hacia adelante, como `/vol5`.
7. En cuanto al tamaño del volumen, puede aumentar o disminuir el tamaño del volumen dentro del rango especificado en la consola Amazon FSx. Para FlexVol volúmenes, el tamaño máximo es de 300 TiB. Para FlexGroup los volúmenes, el tamaño máximo es de 300 TiB multiplicado por el número total de volúmenes constitutivos que FlexGroup tenga, hasta un máximo de 20 TiB.
8. En Eficiencia de almacenamiento, seleccione Enabled (Activado) para activar las características de eficiencia de almacenamiento de ONTAP (deduplicación, compresión y compactación), o seleccione Disabled (Desactivado) para desactivarlas.
9. Para la Política de niveles del pool de capacidad, elija una nueva política de niveles del grupo de almacenamiento para el volumen, que puede ser Auto (la predeterminada), Sólo instantáneas, Todas o Ninguna. Para obtener más información acerca de las políticas de niveles de grupos de capacidad, consulte Políticas de estratificación de volúmenes.
10. Para el Estilo de seguridad de los volúmenes, elija Unix (Linux), NTFS o Mixto. El estilo de seguridad de un volumen determina si se da preferencia a las ACL de NTFS o UNIX para el acceso multiprotocolo. El modo MIXTO no es necesario para el acceso multiprotocolo y solo se recomienda para usuarios avanzados.
11. Para la Política de instantáneas, elija una política de instantáneas para el volumen. Para obtener más información acerca de las políticas de instantáneas, consulte Políticas de instantáneas.

    Si elige Política personalizada, debe especificar el nombre de la política en el campo de política personalizada. La política personalizada ya debe existir en la SVM o en el sistema de archivos. Puede crear una política de instantáneas personalizada con la CLI de ONTAP o la API de REST. Para obtener más información, consulte Creación de una política de instantáneas en la documentación del producto de NetApp ONTAP.

12. Para el Periodo de enfriamiento de la política de niveles, los valores válidos son de 2 a 183 días. El periodo de enfriamiento de la política de niveles de un volumen define el número de días que transcurren antes de que los datos a los que no se ha accedido se marquen como fríos y se trasladen al repositorio de capacidad. Esta configuración solo afecta a las políticas `Auto` y `Snapshot-only`.
13. Seleccione Actualizar para actualizar el volumen.

Para actualizar la configuración de un volumen (CLI)

- Para actualizar la configuración de un volumen FSx para ONTAP, utilice el comando CLI update-volume (o la operación UpdateVolumeAPI equivalente), como se muestra en el siguiente ejemplo.

```
aws fsx update-volume \
    --volume-id fsvol-1234567890abcdefa \
    --name new_vol \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/new_vol, \
           SizeInMegabytes=2048,SnapshotPolicy=default-1weekly, \
           StorageEfficiencyEnabled=true, \
           TieringPolicy=all
```

Eliminación de un volumen

Puede eliminar un volumen FSx para ONTAP mediante la consola Amazon FSx, la y la API Amazon FSx, además de AWS CLI la interfaz de línea de NetApp comandos (CLI) de ONTAP y la API REST.

> **Important**
>
> Solo puede eliminar volúmenes mediante la consola, la API o la CLI de Amazon FSx si el volumen tiene habilitadas las copias de seguridad de Amazon FSx.

> **Important**
>
> Al eliminar un volumen mediante la consola Amazon FSx, tiene la opción de realizar una copia de seguridad final del volumen. Puede crear nuevos volúmenes a partir de copias de seguridad. Le recomendamos que opte por realizar una copia de seguridad final como

práctica recomendada. Si descubre que no la necesita después de un período de tiempo determinado, puede eliminar esta y otras copias de seguridad por volumen creadas manualmente. Al eliminar un volumen mediante el comando `delete-volume` CLI, Amazon FSx realiza una copia de seguridad final de forma predeterminada.

Antes de eliminar un volumen, asegúrese de que ninguna aplicación esté accediendo a los datos del volumen que desea eliminar.

Para eliminar un volumen (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación izquierdo, elija Sistemas de archivos y, a continuación, elija el sistema de archivos de ONTAP del que desee eliminar un volumen.
3. Seleccione la pestaña Volúmenes.
4. Elija el volumen que desea eliminar.
5. En Acciones, elija Eliminar.
6. En el cuadro de diálogo de confirmación, para Crear una copia de seguridad final, tiene dos opciones:
   - Seleccione Sí para realizar una copia de seguridad final del volumen. Aparece el nombre de la copia de seguridad final.
   - Seleccione No si no desea realizar una copia de seguridad final del volumen. Se le pedirá que confirme que, una vez eliminado el volumen, las copias de seguridad automáticas dejarán de estar disponibles.
7. Para confirmar la eliminación del volumen, escriba delete en el campo Confirmar eliminación.
8. Seleccione Eliminar volúmenes.

Para eliminar un volumen (CLI)

- Para eliminar un volumen FSx para ONTAP, utilice el comando CLI delete-volume (o la operación DeleteVolumeAPI equivalente), como se muestra en el siguiente ejemplo.

```
aws fsx delete-volume --volume-id fsvol-1234567890abcde
```

Visualización de un volumen

Puede ver los volúmenes de FSx para ONTAP que se encuentran actualmente en su sistema de archivos mediante la consola Amazon FSx, la API y AWS CLI los SDK de Amazon FSx.

Para ver los volúmenes de su sistema de archivos:

- Uso de la consola: elija un sistema de archivos para ver la página de detalles del Sistema de archivos. Seleccione la pestaña Volúmenes para ver todos los volúmenes del sistema de archivos y, a continuación, elija el volumen que desee ver.
- Uso de la CLI o la API: utilice el comando de CLI describe-volumes o DescribeVolumesla operación de API.

Creación de un iSCSI LUN

Este proceso describe cómo crear un LUN iSCSI en un sistema de archivos escalable Amazon FSx for NetApp ONTAP mediante el comando CLI de ONTAP. NetApp lun create Para obtener más información, consulte el Centro de documentación de ONTAP. lun create NetApp

> **Note**
>
> El protocolo iSCSI no es compatible con los sistemas de archivos escalables.

Este proceso supone que ya ha creado un volumen en el sistema de archivos. Para obtener más información, consulte Creación de volúmenes.

1. Para acceder a la CLI de NetApp ONTAP, ejecute el siguiente comando para establecer una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP. Reemplace *management_endpoint_ip* con la dirección IP del puerto de gestión del sistema de archivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obtener más información, consulte Administración de sistemas de archivos con la ONTAP CLI.
2. Cree un LUN mediante el comando lun create NetApp CLI y sustituya los valores siguientes:

- ***svm_name***: el nombre de la máquina virtual de almacenamiento (SVM) que proporciona el destino iSCSI. El host usa este valor para llegar al LUN.
- ***vol_name***: el nombre del volumen que aloja al LUN.
- ***lun_name***: el nombre que desea asignar al LUN.
- ***size***: el tamaño, en bytes, del LUN. El tamaño máximo del LUN que puede crear es de 128 TB.

> **Note**
>
> Le recomendamos que utilice un volumen al menos un 5% mayor que el tamaño de su LUN. Este margen deja espacio para las instantáneas de volumen.

- ***ostype***: el sistema operativo del host, ya sea `windows_2008` o `linux`. Se usa `windows_2008` para todas las versiones de Windows; esto garantiza que el LUN tenga la compensación de bloques adecuada para el sistema operativo y optimiza el rendimiento.

> **Note**
>
> Recomendamos habilitar la asignación de espacio en su LUN. Con la asignación de espacio habilitada, ONTAP puede informar a su host cuando el LUN está agotado y puede recuperar espacio al eliminar datos del LUN.

Para obtener más información, consulte la documentación `lun create`de la CLI de NetApp ONTAP.

```
> lun create -vserver svm_name -path /vol/vol_name/lun_name -size size -
ostype ostype -space-allocation enabled
```

```
Created a LUN of size 10g (10737418240)
```

3. Confirme que el LUN esté creado, conectado y mapeado.

```
> lun show
```

El sistema responde con lo siguiente:

```
Vserver   Path                            State   Mapped   Type         Size
--------- ------------------------------- ------- -------- ------------ --------
svm_name
          /vol/vol_name/lun_name          online  unmapped windows_2008 10GB
```

Siguientes pasos

Ahora que ha creado un iSCSI LUN, el siguiente paso en el proceso de utilizar un iSCSI LUN como almacenamiento de bloques es asignar el LUN a un `igroup`. Para obtener más información, consulte Montaje de LUNs iSCSI en un cliente Linux o Montaje de LUNs iSCSI en un cliente de Windows.

Gestión de recursos compartidos SMB

Para gestionar los archivos compartidos SMB en su sistema de archivos Amazon FSx, puede utilizar la GUI de carpetas compartidas de Microsoft Windows. La GUI de carpetas compartidas proporciona una ubicación central para administrar todas las carpetas compartidas de su máquina virtual de almacenamiento (SVM). Los procedimientos que aparecen a continuación le muestran cómo crear, actualizar y eliminar los archivos compartidos.

> **Note**
>
> También puede gestionar los recursos compartidos de archivos SMB mediante el Administrador del NetApp sistema. Para obtener más información, consulte Uso de NetApp System Manager con BlueXP.

Para conectar carpetas compartidas al sistema de archivos Amazon FSx

1. Lance su instancia de Amazon EC2 y conéctela al Microsoft Active Directory al que está unido su sistema de archivos de Amazon FSx. Para ello, elija uno de los procedimientos siguientes de la Guía de administración AWS Directory Service :

   - Cómo unir fácilmente una instancia EC2 de Windows
   - Cómo unir manualmente una instancia de Windows

2. Conéctese a su instancia como un usuario que es miembro del grupo de administradores del sistema de archivos. Para obtener más información, consulte Conexión con la instancia de Windows en la Guía del usuario de Amazon EC2 para instancias de Windows.
3. Abra el menú Start y ejecute fsmgmt.msc utilizando Run As Administrator. Al hacerlo, se abre la herramienta GUI de carpetas compartidas.
4. En Action, elija Connect to another computer.
5. Para Another computer, introduzca el nombre DNS de su máquina virtual de almacenamiento (SVM), por ejemplo **`netbios_name.corp.example.com`**.

   Para encontrar el nombre DNS de su SVM en la consola de Amazon FSx, elija Storage virtual machines, elija su SVM y desplácese hacia abajo hasta Endpoints hasta que encuentre SMB DNS name. También puede obtener el nombre DNS en la respuesta a la operación de la DescribeStorageVirtualMachinesAPI.
6. Elija OK. A continuación, aparecerá una entrada para su sistema de archivos Amazon FSx en la lista de la herramienta de carpetas compartidas.

Ahora que las carpetas compartidas están conectadas a su sistema de archivos Amazon FSx, puede gestionar los archivos compartidos de Windows en el sistema de archivos con las siguientes acciones:

> **Note**
>
> Le recomendamos que ubique sus recursos compartidos SMB en un volumen que no sea el volumen raíz.

- Create a new file share: en la herramienta de carpetas compartidas, elija Shares en el panel izquierdo para ver los recursos compartidos activos de su sistema de archivos Amazon FSx. Los volúmenes se muestran montados en la ruta elegida durante la creación del volumen. Seleccione New Share y complete el asistente para crear una carpeta compartida.

  Debe crear la carpeta local antes de crear el nuevo recurso compartido de archivos. Puede hacerlo de la siguiente manera:

  - Utilizando la herramienta de carpetas compartidas: elija Browse cuando especifique una ruta de carpeta local, elija Make new folder para crear la carpeta local.
  - Utilizando la línea de comandos:

```
New-Item -Type Directory -Path \\netbios_name.corp.example.com\C
$volume_path\MyNewFolder
```

- Modify a file share: en la herramienta de carpetas compartidas, abra el menú contextual (haga clic con el botón derecho) del recurso compartido de archivos que desea modificar en el panel derecho y elija Properties. Modifique las propiedades y elija OK.
- Remove a file share: en la herramienta de carpetas compartidas, abra el menú contextual (haga clic con el botón derecho) del archivo compartido que desea eliminar y, a continuación, elija Stop Sharing.

> **Note**
>
> Solo es posible eliminar recursos compartidos de archivos desde la GUI si se ha conectado a fsmgmt.msc utilizando el nombre DNS del sistema de archivos Amazon FSx. Si se conectó mediante la dirección IP o el alias DNS del sistema de archivos, la opción Stop Sharing no funcionará y el archivo compartido no se eliminará.

Auditoría de acceso a archivos

Amazon FSx para NetApp ONTAP admite la auditoría de los accesos de los usuarios finales a los archivos y directorios de una máquina virtual de almacenamiento (SVM).

Temas

Descripción general de la auditoría de acceso a archivos

La auditoría de acceso a los archivos le permite registrar los accesos de los usuarios finales a archivos y directorios individuales en función de las políticas de auditoría que defina. La auditoría del acceso a los archivos puede ayudarle a mejorar la seguridad del sistema y reducir el riesgo de acceso no autorizado a los datos del sistema. La auditoría del acceso a los archivos ayuda a sus organizaciones a cumplir con los requisitos de protección de datos, identificar las posibles amenazas de forma temprana y reducir el riesgo de una violación de datos.

En todos los accesos a archivos y directorios, Amazon FSx admite el registro de los intentos exitosos (por ejemplo, si un usuario con permisos suficientes accede correctamente a un archivo), los intentos fallidos o ambos. También puede desactivar la auditoría de acceso a archivos en cualquier momento.

De forma predeterminada, los registros de eventos de auditoría se almacenan en formato de archivo `EVTX`, lo que le permite verlos mediante Microsoft Event Viewer.

Eventos de acceso de pequeñas y medianas empresas que se pueden auditar

En la siguiente tabla se enumeran los eventos de acceso a archivos y carpetas SMB que se pueden auditar.

ID de evento (EVT/EVTX)	Evento	Descripción	Categoría
560/4656	Abrir objeto/Crear objeto	ACCESO A OBJETOS: objeto (archivo o directorio) abierto	Acceso a archivos
563/4659	Abra un objeto con la intención de eliminarlo	ACCESO AL OBJETO: se solicitó el identificador de un objeto (archivo o directorio) con la intención de eliminarlo	Acceso a archivos
564/4660	Eliminar objeto	ACCESO AL OBJETO: eliminar el objeto (archivo o directorio). ONTAP genera este evento cuando un cliente de Windows intenta eliminar el objeto (archivo o directorio)	Acceso a archivos
567/4663	Leer objeto/Escribir objeto/Obtener	ACCESO AL OBJETO: intento de	Acceso a archivos

ID de evento (EVT/ EVTX)	Evento	Descripción	Categoría
	atributos de objeto/Establecer atributos de objeto	acceso al objeto (leer, escribir, obtener un atributo, establecer un atributo). **Note** En este caso, ONTAP sólo audita la primera operación de lectura y la primera operación de escritura SMB (correcta o fallida) en un objeto. Esto evita que ONTAP cree demasiadas entradas de registro cuando un solo cliente abre un objeto y realiza varias operaciones sucesivas de lectura o	

ID de evento (EVT/ EVTX)	Evento	Descripción	Categoría
		escritura en el mismo objeto.	
N/A/4664	Enlace duro	ACCESO AL OBJETO: se intentó crear un enlace duro	Acceso a archivos
N/A/N/A ID de evento ONTAP 9999	Renombrar objeto	ACCESO A OBJETOS: objeto renombrado. Se trata de un evento de ONTAP. Actualmente, Windows no lo admite como evento único.	Acceso a archivos
N/A/N/A ID de evento ONTAP 9998	Desvincular el objeto	ACCESO AL OBJETO: objeto desvinculado. Este es un evento de ONTAP. Actualmente, Windows no lo admite como evento único.	Acceso a archivos

Eventos de acceso a NFS que se pueden auditar

Se pueden auditar los siguientes eventos de acceso a archivos y carpetas de NFS.

- LEER
- OPEN
- CLOSE
- READDIR
- ESCRIBIR
- SETATTR

- CREATE
- LINK
- OPENATTR
- REMOVE
- GETATTR
- VERIFY
- NVERIFY
- RENAME

Descripción general de las tareas para configurar la auditoría de acceso a los archivos

La configuración de FSx para ONTAP para la auditoría de acceso a los archivos implica las siguientes tareas de alto nivel:

1. Conocer los requisitos y consideraciones de la auditoría de acceso a ficheros.
2. Crear una configuración de auditoría en una SVM específica.
3. Habilitar la auditoría en esa SVM.
4. Configurar políticas de auditoría en sus archivos y directorios.
5. Ver los registros de eventos de auditoría después de que FSx for ONTAP los emita.

Los detalles de la tarea se proporcionan en los siguientes procedimientos.

Repita las tareas con cualquier otra SVM del sistema de archivos para el que desee habilitar la auditoría de acceso a los archivos.

Requisitos de auditoría

Antes de configurar y habilitar la auditoría en una SVM, se deben tener en cuenta los siguientes requisitos y consideraciones.

- La auditoría de NFS permite auditar las entradas de control de acceso (ACE) designadas como tipo u, que generan una entrada en el registro de auditoría cuando se intenta acceder al objeto. Para la auditoría de NFS, no hay ningún mapeo entre los bits de modo y las ACE de auditoría. Al

convertir las ACL en bits de modo, se omiten las ACE de auditoría. Al convertir los bits de modo en ACL, no se generan las ACE de auditoría.

- La auditoría depende de la disponibilidad de espacio en los volúmenes de estadificación. (Un volumen de estadificación es un volumen dedicado creado por ONTAP para almacenar archivos de estadificación, que son archivos binarios intermedios en nodos individuales donde se almacenan los registros de auditoría antes de su conversión a un formato de archivo EVTX o XML). Debe asegurarse de que hay espacio suficiente para los volúmenes de estadificación en los agregados que contienen volúmenes auditados.
- La auditoría depende de que haya espacio disponible en el volumen que contiene el directorio donde se almacenan los registros de eventos de auditoría convertidos. Debe asegurarse de que haya suficiente espacio en los volúmenes utilizados para almacenar los registros de eventos. Puede especificar el número de registros de auditoría que desea retener en el directorio de auditoría con el parámetro de `-rotate-limit` al crear una configuración de auditoría, lo que puede ayudar a garantizar que haya suficiente espacio disponible para los registros de auditoría en el volumen.

Crear configuraciones de auditoría en las SVM

Antes de empezar a auditar los eventos de archivos y directorios, debe crear una configuración de auditoría en la máquina virtual de almacenamiento (SVM). Después de crear la configuración de auditoría, debe habilitarla en la SVM.

Antes de usar el comando `vserver audit create` para crear la configuración de auditoría, asegúrese de haber creado un directorio para usarlo como destino de los registros y de que el directorio no tenga enlaces simbólicos. El directorio de destino se especifica con el parámetro `-destination`.

Puede crear una configuración de auditoría que rote los registros de auditoría en función del tamaño del registro o de una programación, de la siguiente manera:

- Para rotar los registros de auditoría en función del tamaño del registro, utilice este comando:

```
vserver audit create -vserver svm_name -destination path [-format {xml|evtx}] [-
rotate-limit integer] [-rotate-size {integer[KB|MB|GB|TB|PB]}]
```

  El siguiente ejemplo crea una configuración de auditoría para la SVM denominada `svm1` que audita las operaciones de los archivos y los eventos de inicio y cierre de sesión de CIFS (SMB) (la

configuración predeterminada) mediante una rotación basada en el tamaño. El formato de registro es EVTX (el predeterminado), los registros se almacenan en el directorio `/audit_log` y tendrá un solo archivo de registro cada vez (con un tamaño máximo de 200 MB).

```
vserver audit create -vserver svm1 -destination /audit_log -rotate-size 200MB
```

- Para rotar los registros de auditoría en función de una programación, utilice este comando:

```
vserver audit create -vserver svm_name -destination path [-format {xml|evtx}]
       [-rotate-limit integer] [-rotate-schedule-month chron_month]
       [-rotate-schedule-dayofweek chron_dayofweek] [-rotate-schedule-
day chron_dayofmonth]
       [-rotate-schedule-hour chron_hour] [-rotate-schedule-minute chron_minute]
```

El parámetro `-rotate-schedule-minute` es obligatorio si va a configurar la rotación de registros de auditoría basada en el tiempo.

En el siguiente ejemplo, se crea una configuración de auditoría para la SVM denominada `svm2` mediante la rotación basada en el tiempo. El formato de registro es EVTX (predeterminado) y los registros de auditoría se rotan mensualmente, a las 12:30 p. m. todos los días de la semana.

```
vserver audit create -vserver svm2 -destination /audit_log -rotate-size 200MB  -
rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour 12 -
rotate-schedule-minute 30
```

Puede usar el parámetro `-format` para especificar si los registros de auditoría se crean en el formato EVTX convertido (el predeterminado) o en el formato de archivo XML. El formato EVTX le permite ver los archivos de registro con Microsoft Event Viewer.

De forma predeterminada, las categorías de eventos que se van a auditar son los eventos de acceso a archivos (tanto SMB como NFS), los eventos de inicio y cierre de sesión de CIFS (SMB) y los eventos de cambio de política de autorización. Puede tener un mayor control sobre los eventos que se van a registrar mediante el parámetro `-events`, que tiene el siguiente formato:

```
-events {file-ops|cifs-logon-logoff|cap-staging|file-share|audit-policy-change|user-
account|authorization-policy-change|security-group}
```

Por ejemplo, el uso de `-events file-share` permite la auditoría de los eventos de uso compartido de archivos.

Para obtener más información sobre el comando `vserver audit create`, consulte Crear una configuración de auditoría.

Habilitar la auditoría en una SVM

Cuando termine de configurar la configuración de auditoría, debe habilitar la auditoría en la SVM. Para ello, utilice el siguiente comando:

```
vserver audit enable -vserver svm_name
```

Por ejemplo, use el siguiente comando para habilitar la auditoría en la SVM denominada `svm1`.

```
vserver audit enable -vserver svm1
```

Puede desactivar la auditoría de acceso en cualquier momento. Por ejemplo, use el siguiente comando para desactivar la auditoría en el SVM denominado `svm4`.

```
vserver audit disable -vserver svm4
```

Al deshabilitar la auditoría, la configuración de auditoría no se elimina en la SVM, lo que significa que puede volver a habilitar la auditoría en esa SVM en cualquier momento.

Configurar las políticas de auditoría de archivos y carpetas

Debe configurar las políticas de auditoría en los archivos y carpetas que desee auditar para los intentos de acceso de los usuarios. Puede configurar políticas de auditoría para supervisar los intentos de acceso correctos y fallidos.

Puede configurar políticas de auditoría tanto para SMB como para NFS. Las políticas de auditoría para pequeñas y medianas empresas y NFS tienen diferentes requisitos de configuración y capacidades de auditoría en función del estilo de seguridad del volumen.

Políticas de auditoría sobre archivos y directorios similares a los de seguridad de NTFS

Puede configurar las políticas de auditoría de NTFS mediante la pestaña Seguridad de Windows o la CLI de ONTAP.

Para configurar las políticas de auditoría de NTFS (pestaña Seguridad de Windows)

Las políticas de auditoría de NTFS se configuran agregando entradas a las SACL de NTFS asociadas a un descriptor de seguridad de NTFS. A continuación, el descriptor de seguridad se

aplica a los archivos y directorios de NTFS. La GUI de Windows gestiona automáticamente estas tareas. El descriptor de seguridad puede contener listas de control de acceso discrecional (DACL) para aplicar permisos de acceso a archivos y carpetas, SACL para la auditoría de archivos y carpetas o ambas.

1. En el menú Herramientas del Explorador de Windows, seleccione Mapear unidad de red.
2. Complete el cuadro Mapear unidad de red:

   a. Elige una letra de Unidad.

   b. En el cuadro Carpeta, escriba el nombre del servidor SMB (CIFS) que contiene el recurso compartido, que contiene los datos que desea auditar y el nombre del recurso compartido.

   c. Elija Finalizar.

   La unidad que ha seleccionado está montada y lista, y la ventana del Explorador de Windows muestra los archivos y carpetas contenidos en el recurso compartido.
3. Seleccione el archivo o directorio para el que desea habilitar el acceso de auditoría.
4. Haga clic con el botón derecho del ratón en el archivo o directorio y, a continuación, seleccione Propiedades.
5. Elija la pestaña Seguridad.
6. Haga clic en Avanzado.
7. Seleccione la pestaña Auditoría.
8. Realice las acciones deseadas:

Si desea…	Haga lo siguiente:
Configurar la auditoría para un nuevo usuario o grupo	1. Elija Agregar. 2. En el cuadro Ingresar el nombre del objeto que desee seleccionar, escriba el nombre del usuario o grupo que desee añadir. 3. Seleccione OK.
Eliminar la auditoría de un usuario o grupo	1. En el cuadro Ingresar el nombre del objeto para seleccionarlo, seleccione el usuario o grupo que desee eliminar. 2. Elija Eliminar. 3. Seleccione OK.

Si desea…	Haga lo siguiente:
	4. Omita el resto de este procedimiento.
Cambie la auditoría de un usuario o grupo	1. En el cuadro Ingresar el nombre del objeto para seleccionar, elija el usuario o grupo que desee cambiar. 2. Elija Editar. 3. Seleccione OK.

Si está configurando la auditoría de un usuario o grupo o está cambiando la auditoría de un usuario o grupo existente, se abre el cuadro Entrada de auditoría del ***objeto***.

9. En el cuadro Aplicar a, seleccione cómo desea aplicar esta entrada de auditoría.

   Si está configurando la auditoría en un solo archivo, el cuadro Aplicar a no está activo, ya que el valor predeterminado es Solo este objeto.

10. En el cuadro Acceso, seleccione lo que desee auditar y si desea auditar los eventos correctos, los eventos fallidos o ambos.

    - Para auditar los eventos exitosos, seleccione la casilla Éxito.
    - Para auditar los eventos de error, seleccione la casilla Fallo.

    Elija las acciones que debe supervisar para cumplir con sus requisitos de seguridad. Para obtener más información acerca de estos eventos auditables, consulte la documentación de Windows. Puede auditoría de los siguientes eventos:

    - Control total
    - Recorre la carpeta o ejecuta el archivo
    - Listar carpeta / leer datos
    - Leer atributos
    - Leer atributos extendidos
    - Crear archivos / escribir datos
    - Crear carpetas / añadir datos
    - Leer atributos
    - Escribir atributos extendidos

- Eliminar subcarpetas y archivos
- Eliminar
- Permisos de lectura
- Cambiar los permisos
- Asumir la responsabilidad

11. Si no desea que la configuración de auditoría se propague a los siguientes archivos y carpetas del contenedor original, seleccione la casilla Aplicar estas entradas de auditoría únicamente a los objetos y/o contenedores de este contenedor.
12. Seleccione Apply (Aplicar).
13. Cuando termine de añadir, eliminar o editar las entradas de auditoría, pulse Aceptar.

    Se cierra el cuadro Entrada de auditoría para el ***objeto***.
14. En el cuadro Auditoría, seleccione la configuración de herencia de esta carpeta. Elija solo el nivel mínimo que proporcione los eventos de auditoría que cumplan con sus requisitos de seguridad.

    Puede elegir una de las siguientes opciones:

    - Seleccione la casilla Incluir entradas de auditoría heredables de la casilla principal de este objeto.
    - Seleccione la casilla Reemplazar todas las entradas de auditoría heredables existentes en todos los descendientes por entradas de auditoría heredables de este objeto.
    - Seleccione ambas casillas.
    - No seleccione ninguna de las casillas.

    Si configura las SACL en un solo archivo, la casilla Reemplazar todas las entradas de auditoría heredables existentes en todos los descendientes por entradas de auditoría heredables de este objeto no aparece en la casilla Auditoría.
15. Seleccione OK (Aceptar).

Para configurar las políticas de auditoría de NTFS (ONTAP CLI)

Mediante la CLI de ONTAP, puede configurar las políticas de auditoría de NTFS sin necesidad de conectarse a los datos mediante un recurso compartido SMB en un cliente de Windows.

- Puede configurar las políticas de auditoría de NTFS mediante la familia de comandos vserver security file-directory.

Por ejemplo, el siguiente comando aplica una política de seguridad denominada p1 al SVM denominado vs0.

```
vserver security file-directory apply -vserver vs0 -policy-name p1
```

Audite las políticas de archivos y directorios de estilo de seguridad de UNIX

Para configurar la auditoría de los archivos y directorios de tipo seguro de UNIX, agregue las ACE de auditoría (expresiones de control de acceso) a las ACL (listas de control de acceso) de NFS v4.x. Esto le permite supervisar determinados eventos de acceso a archivos y directorios de NFS por motivos de seguridad.

> **Note**
>
> En el caso de NFS v4.x, las ACE discrecionales y de sistema se almacenan en la misma ACL. Por lo tanto, debe tener cuidado al agregar las ACE de auditoría a una ACL existente para evitar sobrescribir y perder una ACL existente. No importa el orden en el que se agreguen las ACE de auditoría a una ACL existente.

Para configurar las políticas de auditoría de UNIX

1. Recupere la ACL existente para el archivo o directorio mediante el comando `nfs4_getfacl` o un comando equivalente.
2. Añada las ACE de auditoría deseadas.
3. Aplique la ACL actualizada al archivo o directorio mediante el comando `nfs4_setfacl` o un comando equivalente.

   En este ejemplo, se utiliza la `-a` opción para conceder a un usuario (llamado `testuser`) permisos de lectura sobre el archivo denominado `file1`.

   ```
   nfs4_setfacl -a "A::testuser@example.com:R" file1
   ```

Visualización de los registros de eventos de auditoría

Puede ver los registros de eventos de auditoría guardados en los formatos de archivo `EVTX` o `XML`.

- Formato de archivo `EVTX`: puede abrir los registros de eventos de auditoría `EVTX` convertidos como archivos guardados con Microsoft Event Viewer.

  Hay dos opciones que puede utilizar para ver los registros de eventos con Event Viewer:

  - Vista general: en el registro de eventos se muestra la información común a todos los eventos. No se muestran los datos específicos del evento para el registro del evento. Puede utilizar la vista detallada para mostrar datos específicos del evento.
  - Vista detallada: hay disponibles una vista descriptiva y una vista XML. La vista descriptiva y la vista XML muestran tanto la información común a todos los eventos como los datos específicos del evento para el registro del evento.
- Formato de archivo `XML`: puede ver y procesar los registros de eventos de auditoría XML en aplicaciones de terceros que admiten el formato de archivo XML. Las herramientas de visualización de XML se pueden utilizar para ver los registros de auditoría, siempre que disponga del esquema XML y de la información sobre las definiciones de los campos XML.

Ampliar la capacidad de almacenamiento de las SSD y las IOPS aprovisionadas

Cuando necesite almacenamiento adicional para la parte activa del conjunto de datos, puede aumentar la capacidad de almacenamiento en unidades de estado sólido (SSD) de su sistema de archivos Amazon FSx for NetApp ONTAP. Puede hacerlo mediante la consola de Amazon FSx, la API de Amazon FSx o la AWS Command Line Interface (AWS CLI).

También puede cambiar las IOPS SSD aprovisionadas para su sistema de archivos, ya sea al aumentar la capacidad de almacenamiento de la SSD principal o de forma independiente. Para obtener más información sobre cómo escalar la capacidad de almacenamiento en SSD principal de un sistema de archivos y la cantidad de IOPS aprovisionadas, consulte Actualización del sistema de archivos, el almacenamiento SSD y las IOPS.

Administración de la capacidad de rendimiento

FSx para ONTAP configura la capacidad de rendimiento al crear el sistema de archivos. Puede modificar la capacidad de procesamiento de su sistema de archivos escalable en cualquier momento,

pero no puede modificar la capacidad de rendimiento de su sistema de archivos escalable. Tenga en cuenta que su sistema de archivos requiere una configuración específica para alcanzar la máxima capacidad de rendimiento. Por ejemplo, para aprovisionar una capacidad de rendimiento de 4 GBps para un sistema de archivos escalable, el sistema de archivos requiere una configuración con una capacidad mínima de almacenamiento SSD de 5120 GiB y 160.000 IOPS de SSD. Para más información, consulte Impacto de la capacidad de rendimiento en el rendimiento.

La capacidad de rendimiento es un factor que determina la velocidad a 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 vienen acompañados de niveles más altos de red, operaciones de E/S de lectura de disco por segundo (IOPS) y capacidad de almacenamiento en caché de datos en el servidor de archivos. Para más información, consulte Rendimiento.

Al modificar la capacidad de rendimiento del sistema de archivos, Amazon FSx desactiva el servidor de archivos que alimenta el sistema de archivos. Tanto los sistemas de archivos Single-AZ como los Multi-AZ experimentan una conmutación por error y una conmutación por recuperación automáticas durante este proceso, que normalmente tarda unos minutos en completarse. Los procesos de conmutación por error y conmutación por recuperación son transparentes para los clientes NFS (intercambio de archivos en red), SMB (bloque de mensajes de servidor) e iSCSI (interfaz de sistemas informáticos pequeños de Internet), lo que permite que sus cargas de trabajo sigan ejecutándose sin interrupciones ni intervenciones manuales. Se le facturará por la nueva cantidad de capacidad de rendimiento una vez que esté disponible para su sistema de archivos.

> **Note**
>
> Para garantizar la integridad de los datos durante las actividades de mantenimiento, FSx para ONTAP cierra todos los bloqueos oportunistas y completa todas las operaciones de escritura pendientes en los volúmenes de almacenamiento subyacentes que alojan el sistema de archivos antes de que comience el mantenimiento. Durante una operación programada de mantenimiento del sistema de archivos, las modificaciones del sistema (como las modificaciones de su capacidad de rendimiento) pueden retrasarse. El mantenimiento del sistema puede provocar que estos cambios se pongan en cola hasta que se procesen. Para más información, consulte the section called “Periodos de mantenimiento”.

Temas

- Cuándo modificar la capacidad de rendimiento
- Cómo se gestionan las solicitudes simultáneas de rendimiento y escalado del almacenamiento

Cuándo modificar la capacidad de rendimiento

Amazon FSx se integra con Amazon CloudWatch, lo que le ayuda a supervisar los niveles de uso del rendimiento continuo de su sistema de archivos. El rendimiento y el desempeño de IOPS que puede utilizar en su sistema de archivos dependen de las características específicas de su carga de trabajo, además de la capacidad de rendimiento de su sistema de archivos. Por regla general, debe disponer de una capacidad de rendimiento suficiente para soportar el rendimiento de lectura de la carga de trabajo más el doble del rendimiento de escritura de la carga de trabajo. Puede utilizar CloudWatch las métricas para determinar cuáles de estas dimensiones debe cambiar para mejorar el rendimiento. Para más información, consulte the section called “Cómo utilizar FSx para las métricas de ONTAP CloudWatch”.

> **Note**
>
> No puede modificar la capacidad de rendimiento de los sistemas de archivos escalables.

Cómo se gestionan las solicitudes simultáneas de rendimiento y escalado del almacenamiento

Puede solicitar una actualización de la capacidad de rendimiento justo antes de que comience el flujo de trabajo de actualización de la capacidad de almacenamiento SSD y las IOPS aprovisionadas o mientras está en curso. La secuencia en la que Amazon FSx gestiona las dos solicitudes es la siguiente:

- Si envía una actualización de SSD/IOPS y una actualización de la capacidad de rendimiento al mismo tiempo, se aceptan ambas solicitudes. Se prioriza la actualización de SSD/IOPS antes que la actualización de la capacidad de rendimiento.
- Si envía una actualización de la capacidad de rendimiento mientras hay una actualización de SSD/IOPS en curso, la solicitud de actualización de la capacidad de rendimiento se acepta y se pone en cola para que se produzca después de la actualización de la SSD/IOPS. La actualización de la capacidad de rendimiento comienza después de actualizar el SSD/IOPS (hay nuevos valores disponibles) y durante el paso de optimización. Esto normalmente dura menos de 10 minutos.

- Si envía una actualización de SSD/IOPS mientras se está realizando una actualización de la capacidad de rendimiento, la solicitud de actualización de almacenamiento de SSD/IOPS se acepta y se pone en cola para que comience una vez finalizada la actualización de la capacidad de rendimiento (hay una nueva capacidad de rendimiento disponible). Esto normalmente dura 20 minutos.

Para obtener más información sobre el almacenamiento en SSD y las actualizaciones de IOPS aprovisionadas, consulte Administración de la capacidad de almacenamiento.

Cómo modificar la capacidad de rendimiento

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

Para modificar la capacidad de rendimiento de un sistema de archivos (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Vaya a File systems (Sistemas de archivos) y elija el sistema de archivos ONTAP para el que desee aumentar 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.
4. Seleccione el valor nuevo para la Throughput capacity (Capacidad de rendimiento) de la lista.

   > **Note**
   >
   > Puede cambiar la capacidad de rendimiento de cualquier sistema de archivos de FSx para ONTAP. Sin embargo, sólo los sistemas de archivos creados a partir del 9 de diciembre de 2021 pueden admitir una capacidad de rendimiento de 128 MB/s o 256 MB/s.

5. Seleccione Update (Actualizar) para iniciar la actualización de la capacidad de rendimiento.
6. Puede supervisar el progreso de la actualización en la página de información de los File systems (Sistemas de archivos), en la pestaña Updates (Actualizaciones).

Puede supervisar el progreso de la actualización con la consola Amazon FSx, la AWS CLI y la API. Para más información, consulte Supervisión de los cambios en la capacidad de rendimiento.

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

Para modificar la capacidad de rendimiento de un sistema de archivos, utilice el comando. AWS CLI update-file-system Establezca los siguientes parámetros:

- `--file-system-id` al ID del sistema de archivos que está actualizando.
- `ThroughputCapacity` al valor deseado al que se vaya a actualizar el sistema de archivos.

Puede supervisar el progreso de la actualización con la consola Amazon FSx, AWS CLI y la API. Para más información, consulte Supervisión de los cambios en la capacidad de rendimiento.

Supervisión de los cambios en la capacidad de rendimiento

Puede supervisar el progreso de una modificación de la capacidad de rendimiento con la consola Amazon FSx, la API y la AWS CLI.

Monitoreo de los cambios en la capacidad de rendimiento en la consola

En la pestaña Updates (Actualizaciones) de la ventana File system details (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

Los tipos admitidos son Capacidad de rendimiento, Capacidad de almacenamiento y Optimización del almacenamiento.

Valor de destino

El valor que se desea alcanzar con la modificación de la capacidad de rendimiento del sistema de archivos.

Status

El estado de la actualización vigente. 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.
- Completa: 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 información sobre la causa de un error en el rendimiento del almacenamiento.

Tiempo de solicitud

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

Monitoreo de los cambios con la API y la AWS CLI

Puede ver y supervisar las solicitudes de modificación de la capacidad de rendimiento del sistema de archivos mediante el comando describe-file-systemsCLI y la acción de la DescribeFileSystemsAPI. La matriz de `AdministrativeActions` enumera las 10 acciones de actualización más recientes para cada tipo de acción administrativa. Al modificar la capacidad de rendimiento de un sistema de archivos, se genera una acción administrativa de `FILE_SYSTEM_UPDATE`.

En el siguiente ejemplo se muestra un extracto de la respuesta de un comando de la CLI `describe-file-systems`. El sistema de archivos tiene una capacidad de rendimiento de 128 MB/s y una capacidad de rendimiento objetivo de 256 MB/s.

```
.
.
.
    "ThroughputCapacity": 128,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "OntapConfiguration": {
            "ThroughputCapacity": 256
          }
```

```
        }
    }
]
```

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 `ThroughputCapacity`. Esto se muestra en el siguiente extracto de respuesta de un comando de la CLI describe-file-systems.

```
.
.
.
    "ThroughputCapacity": 256,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "COMPLETED",
        "TargetFileSystemValues": {
          "OntapConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

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.

Optimización del rendimiento con las ventanas de mantenimiento de Amazon FSx

Como servicio totalmente gestionado, FSx para ONTAP realiza el mantenimiento y las actualizaciones de su sistema de archivos de forma periódica. Este mantenimiento no afecta a la mayoría de las cargas de trabajo. En el caso de las cargas de trabajo que son sensibles al rendimiento, en raras ocasiones puede observar un impacto breve (menos de 60 segundos) en el desempeño cuando se lleva a cabo el mantenimiento; Amazon FSx le permite utilizar el período de mantenimiento para controlar cuándo se produce una posible actividad de mantenimiento de este tipo.

Los parches se aplican con poca frecuencia, normalmente una vez cada varias semanas. En el caso de los sistemas de archivos ampliables, la aplicación de parches normalmente solo requiere 30 minutos desde el inicio del período de mantenimiento. En el caso de los sistemas de archivos escalables, la aplicación de parches requiere hasta 90 minutos desde el inicio del período de mantenimiento. Durante estos pocos minutos, los sistemas de archivos realizan automáticamente la conmutación por error y la recuperación. La ventana de mantenimiento se selecciona durante la creación del sistema de ficheros. Si no tiene preferencia horaria, se le asigna una hora de inicio de 30 minutos.

FSx para ONTAP permite ajustar la ventana de mantenimiento según sea necesario para adaptarse a la carga de trabajo y a los requisitos operativos. Puede cambiar la ventana de mantenimiento con la frecuencia que necesite, siempre que se programe uno al menos una vez cada 14 días. Si se publica un parche y no se ha programado una ventana de mantenimiento en un plazo de 14 días, FSx para ONTAP procederá al mantenimiento del sistema de ficheros para garantizar su seguridad y fiabilidad.

> **Note**
>
> Para garantizar la integridad de los datos durante las actividades de mantenimiento, FSx para ONTAP cierra todos los bloqueos oportunistas y completa todas las operaciones de escritura pendientes en los volúmenes de almacenamiento subyacentes que alojan el sistema de archivos antes de que comience el mantenimiento.

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 semanal (consola)

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. Seleccione Sistemas de archivos en la columna de navegación de la izquierda.
3. Elija el sistema de archivos cuyo período de mantenimiento semanal desea cambiar. Aparecerá la página Summary (Resumen) de detalles del sistema de archivos.
4. Seleccione Administration (Administración) para mostrar el panel de Settings (Ajustes) de administración del sistema de archivos.
5. Seleccione Actualizar para que aparezca la ventana Cambiar período de mantenimiento.

6. Ingrese el nuevo día y la hora en que desea que comience el período de mantenimiento semanal.
7. Elija Guardar para guardar los cambios. La nueva hora de inicio del mantenimiento se muestra en el panel de Settings (Configuración) de administración del sistema de archivos.

Para cambiar el período de mantenimiento semanal mediante el comando update-file-systemCLI, consultePara actualizar un sistema de archivos (CLI).

Etiquetar los recursos de Amazon FSx

Para ayudarlo a administrar sus sistemas de archivos y otros recursos de Amazon FSx, puede asignar sus propios metadatos a cada recurso en forma de etiquetas. Con las etiquetas, puede clasificar los recursos de AWS de diversas maneras, por ejemplo, según su finalidad, propietario o entorno. Esta categorización resulta útil cuando se tienen muchos recursos del mismo tipo: se puede identificar rápidamente un recurso específico en función de las etiquetas que se le hayan asignado. En este tema se describe qué son las etiquetas y cómo crearlas.

Temas

- Conceptos básicos de etiquetas
- Etiquetado de los recursos de
- Copiar etiquetas en copias de seguridad
- Restricciones de las etiquetas
- Permisos y etiqueta

Conceptos básicos de etiquetas

Una etiqueta es una marca que se asigna a un recurso de AWS. Cada etiqueta consta de dos partes que define:

- Una clave de etiqueta (por ejemplo, `CostCenter`, `Environment` o `Project`). Las claves de etiqueta distinguen entre mayúsculas y minúsculas.
- Un valor de etiqueta (por ejemplo, `111122223333` o `Production`). Al igual que las claves de etiqueta, los valores de etiqueta distinguen entre mayúsculas y minúsculas. Los valores de las etiquetas son opcionales.

Puede usar etiquetas para clasificar los recursos de AWS de diversas maneras, por ejemplo, según su finalidad, propietario o entorno. Por ejemplo, podría definir un conjunto de etiquetas para los sistemas de archivos Amazon FSx 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. Para obtener más información sobre cómo implementar una estrategia eficaz de etiquetado de recursos, consulte Recursos de etiquetado de AWS en el Referencia general de AWS.

Algunos comportamientos de etiquetado para considerar:

- 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 a `null`.
- 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, el AWS Command Line Interface (AWS CLI) o un SDK AWS, puede hacer lo siguiente:
  - Puede aplicar etiquetas a recursos existentes a través de la acción de la API `TagResource`.
  - Para algunas acciones de creación de recursos, puede especificar etiquetas para un recurso al crear dicho recurso. 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.

    Si no se pueden aplicar etiquetas durante la creación del recurso, Amazon FSx revierte el proceso de creación del recurso. Este comportamiento ayuda a garantizar que los recursos se creen con etiquetas o, de lo contrario, no se creen y que ningún recurso se quede jamás sin etiqueta.

> **Note**
>
> Para etiquetar recursos al crear, se requieren ciertos permisos de AWS Identity and Access Management (IAM). Para obtener más información, consulte Conceder permisos para etiquetar recursos durante la creación.

Etiquetado de los recursos de

Puede etiquetar los recursos de Amazon FSx que existen en la cuenta. Si utiliza la consola de Amazon FSx, puede aplicar etiquetas a los recursos mediante la pestaña Etiquetas de la pantalla correspondiente al recurso. Al crear recursos, puede aplicar la clave de Nombre con un valor y puede aplicar las etiquetas que desee al crear un nuevo sistema de archivos. Sin embargo, aunque la consola organiza los recursos según la clave de Nombre, esta clave no tiene significado semántico para el servicio de Amazon FSx.

En sus políticas de IAM, puede aplicar permisos de nivel de recursos basados en etiquetas a las acciones de la API de Amazon FSx 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. Al utilizar dichos permisos en sus políticas, obtendrá los siguientes beneficios:

- Sus recursos se encuentran debidamente protegidos de la creación.
- Debido a que las etiquetas se aplican inmediatamente a los recursos, 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.

Puede aplicar permisos de nivel de recursos para las acciones `TagResource` y `UntagResource` de la API de Amazon FSx en las políticas de IAM para controlar qué claves y valores de etiquetas se usan en los recursos existentes.

Para obtener más información sobre los permisos requeridos para etiquetar recursos de Amazon FSx en la creación, consulte Conceder permisos para etiquetar recursos durante la creación.

Para obtener más información sobre el uso de etiquetas para restringir el acceso a los recursos de Amazon FSx en las políticas de IAM, consulte Uso de etiquetas para controlar el acceso a los recursos de Amazon FSx .

Para obtener información acerca del etiquetado de recursos para facturación, consulte Uso de etiquetas de asignación de costos en la Guía del usuario de AWS Billing.

Copiar etiquetas en copias de seguridad

Cuando crea o actualiza un volumen en la API de Amazon FSx o AWS CLI, puede habilitar `CopyTagsToBackups` para copiar automáticamente etiquetas de sus volúmenes a las copias de seguridad.

> **Note**
>
> Si especifica etiquetas al crear una copia de seguridad iniciada por el usuario (incluida la etiqueta de nombre cuando crea una copia de seguridad con la consola Amazon FSx), las etiquetas no se copian del volumen, aunque haya activado `CopyTagsToBackups`.

Para obtener más información acerca de las copias de seguridad, consulte Trabajo con copias de seguridad. Para obtener más información sobre habilitar `CopyTagsToBackups`, consulte Para crear un volumen (CLI) y Para actualizar la configuración de un volumen (CLI) en la Guía del usuario de Amazon FSx para NetApp ONTAP o CreateVolume y UpdateVolume en la Referencia de la API de Amazon FSx para NetApp ONTAP.

Restricciones de las etiquetas

Se aplican las siguientes restricciones básicas a las etiquetas:

- El número máximo de etiquetas por recurso es 50.
- La longitud máxima de la clave es de 128 caracteres Unicode en UTF-8.
- La longitud máxima del valor es de 256 caracteres Unicode en UTF-8.
- Los caracteres permitidos en los servicios son: letras, números y espacios representables en UTF-8, además de los siguientes caracteres: `+ - =` (guion) `. _` (guion bajo) `: / @`.
- Para cada recurso, cada clave de etiqueta debe ser única y solo puede tener un valor.
- 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 que etiquetó con una clave de etiqueta llamada `DeleteMe`, debe utilizar la acción `DeleteFileSystem` con el identificador del 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 requeridos para etiquetar recursos de Amazon FSx en la creación, consulte Conceder permisos para etiquetar recursos durante la creación.

Para obtener más información sobre el uso de etiquetas para restringir el acceso a los recursos de Amazon FSx en las políticas de IAM, consulte Uso de etiquetas para controlar el acceso a los recursos de Amazon FSx .

Gestión de los recursos de FSx para ONTAP mediante aplicaciones NetApp

Además de la AWS API y los SDK AWS Management Console AWS CLI, también puede utilizar estas herramientas y aplicaciones de NetApp administración para gestionar sus FSx para los recursos de ONTAP:

Temas

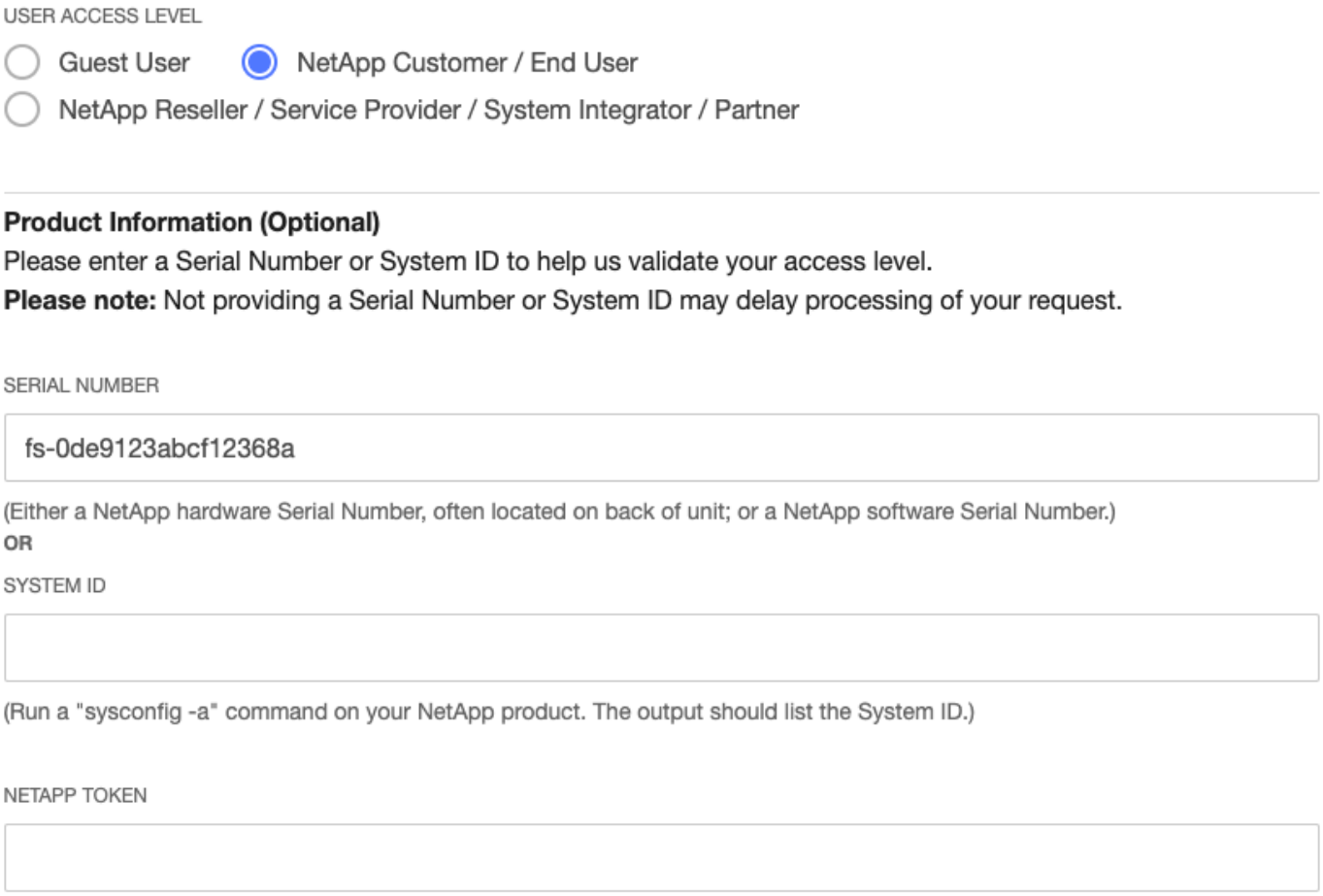
- Registrarse para obtener una cuenta NetApp
- Uso de NetApp BlueXP
- Uso de la NetApp ONTAP CLI
- Uso de la API de REST ONTAP

> **Important**
>
> Amazon FSx se sincroniza periódicamente ONTAP para garantizar la coherencia. Si crea o modifica volúmenes mediante NetApp aplicaciones, estos cambios pueden tardar varios minutos en reflejarse en la AWS Management Console API y AWS CLI los SDK.

Registrarse para obtener una cuenta NetApp

Para descargar algún NetApp software, como BlueXPSnapCenter, y el conector ONTAP antivirus, es necesario tener una NetApp cuenta. Para crear una NetApp cuenta, lleve a cabo los siguientes pasos:

1. Vaya a la página NetAppde registro de usuarios y regístrese para obtener una nueva cuenta NetApp de usuario.
2. Complete los formularios con su información. Asegúrese de seleccionar el nivel de acceso del NetAppcliente/usuario final. En el campo NÚMERO DE SERIE, copie y pegue el ID del sistema de archivos de su sistema de archivos de FSx for ONTAP. Vea el siguiente ejemplo:



Qué esperar después de registrarse

Los clientes con NetApp productos existentes pasarán de tener acceso a la cuenta de NSS al nivel de cliente en el plazo de un día laborable. Los clientes nuevos se NetApp incorporarán siguiendo las prácticas comerciales estándar, además de que su cuenta de NSS se equiparará al acceso a nivel de cliente. Proporcionar el identificador del sistema de archivos ayuda a agilizar este proceso. Para comprobar el estado de su cuenta NSS, inicie sesión en mysupport.netapp.com y vaya a la página de Bienvenida. El nivel de acceso de su cuenta debe ser Acceso al cliente.

Uso de NetApp BlueXP

NetApp BlueXP es un plano de control unificado que simplifica las experiencias de administración de los servicios de almacenamiento y datos en entornos locales y en la nube. BlueXP proporciona una interfaz de usuario centralizada para gestionar, supervisar y automatizar las implementaciones de ONTAP dentro y fuera de las instalaciones. AWS Para obtener más información, consulte la

documentación de NetApp BlueXP y la documentación de NetApp BlueXP for Amazon FSx for ONTAP. NetApp

> **Note**
>
> NetApp BlueXPno es compatible con los sistemas de archivos escalables.

Uso de NetApp System Manager con BlueXP

Puede gestionar sus sistemas de archivos Amazon FSx para NetApp ONTAP mediante System Manager directamente desde. BlueXP BlueXPle permite utilizar la misma interfaz de System Manager a la que está acostumbrado, de forma que pueda gestionar su infraestructura híbrida multinube desde un único plano de control. También tiene acceso a las demás funciones de BlueXP. Para obtener más información, consulte el tema sobre la integración de System Manager con BlueXP en la NetApp documentación de ONTAP.

> **Note**
>
> NetApp System Manager no es compatible con los sistemas de archivos escalables.

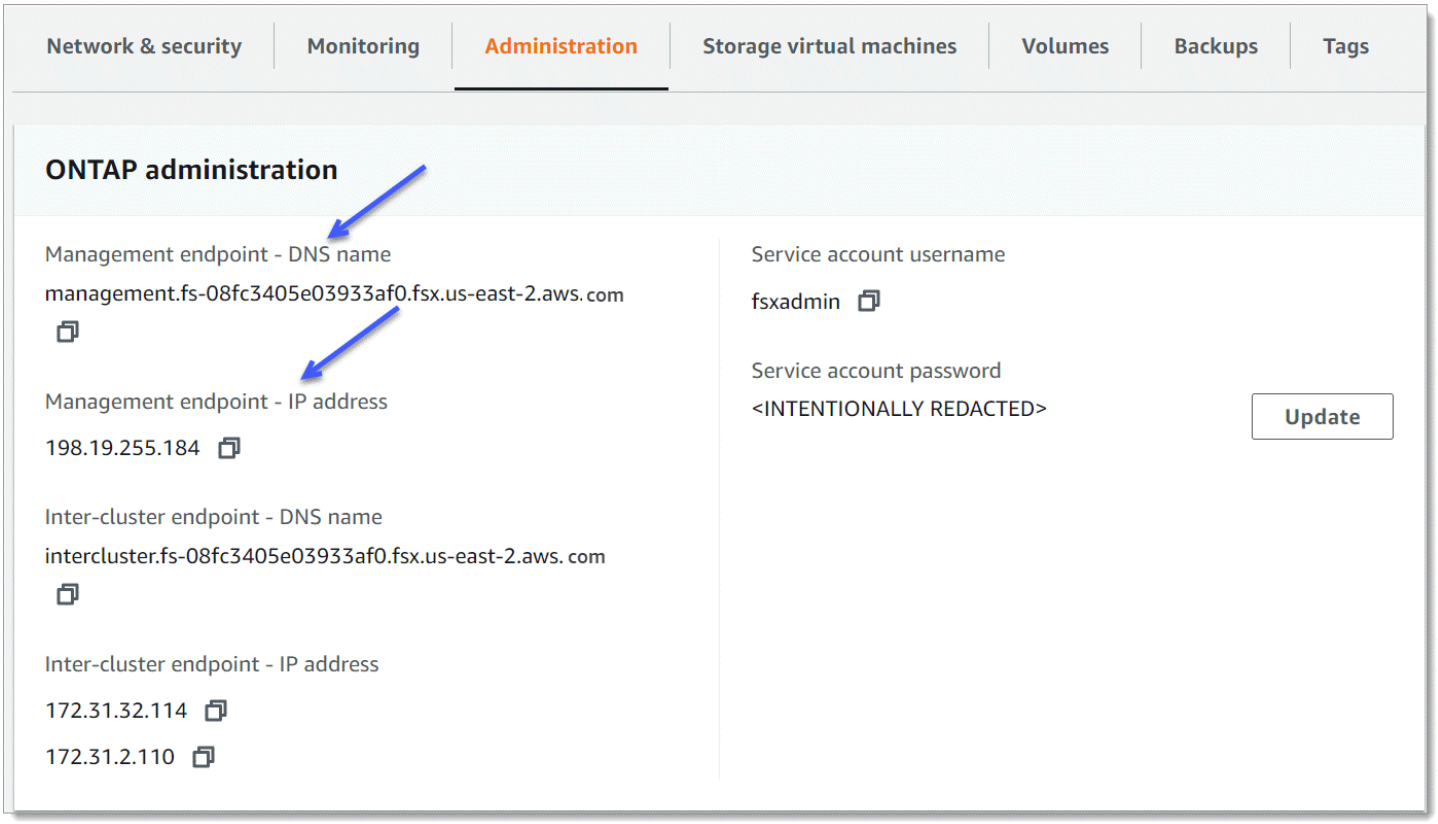
Uso de la NetApp ONTAP CLI

Puede administrar sus recursos de Amazon FSx para NetApp ONTAP mediante la CLI. NetApp ONTAP Puede administrar los recursos en el nivel del sistema de archivos (análogo al clúster de NetApp ONTAP) y en el nivel de SVM.

Administración de sistemas de archivos con la ONTAP CLI

Puede ejecutar comandos ONTAP CLI en su sistema de archivos FSx para ONTAP, de forma análoga a ejecutarlos en un clúster. NetApp ONTAP Para acceder a la ONTAP CLI del sistema de archivos, debe establecer una conexión shell segura (SSH) con el punto final de administración del sistema de archivos e iniciar sesión con el `fsxadmin` nombre de usuario y la contraseña. Tiene la opción de establecer la contraseña al crear el sistema de archivos mediante el flujo de creación personalizado o mediante el AWS CLI. Si creó el sistema de archivos mediante la opción de creación rápida, no se estableció la `fsxadmin` contraseña, por lo que deberá configurar una para iniciar sesión en la CLI de ONTAP. Para obtener más información, consulte Actualización de un sistema

de archivos. Puede encontrar el nombre DNS y la dirección IP del terminal de administración de su sistema de archivos en la consola de Amazon FSx, en la pestaña Administración de la página de detalles del sistema de archivos fSx for ONTAP, que se muestra en el siguiente gráfico.



Para conectarse al terminal de administración del sistema de archivos mediante SSH, utilice el `fsxadmin` usuario y la contraseña. Puede utilizar SSH en la dirección IP del terminal de administración del sistema de archivos o en el nombre de DNS desde un cliente que se encuentre en la misma VPC que el sistema de archivos, como en los ejemplos siguientes.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

El comando SSH con valores de muestra:

```
ssh fsxadmin@198.51.100.0
```

El comando SSH utilizando el nombre DNS del punto de conexión de gestión:

```
ssh fsxadmin@file-system-management-endpoint-dns-name
```

El comando SSH con un nombre DNS de ejemplo:

```
$ ssh fsxadmin@management.fs-0abcdef123456789.fsx.us-east-2.aws.com
  Password: fsxadmin-password

This is your first recorded login.
FsxId0abcdef123456789::>
```

Alcance de los comandos ONTAP CLI disponibles para **`fsxadmin`**

La `fsxadmin` vista administrativa se encuentra en el nivel del sistema de archivos, que incluye todas las SVM y los volúmenes del sistema de archivos. La `fsxadmin` función desempeña la función de administrador del ONTAP clúster. Como los sistemas de archivos Amazon FSx para NetApp ONTAP están completamente gestionados, la `fsxadmin` función puede ejecutar un subconjunto de los comandos CLI disponibles. ONTAP

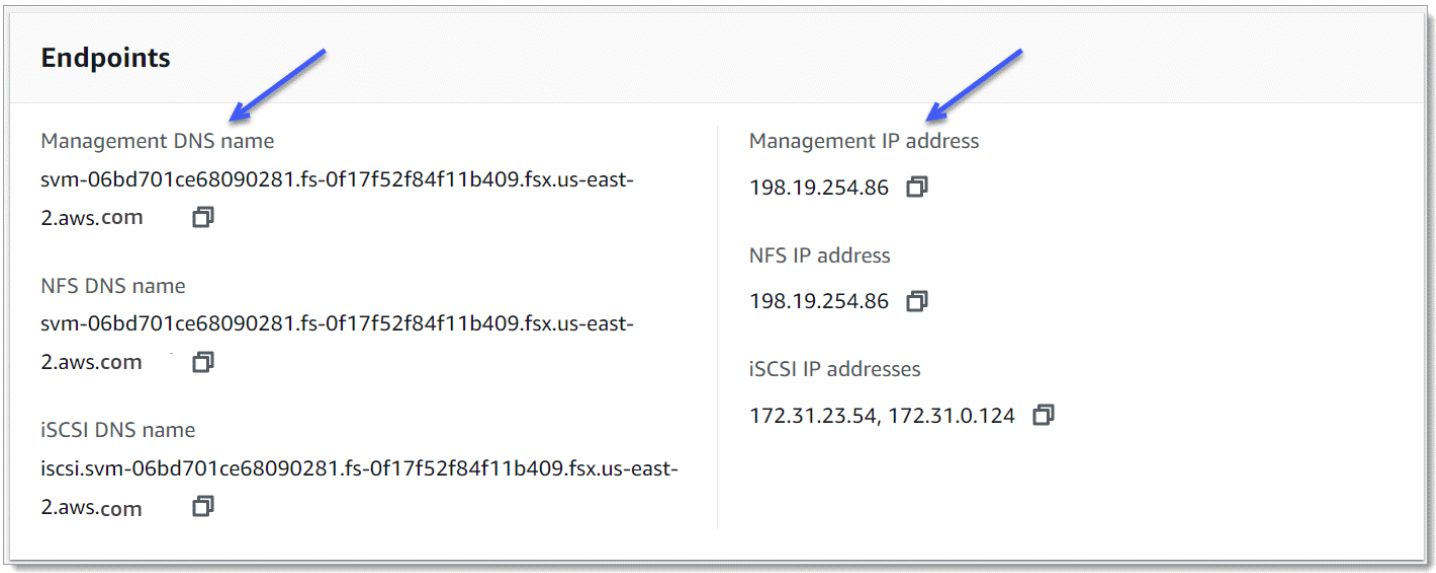
Para ver una lista de los comandos que `fsxadmin` se pueden ejecutar, utilice el siguiente comando [security login role show](ONTAPCLI):

```
FsxId0abc123def456::> security login role show -role fsxadmin -access !none
           Role          Command/                                    Access
Vserver    Name          Directory                             Query Level
---------- ------------- --------- ----------------------------------- --------
FsxId0abcdef123456789
           fsxadmin      application                                   all
                         cluster application-record                    all
                         cluster date show                             readonly
                         cluster ha modify                             readonly
                         cluster ha show                               readonly
                         cluster identity modify                       readonly
                         cluster identity show                         readonly
                         cluster log-forwarding           -port !55555 all
                         cluster modify                                readonly
                         cluster peer                                  all
                         cluster show                                  readonly
                         cluster statistics show                       readonly
                         cluster time-service ntp server create        readonly
                         cluster time-service ntp server delete        readonly
                         cluster time-service ntp server modify        readonly
                         cluster time-service ntp server show          readonly
                         debug network tcpdump       -ipspace !Cluster all
                         debug san lun                                 all
                         df         -vserver !FsxId* -vserver !Cluster readonly
                         echo                                          all
```

```
                          event catalog show                              readonly
                          event config                                    all
.
.
.
363 entries were displayed.
```

Administración de SVM con la CLI ONTAP

Puede acceder a la ONTAP CLI de su SVM estableciendo una conexión shell segura (SSH) con el punto final de administración de la SVM mediante el nombre de usuario y la contraseña `fsxadmin` o el nombre de `vsadmin` usuario. Puede encontrar el nombre DNS y la dirección IP del punto de conexión de la SVM en la consola Amazon FSx, en el panel de puntos finales de la página de detalles de las máquinas virtuales de almacenamiento, que se muestra en el siguiente gráfico.



Para conectarse al terminal de administración de la SVM mediante SSH, puede utilizar el nombre de usuario y la contraseña `vsadmin` o bien el nombre de `fsxadmin` usuario y la contraseña. Si no estableció una contraseña para el `vsadmin` usuario cuando se creó la SVM, puede configurarla en cualquier momento. `vsadmin` Para obtener más información, consulte Actualización de una máquina virtual de almacenamiento. Puede acceder mediante SSH a la SVM desde un cliente que esté en la misma VPC que el sistema de archivos, mediante la dirección IP del punto de conexión de gestión o el nombre DNS.

```
ssh vsadmin@svm-management-endpoint-ip-address
```

El comando con valores de muestra:

```
ssh vsadmin@198.51.100.10
```

El comando SSH utilizando el nombre DNS del punto de conexión de gestión:

```
ssh vsadmin@svm-management-endpoint-dns-name
```

El comando SSH con un nombre DNS de ejemplo:

```
ssh vsadmin@management.svm-abcdef01234567892fs-0abcdef123456789.fsx.us-east-2.aws.com
```

```
Password: vsadmin-password

This is your first recorded login.
FsxId0abcdef123456789::>
```

Amazon FSx para NetApp ONTAP admite los comandos CLINetApp ONTAP.

Para obtener una referencia completa de los comandos NetApp ONTAP CLI, consulte la página de referencia de comandos ONTAP: manual.

Uso de la API de REST ONTAP

Al acceder a su sistema de archivos FSx for ONTAP mediante la API ONTAP REST con las `fsxadmin` credenciales, realice una de las siguientes acciones:

- Desactive la validación de TLS.

  Or (Disyunción)

- Confíe en las autoridades de AWS certificación (CA): el paquete de certificados para las CA de cada región se encuentra en las siguientes direcciones URL:
  - fsx-aws-certificates*https://.s3.amazonaws.com/bundle- aws-region .pem para público* Regiones de AWS
  - fsx-aws-us-govhttps://-certificates.s3. us-gov-west*-1.amazonaws.com/bundle- aws-region .pem para regiones* AWS GovCloud
  - *https://fsx-aws-cn-certificates. s3.cn-north-1.amazonaws.com .cn/ bundle- aws-region .pem para las regiones de China* AWS

Para obtener una referencia completa de los comandos de la API de NetApp ONTAP REST, consulte la referencia en línea de la API de REST. NetApp ONTAP

Seguridad en Amazon FSx para ONTAP NetApp

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener información sobre los programas de conformidad que se aplican a Amazon FSx for NetApp ONTAP, consulte AWS Servicios incluidos en el ámbito de aplicación por programa de conformidad Servicios en el ámbito de programaAWS de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le permite comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Amazon FSx. En los siguientes temas, se mostrará cómo configurar Amazon FSx para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus recursos de Amazon FSx.

Temas

- Utilice NetApp ONTAP Vscan con FSx para ONTAP
- Funciones y usuarios en Amazon FSx para ONTAP NetApp

Protección de datos en Amazon FSx para ONTAP NetApp

El modelo de se aplica a protección de datos en Amazon FSx for NetApp ONTAP. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los. Nube de AWS Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre,

tales como el campo Nombre. Esto incluye cuando trabaja con Amazon FSx u otro dispositivo Servicios de AWS mediante la consola, la API o AWS los AWS CLI SDK. Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Cifrado de datos en FSx para ONTAP

Amazon FSx para NetApp ONTAP admite 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. Amazon FSx para NetApp ONTAP admite el cifrado basado en Kerberos en tránsito a través de los protocolos NFS y SMB si accede a los datos de una máquina virtual de almacenamiento (SVM) que está unida a un Active Directory o a un dominio mediante el Protocolo ligero de acceso a directorios (LDAP).

Cuando utilizar el cifrado

Si su organización está sujeta a políticas corporativas o reglamentarias que exigen el cifrado de los datos y metadatos en reposo, sus datos se cifran automáticamente en reposo. También le recomendamos que habilite el cifrado de los datos en tránsito montando su sistema de archivos mediante el cifrado de los datos en tránsito.

Para obtener más información sobre el cifrado de datos con Amazon FSx para NetApp ONTAP, consulte y. Cifrado de datos en reposo Cifrado de datos en tránsito

Cifrado de datos en reposo

Todos los sistemas de archivos Amazon FSx para NetApp ONTAP están cifrados en reposo con claves administradas mediante AWS Key Management Service ().AWS KMS Los datos se cifran de manera automática antes de escribirse en el sistema de archivos y se descifran de la misma manera a medida que se leen. Estos procesos los administra Amazon FSx de forma transparente, por lo que no tiene que modificar las aplicaciones.

Amazon FSx utiliza un algoritmo de cifrado AES-256 estándar de la industria para cifrar los datos y metadatos en reposo de Amazon FSx. Para obtener más información, consulte los Conceptos básicos de la criptografía en la Guía del desarrollador de AWS Key Management Service .

> **Note**
>
> La infraestructura de administración de AWS claves utiliza algoritmos criptográficos aprobados por la norma federal de procesamiento de información (FIPS) 140-2. La infraestructura se adhiere a las recomendaciones del Instituto Nacional de Normas y Tecnología (NIST) 800-57.

Cómo utiliza Amazon FSx AWS KMS

Amazon FSx se integra con la administración AWS KMS de claves. Amazon FSx utiliza claves KMS para cifrar su sistema de archivos. Usted elige la clave de KMS que se utiliza para cifrar y descifrar los sistemas de archivos (tanto de datos como de metadatos). 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 de KMS gestionada por AWS: Esta es la clave de KMS por defecto y su uso es gratuito.
- clave de KMS gestionada por el cliente: se trata de la clave de KMS más flexible, ya que puede configurar las políticas de claves y concesiones para varios usuarios o servicios. Para obtener más información sobre la creación de claves de KMS, consulte Creación de claves en la Guía para AWS Key Management Service desarrolladores.

> **Important**
>
> Amazon FSx solo admite claves KMS de cifrado simétricas. No puede utilizar claves KMS asimétricas con Amazon FSx.

Si utiliza una clave de KMS gestionada 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 de KMS. Para más información, consulte la sección sobre Rotar AWS KMS keys y Habilitar y deshabilitar claves en la Guía del desarrollador de AWS Key Management Service .

Políticas clave de Amazon FSx para AWS KMS

Las políticas de claves son la forma principal de controlar el acceso a las claves KMS. Para obtener más información sobre 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 AWS KMS relacionados que admite Amazon FSx para los sistemas de archivos cifrados en reposo:

- kms:Encrypt - (opcional): cifra texto plano en texto cifrado. Este permiso está incluido en la política de claves predeterminada.
- kms: Decrypt - (obligatorio): descifra texto cifrado. El texto cifrado es texto plano que se ha cifrado previamente. Este permiso está incluido en la política de claves predeterminada.
- kms: ReEncrypt — (opcional) Cifra los datos del lado del servidor con uno nuevo AWS KMS key, sin exponer el texto sin formato de los datos del lado del cliente. Los datos se descifran en primer lugar y luego se vuelven a cifrar. Este permiso está incluido en la política de claves predeterminada.
- kms: GenerateDataKeyWithoutPlaintext — (Obligatorio) Devuelve una clave de cifrado de datos cifrada con una clave KMS. Este permiso está incluido en la política de claves predeterminada en kms: GenerateDataKey *.
- kms: CreateGrant — (Obligatorio) Añade una concesión a una clave para especificar quién puede utilizarla y en qué condiciones. Las concesiones son mecanismos de permiso alternativo para las políticas de claves. Para obtener más información sobre las concesiones, consulte Uso de concesiones en la Guía para desarrolladores de AWS Key Management Service . Este permiso está incluido en la política de claves predeterminada.
- kms: DescribeKey — (Obligatorio) Proporciona información detallada sobre la clave KMS especificada. Este permiso está incluido en la política de claves predeterminada.
- kms: ListAliases — (opcional) Muestra todos los alias clave de la cuenta. Si utiliza la consola para crear un sistema de archivos cifrados, este permiso rellena la lista de claves 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

En este tema se explican las diferentes opciones disponibles para cifrar los datos de los archivos mientras están en tránsito entre un sistema de archivos FSx for ONTAP y los clientes conectados. También proporciona orientación para ayudarle a elegir el método de cifrado que mejor se adapte a su flujo de trabajo.

Todos los datos que circulan Regiones de AWS por la red AWS global se cifran automáticamente en la capa física antes de salir de las instalaciones AWS seguras. Se cifra todo el tráfico entre las zonas

de disponibilidad. Las capas adicionales de cifrado, incluidas las que aparecen en esta sección, pueden proporcionar una protección adicional. Para obtener más información sobre cómo se AWS protege el flujo de datos entre Regiones de AWS las zonas disponibles y las instancias, consulte Encryption in transit en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux.

Amazon FSx para NetApp ONTAP admite los siguientes métodos para cifrar los datos en tránsito entre los sistemas de archivos fSx for ONTAP y los clientes conectados:

- Cifrado automático basado en Nitro en todos los protocolos y clientes compatibles que se ejecutan en los tipos de instancias de Amazon EC2 de Linux y Windows compatibles.
- Cifrado basado en Kerberos mediante protocolos NFS y SMB.
- Cifrado basado en IPsec mediante protocolos NFS, iSCSI y SMB

Todos los métodos compatibles para cifrar los datos en tránsito utilizan algoritmos criptográficos AES-256 estándar del sector que proporcionan un cifrado de nivel empresarial.

Temas

Elección de un método para cifrar datos en tránsito

En esta sección se proporciona información que puede ayudarle a decidir cuál de los métodos de cifrado en tránsito admitidos es el mejor para su flujo de trabajo. Vuelva a consultar esta sección para explorar las opciones compatibles que se describen en detalle en las secciones siguientes.

Hay varios factores que se deben tener en cuenta a la hora de elegir cómo se van a cifrar los datos en tránsito entre el sistema de archivos de FSx para ONTAP y los clientes conectados. Estos factores incluyen:

- En el Región de AWS que se ejecuta su sistema de archivos FSx for ONTAP.
- Tipo de instancia en la que se ejecuta el cliente.
- La ubicación del cliente que accede al sistema de archivos.
- Requisitos de rendimiento de red.
- El protocolo de datos que desea cifrar.
- Si utiliza Microsoft Active Directory.

Región de AWS

El sistema de archivos en el Región de AWS que se ejecuta determina si puede utilizar o no el cifrado basado en Amazon Nitro. El cifrado basado en Nitro está disponible en las siguientes Regiones de AWS:

- Este de EE. UU. (Norte de Virginia)
- Este de EE. UU. (Ohio)
- Oeste de EE. UU. (Oregón)
- Europa (Irlanda)

Además, el cifrado basado en Nitro está disponible para los sistemas de archivos ampliables de la región Asia-Pacífico (Sídney). Región de AWS

Tipo de instancia del cliente

Puede utilizar el cifrado basado en Amazon Nitro si el cliente que accede a su sistema de archivos se ejecuta en alguno de los tipos de instancias de Amazon EC2 para Mac, Linux o Windows compatibles y su flujo de trabajo cumple todos los demás requisitos para utilizar el cifrado basado en Nitro. No hay ningún requisito de tipo de instancia de cliente para utilizar el cifrado de Kerberos o IPsec.

Ubicación del cliente

La ubicación del cliente que accede a los datos con respecto a la ubicación del sistema de archivos influye en los métodos de cifrado en tránsito disponibles para su uso. Puede usar cualquiera de los métodos de cifrado compatibles si el cliente y el sistema de archivos están ubicados en la misma VPC. Lo mismo ocurre si el cliente y el sistema de archivos se encuentran en una VPC emparejada, siempre que el tráfico no pase a través de un dispositivo o servicio de red virtual, como una puerta de enlace. El cifrado basado en Nitro no está disponible si el cliente

no está en la misma VPC o en una VPC emparejada, o si el tráfico pasa a través de un dispositivo o servicio de red virtual.

Rendimiento de la red

El uso del cifrado basado en Amazon Nitro no tiene impacto en el rendimiento de la red. Esto se debe a que las instancias de Amazon EC2 compatibles utilizan las capacidades de descarga del hardware de Nitro System subyacente para cifrar de manera automática el tráfico en tránsito entre instancias.

El uso del cifrado de Kerberos o IPsec tiene impacto en el rendimiento de la red. Esto se debe a que ambos métodos de cifrado están basados en software, lo que requiere que el cliente y el servidor utilicen recursos de computación para cifrar y descifrar el tráfico en tránsito.

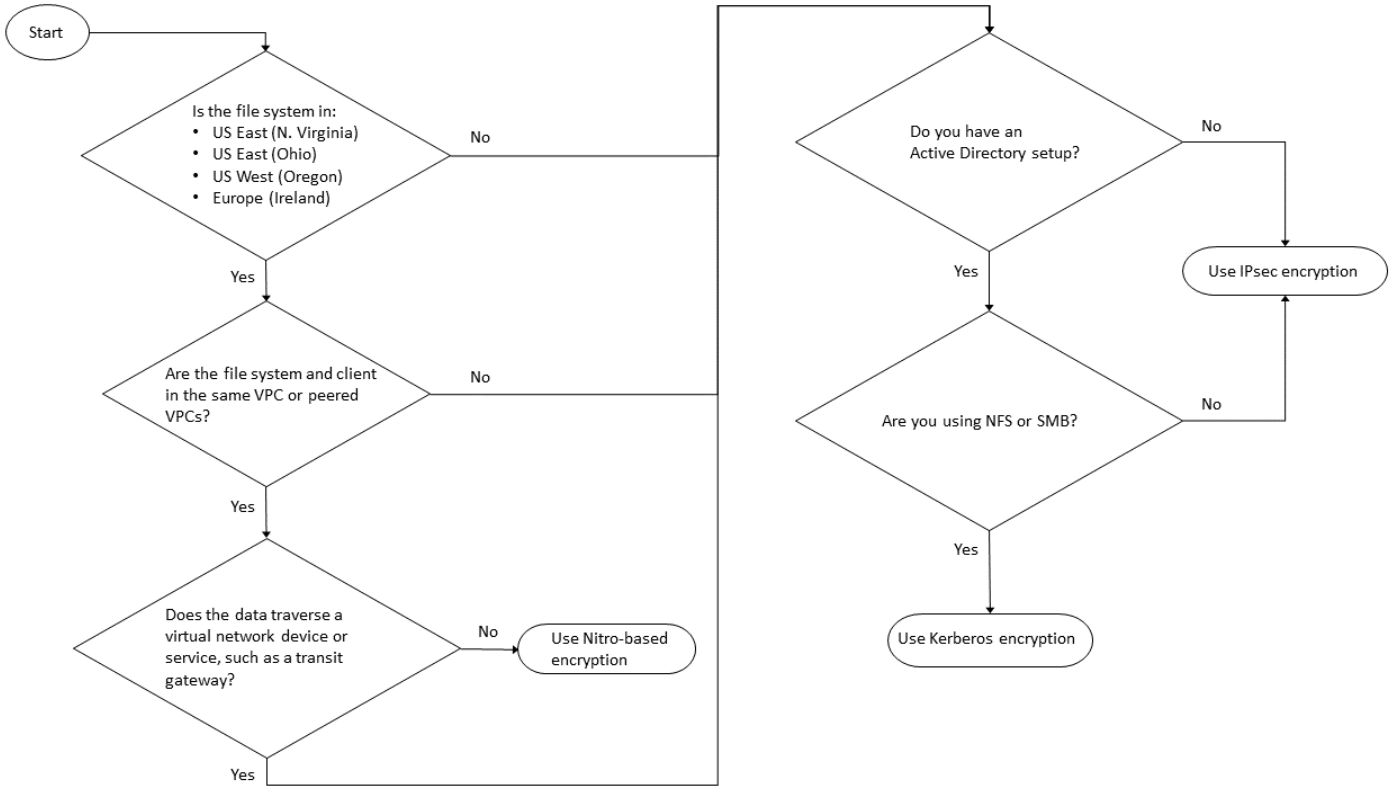
Protocolo de datos

Puede utilizar el cifrado basado en Amazon Nitro y el cifrado de IPsec con todos los protocolos compatibles: NFS, SMB e iSCSI. Puede utilizar el cifrado de Kerberos con los protocolos NFS y SMB (con un Active Directory).

Active Directory

Si utiliza Microsoft Active Directory, puede utilizar el cifrado de Kerberos a través de los protocolos NFS y SMB.

Utilice el siguiente diagrama como ayuda para decidir qué método de cifrado en tránsito debe utilizar.



El cifrado de IPsec es la única opción disponible cuando se cumplen todas las condiciones siguientes al flujo de trabajo:

- Está utilizando el protocolo NFS, SMB o iSCSI.
- Su flujo de trabajo no admite el uso del cifrado basado en Amazon Nitro.
- No está utilizando un dominio de Microsoft Active Directory.

Cifrado de datos en tránsito con Nitro System AWS

Con el cifrado basado en Nitro, los datos en tránsito se cifran automáticamente cuando los clientes que acceden a sus sistemas de archivos utilizan tipos de instancias de Amazon EC2 de Linux o Windows compatibles.

El uso del cifrado basado en Amazon Nitro no tiene impacto en el rendimiento de la red. Esto se debe a que las instancias de Amazon EC2 compatibles utilizan las capacidades de descarga del hardware de Nitro System subyacente para cifrar de manera automática el tráfico en tránsito entre instancias.

El cifrado basado en Nitro se habilita automáticamente cuando los tipos de instancias de cliente compatibles se encuentran en la misma Región de AWS y en la misma VPC o en una VPC emparejada con la VPC del sistema de archivos. Además, si el cliente se encuentra en una VPC emparejada, los datos no pueden atravesar un dispositivo o servicio de red virtual (como una puerta de enlace de tránsito) para que el cifrado basado en Nitro se habilite automáticamente. Para obtener más información sobre el cifrado basado en Nitro, consulte la sección Cifrado en tránsito de la Guía del usuario de Amazon EC2 para tipos de instancia de Linuxhttps://docs.aws.amazon.com/AWSEC2/latest/UserGuide/data-protection.html#encryption-transit o Windows.

El cifrado en tránsito basado en Nitro está disponible para los siguientes sistemas de archivos creados después del 28 de noviembre de 2022: Regiones de AWS

- Este de EE. UU. (Norte de Virginia)
- Este de EE. UU. (Ohio)
- Oeste de EE. UU. (Oregón)
- Europa (Irlanda)

Además, el cifrado basado en Nitro está disponible para los sistemas de archivos ampliables de la región Asia-Pacífico (Sídney). Región de AWS

Para obtener más información sobre Regiones de AWS dónde está disponible fSx para ONTAP, consulte los precios de Amazon FSx for ONTAP. NetApp

Para obtener más información sobre las especificaciones de rendimiento de los sistemas de archivos de FSx para ONTAP, consulte Impacto de la capacidad de rendimiento en el rendimiento.

Cifrado de los datos en tránsito con un cifrado basado en Kerberos

Si usa Microsoft Active Directory, puede usar el cifrado basado en Kerberos a través de los protocolos NFS y SMB para cifrar los datos en tránsito de los volúmenes secundarios de las SVM que están unidas a un Microsoft Active Directory.

Cifrar los datos en tránsito a través de NFS mediante Kerberos

Los protocolos NFSv3 y NFSv4 admiten el cifrado de datos en tránsito mediante Kerberos. Para habilitar el cifrado en tránsito mediante Kerberos para el protocolo NFS, consulte Uso de Kerberos con NFS para una mayor seguridad en el Centro de documentación de NetApp ONTAP.

Cifrar los datos en tránsito a través de SMB mediante Kerberos

El cifrado de los datos en tránsito a través del protocolo SMB se admite en los archivos compartidos que están mapeados en una instancia de procesamiento que admite el protocolo SMB 3.0 o posterior. Esto incluye todas Microsoft Windows las versiones de Microsoft Windows Server 2012 y posteriores, y Microsoft Windows 8 y versiones posteriores. Si está activado, FSx para ONTAP cifra automáticamente los datos en tránsito mediante cifrado SMB a medida que se accede al sistema de archivos, sin necesidad de modificar las aplicaciones.

FSx para ONTAP SMB admite el cifrado de 128 y 256 bits, que se determina mediante la solicitud de sesión del cliente. Para obtener descripciones de los diferentes niveles de cifrado, consulte la sección Establecer el nivel de seguridad de autenticación mínimo del servidor SMB de Gestionar SMB con la CLI en el Centro de documentación de NetApp ONTAP.

> **Note**
>
> El cliente determina el algoritmo de cifrado. Tanto la autenticación de NTLM como la de Kerberos funcionan con el cifrado de 128 y 256 bits. El servidor FSx para ONTAP SMB acepta todas las solicitudes estándar de los clientes de Windows y los controles detallados se gestionan mediante la política de grupo de Microsoft o la configuración del registro.

Utilice la CLI de ONTAP para gestionar la configuración de cifrado en tránsito en FSx para SVM y volúmenes ONTAP. Para acceder a la CLI de NetApp ONTAP, establezca una sesión SSH en la SVM en la que está realizando la configuración de cifrado en tránsito, como se describe en Administración de SVM con la CLI ONTAP.

Para obtener instrucciones sobre cómo habilitar el cifrado SMB en un SVM o volumen, consulte. Habilitar el cifrado SMB de los datos en tránsito

Cifrado de datos en tránsito con cifrado de IPsec

FSx para ONTAP admite el uso del protocolo de IPsec en el modo de transporte para garantizar que los datos estén protegidos y cifrados de forma continua mientras están en tránsito. IPsec ofrece el end-to-end cifrado de los datos en tránsito entre los clientes y FSx para los sistemas de archivos ONTAP para todo el tráfico IP compatible: protocolos NFS, iSCSI y SMB. Con el cifrado de IPsec, se establece un túnel de IPsec entre un FSx para ONTAP SVM configurado con IPsec activado y un cliente de IPsec que se ejecuta en el cliente conectado que accede a los datos.

Le recomendamos que utilice IPsec para cifrar los datos en tránsito a través de los protocolos NFS, SMB e iSCSI al acceder a los datos desde clientes que no admiten el Cifrado basado en Nitro y si su cliente y las SVM no están unidos a un Active Directory, que es necesario para el cifrado basado en Kerberos. El cifrado de IPsec es la única opción disponible para cifrar los datos en tránsito para el tráfico iSCSI cuando el cliente iSCSI no admite el cifrado basado en Nitro.

Para la autenticación de IPsec, puede usar claves previamente compartidas (PSK) o certificados. Si utiliza un PSK, el cliente IPSec que utilice debe ser compatible con la versión 2 del intercambio de claves de Internet (IKEv2) con un PSK. Los pasos de alto nivel para configurar el cifrado IPsec tanto en FSx para ONTAP como para el cliente son los siguientes:

1. Habilite y configure IPsec en su sistema de archivos.
2. Instale y configure IPsec en su cliente
3. Configure IPsec para el acceso de varios clientes

Para obtener más información sobre cómo configurar IPSec mediante PSK, consulte Configuración de la seguridad IP (IPSec) mediante cifrado por cable en el centro de documentación. NetApp ONTAP

Para obtener más información sobre cómo configurar IPSec mediante certificados, consulte. Configuración de IPsec mediante la autenticación PSK

Habilitar el cifrado SMB de los datos en tránsito

De forma predeterminada, al crear un SVM, el cifrado SMB está desactivado. Puede habilitar el cifrado SMB, que se requiere en los recursos compartidos individuales, o bien en una SVM, que lo activa para todos los recursos compartidos de la SVM.

> **Note**
>
> Cuando el cifrado SMB obligatorio está habilitado en una SVM o recurso compartido, los clientes SMB que no admiten el cifrado no pueden conectarse a esa SVM o recurso compartido.

Para requerir el cifrado SMB para el tráfico SMB entrante en una SVM

Utilice el siguiente procedimiento para requerir el cifrado SMB en una SVM mediante la CLI de NetApp ONTAP.

1. Para conectarse al punto de conexión de gestión de la SVM con SSH, utilice el nombre de usuario `vsadmin` y la contraseña de vsadmin que estableció al crear la SVM. Si no estableció una contraseña de vsadmin, utilice el nombre de usuario `fsxadmin` y la contraseña fsxadmin. Puede acceder mediante SSH a la SVM desde un cliente que esté en la misma VPC que el sistema de archivos, mediante la dirección IP del punto de conexión de gestión o el nombre DNS.

   ```
   ssh vsadmin@svm-management-endpoint-ip-address
   ```

   El comando con valores de muestra:

   ```
   ssh vsadmin@198.51.100.10
   ```

   El comando SSH utilizando el nombre DNS del punto de conexión de gestión:

   ```
   ssh vsadmin@svm-management-endpoint-dns-name
   ```

   El comando SSH con un nombre DNS de ejemplo:

   ```
   ssh vsadmin@management.svm-abcdef01234567892fs-08fc3405e03933af0.fsx.us-
   east-2.aws.com
   ```

   ```
   Password: vsadmin-password

   This is your first recorded login.
   FsxIdabcdef01234567892::>
   ```

2. Utilice el comando `vserver cifs security modify`NetApp ONTAPCLI para requerir el cifrado SMB para el tráfico SMB entrante a la SVM.

   ```
   vserver cifs security modify -vserver vserver_name -is-smb-encryption-required true
   ```

3. Para dejar de requerir el cifrado SMB para el tráfico SMB entrante, utilice el siguiente comando.

   ```
   vserver cifs security modify -vserver vserver_name -is-smb-encryption-required
    false
   ```

4. Para ver la `is-smb-encryption-required` configuración actual en una SVM, utilice el comando `vserver cifs security show`NetApp ONTAPCLI:

```
vserver cifs security show -vserver vs1 -fields is-smb-encryption-required

vserver  is-smb-encryption-required
-------- -------------------------
vs1      true
```

Para obtener más información sobre la gestión del cifrado SMB en una SVM, consulte Configurar el cifrado SMB necesario en los servidores SMB para las transferencias de datos a través de SMB en el Centro de documentación de NetApp ONTAP.

Para habilitar el cifrado SMB en un volumen

Utilice el siguiente procedimiento para requerir el cifrado SMB en una SVM mediante la CLI de NetApp ONTAP.

1. Establezca una conexión Secure Shell (SSH) al punto de conexión de gestión de la SVM, tal y como se describe en Administración de SVM con la CLI ONTAP.
2. Utilice el siguiente comando CLI NetApp ONTAP para crear un nuevo recurso compartido SMB y requerir el cifrado SMB al acceder a este recurso compartido.

   ```
   vserver cifs share create -vserver vserver_name -share-name share_name -
   path share_path -share-properties encrypt-data
   ```

   Para obtener más información, consulte vserver cifs share create en las páginas del comando CLI de NetApp ONTAP.
3. Para requerir el cifrado SMB en un recurso compartido de SMB existente, utilice el siguiente comando.

   ```
   vserver cifs share properties add -vserver vserver_name -share-name share_name -
   share-properties encrypt-data
   ```

   Para obtener más información, consulte vserver cifs share create en las páginas del comando CLI de NetApp ONTAP.
4. Para desactivar el cifrado SMB en un recurso compartido SMB existente, utilice el siguiente comando.

```
vserver cifs share properties remove -vserver vserver_name -share-name share_name -
share-properties encrypt-data
```

Para obtener más información, consulte vserver cifs share properties remove en las páginas del comando CLI de NetApp ONTAP.

5. Para ver la configuración actual de `is-smb-encryption-required` de un recurso compartido SMB, utilice el siguiente comando CLI de NetApp ONTAP:

```
vserver cifs share properties show -vserver vserver_name -share-name share_name -
fields share-properties
```

Si una de las propiedades devueltas por el comando es la propiedad `encrypt-data`, dicha propiedad especifica que se debe utilizar el cifrado SMB al acceder a este recurso compartido.

Para obtener más información, consulte vserver cifs share properties show en las páginas del comando CLI de NetApp ONTAP.

Configuración de IPsec mediante la autenticación PSK

Si utiliza PSK para la autenticación, los pasos para configurar el cifrado de IPsec tanto en FSx para ONTAP como para el cliente son los siguientes:

1. Habilite y configure IPsec en su sistema de archivos.
2. Instale y configure IPsec en su cliente
3. Configure IPsec para el acceso de varios clientes

Para obtener información detallada sobre la configuración de IPsec mediante PSK, consulte Configuración de la seguridad IP (IPsec) mediante cifrado por cable en el centro de documentación de NetApp ONTAP.

Configuración de IPsec mediante la autenticación PSK

En los temas siguientes se proporcionan instrucciones para configurar el cifrado IPSec mediante la autenticación por certificado en un sistema de archivos FSx para ONTAP y en un cliente que ejecute Libreswan IPsec. Esta solución utiliza AWS Certificate Manager y crea una entidad AWS Private Certificate Authority de certificación privada y genera los certificados.

Los pasos de alto nivel para configurar el cifrado IPSec mediante la autenticación por certificado en FSx para los sistemas de archivos ONTAP y los clientes conectados son los siguientes:

1. Contar con una autoridad de certificación para emitir los certificados.
2. Genere y exporte los certificados de CA para el sistema de archivos y el cliente.
3. Instale el certificado y configure IPSec en la instancia del cliente.
4. Instale el certificado y configure IPSec en su sistema de archivos.
5. Defina la base de datos de políticas de seguridad (SPD).
6. Configure IPsec para el acceso de varios clientes.

Creación e instalación del certificado para una CA

Para la autenticación de certificados, debe generar e instalar los certificados de una autoridad de certificación en su sistema de archivos de FSx para ONTAP y de los clientes que accederán a los datos de su sistema de archivos. El siguiente ejemplo se utiliza AWS Private Certificate Authority para configurar una entidad de certificación privada y generar los certificados que se van a instalar en el sistema de archivos y en el cliente. Con AWS Private Certificate Authorityél, puede crear una jerarquía completamente AWS alojada de autoridades de certificación (CA) raíz y subordinadas para uso interno de su organización. Este proceso consta de cinco pasos:

1. Cree una autoridad de certificación (CA) privada mediante AWS Private CA
2. Emita e instale el certificado raíz en la CA privada
3. Solicite un certificado privado AWS Certificate Manager para su sistema de archivos y sus clientes
4. Exporte el certificado para el sistema de archivos y los clientes.

Para obtener más información, consulte Administración de una CA privada en la Guía del AWS Private Certificate Authority usuario.

Para crear la CA privada raíz

1. Al crear una CA, debe especificar la configuración de la CA en un archivo que suministre. El siguiente comando utiliza el editor de texto Nano para crear el archivo `ca_config.txt`, que especifica la siguiente información:

   - El nombre del algoritmo
   - El tipo de algoritmo de firma que la CA utiliza para firmar

- La información del sujeto de X.500

```
$ > nano ca_config.txt
```

Aparece el editor de texto.

2. Edite el archivo con las especificaciones de su CA.

```
{
   "KeyAlgorithm":"RSA_2048",
   "SigningAlgorithm":"SHA256WITHRSA",
   "Subject":{
      "Country":"US",
      "Organization":"Example Corp",
      "OrganizationalUnit":"Sales",
      "State":"WA",
      "Locality":"Seattle",
      "CommonName":"*.ec2.internal"
   }
}
```

3. Guarde el archivo y salga del editor de texto. Para obtener más información, consulte el Procedimiento para crear una CA en la Guía del AWS Private Certificate Authority usuario.
4. Utilice el comando create-certificate-authority AWS Private CA CLI para crear una CA privada.

```
~/home > aws acm-pca create-certificate-authority \
     --certificate-authority-configuration file://ca_config.txt \
     --certificate-authority-type "ROOT" \
     --idempotency-token 01234567 --region aws-region
```

Si se ejecuta correctamente, este comando devuelve el nombre de recurso de Amazon (ARN) de la CA.

```
{
   "CertificateAuthorityArn": "arn:aws:acm-pca:aws-region:111122223333:certificate-
authority/12345678-1234-1234-1234-123456789012"
}
```

Para crear e instalar un certificado para su CA raíz privada (AWS CLI)

1. Genere una solicitud de firma de certificado (CSR) mediante el comando `get-certificate-authority-csr` AWS CLI.

```
$ aws acm-pca get-certificate-authority-csr \
     --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
     --output text \
     --endpoint https://acm-pca.aws-region.amazonaws.com \
     --region eu-west-1 > ca.csr
```

   El archivo resultante `ca.csr`, un archivo PEM codificado en formato base64, tiene el siguiente aspecto.

```
-----BEGIN CERTIFICATE-----
 MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
 VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
 b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
 BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
 MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
 VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
 b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
 YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
 21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
 rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
 Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
 nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
 FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
 NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
 -----END CERTIFICATE-----
```

   Para obtener más información, consulte Instalación de un certificado de CA raíz en la Guía del AWS Private Certificate Authority usuario.

2. Utilice el `issue-certificate` AWS CLI comando para emitir e instalar el certificado raíz en su CA privada.

```
$ aws acm-pca issue-certificate \
     --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
     --csr file://ca.csr \
```

```
    --signing-algorithm SHA256WITHRSA \
    --template-arn arn:aws:acm-pca:::template/RootCACertificate/V1 \
    --validity Value=3650,Type=DAYS --region aws-region
```

3. Descargue el certificado raíz mediante el `get-certificate` AWS CLI comando.

```
$ aws acm-pca get-certificate \
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
    --certificate-arn arn:aws:acm-pca:aws-region:486768734100:certificate-
authority/12345678-1234-1234-1234-123456789012/certificate/
abcdef0123456789abcdef0123456789 \
    --output text --region aws-region > rootCA.pem
```

4. Instale el certificado raíz en su CA privada mediante el `import-certificate-authority-certificate` AWS CLI comando.

```
$ aws acm-pca import-certificate-authority-certificate \
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
    --certificate file://rootCA.pem --region aws-region
```

Genere y exporte el sistema de archivos y el certificado de cliente

1. Use el `request-certificate` AWS CLI comando para solicitar un AWS Certificate Manager certificado para usarlo en su sistema de archivos y sus clientes.

```
$ aws acm request-certificate \
    --domain-name *.ec2.internal \
    --idempotency-token 12345 \
    --region aws-region \
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012
```

   Si la solicitud se realiza correctamente, se devuelve el ARN del certificado emitido.

2. Por motivos de seguridad, debe asignar una contraseña a la clave privada al exportarla. Cree una contraseña y guárdela en un archivo llamado `passphrase.txt`

3. Utilice el `export-certificate` AWS CLI comando para exportar el certificado privado emitido anteriormente. El archivo exportado contiene el certificado, la cadena de certificados

y la clave RSA privada cifrada de 2048 bits asociada a la clave pública que está incrustada en el certificado. Por motivos de seguridad, debe asignar una contraseña a la clave privada al exportarla. A continuación se muestra un ejemplo para una instancia EC2 Linux.

```
$ aws acm export-certificate \
     --certificate-arn arn:aws:acm:aws-
region:111122223333:certificate/12345678-1234-1234-1234-123456789012 \
     --passphrase $(cat passphrase.txt | base64)) --region aws-region >
 exported_cert.json
```

4. Utilice los siguientes comandos `jq` para extraer la clave privada y el certificado de la respuesta en formato JSON.

```
$ cat exported_cert.json | jq -r .PrivateKey > prv.key

cat exported_cert.json | jq -r .Certificate > cert.pem
openssl rsa -in prv.key -passin pass:$passphrase -out decrypted.key
```

5. Utilice los siguientes comandos `openssl` para descifrar la clave privada de la respuesta en formato JSON. Después de introducir el comando, se le solicitará la contraseña.

```
$ openssl rsa -in prv.key -passin pass:$passphrase -out decrypted.key
```

Instalación y configuración de Libreswan IPsec en un cliente de Amazon Linux 2

En las siguientes secciones se proporcionan instrucciones para instalar y configurar Libreswan IPsec en una instancia de Amazon EC2 que ejecute Amazon Linux 2.

Para instalar y configurar Libreswan

1. Conéctese a la instancia EC2 mediante SSH. Para obtener instrucciones específicas sobre cómo hacerlo, consulte Conectarse a la instancia de Linux mediante un cliente SSH en la Guía del usuario de Amazon Elastic Compute Cloud para las instancias de Linux.
2. Ejecute el siguiente comando para instalar `libreswan`:

```
$ sudo yum install libreswan
```

3. (Opcional) Al verificar IPsec en un paso posterior, es posible que estas propiedades se marquen sin estos ajustes. Le sugerimos que primero pruebe la configuración sin estas configuraciones. Si tiene problemas de conexión, vuelva a este paso y realice los siguientes cambios.

   Una vez completada la instalación, utilice el editor de texto que prefiera para añadir las siguientes entradas al archivo `/etc/sysctl.conf`.

   ```
   net.ipv4.ip_forward=1
   net.ipv4.conf.all.accept_redirects = 0
   net.ipv4.conf.all.secure_redirects = 0
   net.ipv4.conf.all.send_redirects = 0
   net.ipv4.conf.default.accept_redirects = 0
   net.ipv4.conf.default.send_redirects = 0
   net.ipv4.conf.lo.accept_redirects = 0
   net.ipv4.conf.lo.send_redirects = 0
   net.ipv4.conf.all.rp_filter = 0
   net.ipv4.conf.default.rp_filter = 0
   net.ipv4.conf.eth0.rp_filter = 0
   ```

   Guarde el archivo y salga del editor de texto.

4. Implemente los cambios:

   ```
   $ sudo sysctl -p
   ```

5. Compruebe la configuración de IPsec.

   ```
   $ sudo ipsec verify
   ```

   Compruebe que la versión de `Libreswan` que ha instalado se esté ejecutando.

6. Inicialice la base de datos NSS de IPsec.

   ```
   $ sudo ipsec checknss
   ```

Para instalar los archivos de certificado en el cliente.

1. Copie el certificado que generó para el cliente en el directorio de trabajo de la instancia EC2. Usted
2. Exporte el certificado generado anteriormente a un formato compatible con`libreswan`.

```
$ openssl pkcs12 -export -in cert.pem -inkey decrypted.key \
    -certfile rootCA.pem -out certkey.p12 -name fsx
```

3. Importe la clave reformateada y proporcione la contraseña cuando se le solicite.

```
$ sudo ipsec import certkey.p12
```

4. Cree un archivo de configuración de IPsec mediante el editor de texto preferido.

```
$ sudo cat /etc/ipsec.d/nfs.conf
```

Agregue lo siguiente al archivo de configuración:

```
conn fsxn
    authby=rsasig
    left=172.31.77.6
    right=198.19.254.13
    auto=start
    type=transport
    ikev2=insist
    keyexchange=ike
    ike=aes256-sha2_384;dh20
    esp=aes_gcm_c256
    leftcert=fsx
    leftrsasigkey=%cert
    leftid=%fromcert
    rightid=%fromcert
    rightrsasigkey=%cert
```

Iniciará IPsec en el cliente después de configurar IPsec en su sistema de archivos.

Configuración de IPsec en el sistema de archivos

En esta sección se proporcionan instrucciones sobre la instalación del certificado en el sistema de archivos de FSx para ONTAP y la configuración de IPsec.

Para instalar el certificado en su sistema de archivos

1. Copie los archivos del certificado raíz (`rootCA.pem`)), el certificado de cliente (`cert.pem`) y la clave descifrada (`decrypted.key`) en su sistema de archivos. Necesitará saber la contraseña del certificado.
2. Para acceder a la CLI de NetApp ONTAP, ejecute el siguiente comando para establecer una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP. Reemplace *`management_endpoint_ip`* con la dirección IP del puerto de gestión del sistema de archivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obtener más información, consulte Administración de sistemas de archivos con la ONTAP CLI.
3. Utilice cat en un cliente (no en su sistema de archivos) para mostrar el contenido de los archivos `rootCA.pem`, `cert.pem` y `decrypted.key` de forma que pueda copiar el resultado de cada archivo y pegarlo cuando se le solicite en los siguientes pasos.

   ```
   $ > cat cert.pem
   ```

   Copie el contenido del certificado.
4. Debe instalar todos los certificados de CA utilizados durante la autenticación mutua, incluidas las CA del lado de ONTAP y del lado del cliente, en la gestión de certificados ONTAP, a menos que ya esté instalada (como es el caso de una CA raíz autofirmada de ONTAP).

   Use el comando `security certificate install` NetApp CLI de la siguiente manera para instalar el certificado de cliente:

   ```
   FSxID123:: > security certificate install -vserver dr -type client -cert-name
    ipsec-client-cert
   ```

   ```
   Please enter Certificate: Press <Enter> when done
   ```

   Pegue el contenido del archivo `cert.pem` que copió anteriormente y pulse Entrar.

   ```
   Please enter Private Key: Press <Enter> when done
   ```

Pegue el contenido del archivo `decrypted.key` y pulse Entrar.

```
Do you want to continue entering root and/or intermediate certificates {y|n}:
```

Introduzca n para completar la introducción del certificado de cliente.

5. Cree e instale un certificado para que lo utilice la SVM. La CA emisora de este certificado ya debe estar instalada en ONTAP y agregada a IPSec.

   Utilice el siguiente comando para instalar el certificado raíz.

```
FSxID123:: > security certificate install -vserver dr -type server-ca -cert-name
 ipsec-ca-cert
```

```
Please enter Certificate: Press <Enter> when done
```

   Pegue el contenido del archivo `rootCA.pem` y pulse Entrar.

6. Para asegurarse de que la CA instalada se encuentra dentro de la ruta de búsqueda de la CA de IPsec durante la autenticación, agregue las CA de gestión de certificados ONTAP al módulo de IPsec mediante el comando “security IPsec ca-certificate add”.

   Introduzca el siguiente comando para instalar el certificado raíz.

```
FSxID123:: > security ipsec ca-certificate add -vserver dr -ca-certs ipsec-ca-cert
```

7. Introduzca el siguiente comando para crear la política de IPsec requerida en la base de datos de políticas de seguridad (SPD).

```
security ipsec policy create -vserver dr -name policy-name -local-ip-
subnets 198.19.254.13/32 -remote-ip-subnets 172.31.0.0/16 -auth-method PKI -action
 ESP_TRA -cipher-suite SUITEB_GCM256 -cert-name ipsec-client-cert -local-identity
 "CN=*.ec2.internal" -remote-identity "CN=*.ec2.internal"
```

8. Utilice el siguiente comando para mostrar la política de IPsec para que el sistema de archivos la confirme.

```
FSxID123:: > security ipsec policy show -vserver dr -instance

                                    Vserver: dr
```

```
                                Policy Name: promise
                             Local IP Subnets: 198.19.254.13/32
                            Remote IP Subnets: 172.31.0.0/16
                                  Local Ports: 0-0
                                 Remote Ports: 0-0
                                    Protocols: any
                                       Action: ESP_TRA
                                Cipher Suite: SUITEB_GCM256
          IKE Security Association Lifetime: 86400
        IPsec Security Association Lifetime: 28800
IPsec Security Association Lifetime (bytes): 0
                            Is Policy Enabled: true
                               Local Identity: CN=*.ec2.internal
                              Remote Identity: CN=*.ec2.internal
                        Authentication Method: PKI
             Certificate for Local Identity: ipsec-client-cert
```

Inicie IPsec en el cliente

Ahora que IPsec está configurado tanto en el sistema de archivos de FSx para ONTAP como en el cliente, puede iniciar IPsec en el cliente.

1. Conéctese al sistema cliente mediante SSH.
2. Inicie Eclipse.

```
$ sudo ipsec start
```

3. Compruebe el estado de IPsec.

```
$ sudo ipsec status
```

4. Monte un volumen en el sistema de archivos.

```
$ sudo mount -t nfs 198.19.254.13:/benchmark /home/ec2-user/acm/dr
```

5. Compruebe la configuración de IPsec mostrando la conexión cifrada en su sistema de archivos de FSx para ONTAP.

```
FSxID123:: > security ipsec show-ikesa -node FsxId123
FsxId08ac16c7ec2781a58::> security ipsec show-ikesa -node FsxId08ac16c7ec2781a58-01
            Policy Local           Remote
```

```
Vserver     Name    Address         Address         Initator-SPI     State
----------- ------ -------------- -------------- ---------------- -----------
dr          policy-name
                    198.19.254.13   172.31.77.6     551c55de57fe8976 ESTABLISHED
fsx         policy-name
                    198.19.254.38   172.31.65.193   4fd3f22c993e60c5 ESTABLISHED
2 entries were displayed.
```

Configuración de IPsec para varios clientes

Cuando un número reducido de clientes necesita utilizar IPSec, basta con utilizar una sola entrada de SPD para cada cliente. Sin embargo, cuando cientos o incluso miles de clientes necesiten aprovechar IPsec, le recomendamos que utilice la configuración de varios clientes de IPsec.

FSx para ONTAP admite la conexión de varios clientes de muchas redes a una única dirección IP de SVM con IPsec activado. Para ello, puede utilizar la configuración `subnet` o la configuración `Allow all clients`, que se explican en los siguientes procedimientos:

Para configurar IPsec para varios clientes mediante una configuración de subred

Para permitir que todos los clientes de una subred concreta (192.168.134.0/24, por ejemplo) se conecten a una única dirección IP de SVM mediante una única entrada de política de SPD, debe especificar el `remote-ip-subnets` en forma de subred. Además, debe especificar el campo `remote-identity` con la identidad correcta del lado del cliente.

> **Important**
>
> Al usar la autenticación por certificado, cada cliente puede usar su propio certificado único o un certificado compartido para autenticarse. FSx para ONTAP IPsec comprueba la validez del certificado en función de las CA instaladas en su almacén de confianza local. FSx para ONTAP también admite la comprobación de la lista de revocación de certificados (CRL).

1. Para acceder a la CLI de NetApp ONTAP, ejecute el siguiente comando para establecer una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP. Reemplace *`management_endpoint_ip`* con la dirección IP del puerto de gestión del sistema de archivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

Para obtener más información, consulte Administración de sistemas de archivos con la ONTAP CLI.

2. Utilice el comando CLI de NetApp ONTAP `security ipsec policy create` de la siguiente manera, sustituyendo los valores de *`muestra`* por sus valores específicos.

```
FsxId123456::> security ipsec policy create -vserver svm_name -name policy_name \
  -local-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 \
  -local-ports 2049 -protocols tcp -auth-method PSK \
  -cert-name my_nfs_server_cert -local-identity ontap_side_identity \
  -remote-identity client_side_identity
```

Para configurar IPsec para múltiples clientes utilizando una configuración de permitir todos los clientes

Para permitir que cualquier cliente, independientemente de su dirección IP de origen, se conecte a la dirección IP de SVM habilitada para IPSec, utilice el comodín `0.0.0.0/0` al especificar el campo `remote-ip-subnets`.

Además, debe especificar el campo `remote-identity` con la identidad correcta del lado del cliente. Para la autenticación de certificados, puede introducir `ANYTHING`.

Además, cuando se utiliza el comodín 0.0.0.0/0, debe configurar un número de puerto local o remoto específico para usarlo. Por ejemplo, el puerto NFS 2049.

1. Para acceder a la CLI de NetApp ONTAP, ejecute el siguiente comando para establecer una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP. Reemplace *`management_endpoint_ip`* con la dirección IP del puerto de gestión del sistema de archivos.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Para obtener más información, consulte Administración de sistemas de archivos con la ONTAP CLI.

2. Utilice el comando CLI de NetApp ONTAP `security ipsec policy create` de la siguiente manera, sustituyendo los valores de *`muestra`* por sus valores específicos.

```
FsxId123456::> security ipsec policy create -vserver svm_name -name policy_name \
```

```
-local-ip-subnets 192.168.134.34/32 -remote-ip-subnets 0.0.0.0/0 \
-local-ports 2049 -protocols tcp -auth-method PSK \
-cert-name my_nfs_server_cert -local-identity ontap_side_identity \
-local-ports 2049 -remote-identity client_side_identity
```

Administración de identidades y accesos para Amazon FSx para ONTAP NetApp

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los recursos. AWS Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y autorizarse (tener permisos) para utilizar los recursos de Amazon FSx. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

- Público
- Autenticación con identidades
- Administración de acceso mediante políticas
- Cómo funciona Amazon FSx para NetApp ONTAP con IAM
- Ejemplos de políticas basadas en la identidad de Amazon FSx para ONTAP NetApp
- Solución de problemas de acceso e identidad de Amazon FSx para NetApp ONTAP
- 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 en función del trabajo que se realice en Amazon FSx.

Usuario de servicio: si utiliza el servicio Amazon FSx para realizar su trabajo, el administrador proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Amazon FSx para realizar su trabajo, es posible que necesite permisos adicionales. Entender

cómo se gestiona el acceso puede ayudarlo a solicitar los permisos correctos a su administrador. Si no puede acceder a una característica de Amazon FSx, consulte Solución de problemas de acceso e identidad de Amazon FSx para NetApp ONTAP.

Administrador de servicio: si está a cargo de los recursos de Amazon FSx en su empresa, probablemente tenga acceso completo a Amazon FSx. Es su trabajo determinar a qué características y recursos de Amazon FSx deben tener acceso los usuarios de su servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con Amazon FSx, consulte Cómo funciona Amazon FSx para NetApp ONTAP con IAM.

Administrador de IAM: Si es administrador de IAM, es posible que desee obtener más información sobre cómo escribir políticas para administrar el acceso a Amazon FSx. Para ver ejemplos de políticas basadas en identidad de Amazon FSx que puede utilizar en IAM, consulte Ejemplos de políticas basadas en la identidad de Amazon FSx para ONTAP NetApp .

Autenticación con identidades

La autenticación es la forma de iniciar sesión para AWS usar sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Uso de la autenticación multifactor (MFA) en AWSen la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS Single Sign-On. Puede crear usuarios y grupos en el Centro de identidades de IAM, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como

contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS Single Sign-On.
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.

- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
  - Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.
- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar una AWS función a una instancia EC2 y ponerla a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de

instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de IAM. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una

entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.

- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo AWS determinar si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona Amazon FSx para NetApp ONTAP con IAM

Antes de utilizar IAM para administrar el acceso a Amazon FSx, conozca qué características de IAM están disponibles para su uso con Amazon FSx.

Funciones de IAM que puede utilizar con Amazon NetApp FSx para ONTAP

Característica de IAM	Soporte de Amazon FSx
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
ACL	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Sesiones de acceso directo (FAS)	Sí
Roles de servicio	No
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo funcionan Amazon FSx y otros AWS servicios con la mayoría de las funciones de IAM, consulte los AWS servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas de Amazon FSx basadas en identidad

Compatibilidad con las políticas basadas en identidades	Sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué

condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en identidad para Amazon FSx

Para ver ejemplos de políticas basadas en identidad de Amazon FSx, consulte Ejemplos de políticas basadas en la identidad de Amazon FSx para ONTAP NetApp .

Políticas basadas en recursos de Amazon FSx

Compatibilidad con las políticas basadas en recursos	No

Acciones de políticas para Amazon FSx

Admite acciones de política	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de Amazon FSx, consulte Acciones definidas por Amazon FSx en la Referencia de autorizaciones de servicio.

Las acciones de políticas de Amazon FSx utilizan el siguiente prefijo antes de la acción:

```
fsx
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "fsx:action1",
      "fsx:action2"
         ]
```

Para ver ejemplos de políticas basadas en identidad de Amazon FSx, consulte Ejemplos de políticas basadas en la identidad de Amazon FSx para ONTAP NetApp .

Recursos de políticas para Amazon FSx

Admite recursos de políticas	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de tipos de recursos de Amazon FSx y sus ARN, consulte Tipos de recurso definidos por Amazon FSx en la Referencia de autorizaciones de servicio. Para obtener información

acerca de las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por Amazon FSx.

Para ver ejemplos de políticas basadas en identidad de Amazon FSx, consulte Ejemplos de políticas basadas en la identidad de Amazon FSx para ONTAP NetApp .

Claves de condición de políticas para Amazon FSx

Admite claves de condición de políticas específicas del servicio	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de las claves de condición de Amazon FSx, consulte Claves de condición para Amazon FSx en la Referencia de autorizaciones de servicio. Para obtener más información sobre

las acciones y los recursos con los que puede utilizar una clave de condición, consulte Acciones definidas por Amazon FSx.

Para ver ejemplos de políticas basadas en identidad de Amazon FSx, consulte Ejemplos de políticas basadas en la identidad de Amazon FSx para ONTAP NetApp .

Listas de control de acceso (ACL) de Amazon FSx

Admite las ACL	No

Control de acceso basado en atributos (ABAC) con Amazon FSx

Admite ABAC (etiquetas en las políticas)	Sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte ¿Qué es ABAC? en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Para obtener más información sobre el etiquetado de recursos de Amazon FSx, consulte Etiquetar los recursos de Amazon FSx.

Para consultar un ejemplo de política basada en la identidad para limitar el acceso a un recurso en función de las etiquetas de ese recurso, consulte Uso de etiquetas para controlar el acceso a los recursos de Amazon FSx .

Uso de credenciales temporales con Amazon FSx

Compatible con el uso de credenciales temporales	Sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluidas las que Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para más información sobre el cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Sesiones de acceso directo para Amazon FSx

Admite Forward access sessions (FAS)	Sí

Cuando utiliza un usuario o un rol de IAM para realizar acciones en él AWS, se le considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar

ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Roles de servicio para Amazon FSx

Compatible con roles de servicio	No

Roles vinculado 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 cómo crear o administrar roles vinculados a servicios de Amazon FSx, consulte Uso de roles vinculados a servicios para Amazon FSx.

Ejemplos de políticas basadas en la identidad de Amazon FSx para ONTAP NetApp

De forma predeterminada, los usuarios y roles no tienen permiso para crear ni modificar los recursos de Amazon FSx. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o la API. AWS Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede agregar las políticas de IAM a los roles, y los usuarios pueden asumirlos.

Para obtener información sobre cómo crear una política basada en identidad de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

A fin de obtener más información sobre las acciones y los tipos de recursos definidos por Amazon FSx, incluido el formato de los ARN para cada tipo de recurso, consulte Acciones, recursos y claves de condición para Amazon FSx en la Referencia de autorizaciones de servicio.

Temas

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidad determinan si alguien puede crear, eliminar o acceder a los recursos de Amazon FSx de la cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para

más información, consulte Política de validación de Analizador de acceso de IAM en la Guía de usuario de IAM.

- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de la consola de Amazon FSx

Para acceder a la consola Amazon FSx for NetApp ONTAP, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de Amazon FSx que tiene en su cuenta. Cuenta de AWS Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No necesita conceder permisos mínimos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y las funciones puedan seguir utilizando la consola de Amazon FSx, adjunte también la política `AmazonFSxConsoleReadOnlyAccess` AWS gestionada a las entidades. Para más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Puede consultar esta `AmazonFSxConsoleReadOnlyAccess` y otras políticas de servicios administrados de Amazon FSx en AWS políticas gestionadas para Amazon FSx.

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la AWS CLI API o. AWS

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Solución de problemas de acceso e identidad de Amazon FSx para NetApp ONTAP

Utilice la siguiente información para diagnosticar y solucionar los problemas habituales que pueden surgir cuando se trabaja con Amazon FSx e IAM.

Temas

- No tengo autorización para realizar una acción en Amazon FSx
- No estoy autorizado a realizar tareas como: PassRole

- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Amazon FSx

No tengo autorización para realizar una acción en Amazon FSx

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `fsx:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fsx:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `fsx:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibe un error que indica que no tiene autorización para llevar a cabo la acción `iam:PassRole`, las políticas se deben actualizar para permitirle pasar un rol a Amazon FSx.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Amazon FSx. Sin embargo, la acción requiere que el servicio cuente con permisos que concede un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Amazon FSx

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para saber si Amazon FSx admite estas características, consulte Cómo funciona Amazon FSx para NetApp ONTAP 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 Cuenta de AWS de su propiedad en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Uso de etiquetas con Amazon FSx

Puede utilizar etiquetas para controlar el acceso a los recursos de Amazon FSx e implementar el control de acceso basado en atributos (ABAC). Para aplicar etiquetas a los recursos de Amazon FSx durante la creación, los usuarios deben tener determinados permisos IAM AWS Identity and Access Management .

Conceder permisos para etiquetar recursos durante la creación

Con algunas acciones del API de creación de recursos de Amazon FSx, puede especificar etiquetas al crear el recurso. Puede utilizar estas etiquetas de recursos para implementar el control de acceso basado en atributos (ABAC). Para obtener más información, consulte ¿Para qué sirve ABAC? AWS en la Guía del usuario de IAM.

Para que los usuarios puedan etiquetar recursos en el momento de su creación, deben tener permiso para utilizar la acción que crea el recurso, como `fsx:CreateFileSystem`, `fsx:CreateStorageVirtualMachine` o `fsx:CreateVolume`. 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 máquinas virtuales de almacenamiento (SVM) y aplicarles etiquetas durante la creación en un lugar específico. Cuenta de AWS

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateFileSystem",
         "fsx:CreateStorageVirtualMachine",
         "fsx:TagResource"
      ],
      "Resource": [
         "arn:aws:fsx:region:account-id:file-system/*",
         "arn:aws:fsx:region:account-id:file-system/*/storage-virtual-machine/*"
      ]
    }
  ]
}
```

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 recursos de Amazon FSx, consulte Etiquetar los recursos de Amazon FSx. Para obtener más información sobre cómo usar etiquetas para controlar el acceso a los recursos de Amazon FSx, consulte Uso de etiquetas para controlar el acceso a los recursos de Amazon FSx .

Uso de etiquetas para controlar el acceso a los recursos de Amazon FSx

Para controlar el acceso a los recursos y las acciones de Amazon FSx, puede utilizar políticas de (IAM) basadas en etiquetas. Puede proporcionar este control de dos maneras:

- Puede controlar el acceso a los recursos de Amazon FSx basándose en las etiquetas de dichos recursos.
- Puede controlar qué etiquetas se pueden pasar en una condición de solicitud IAM.

Para obtener 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 acerca del etiquetado de recursos de Amazon FSx en la creación, consulte Conceder permisos para etiquetar recursos durante la creación. Para obtener más información acerca del etiquetado de recursos, consulte Etiquetar los recursos de Amazon FSx.

Control del acceso a un recurso en función de las etiquetas

Para controlar qué acciones puede realizar un usuario o rol en un recurso de Amazon FSx, puede utilizar etiquetas en el recurso. Por ejemplo, es posible que desee permitir o denegar acciones de la API específicas en un recurso del sistema de archivos en función del par clave-valor de la etiqueta del recurso.

Example Ejemplo de política: crear un sistema de archivos únicamente cuando se utiliza 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: cree copias de seguridad únicamente de Amazon FSx para volúmenes NetApp ONTAP con una etiqueta específica

Esta política permite a los usuarios crear copias de seguridad únicamente de los volúmenes FSx para ONTAP etiquetados con el par clave-valor `key=Department`, `value=Finance`. La copia de seguridad se crea con la etiqueta `Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }

    ]
}
```

Example Ejemplo de política: crear un volumen con una etiqueta específica a partir de copias de seguridad con una etiqueta específica

Esta política permite a los usuarios crear volúmenes etiquetados con `Department=Finance` únicamente a partir de copias de seguridad etiquetadas con `Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup",
                "fsx:TagResource"
```

```
            ],
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example Política de ejemplo: eliminar los sistemas de archivos con etiquetas específicas

Esta política permite que un usuario elimine únicamente los sistemas de archivos que estén etiquetados con `Department=Finance`. Si crea una copia de seguridad final, debe etiquetarla con `Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteFileSystem"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example Ejemplo de política: eliminar un volumen con etiquetas específicas

Esta política permite a un usuario eliminar únicamente los sistemas de archivos etiquetados con `Department=Finance`. Si crean una copia de seguridad final, deberá etiquetarse con `Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteVolume"
            ],
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
```

```
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Uso de roles vinculados a servicios para Amazon FSx

Amazon FSx utiliza funciones vinculadas a AWS Identity and Access Management servicios (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que se encuentra vinculado directamente a Amazon FSx. Amazon FSx predefine las funciones vinculadas al servicio e incluyen todos los permisos que el servicio necesita para llamar a otros AWS servicios en su nombre.

Un rol vinculado al servicio simplifica la configuración de Amazon FSx, porque ya no tendrá que agregar manualmente los permisos requeridos. Amazon FSx define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo Amazon FSx puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. De esta forma, se protegen los recursos de Amazon FSx, ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Para obtener información sobre otros servicios que son compatibles con los roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Rol vinculado a servicios. Seleccione una opción Sí con un enlace para ver la documentación sobre el rol vinculado al servicio en cuestión.

Permisos de roles vinculados a servicios para Amazon FSx

Amazon FSx utiliza el rol vinculado al servicio denominado AWSServiceRoleForAmazonFSx—que realiza determinadas acciones en su cuenta, como crear interfaces de red elásticas para sus sistemas de archivos en su VPC y publicar métricas del sistema de archivos y el volumen en ella. CloudWatch

Para ver las actualizaciones de esta política, consulte AmazonF SxServiceRolePolicy

Detalles de los permisos

Detalles de los permisos

Los permisos de los AWSServiceRoleForAmazonFSx roles se definen en la política SxServiceRolePolicy AWS gestionada de AmazonF. AWSServiceRoleForAmazonFSx Tiene los siguientes permisos:

> **Note**
>
> Lo AWSServiceRoleForAmazonFSx utilizan todos los tipos de sistemas de archivos de Amazon FSx; algunos de los permisos enumerados no se aplican a fSx para ONTAP.

- `ds`— Permite a Amazon FSx ver, autorizar y desautorizar las aplicaciones de su directorio. AWS Directory Service
- `ec2`: permite a Amazon FSx realizar lo siguiente:
  - Ver, crear y desasociar las interfaces de red asociadas a un sistema de archivos Amazon FSx.
  - Ver una o varias direcciones IP elásticas asociadas a un sistema de archivos de Amazon FSx.
  - Ver las VPC de Amazon, los grupos de seguridad y las subredes asociadas a un sistema de archivos de Amazon FSx.
  - Proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una VPC.
  - Cree un permiso para que un usuario AWS autorizado realice determinadas operaciones en una interfaz de red.
- `cloudwatch`— Permite a Amazon FSx publicar puntos de datos métricos en el espacio de nombres CloudWatch AWS/FSx.
- `route53`: permite que Amazon FSx asocie una Amazon VPC con una zona alojada privada.
- `logs`— Permite a Amazon FSx describir y escribir en los flujos de registro de CloudWatch Logs. Esto permite a los usuarios enviar los registros de auditoría de acceso a los archivos de un sistema de archivos FSx for Windows File Server a CloudWatch una secuencia de registros.
- `firehose`— Permite a Amazon FSx describir y escribir en las transmisiones de entrega de Amazon Data Firehose. Esto permite a los usuarios publicar los registros de auditoría de acceso a los archivos de un sistema de archivos de Amazon FSx for Windows File Server en una transmisión de entrega de Amazon Data Firehose.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateFileSystem",
            "Effect": "Allow",
            "Action": [
                "ds:AuthorizeApplication",
                "ds:GetAuthorizedApplicationDetails",
                "ds:UnauthorizeApplication",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAddresses",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVPCs",
                "ec2:DisassociateAddress",
                "ec2:GetSecurityGroupsForVpc",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PutMetrics",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/FSx"
                }
            }
        },

        {
            "Sid": "TagResourceNetworkInterface",
            "Effect": "Allow",
```

```
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "AmazonFSx.FileSystemId"
                }
            }
        },
        {
            "Sid": "ManageNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
                }
            }
        },
        {
            "Sid": "ManageRouteTable",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
```

```
                "StringEquals": {
                    "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
                }
            }
        },
        {
            "Sid": "PutCloudWatchLogs",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/fsx/*"
        },
        {
            "Sid": "ManageAuditLogs",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
        }
    ]
}
```

Todas las actualizaciones de esta política están detalladas en Amazon FSx actualiza las políticas gestionadas AWS.

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a un servicio para Amazon FSx

No necesita crear manualmente un rol vinculado a servicios. Al crear un sistema de archivos en la AWS Management Console CLI de IAM o en la API de IAM, Amazon FSx crea automáticamente el rol vinculado al servicio.

> **Important**
>
> Este rol vinculado a servicios puede aparecer en su cuenta si se ha completado una acción en otro servicio que utilice las características compatibles con este rol. Para obtener más información, consulte Un nuevo rol ha aparecido en mi cuenta de IAM.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al crear un sistema de archivos, Amazon FSx vuelve a crear el rol vinculado al servicio por usted.

Edición de un rol vinculado a servicios para Amazon FSx

Amazon FSx no le permite editar el rol vinculado al AWSServiceRoleForAmazonFSx servicio. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminación de un rol vinculado a un servicio para Amazon FSx

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Sin embargo, debe eliminar todos los sistemas de archivo y copias de seguridad para poder eliminar el rol vinculado al servicio de forma manual.

> **Note**
>
> Si el servicio de Amazon FSx utiliza el rol al intentar eliminar los recursos, se podría generar un error en la eliminación. En tal caso, espere unos minutos e intente de nuevo la operación.

Cómo eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM, la CLI de IAM o la API de IAM para eliminar el rol vinculado al AWSServiceRoleForAmazonFSx servicio. Para más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados al servicio de Amazon FSx

Amazon FSx admite el uso de roles vinculados al servicio en todas las regiones en las que se encuentra disponible el servicio. Para obtener más información, consulte Regiones y puntos de conexión de AWS.

AWS políticas gestionadas para Amazon FSx

Una política AWS administrada es una política independiente creada y administrada por. AWS AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

AmazonF SxServiceRolePolicy

Permite a Amazon FSx gestionar los AWS recursos en su nombre. Consulte Uso de roles vinculados a servicios para Amazon FSx para obtener más información.

AWS política gestionada: AmazonF SxDeleteServiceLinkedRoleAccess

No puede asociar `AmazonFSxDeleteServiceLinkedRoleAccess` a sus entidades IAM. Esta política está vinculada a un servicio, y se utiliza únicamente con un rol vinculado a un servicio de dicho servicio. No puede adjuntar, separar, modificar ni eliminar esta política. Para obtener más información, consulte Uso de roles vinculados a servicios para Amazon FSx.

Esta política concede permisos administrativos que permiten a Amazon FSx eliminar su función vinculada a servicios para el acceso a Amazon S3, que solo utiliza Amazon FSx para Lustre.

Detalles de los permisos

Esta política incluye permisos 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, consulta AmazonF SxDeleteServiceLinkedRoleAccess en la Guía de referencia de políticas AWS gestionadas.

AWS política gestionada: AmazonF SxFullAccess

Puede adjuntar AmazonF SxFullAccess a sus entidades de IAM. Amazon FSx también asocia esta política a un rol de servicio que permite a Amazon FSx realizar acciones en su nombre.

Proporciona acceso total a Amazon FSx y acceso a los servicios relacionados AWS .

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `fsx`: permite que las entidades principales tengan acceso completo para realizar todas las acciones de Amazon FSx, excepto `BypassSnaplockEnterpriseRetention`.
- `ds`— Permite a los directores ver información sobre los AWS Directory Service directorios.
- `ec2`
  - Permite a los directores crear etiquetas en las condiciones especificadas.
  - Proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una VPC.
- `iam`: permite que las entidades principales creen un rol vinculado al servicio Amazon FSx en nombre del usuario. Esto es necesario para que Amazon FSx pueda gestionar AWS los recursos en nombre del usuario.
- `logs`: permite que las entidades principales creen grupos de registros, registren flujos y escriban eventos en los flujos de registro. Esto es necesario para que los usuarios puedan supervisar el acceso al sistema de archivos de FSx for Windows File Server enviando los registros de acceso de auditoría CloudWatch a Logs.
- `firehose`— Permite a los directores escribir registros en una Amazon Data Firehose. Esto es necesario para que los usuarios puedan supervisar el acceso al sistema de archivos de FSx for Windows File Server enviando registros de acceso de auditoría a Firehose.

Para ver los permisos de esta política, consulte AmazonF SxFullAccess en la Guía de referencia de políticas AWS administradas.

AWS política gestionada: AmazonF SxConsoleFullAccess

Puede adjuntar la política `AmazonFSxConsoleFullAccess` a las identidades de IAM.

Esta política concede permisos administrativos que permiten el acceso total a Amazon FSx y a los AWS servicios relacionados a través del. AWS Management Console

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `fsx`: permite a las entidades principales realizar todas las acciones en la consola de administración de Amazon FSx, excepto `BypassSnaplockEnterpriseRetention`.
- `cloudwatch`— Permite a los directores ver CloudWatch las alarmas y las métricas en la consola de administración de Amazon FSx.
- `ds`— Permite a los directores enumerar información sobre un directorio. AWS Directory Service
- `ec2`
  - Permite a los directores crear etiquetas en las tablas de enrutamiento, enumerar las interfaces de red, las tablas de enrutamiento, los grupos de seguridad, las subredes y la VPC asociada a un sistema de archivos Amazon FSx.
  - Permite a los directores proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una VPC.
- `kms`— Permite a los directores enumerar los alias de las claves. AWS Key Management Service
- `s3`: permite que las entidades principales creen listas de algunos o todos los objetos de un bucket de Amazon S3 (hasta 1000).
- `iam`: concede permiso para crear un rol de IAM que permite a un servicio de Amazon FSx realizar acciones en su nombre.

Para ver los permisos de esta política, consulta AmazonF SxConsoleFullAccess en la Guía de referencia de políticas AWS gestionadas.

AWS política gestionada: AmazonF SxConsoleReadOnlyAccess

Puede adjuntar la política `AmazonFSxConsoleReadOnlyAccess` a las identidades de IAM.

Esta política concede permisos de solo lectura a Amazon FSx y a los AWS servicios relacionados para que los usuarios puedan ver información sobre estos servicios en. AWS Management Console

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `fsx`: permite que las entidades principales vean información sobre los sistemas de archivos de Amazon FSx, incluidas todas las etiquetas, en la consola de administración de Amazon FSx.
- `cloudwatch`— Permite a los directores ver CloudWatch las alarmas y las métricas en la consola de administración de Amazon FSx.
- `ds`— Permite a los directores ver información sobre un AWS Directory Service directorio en la consola de administración de Amazon FSx.
- `ec2`
  - Permite a los directores ver las interfaces de red, los grupos de seguridad, las subredes y la VPC asociada a un sistema de archivos de Amazon FSx en la consola de administración de Amazon FSx.
  - Proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una VPC.
- `kms`— Permite a los directores ver los alias de AWS Key Management Service las claves en la consola de administración de Amazon FSx.
- `log`— Permite a los directores describir los grupos de CloudWatch registros de Amazon Logs asociados a la cuenta que realiza la solicitud. Esto es necesario para que las entidades principales puedan ver la configuración existente de auditoría de acceso a archivos para un sistema de archivos de FSx para Windows File Server.
- `firehose`— Permite a los directores describir los flujos de entrega de Amazon Data Firehose asociados a la cuenta que realiza la solicitud. Esto es necesario para que las entidades principales puedan ver la configuración existente de auditoría de acceso a archivos para un sistema de archivos de FSx para Windows File Server.

Para ver los permisos de esta política, consulte AmazonF SxConsoleReadOnlyAccess en la Guía de referencia de políticas AWS gestionadas.

AWS política gestionada: AmazonF SxReadOnlyAccess

Puede adjuntar la política `AmazonFSxReadOnlyAccess` a las identidades de IAM.

Esta política incluye los siguientes permisos.

- `fsx`: permite que las entidades principales vean información sobre los sistemas de archivos de Amazon FSx, incluidas todas las etiquetas, en la consola de administración de Amazon FSx.
- `ec2`— Proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una VPC.

Para ver los permisos de esta política, consulte AmazonF SxReadOnlyAccess en la Guía de referencia de políticas AWS administradas.

Amazon FSx actualiza las políticas gestionadas AWS

Consulte los detalles sobre las actualizaciones de las políticas AWS gestionadas para Amazon FSx desde que este servicio comenzó a realizar el seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página Historial de documentos de Amazon FSx para ONTAP NetApp de Amazon FSx.

Cambio	Descripción	Fecha
AmazonF SxServiceRolePolicy: actualización de una política existente	Amazon FSx agregó un nuevo permiso `ec2:GetSecurityGroupsForVpc` que permite a los directores proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una VPC.	9 de enero de 2024
AmazonF SxReadOnlyAccess: actualización a una política existente	Amazon FSx agregó un nuevo permiso `ec2:GetSecurityGroupsForVpc` que permite a los directores proporcionar una validación mejorada de los grupos de seguridad de todos los grupos	9 de enero de 2024

Cambio	Descripción	Fecha
	de seguridad que se pueden usar con una VPC.	
AmazonF SxConsole ReadOnlyAccess: actualización a una política existente	Amazon FSx agregó un nuevo permiso `ec2:GetSecurityGroupsForVpc` que permite a los directores proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una VPC.	9 de enero de 2024
AmazonF SxFullAccess: actualización a una política existente	Amazon FSx agregó un nuevo permiso `ec2:GetSecurityGroupsForVpc` que permite a los directores proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una VPC.	9 de enero de 2024
AmazonF SxConsole FullAccess: actualización a una política existente	Amazon FSx agregó un nuevo permiso `ec2:GetSecurityGroupsForVpc` que permite a los directores proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una VPC.	9 de enero de 2024

Cambio	Descripción	Fecha
AmazonF SxFullAccess: actualización a una política existente	Amazon FSx agregó un nuevo permiso para permitir a los usuarios realizar la replicación de datos entre regiones y cuentas de FSx para los sistemas de archivos OpenZFS.	20 de diciembre de 2023
AmazonF SxConsole FullAccess: actualización de una política existente	Amazon FSx agregó un nuevo permiso para permitir a los usuarios realizar la replicación de datos entre regiones y cuentas de FSx para los sistemas de archivos OpenZFS.	20 de diciembre de 2023
AmazonF SxFullAccess: actualización de una política existente	Amazon FSx agregó un nuevo permiso para permitir a los usuarios realizar la replicación bajo demanda de volúmenes de FSx para sistemas de archivos OpenZFS.	26 de noviembre de 2023
AmazonFSxConsoleFu llAccess: actualización de una política existente	Amazon FSx agregó un nuevo permiso para permitir a los usuarios realizar la replicación bajo demanda de volúmenes de FSx para sistemas de archivos OpenZFS.	26 de noviembre de 2023

Cambio	Descripción	Fecha
AmazonFSxFullAccess: actualización de una política existente	Amazon FSx ha añadido nuevos permisos para que los usuarios puedan ver, activar y desactivar el soporte de VPC compartido para FSx en los sistemas de archivos Multi-AZ de ONTAP.	14 de noviembre de 2023
AmazonF SxConsole FullAccess: actualización de una política existente	Amazon FSx ha añadido nuevos permisos para que los usuarios puedan ver, activar y desactivar el soporte de VPC compartido para FSx en los sistemas de archivos Multi-AZ de ONTAP.	14 de noviembre de 2023
AmazonF SxFullAccess: actualización de una política existente	Amazon FSx añadió nuevos permisos para que Amazon FSx pueda administrar las configuraciones de red de FSx de los sistemas de archivos OpenZFS Multi-AZ.	9 de agosto de 2023
AWS política gestionada: AmazonF SxServiceRolePolicy: actualización a una política existente	Amazon FSx modificó el `cloudwatch:PutMetricData` permiso existente para que Amazon FSx publique CloudWatch métricas en el espacio de nombres. `AWS/FSx`	24 de julio de 2023
AmazonFSxFullAccess: actualización de una política existente	Amazon FSx actualizó la política para eliminar el permiso de `fsx:*` y añadir acciones específicas de `fsx`.	13 de julio de 2023

Cambio	Descripción	Fecha
AmazonF SxConsole FullAccess: actualización a una política existente	Amazon FSx actualizó la política para eliminar el permiso de `fsx:*` y añadir acciones específicas de `fsx`.	13 de julio de 2023
AmazonF SxConsole ReadOnlyAccess: actualiza ción a una política existente	Amazon FSx añadió nuevos permisos para que los usuarios puedan ver las métricas de rendimiento mejoradas y las acciones recomendadas de los sistemas de archivos de FSx para Windows File Server en la consola de Amazon FSx.	21 de septiembre de 2022
AmazonF SxConsole FullAccess: actualización a una política existente	Amazon FSx añadió nuevos permisos para que los usuarios puedan ver las métricas de rendimiento mejoradas y las acciones recomendadas de los sistemas de archivos de FSx para Windows File Server en la consola de Amazon FSx.	21 de septiembre de 2022
AmazonF SxReadOnlyAccess — Se inició la política de seguimiento	Esta política concede acceso de solo lectura a todos los recursos de Amazon FSx y a cualquier etiqueta asociada a ellos.	4 de febrero de 2022

Cambio	Descripción	Fecha
AmazonF SxDeleteServiceLinkedRoleAccess — Se inició la política de seguimiento	Esta política concede permisos administrativos que permiten que Amazon FSx elimine el rol vinculado a servicios para el acceso a Amazon S3.	7 de enero de 2022
AmazonF SxServiceRolePolicy: actualización a una política existente	Amazon FSx ha añadido nuevos permisos que permiten a Amazon FSx gestionar las configuraciones de red de Amazon FSx para los sistemas de archivos ONTAP. NetApp	2 de septiembre de 2021
AmazonFSxFullAccess: actualización de una política existente	Amazon FSx añadió nuevos permisos para que Amazon FSx cree etiquetas en las tablas de enrutamiento de EC2 para llamadas restringidas.	2 de septiembre de 2021
AmazonF SxConsoleFullAccess: actualización a una política existente	Amazon FSx ha añadido nuevos permisos para permitir a Amazon FSx crear Amazon FSx para los sistemas de archivos Multi-AZ de ONTAP. NetApp	2 de septiembre de 2021
AmazonF SxConsoleFullAccess: actualización de una política existente	Amazon FSx añadió nuevos permisos para que Amazon FSx cree etiquetas en las tablas de enrutamiento de EC2 para llamadas restringidas.	2 de septiembre de 2021

Cambio	Descripción	Fecha
AmazonF SxServiceRolePolicy: actualización a una política existente	Amazon FSx ha añadido nuevos permisos para permitir a Amazon FSx describir y escribir en los flujos de registro de Logs. CloudWatch Esto es necesario para que los usuarios puedan ver los registros de auditoría de acceso a los archivos de los sistemas de archivos FSx for Windows File Server CloudWatch mediante registros.	8 de junio de 2021
AmazonF SxServiceRolePolicy: actualización de una política existente	Amazon FSx ha añadido nuevos permisos para permitir a Amazon FSx describir y escribir en las transmisiones de entrega de Amazon Data Firehose. Esto es necesario para que los usuarios puedan ver los registros de auditoría de acceso a los archivos de un sistema de archivos FSx for Windows File Server mediante Amazon Data Firehose.	8 de junio de 2021

Cambio	Descripción	Fecha
AmazonF SxFullAccess: actualización a una política existente	Amazon FSx agregó nuevos permisos para permitir a los directores describir y crear grupos de CloudWatch registros, flujos de registro y escribir eventos en flujos de registro. Esto es necesario para que los directores puedan ver los registros de auditoría de acceso a los archivos de los sistemas CloudWatch de archivos FSx for Windows File Server mediante registros.	8 de junio de 2021
AmazonF SxFullAccess: actualización de una política existente	Amazon FSx ha añadido nuevos permisos para permitir a los directores describir y escribir registros en una Amazon Data Firehose. Esto es necesario para que los usuarios puedan ver los registros de auditoría de acceso a los archivos de un sistema de archivos FSx for Windows File Server mediante Amazon Data Firehose.	8 de junio de 2021

Cambio	Descripción	Fecha
AmazonF SxConsole FullAccess: actualización a una política existente	Amazon FSx ha añadido nuevos permisos para que los directores puedan describir los grupos de CloudWatch registros de Amazon Logs asociados a la cuenta que realiza la solicitud. Esto es necesario para que los directores puedan elegir un grupo de CloudWatch registros existente al configura r la auditoría de acceso a los archivos para un sistema de archivos FSx for Windows File Server.	8 de junio de 2021
AmazonF SxConsole FullAccess: actualización a una política existente	Amazon FSx ha añadido nuevos permisos para que los directores puedan describir las transmisiones de entrega de Amazon Data Firehose asociadas a la cuenta que realiza la solicitud. Esto es necesario para que los directores puedan elegir un flujo de entrega de Firehose existente al configurar la auditoría de acceso a los archivos para un sistema de archivos FSx for Windows File Server.	8 de junio de 2021

Cambio	Descripción	Fecha
AmazonF SxConsole ReadOnlyAccess: actualización a una política existente	Amazon FSx ha añadido nuevos permisos para que los directores puedan describir los grupos de CloudWatch registros de Amazon Logs asociados a la cuenta que realiza la solicitud. Esto es necesario para que las entidades principales puedan ver la configuración existente de auditoría de acceso a archivos para un sistema de archivos de FSx para Windows File Server.	8 de junio de 2021
AmazonF SxConsole ReadOnlyAccess: actualización de una política existente	Amazon FSx ha añadido nuevos permisos para que los directores puedan describir las transmisiones de entrega de Amazon Data Firehose asociadas a la cuenta que realiza la solicitud. Esto es necesario para que las entidades principales puedan ver la configuración existente de auditoría de acceso a archivos para un sistema de archivos de FSx para Windows File Server.	8 de junio de 2021

Cambio	Descripción	Fecha
Amazon FSx inició un seguimiento de los cambios	Amazon FSx comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	8 de junio de 2021

Control de acceso al sistema de archivos con Amazon VPC

Puede acceder a sus sistemas de archivos y SVM de Amazon FSx for NetApp ONTAP mediante el nombre DNS o la dirección IP de uno de sus puntos de enlace, según el tipo de acceso del que se trate. El nombre DNS se asigna a la dirección IP privada de la interfaz de red elástica del sistema de archivos o SVM en su VPC. Solo los recursos de la VPC asociada, o los recursos conectados a la VPC asociada mediante una VPN, pueden acceder a los datos del sistema de archivos a través de los protocolos NFS, SMB AWS Direct Connect o iSCSI. Para obtener más información, consulte ¿Qué es Amazon VPC? en la Guía del usuario de Amazon VPC.

> **Warning**
>
> No debe modificar ni eliminar las interfaces elásticas de red asociadas al 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.

Grupos de seguridad de Amazon VPC

Un grupo de seguridad funciona como un firewall virtual para sus sistemas de ficheros FSx para ONTAP para controlar el tráfico entrante y saliente. Las reglas de entrada controlan el tráfico entrante a su sistema de archivos y las reglas de salida controlan el tráfico saliente de su sistema de archivos. Al crear un sistema de archivos, se especifica la VPC en la que se crea y se aplica el grupo de seguridad predeterminado para esa VPC. Puede añadir reglas a cada grupo de seguridad que permitan el tráfico hacia o desde sus sistemas de archivos y SVM asociadas. Puede modificar las reglas de un grupo de seguridad en cualquier momento. Las reglas nuevas y modificadas se aplican automáticamente a todos los recursos que están asociados al grupo de seguridad. Cuando Amazon FSx decide si permite que el tráfico llegue a un recurso, evalúa todas las reglas de todos los grupos de seguridad asociados al recurso.

Para poder usar un grupo de seguridad para controlar el acceso al sistema de archivos Amazon FSx, agregue las reglas de entrada y salida. Las reglas de entrada controlan el tráfico que ingresa a la instancia, y las de salida, el que sale. Asegúrese de que dispone de las reglas de tráfico de red adecuadas en su grupo de seguridad para asignar el recurso compartido de archivos de su sistema de archivos de Amazon FSx a una carpeta de su instancia de computación compatible.

Para obtener más información sobre las reglas del grupo de seguridad, consulte las Reglas del grupo de seguridad en la Guía del usuario de Amazon EC2 para instancias de Linux.

Creación de un grupo de seguridad de VPC

Para crear un grupo de seguridad para Amazon FSx

1. Abra la consola Amazon EC2 en https://console.aws.amazon.com/ec2.
2. En el panel de navegación, elija Grupos de seguridad.
3. Elija Crear grupo de seguridad.
4. Especifique un nombre y una descripción para el grupo de seguridad.
5. Para la VPC, elija la VPC de Amazon asociada al sistema de archivos para crear el grupo de seguridad dentro de esa VPC.
6. Para las reglas de salida, permita todo el tráfico en todos los puertos.
7. Agregue las siguientes reglas de entrada al grupo de seguridad. Para el campo de source, debe elegir custom e introducir los grupos de seguridad o los rangos de direcciones IP asociados a las instancias que necesitan acceder a su sistema de archivos de FSx para ONTAP, incluidos:

   - Clientes de Linux, Windows o macOS que acceden a los datos de su sistema de archivos a través de NFS, SMB o iSCSI.
   - Cualquier sistema de archivos o clúster de ONTAP que vaya a vincular a su sistema de archivos (por ejemplo, para usar SnapMirror, SnapVault o). FlexCache
   - Cualquier cliente que vaya a utilizar para acceder a la API REST, CLI o ZAPI de ONTAP (por ejemplo, una instancia de Harvest/Grafana, Connector o BlueXP). NetApp NetApp

Protocolo	Puertos	Rol
Todos los ICMP	Todos	Hacer ping a la instancia

Protocolo	Puertos	Rol
SSH	22	Acceso SSH a la dirección IP del LIF de administración del clúster o del LIF de administración de nodos
TCP	111	Llamada a procedimiento remoto para NFS
TCP	135	Llamada a procedimiento remoto para CIFS
TCP	139	Sesión de servicio de NetBIOS para CIFS
TCP	161-162	Protocolo simple de gestión de red (SNMP)
TCP	443	Acceso de la API de REST de ONTAP a la dirección IP del LIF de administración del clúster o a un LIF de administración de SVM
TCP	445	Microsoft SMB/CIFS sobre TCP con entramado de NetBIOS
TCP	635	Montaje NFS
TCP	749	Kerberos
TCP	2049	Daemon de servidor NFS
TCP	3260	Acceso iSCSI a través del LIF de datos iSCSI
TCP	4045	Daemon de bloqueo NFS
TCP	4046	Monitor de estado de red para NFS
TCP	10000	Protocolo de administración de datos de red (NDMP) y NetApp SnapMirror comunicación entre clústeres
TCP	11104	Gestión de la comunicación NetApp SnapMirror entre clústeres
TCP	11105	SnapMirror transferencia de datos mediante LiF entre clústeres

Protocolo	Puertos	Rol
UDP	111	Llamada a procedimiento remoto para NFS
UDP	135	Llamada a procedimiento remoto para CIFS
UDP	137	Resolución de nombres de NetBIOS para CIFS
UDP	139	Sesión de servicio de NetBIOS para CIFS
UDP	161-162	Protocolo simple de gestión de red (SNMP)
UDP	635	Montaje NFS
UDP	2049	Daemon de servidor NFS
UDP	4045	Daemon de bloqueo NFS
UDP	4046	Monitor de estado de red para NFS
UDP	4049	Protocolo de cuotas NFS

8. Agregue el grupo de seguridad a la interfaz de red elástica del sistema de archivos.

Denegar el acceso a un sistema de archivos

Para impedir temporalmente que los clientes tengan acceso de red al sistema de archivos, puede eliminar los grupos de seguridad asociados a las interfaces de red elásticas del sistema de archivos y sustituirlos por un grupo que no tenga reglas de entrada y salida.

Validación de conformidad de Amazon FSx para ONTAP NetApp

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

> **Note**
>
> No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS consumo para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Amazon FSx para NetApp ONTAP y puntos de enlace 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 enlace de VPC de interfaz cuentan con una tecnología que le permite acceder de forma privada a las API de Amazon FSx sin necesidad de una pasarela de Internet, un dispositivo NAT, una conexión VPN o una conexión. AWS PrivateLink AWS Direct Connect Las instancias de la VPC no necesitan direcciones IP públicas para comunicarse con las API de Amazon FSx. El tráfico entre la VPC y Amazon FSx no sale de la red. AWS

Cada punto de conexión de VPC de la interfaz está representado por una o más interfaces de red elásticas en las subredes. Una interfaz de red proporciona una dirección IP privada que sirve como punto de entrada del tráfico dirigido a la API de Amazon FSx.

Consideraciones sobre los puntos de conexión de VPC de interfaz para Amazon FSx

Antes de configurar un punto de conexión de VPC de interfaz para Amazon FSx, revise el tema Propiedades y limitaciones de los puntos de conexión de interfaz en la Guía del usuario de Amazon VPC.

Puede llamar a cualquiera de las operaciones de API de Amazon FSx desde su VPC. Por ejemplo, puede crear un sistema de archivos FSx para ONTAP llamando a la CreateFileSystem API desde su VPC. Para ver la lista completa de las API de Amazon FSx, consulte Actions 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 versiones diferentes. Regiones de AWS

El tráfico entre las VPC interconectadas permanece en la AWS red y no atraviesa la Internet pública. 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 enlace de VPC para la API de Amazon FSx mediante la consola de Amazon VPC o el (). 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 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.

A excepción Regiones de AWS de China, si habilita el DNS privado para el punto de conexión, puede realizar solicitudes de API a Amazon FSx con el punto de enlace de la VPC utilizando su nombre de DNS predeterminado, por ejemplo. Región de AWS`fsx.us-east-1.amazonaws.com` Para China (Pekín) y China (Ningxia) Regiones de AWS, puede realizar solicitudes de API con el punto final de la VPC `fsx-api.cn-north-1.amazonaws.com.cn` mediante `fsx-api.cn-northwest-1.amazonaws.com.cn` y, 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 el acceso a la API de Amazon FSx, puede adjuntar una política AWS Identity and Access Management (IAM) a su punto de enlace 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 más información, consulte Control del acceso a los servicios con puntos de enlace de la VPC en la Guía del usuario de Amazon VPC.

Resiliencia en Amazon FSx para ONTAP NetApp

La infraestructura AWS global se basa Regiones de AWS en distintas zonas de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS

Además de la infraestructura AWS global, Amazon FSx ofrece varias funciones para respaldar sus necesidades de respaldo y resiliencia de datos.

Copia de seguridad y restauración

Amazon FSx crea y guarda copias de seguridad automatizadas de los volúmenes del sistema de archivos Amazon FSx para NetApp ONTAP. Amazon FSx crea copias de seguridad automatizadas de sus volúmenes durante la ventana de copia de seguridad de su sistema de archivos Amazon FSx para NetApp ONTAP. Amazon FSx guarda las copias de seguridad automatizadas de la instancia de base de datos en función del periodo de retención de copia de seguridad especificado. Además, puede realizar una copia de seguridad de los volúmenes manualmente, mediante la creación de una copia de seguridad iniciada por el usuario. Para restaurar una copia de seguridad de un volumen en cualquier momento, debe crear un volumen nuevo con la copia de seguridad especificada como origen.

Para obtener más información, consulte Trabajo con copias de seguridad.

Instantáneas

Amazon FSx crea copias instantáneas del Amazon FSx para los volúmenes de ONTAP. NetApp Las copias instantáneas ofrecen protección contra la eliminación o modificación accidental de los archivos de sus volúmenes por parte de los usuarios finales. Para obtener más información, consulte Uso de instantáneas.

Zonas de disponibilidad

Los sistemas de archivos Amazon FSx para NetApp ONTAP están diseñados para ofrecer una disponibilidad continua de los datos incluso en caso de que se produzca un fallo en el servidor. Cada sistema de archivos funciona con dos servidores de archivos en al menos una zona de disponibilidad, cada uno con su propio almacenamiento. Amazon FSx replica automáticamente sus datos para protegerlos de posibles fallos en los componentes, monitorea de forma continua los fallos de hardware y reemplaza automáticamente los componentes de la infraestructura en caso de que se produzca un fallo. Los sistemas de archivos conmutan automáticamente cuando es necesario (normalmente en 60 segundos) y los clientes conmutan automáticamente con el sistema de archivos.

Sistemas de archivos de Multi-AZ

Los sistemas de archivos Amazon FSx para NetApp ONTAP ofrecen una alta disponibilidad y durabilidad en todas las zonas de AWS disponibilidad, y están diseñados para proporcionar una disponibilidad continua de los datos incluso en el caso de que una zona de disponibilidad no esté disponible.

Para obtener más información, consulte Disponibilidad y durabilidad.

Sistemas de archivos Single-AZ

Los sistemas de archivos Amazon FSx para NetApp ONTAP ofrecen una alta disponibilidad y durabilidad dentro de una única zona de AWS disponibilidad, y están diseñados para ofrecer una disponibilidad continua dentro de esa zona de disponibilidad en caso de que se produzca un fallo en un servidor de archivos individual o en un disco.

Para obtener más información, consulte Disponibilidad y durabilidad.

Seguridad de infraestructura en Amazon FSx para ONTAP NetApp

Como servicio gestionado, Amazon FSx para NetApp ONTAP está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a Amazon FSx a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Utilice NetApp ONTAP Vscan con FSx para ONTAP

Puede utilizar la función Vscan de NetApp ONTAP para ejecutar software antivirus de terceros compatible. Para obtener más información, consulte los siguientes recursos para cada una de las soluciones compatibles.

- McAfee — Guía de soluciones antivirus para datos agrupados ONTAP: McAfee
- SentinelOne — Soluciones asociadas a Vscan y SentinelOne Singularity Cloud Data Security
- Symantec: soluciones asociadas a Vscan y Symantec Protection Engine
- Trend Micro: Guía de soluciones antivirus para datos en clúster ONTAP: Trend Micro

Funciones y usuarios en Amazon FSx para ONTAP NetApp

ONTAP incluye una capacidad sólida y ampliable de control de acceso basado en roles (RBAC). Puede asignar a los usuarios una función para controlar su acceso a los recursos expuestos a través de la CLI y la API REST de ONTAP. Los roles definen diferentes niveles de acceso administrativo para los distintos usuarios de ONTAP. Puede utilizar roles y usuarios en FSx para ONTAP para definir las capacidades y privilegios de los usuarios al utilizar la CLI y la API de REST de ONTAP. Todos los roles y usuarios de ONTAP están asociados a su sistema de archivos o a una máquina virtual de almacenamiento (SVM).

De forma predeterminada, el sistema de archivos de FSx para ONTAP tiene un usuario de nivel de sistema de archivos denominado fsxadmin, que tiene el rol `fsxadmin` asignado. En el nivel del sistema de archivos, solo puede crear nuevos usuarios con el rol `fsxadmin`. No puede crear nuevos roles ni modificar el rol `fsxadmin`.

Para cada SVM del sistema de archivos, hay un usuario predeterminado llamado vsadmin, al que se le ha asignado el rol `vsadmin`. En el nivel de SVM, puede crear nuevos usuarios y nuevos roles. Además del `vsadmin` rol, hay varios roles de SVM predefinidos que puede asignar a los usuarios de SVM. También puede crear funciones que proporcionen el nivel de control de acceso que satisfaga las necesidades de su organización.

Roles predefinidos en una SVM

Las SVM tienen los siguientes roles predefinidos:

Nombre de rol	Capacidades
`vsadmin`	• Administrar cuenta de usuario, contraseña local e información clave • Administrar los volúmenes, excepto los movimientos de volumen • Administrar las cuotas, los qtrees, las copias instantáneas y los archivos • Administrar los LUN • Realice SnapLock operaciones, excepto la eliminación privilegiada • Configurar protocolos: NFS, SMB e iSCSI • Configurar los servicios: DNS, LDAP y NIS • Monitorear trabajos • Monitorear las conexiones de red y la interfaz de red • Monitorear el estado de la SVM
`vsadmin-volume`	• Administrar cuenta de usuario, contraseña local e información clave • Administrar los volúmenes, incluidos los movimientos de volúmenes • Administrar las cuotas, los qtrees, las copias instantáneas y los archivos • Administrar los LUN

Nombre de rol	Capacidades
	• Configurar protocolos: NFS, SMB e iSCSI • Configurar los servicios: DNS, LDAP y NIS • Monitorear la interfaz de red • Monitorear el estado de la SVM
`vsadmin-protocol`	• Administrar cuenta de usuario, contraseña local e información clave • Administrar los LUN • Configurar protocolos: NFS, SMB e iSCSI • Configurar los servicios: DNS, LDAP y NIS • Monitorear la interfaz de red • Monitorear el estado de la SVM
`vsadmin-backup`	• Administrar cuenta de usuario, contraseña local e información clave • Administrar las operaciones de NDMP • Hacer que un volumen restaurado sea de lectura/escritura • Gestione SnapMirror las relaciones y las copias instantáneas • Ver los volúmenes y la información de la red

Nombre de rol	Capacidades
`vsadmin-snaplock`	• Administrar cuenta de usuario, contraseña local e información clave • Administrar los volúmenes, excepto los movimientos de volumen • Administrar las cuotas, los qtrees, las copias instantáneas y los archivos • Realice SnapLock operaciones, incluida la eliminación privilegiada • Configurar protocolos: NFS, SMB • Configurar los servicios: DNS, LDAP y NIS • Monitorear trabajos • Monitorear las conexiones de red y la interfaz de red
`vsadmin-readonly`	• Administrar cuenta de usuario, contraseña local e información clave • Monitorear el estado de la SVM • Monitorear la interfaz de red • Ver los volúmenes y los LUN • Ver los servicios y protocolos

Temas

- Crear nuevos roles o usuarios
- No se puede actualizar la contraseña de la fsxadmin cuenta
- Creación de nuevas funciones para una SVM mediante la CLI de NetApp ONTAP
- Uso de cuentas de usuario de Active Directory con el sistema de archivos
- Configuración de la autenticación de clave pública

Crear nuevos roles o usuarios

Cada usuario de FSx para ONTAP está asociado a una SVM o al propio sistema de archivos. Puede crear nuevas funciones o usuarios mediante el `security login create` comando de la CLI de NetApp ONTAP con la `vsadmin` función para las SVM y la `fsxadmin` función predeterminada para el sistema de archivos.

El `security login create` comando crea un método de inicio de sesión para la utilidad de administración. Un método de inicio de sesión consta de un nombre de usuario, una aplicación (método de acceso) y un método de autenticación. Un nombre de usuario se puede asociar a varias aplicaciones. Opcionalmente, puede incluir un nombre de función de control de acceso. Si se utiliza un nombre de grupo de Active Directory, LDAP o NIS, el método de inicio de sesión permite el acceso a los usuarios que pertenecen al grupo especificado. Si el usuario es miembro de varios grupos aprovisionados en la tabla de inicio de sesión de seguridad, tendrá acceso a una lista combinada de los comandos autorizados para los grupos individuales. Para obtener más información, consulte `security login create`la documentación del NetApp ONTAP producto.

Para crear un nuevo usuario para un SVM o un sistema de archivos (NetApp ONTAPCLI)

1. Para acceder a la CLI de NetApp ONTAP, ejecute el siguiente comando para establecer una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP. Reemplace *`management_endpoint_ip`* con la dirección IP del puerto de gestión del sistema de archivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obtener más información, consulte Administración de sistemas de archivos con la ONTAP CLI.

2. Utilice el comando `security login create` ONTAP CLI para crear una nueva cuenta de usuario en su FSx para el sistema de archivos ONTAP o SVM.

   ```
   Fsx0123456::> security login create -vserver vserver_name -user-or-group-
   name user_or_group_name -application login_application -authentication-
   method auth_method -role role_or_account_name
   ```

   Introduzca los datos de los marcadores de posición del ejemplo para definir las siguientes propiedades obligatorias:

- `-vserver`— Especifica el nombre del sistema de archivos o SVM en el que desea crear el nuevo rol o usuario.
- `-user-or-group-name`— Especifica el nombre de usuario o el nombre del grupo de Active Directory del método de inicio de sesión. El nombre del grupo de Active Directory solo se puede especificar con el método de `domain` autenticación y las `ssh` aplicaciones `ontapi` y.
- `-application`— Especifica la aplicación del método de inicio de sesión. Los valores posibles incluyen http, ontapi y ssh.
- `-authentication-method`— Especifica el método de autenticación para el inicio de sesión. Entre los valores posibles se incluyen:
  - dominio: se utiliza para la autenticación de Active Directory
  - contraseña: se utiliza para la autenticación con contraseña
  - publickey: usuario para la autenticación con clave pública
- `-role`— Especifica el nombre de la función de control de acceso para el método de inicio de sesión. En el nivel del sistema de archivos, el único rol que se puede especificar es `fsxadmin`.

(Opcional) También puede utilizar uno o más de los siguientes parámetros con el comando:

- `[-comment]`: el texto del comentario de la cuenta de usuario. Por ejemplo, **`Guest account`**. La longitud máxima es de 128 caracteres.
- `[-second-authentication-method {none|publickey|password|nsswitch}]`: especifica el método de autenticación de segundo factor. Puede especificar los métodos siguientes:
  - contraseña: se utiliza para la autenticación con contraseña
  - publickey: se utiliza para la autenticación con clave pública
  - nsswitch: se utiliza para la autenticación NIS o LDAP
  - none: el valor predeterminado si no se especifica ninguno

No se puede actualizar la contraseña de la **`fsxadmin`** cuenta

Al actualizar la contraseña del `fsxadmin` usuario, es posible que reciba un mensaje de error si no cumple los requisitos de contraseña establecidos en el sistema de archivos. Puede ver los requisitos

de contraseña mediante el comando `security login role config show` ONTAP CLI o REST API.

Para ver los requisitos de contraseña de la **`fsxadmin`** cuenta

1. Para acceder a la CLI de NetApp ONTAP, ejecute el siguiente comando para establecer una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP. Reemplace *`management_endpoint_ip`* con la dirección IP del puerto de gestión del sistema de archivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para obtener más información, consulte Administración de sistemas de archivos con la ONTAP CLI.

2. El `security login role config show` comando devuelve los requisitos de contraseña de una cuenta.

   ```
   FsxId0123456::> security login role config show -role fsxadmin -
   fields password_requirement_fields
   ```

   Para el `-fields` parámetro, especifique alguno de los siguientes elementos o todos ellos:

   - `passwd-minlength`: la longitud de la contraseña.
   - `passwd-min-special-chars`: el número mínimo de caracteres especiales de la contraseña.
   - `passwd-min-lowercase-chars`: el número mínimo de caracteres en minúsculas de la contraseña.
   - `passwd-min-uppercase-chars`: el número mínimo de caracteres en mayúsculas de la contraseña.
   - `passwd-min-digits`: el número mínimo de dígitos en la contraseña.
   - `passwd-alphanum`: información sobre la inclusión o exclusión de caracteres alfanuméricos.
   - `passwd-expiry-time`: fecha de caducidad de la contraseña.
   - `passwd-expiry-warn-time`: la hora de aviso de caducidad de la contraseña.

3. Ejecute el siguiente comando para ver todos los requisitos de contraseña:

```
Fsx0123456::> security login role config show -role fsxadmin -fields passwd-
minlength, passwd-min-special-chars, passwd-min-lowercase-chars, passwd-min-
digits, passwd-alphanum, passwd-expiry-time, passwd-expiry-warn-time, passwd-min-
uppercase-chars
```

Obtendrá una respuesta similar a la del ejemplo siguiente, que muestra la información de los campos especificados.

```
vserver                role     passwd-minlength passwd-alphanum passwd-min-
special-chars passwd-expiry-time passwd-min-lowercase-chars passwd-min-uppercase-
chars passwd-min-digits passwd-expiry-warn-time
---------------------- -------- ---------------- --------------
 ------------------------ ------------------ --------------------------
 -------------------------- ----------------- ----------------------
FsxId0ae30e5b7f1a50b6a fsxadmin 3                 enabled         0
       unlimited          0                        0                        0
               unlimited
```

Para modificar los requisitos de contraseña (ONTAPCLI)

- Para modificar los requisitos de la contraseña, utilice el comando `security login role config modify` con los campos de contraseña que desea. El siguiente ejemplo muestra cómo cambiar la longitud mínima de la contraseña a 4 y el número mínimo de caracteres especiales a 1 para el `fsxadmin` rol en un sistema de archivos.

```
Fsx0123456::> security login role config modify -role fsxadmin -passwd-minlength 4
 -passwd-min-special-chars 1
```

Creación de nuevas funciones para una SVM mediante la CLI de NetApp ONTAP

Cada SVM que cree tiene un administrador de SVM predeterminado al que se le asigna el rol `vsadmin` predefinido, pero no se pueden crear nuevos roles utilizando `vsadmin`. Si necesita crear nuevas funciones para su SVM, utilice el `security login role create` comando con la `fsxadmin` función en la NetApp CLI de ONTAP.

Para crear un nuevo rol en su SVM mediante la CLI de NetApp ONTAP

1. Copie el siguiente comando `security login role create`:

```
Fsx0123456::> security login role create -role vol_role -cmddirname "volume"
```

2. Especifique los siguientes parámetros necesarios en el comando:

   - `-role`: nombre del rol
   - `-cmddirname`: el comando o el directorio de comandos al que da acceso el rol. Escriba los nombres de los subdirectorios de comandos entre comillas. Por ejemplo, `"volume snapshot"`. Introduzca `DEFAULT` para especificar todos los directorios de comandos.

3. (Opcional) También puede añadir uno o más de los siguientes parámetros al comando:

   - `-vserver`: nombre de la SVM asociada al rol.
   - `-access`: el nivel de acceso del rol. En el caso de los directorios de comandos, esto incluye:
     - `none`: deniega el acceso a los comandos del directorio de comandos. Este es el valor predeterminado para los roles personalizados.
     - `readonly`: concede acceso a los comandos show en el directorio de comandos y sus subdirectorios.
     - `all`: concede acceso a todos los comandos del directorio de comandos y sus subdirectorios. Para conceder o denegar el acceso a los comandos tipos intrínsecos, debe especificar el directorio de comandos.

     Para los comandos de tipos no intrínsecos (comandos que no terminan en`create`, `modify`, `delete` o `show`):

     - `none`: deniega el acceso a los comandos del directorio de comandos. Este es el valor predeterminado para los roles personalizados.
     - `readonly`: no aplicable No utilice.
     - `all`: concede acceso al comando.
   - `-query`: el objeto de consulta que se utiliza para filtrar el nivel de acceso, que se especifica en forma de una opción válida para el comando o para un comando del directorio de comandos. Escriba el objeto de consulta entre comillas.

4. Ejecute el comando `security login role create`.

Uso de cuentas de usuario de Active Directory con el sistema de archivos

Si es administrador de un sistema de archivos, puede usar el `security login domain-tunnel create` comando de la CLI de NetApp ONTAP para autenticarse en el sistema de archivos y en las SVM mediante cuentas de Active Directory.

Para autenticarse en su sistema de archivos o SVM mediante Active Directory

1. Para conectarse mediante SSH a la NetApp CLI de ONTAP de su sistema de archivos, siga los pasos descritos en la Uso de la NetApp ONTAP CLI sección de la guía del usuario de FSx for ONTAP.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Para autenticarse en su sistema de archivos con las credenciales de Active Directory en lugar de utilizar una SVM individual, copie el siguiente comando `security login domain-tunnel create` para configurar la tunelización de dominios. Seleccione una SVM que esté unida a su Active Directory para que sirva como túnel de dominio para autenticar los inicios de sesión en su Active Directory.

   ```
   FsxIdabcdef0123456789a::> security login domain-tunnel create -vserver svm01
   ```

3. Utilice el comando `security login create` para crear una o más cuentas de usuario de dominio de Active Directory a las que se le concederá acceso al sistema de archivos.
4. Especifique los siguientes parámetros necesarios en el comando:

   - `-vserver`: el nombre del sistema de archivos o SVM en el que se creará el nuevo rol o usuario.
   - `-user-or-group-name`: el nombre de usuario o el nombre del grupo de Active Directory del método de inicio de sesión. El nombre del grupo de Active Directory solo se puede especificar con el método de autenticación `domain`, `ontapi` y la aplicación `ssh`.
   - `-application`: la aplicación del método de inicio de sesión. Los valores posibles incluyen http, ontapi y ssh.
   - `-authentication-method`— El método de autenticación utilizado para iniciar sesión. Entre los valores posibles se incluyen:
     - dominio: para la autenticación de Active Directory
     - contraseña: para la autenticación con contraseña

- clave pública: para la autenticación con clave pública
- `-role`: el nombre del rol de control de acceso del método de inicio de sesión. En el nivel del sistema de archivos, el único rol que se puede especificar es `-role fsxadmin`.

5. En el siguiente ejemplo, se muestra cómo utilizar SSH en el sistema de archivos con las credenciales de Active Directory si se elige `ssh` para el tipo `-application`. El `username` tiene el formato `"domain-name\user-name"`, que es el nombre de dominio y el nombre de usuario que proporcionó al crear la cuenta, separados por una barra invertida y entre comillas.

```
Fsx0123456::> ssh "CORP\user"@management.fs-abcdef01234567892.fsx.us-east-2.aws.com
```

Cuando se le pida que introduzca una contraseña, utilice la contraseña del usuario de Active Directory.

> **Note**
>
> La SVM que se utiliza para la construcción de túneles debe tener el CIFS activado o estar unido a un Active Directory. Si no está habilitando el CIFS y solo va a unir la SVM de túnel a un Active Directory, asegúrese de que la SVM esté unida a su Active Directory. Para obtener más información, consulte Unir las SVM a Microsoft Active Directory.

Configuración de la autenticación de clave pública

Para habilitar la autenticación de clave pública SSH, primero debe generar una clave SSH y asociarla a una cuenta de administrador mediante el comando `security login publickey create`. Esto permite que la cuenta acceda a la SVM. El comando `security login publickey create` acepta los siguientes parámetros.

Parámetro	Descripción
`-vserver` (Opcional)	El nombre de la SVM a la que accede la cuenta.
`-username`	El nombre de usuario de la cuenta. El valor predeterminado, `admin`, es el nombre predeterminado del administrador del clúster.

Parámetro	Descripción
`-index`	El número de índice de la clave pública. El valor predeterminado es 0 si la clave es la primera clave que se crea para la cuenta. De lo contrario, el valor predeterminado es uno más que el número de índice más alto existente para la cuenta.
`-publickey`	La clave pública de OpenSSH. Escriba la clave entre comillas.
`-role`	El rol de control de acceso que se asigna a la cuenta.
`-comment` (Opcional)	Texto descriptivo de la clave pública. Escriba el texto entre comillas.

El siguiente ejemplo asocia una clave pública con la cuenta de administrador SVM `svmadmin` para la SVM `svm01`. A la clave pública se le asigna un número de índice `5`.

```
Fsx0123456::> security login publickey create -vserver svm01 -username svmadmin
 -index 5 -publickey "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAspH64CYbUsDQCdW22JnK6J/
vU9upnKzd2zAk9C1f7YaWRUAFNs2Qe5lUmQ3ldi8AD0Vfbr5T6HZPCixNAIzaFciDy7hgnmdj9eNGedGr/
JNrftQbLD1hZybX
+72DpQB0tYWBhe6eDJ1oPLobZBGfMlPXh8VjeU44i7W4+s0hG0E=tsmith@publickey.example.com"
```

> **Important**
>
> Debe ser administrador de SVM o sistema de archivos para realizar esta tarea.

Migración a Amazon NetApp FSx para ONTAP

En las siguientes secciones se proporciona información sobre cómo migrar sus sistemas de archivos NetApp ONTAP existentes a Amazon FSx NetApp for ONTAP.

> **Note**
>
> Si planea usar la política de organización por niveles `All` para migrar sus datos al nivel del pool de capacidad, tenga en cuenta que los metadatos de los archivos siempre se almacenan en el nivel SSD y que todos los datos de los usuarios nuevos se escriben primero en el nivel SSD. Cuando los datos se escriben en el nivel SSD, el proceso de organización en niveles en segundo plano comenzará a organizar los datos en niveles para almacenar en grupos de capacidad, pero el proceso de organización en niveles no es inmediato y consume recursos de la red. Debe ajustar el tamaño de su nivel de SSD para incluir los metadatos de los archivos (del 3 al 7% del tamaño de los datos de usuario), como búfer para los datos de los usuarios antes de que se clasifiquen en niveles para formar un conjunto de capacidad de almacenamiento. Le recomendamos que no utilice más del 80% de su nivel de SSD.
> Al migrar los datos, asegúrese de supervisar su nivel de SSD utilizando las métricas del sistema de CloudWatch archivos para asegurarse de que no se llene más rápido de lo que el proceso de organización en niveles puede mover los datos al conjunto de capacidad de almacenamiento.

Temas

Migración a FSx para ONTAP mediante NetApp SnapMirror

Puede migrar sus sistemas de archivos NetApp ONTAP a Amazon FSx NetApp para ONTAP mediante. NetApp SnapMirror

NetApp SnapMirror emplea la replicación a nivel de bloques entre dos sistemas de archivos de ONTAP, replicando los datos de un volumen de origen específico a un volumen de destino. Recomendamos usarlo SnapMirror para migrar los sistemas de archivos NetApp ONTAP locales a

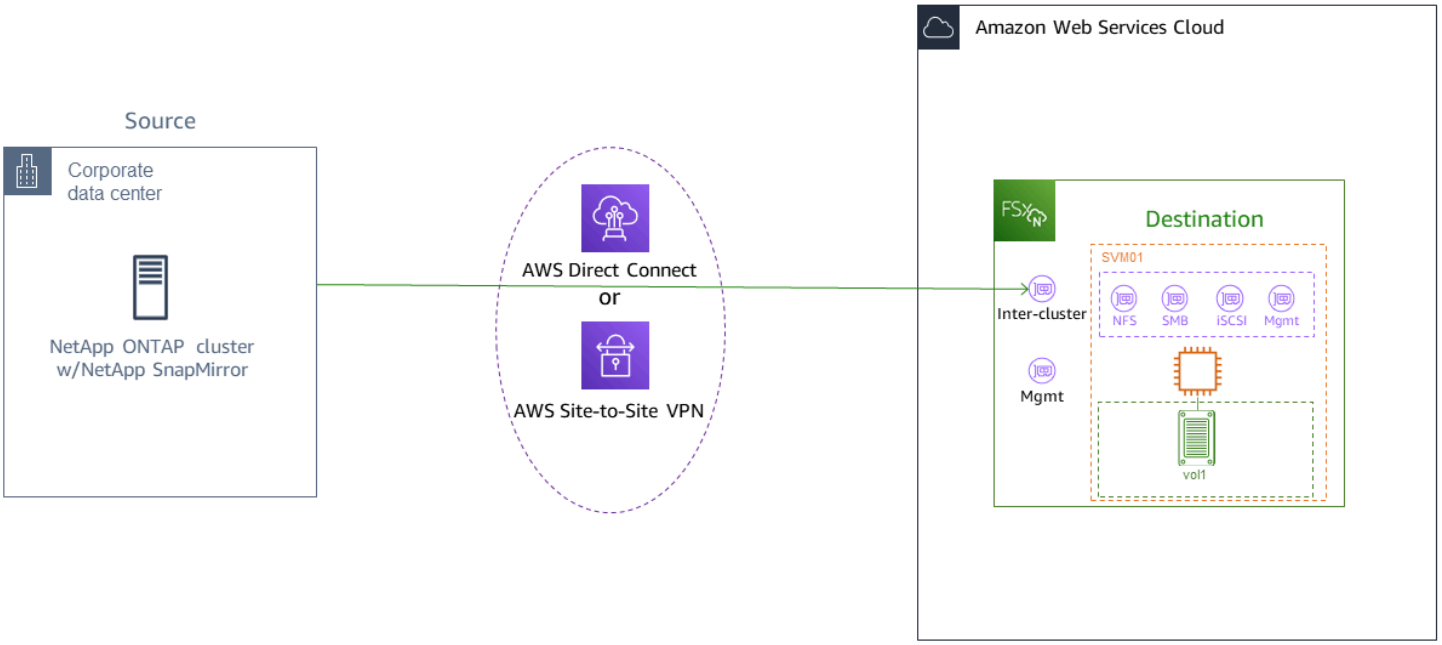
fSx para ONTAP. NetApp SnapMirrorLa replicación a nivel de bloque es rápida y eficaz incluso para sistemas de archivos con:

- Estructuras de directorio complejas
- Más de 50 millones de archivos
- Tamaños de archivo muy pequeños (del orden de kilobytes)

Al migrar SnapMirror a FSx para ONTAP, los datos deduplicados y comprimidos permanecen en esos estados, lo que reduce los tiempos de transferencia y la cantidad de ancho de banda necesaria para la migración. Las instantáneas que existen en los volúmenes de ONTAP de origen se conservan cuando se migran a los volúmenes de destino. La migración de sus sistemas de archivos NetApp ONTAP locales a FSx para ONTAP implica las siguientes tareas de alto nivel:

1. Cree el volumen de destino en Amazon FSx.
2. Recopile las interfaces lógicas (LIF) de origen y destino.
3. Establezca un emparejamiento de clústeres entre sistemas de archivos de origen y de destino.
4. Cree una relación de emparejamiento de SVM.
5. SnapMirror Cree la relación.
6. Mantenga un clúster de destino actualizado.
7. Utilice su sistema de archivos de FSx para ONTAP.

El siguiente diagrama ilustra el escenario de migración que se describe en esta sección.



Temas

- Antes de empezar
- Crear el volumen de destino
- Registre los LIF entre clústeres de origen y destino
- Establezca el emparejamiento de clústeres entre el origen y el destino
- Cree una relación de emparejamiento SVM
- Cree la relación SnapMirror
- Transfiera datos a su sistema de archivos de FSx para ONTAP
- Transición a Amazon FSx

Antes de empezar

Antes de empezar a utilizar los procedimientos descritos en las siguientes secciones, asegúrese de cumplir los siguientes requisitos previos:

- FSx para ONTAP prioriza el tráfico de los clientes sobre las tareas en segundo plano, como la organización de datos en niveles, la eficiencia del almacenamiento y las copias de seguridad. Al migrar datos, y como práctica recomendada general, le recomendamos que supervise la capacidad de su nivel de SSD para asegurarse de que no supere el 80% de utilización. Puede

supervisar el uso de su nivel de SSD mediante las métricas del sistema de archivos. CloudWatch Para obtener más información, consulte Métricas de volumen.

- Si establece la política de niveles de datos del volumen de destino en `All` al migrar los datos, todos los metadatos de los archivos se almacenan en el nivel de almacenamiento SSD principal. Los metadatos de los archivos siempre se almacenan en el nivel principal basado en SSD, independientemente de la política de niveles de datos del volumen. Le recomendamos que asuma una proporción de 1:10 para la capacidad de almacenamiento entre el nivel principal y el nivel del pool de capacidad.
- Los sistemas de archivos de origen y destino están conectados en la misma VPC o se encuentran en redes interconectadas mediante Amazon VPC Peering, Transit Gateway, AWS Direct Connect o AWS VPN. Para obtener más información, consulte Acceder a los datos desde dentro AWS y ¿Qué es el peering de VPC? en la Guía de Amazon VPC Peering.
- El grupo de seguridad de VPC para el sistema de archivos de FSx for ONTAP tiene reglas de entrada y salida que permiten el ICMP y el TCP en los puertos 443, 10000, 11104 y 11105 para los puntos de conexión entre clústeres (LIF).
- Compruebe que los volúmenes de origen y destino ejecutan versiones de NetApp ONTAP compatibles antes de crear una relación de protección de SnapMirror datos. Para obtener más información, consulte las SnapMirror relaciones entre las versiones de ONTAP compatibles en la documentación NetApp de usuario de ONTAP. Los procedimientos que se presentan aquí utilizan un sistema de archivos NetApp ONTAP local como fuente.
- Su sistema de archivos NetApp ONTAP local (fuente) incluye una licencia. SnapMirror
- Ha creado un FSx de destino para el sistema de archivos ONTAP con una SVM, pero no ha creado un volumen de destino. Para obtener más información, consulte Creación de FSx para sistemas de archivos ONTAP.

Los comandos de estos procedimientos utilizan los siguientes alias de clúster, SVM y volumen:

- *`FSx-Dest`*— el ID del clúster de destino (FSx) (con el formato F SxIdabcdef 1234567890a).
- *`OnPrem-Source`*: el ID del clúster de origen.
- *`DestSVM`*: el nombre de destino.
- *`SourceSVM`*: el nombre de la SVM de origen.
- Tanto el nombre del volumen de origen como el de destino son `vol1`.

> **Note**
>
> Un sistema de archivos de FSx para ONTAP se denomina clúster en todos los comandos CLI de ONTAP.

Los procedimientos de esta sección utilizan los siguientes comandos CLI de NetApp ONTAP.

- comando create volume
- comandos cluster
- comandos vserver peer
- comandos snapmirror

Utilizará la CLI de NetApp ONTAP para crear y gestionar una SnapMirror configuración en su sistema de archivos FSx para ONTAP. Para obtener más información, consulte Uso de la NetApp ONTAP CLI.

Crear el volumen de destino

Puede crear un volumen de destino de protección de datos (DP) mediante la consola Amazon FSx, la API Amazon FSx y la API de Amazon FSxAWS CLI, además de la NetApp CLI de ONTAP y la API REST. Para obtener información sobre la creación de un volumen de destino mediante la consola Amazon FSx y AWS CLI, consulte Creación de volúmenes.

En el siguiente procedimiento, utilizará la CLI de NetApp ONTAP para crear un volumen de destino en su sistema de archivos FSx for ONTAP. Necesitará la `fsxadmin` contraseña y la dirección IP o el nombre DNS del puerto de administración del sistema de archivos.

1. Establezca una sesión SSH con el sistema de archivos de destino utilizando el usuario `fsxadmin` y la contraseña que estableció al crear el sistema de archivos.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Cree un volumen en el clúster de destino que tenga una capacidad de almacenamiento igual como mínimo a la capacidad de almacenamiento del volumen de origen. Se utiliza `-type DP` para designarlo como destino de una relación. SnapMirror

Si planea usar la organización de datos por niveles, le recomendamos que configure `-tiering-policy` en `all`. Esto garantiza que sus datos se transfieran inmediatamente al almacenamiento del pool de capacidad y evita que se quede sin capacidad en su nivel de SSD. Tras la migración, puede cambiar `-tiering-policy` a `auto`.

> **Note**
>
> Los metadatos de los archivos siempre se almacenan en el nivel principal basado en SSD, independientemente de la política de niveles de datos del volumen.

```
FSx-Dest::> vol create -vserver DestSVM -volume vol1 -aggregate aggr1 -size 1g -
type DP -tiering-policy all
```

Registre los LIF entre clústeres de origen y destino

SnapMirror utiliza interfaces lógicas (LIF) entre clústeres, cada una con una dirección IP única, para facilitar la transferencia de datos entre los clústeres de origen y destino.

1. Para el FSx de destino para los sistemas de archivos ONTAP, puede recuperar las direcciones IP de punto de conexión entre clústeres desde la consola de Amazon FSx navegando a la pestaña Administración de la página de detalles del sistema de archivos.
2. Para el clúster NetApp ONTAP de origen, recupere las direcciones IP LIF entre clústeres mediante la CLI de ONTAP. Ejecute el siguiente comando:

```
OnPrem-Source::> network interface show -role intercluster

Logical                         Network
Vserver     Interface  Status  Address/Mask
----------- ---------- ------- ------------
FSx-Dest
             inter_1    up/up  10.0.0.36/24
             inter_2    up/up  10.0.1.69/24
```

> **Note**
>
> En el caso de los sistemas de archivos escalables, hay dos direcciones IP entre clústeres para cada par de alta disponibilidad (HA). Guarde estos valores para más adelante.

Guarde las direcciones IP `inter_1` `yinter_2`. Se hace referencia a ellas en `FSx-Dest` como `dest_inter_1` y `dest_inter_2` y para `OnPrem-Source` como `source_inter_1` `ysource_inter_2`.

Establezca el emparejamiento de clústeres entre el origen y el destino

Establezca una relación de pares entre clústeres en el clúster de destino proporcionando las direcciones IP entre clústeres. También tendrá que crear una contraseña que tendrá que introducir cuando establezca el emparejamiento de clústeres en el clúster de origen.

1. Configure la interconexión en el clúster de destino mediante el siguiente comando. Para los sistemas de archivos escalables, tendrás que proporcionar cada dirección IP entre clústeres.

```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-
addrs source_inter_1,source_inter_2

Enter the passphrase:
Confirm the passphrase:
Notice: Now use the same passphrase in the "cluster peer create" command in the
 other cluster.
```

2. A continuación, establezca la relación entre pares del clúster en el clúster de origen. Deberá ingresar la contraseña que creó anteriormente para autenticarse. En el caso de los sistemas de archivos escalables, tendrá que proporcionar cada dirección IP entre clústeres.

```
OnPrem-Source::> cluster peer create -address-family ipv4 -peer-
addrs dest_inter_1,dest_inter_2

Enter the passphrase:
Confirm the passphrase:
```

3. Compruebe que el emparejamiento se haya realizado correctamente mediante el siguiente comando en el clúster de origen. En la salida, `Availability` debe configurarse en `Available`.

```
OnPrem-Source::> cluster peer show

Peer Cluster Name  Availability   Authentication
-----------------  -------------- --------------
FSx-Dest           Available      ok
```

Cree una relación de emparejamiento SVM

Una vez establecido el emparejamiento de clústeres, el siguiente paso es emparejar las SVM. Cree una relación de emparejamiento de SVM en el clúster de destino (FSX-dest) mediante el comando. `vserver peer` Los alias adicionales que se utilizan en los siguientes comandos son los siguientes:

- `DestLocalName`: este es el nombre que se utiliza para identificar la SVM de destino al configurar el emparejamiento de la SVM en la SVM de origen.
- `SourceLocalName`: este es el nombre que se utiliza para identificar la SVM de origen al configurar el emparejamiento de SVM en el SVM de destino.

1. Utilice el siguiente comando para crear una relación de emparejamiento de SVM entre las SVM de origen y de destino.

```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver SourceSVM -peer-
cluster OnPrem-Source -applications snapmirror -local-name SourceLocalName

 Info: [Job 207] 'vserver peer create' job queued
```

2. Acepte la relación de emparejamiento en el clúster de origen:

```
OnPrem-Source::> vserver peer accept -vserver SourceSVM -peer-vserver DestSVM -
local-name DestLocalName

 Info: [Job 211] 'vserver peer accept' job queued
```

3. Compruebe el estado de emparejamiento de la SVM mediante el siguiente comando; `Peer State` debe configurarse en `peered` en la respuesta.

```
OnPrem-Source::> vserver peer show

Peer    Peer     Peer   Peering  Remote
vserver Vserver  State  Cluster  Applications  Vserver
------- -------- ------ -------- ------------ ---------
svm01   destsvm1 peered FSx-Dest snapmirror    svm01
```

Cree la relación SnapMirror

Ahora que ha emparejado las SVM de origen y destino, los siguientes pasos son crear e inicializar la SnapMirror relación en el clúster de destino.

> **Note**
>
> Una vez creada e inicializada una SnapMirror relación, los volúmenes de destino son de solo lectura hasta que se rompa la relación.

- Utilice el `snapmirror create` comando para crear la SnapMirror relación en el clúster de destino. El comando `snapmirror create` debe usarse desde la SVM de destino.

  Opcionalmente, se puede utilizar `-throttle` para establecer el ancho de banda máximo (en KB/seg) para la SnapMirror relación.

  ```
  FSx-Dest::> snapmirror create -source-path SourceLocalName:vol1 -destination-
  path DestSVM:vol1 -vserver DestSVM -throttle unlimited

   Operation succeeded: snapmirror create for the relationship with destination
   "DestSVM:vol1".
  ```

Transfiera datos a su sistema de archivos de FSx para ONTAP

Ahora que ha creado la SnapMirror relación, puede transferir los datos al sistema de archivos de destino.

1. Puede transferir datos al sistema de archivos de destino ejecutando el siguiente comando en el sistema de archivos de destino.

> **Note**
>
> Una vez que ejecute este comando, SnapMirror empezará a transferir las instantáneas de los datos del volumen de origen al volumen de destino.

```
FSx-Dest::> snapmirror initialize -destination-path DestSVM:vol1 -source-
path SourceLocalName:vol1
```

2. Si está migrando datos que se utilizan activamente, tendrá que actualizar el clúster de destino para que permanezca sincronizado con el clúster de origen. Para realizar una actualización de una sola vez en el clúster de destino, ejecute el siguiente comando.

```
FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
```

3. También puede programar actualizaciones diarias o cada hora antes de completar la migración y trasladar sus clientes a FSx para ONTAP. Puede establecer un programa de SnapMirror actualización mediante el `snapmirror modify`comando.

```
FSx-Dest::> snapmirror modify -destination-path DestSVM:vol1 -schedule hourly
```

Transición a Amazon FSx

Para preparar la transición a su sistema de archivos de FSx para ONTAP, haga lo siguiente:

- Desconecte todos los clientes que escriban en el clúster de origen.
- Realice una SnapMirror transferencia final para asegurarse de que no se pierdan datos al cortar.
- Rompe la SnapMirror relación.
- Conecte todos los clientes a su sistema de archivos de FSx para ONTAP.

1. Para garantizar que todos los datos del clúster de origen se transfieran al sistema de archivos de FSx para ONTAP, realice una transferencia final de Snapmirror.

```
FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
```

2. Asegúrese de que la migración de datos se haya completado verificando que `Mirror State` esté configurado en `Snapmirrored`, y `Relationship Status` esté configurado en `Idle`. También debe asegurarse de que la fecha `Last Transfer End Timestamp` sea la esperada, ya que indica cuándo se realizó la última transferencia al volumen de destino.
3. Ejecute el siguiente comando para mostrar el SnapMirror estado.

```
FSx-Dest::> snapmirror show -fields state,status,last-transfer-end-timestamp

Source     Destination   Mirror        Relationship Last Transfer End
Path       Path          State         Status       Timestamp
---------- -----------   ----------    -------      ---------------
Svm01:vol1 svm02:DestVol Snapmirrored  Idle         09/02 09:02:21
```

4. Deshabilite cualquier SnapMirror transferencia futura mediante el `snapmirror quiesce` comando.

```
FSx-Dest::> snapmirror quiesce -destination-path DestSVM:vol1
```

5. Compruebe que `Relationship Status` ha cambiado a `Quiesced` a través de `snapmirror show`.

```
FSx-Dest::> snapmirror show

Source            Destination   Mirror        Relationship
Path              Path          State         Status
-----------       ------------  ------------- --------
sourcesvm1:vol1   svm01:DestVol Snapmirrored  Quiesced
```

6. Durante la migración, el volumen de destino es sólo de lectura. Para habilitar la lectura/escritura, debe romper la SnapMirror relación y pasar a su sistema de archivos FSx for ONTAP. Rompa la SnapMirror relación con el siguiente comando.

```
FSx-Dest::> snapmirror break -destination-path DestSVM:vol1

Operation succeeded: snapmirror break for destination "DestSVM:vol1".
```

7. Una vez que se haya completado la SnapMirror replicación y se haya roto la SnapMirror relación, puede montar el volumen para que los datos estén disponibles.

```
FSx-Dest::> vol mount -vserver fsx -volume vol1 -junction-path /vol1
```

El volumen ahora está disponible y los datos del volumen de origen se han migrado completamente al volumen de destino. Los clientes también pueden leer y escribir en él. Si anteriormente configuró el `tiering-policy` de este volumen en `all`, puede cambiarlo por `auto` o `snapshot-only` y sus datos pasarán automáticamente de un nivel de almacenamiento a otro según los patrones de acceso. Para que los clientes y las aplicaciones puedan acceder a estos datos, consulte Acceso a datos.

Migración a FSx para ONTAP con AWS DataSync

Recomendamos usar AWS DataSync para transferir datos entre FSx para sistemas de archivos ONTAP y sistemas de archivos que no sean de ONTAP, incluidos FSx for Lustre, FSx para OpenZFS, FSx para Windows File Server, Amazon EFS, Amazon S3 y archivadores locales. Si está transfiriendo archivos entre FSx para ONTAP y NetApp ONTAP, le recomendamos que utilice. NetApp SnapMirror AWS DataSynces un servicio de transferencia de datos que simplifica, automatiza y acelera el traslado y la replicación de datos entre sistemas de almacenamiento autogestionados y servicios de almacenamiento a través de Internet o. AWS AWS Direct Connect DataSync puede transferir los datos y metadatos del sistema de archivos, como la propiedad, las marcas horarias y los permisos de acceso.

Se puede utilizar DataSync para transferir archivos entre dos FSx para los sistemas de archivos ONTAP y también para mover datos a un sistema de archivos de una cuenta o sistema de archivos diferenteRegión de AWS. AWS También se puede utilizar DataSync con FSx para sistemas de archivos ONTAP para otras tareas. Por ejemplo, puede realizar la migración de datos de una sola vez, incorporar datos de forma periódica de cargas de trabajo distribuidas, y programar la replicación para la protección de datos y la recuperación.

En DataSync, una ubicación es un punto final de un sistema de archivos FSx para ONTAP. Para obtener información sobre escenarios de transferencia específicos, consulte Trabajar con ubicaciones en la AWS DataSyncGuía del usuario.

> **Note**
>
> Si planea usar la política de organización por niveles `All` para migrar sus datos al nivel del pool de capacidad, tenga en cuenta que los metadatos de los archivos siempre se almacenan en el nivel SSD y que todos los datos de los usuarios nuevos se escriben primero en el nivel SSD. Cuando los datos se escriben en el nivel SSD, el proceso de organización en niveles en segundo plano comenzará a organizar los datos en niveles para almacenar en grupos de capacidad, pero el proceso de organización en niveles no es inmediato y

consume recursos de la red. Debe ajustar el tamaño de su nivel SSD para tener en cuenta los metadatos de archivo (3-7% del tamaño de los datos de usuario), como un búfer para los datos de usuario antes de que se escalonen en el almacenamiento del pool de capacidad. Le recomendamos que no supere el 80% de uso de SSD.
Al migrar los datos, asegúrese de supervisar el nivel de su SSD utilizando las métricas del sistema de CloudWatch archivos para asegurarse de que no se llene más rápido de lo que el proceso de organización en niveles puede mover los datos al almacenamiento del pool de capacidad. También puede limitar las DataSync transferencias a una velocidad inferior a la velocidad a la que se produce la organización por niveles para garantizar que el nivel de SSD no supere el 80% de utilización. Por ejemplo, en el caso de los sistemas de archivos con una capacidad de rendimiento de al menos 512 MBps, una limitación de 200 MBps normalmente equilibrará las velocidades de transferencia y organización de datos por niveles.

Requisitos previos

Para migrar los datos a su configuración de FSx for ONTAP, necesita un servidor y una red que cumplan los requisitos. DataSync Para obtener más información, consulte los requisitos de DataSync la Guía del AWS DataSyncusuario.

Pasos básicos para migrar archivos mediante DataSync

La transferencia de archivos de un origen a un destino mediante el uso de DataSync este método implica los siguientes pasos básicos:

- Descargue e implemente un agente en su entorno y actívelo (no es necesario si se realiza una transferencia entre Servicios de AWS uno y otro).
- Cree una ubicación de origen y de destino.
- Cree una tarea.
- Ejecute la tarea para transferir archivos desde el origen al destino.

Para obtener más información, consulte los siguientes temas en la Guía del usuario deAWS DataSync:

- Transferencia de datos entre el almacenamiento autogestionado y AWS
- Creación de una ubicación para Amazon FSx para ONTAP NetApp

Supervisión de Amazon FSx para ONTAP NetApp

Puede utilizar los siguientes servicios y herramientas para supervisar Amazon FSx y comprobar el uso y la actividad de NetApp ONTAP:

- Amazon CloudWatch: puede supervisar los sistemas de archivos con Amazon CloudWatch, que recopila y procesa automáticamente los datos sin procesar de FSx para ONTAP para convertirlos en métricas legibles. Estas estadísticas se retienen durante un periodo de 15 meses para que pueda acceder a la información histórica y ver el rendimiento de su sistema de archivos. También puede establecer alarmas basadas en sus métricas durante un periodo de tiempo especificado y realizar una o más acciones basadas en el valor de las métricas en relación con los umbrales que especifique.
- Eventos EMS de ONTAP: puede monitorizar su FSx para el sistema de archivos de ONTAP mediante eventos generados por el Sistema de Gestión de Eventos (EMS) de ONTAP. Los eventos EMS son notificaciones de sucesos en el sistema de archivos, como la creación de un LUN iSCSI o el ajuste automático del tamaño de los volúmenes.
- NetApp Cloud Insights: puede supervisar las métricas de configuración, capacidad y rendimiento de sus sistemas de archivos FSx para ONTAP mediante el servicio NetApp Cloud Insights. También puede crear alertas en función de las condiciones métricas.
- NetApp Harvest y NetApp Grafana: puede monitorizar su sistema de archivos FSx para ONTAP mediante Harvest y Grafana. NetApp NetApp NetApp Harvest supervisa los sistemas de archivos ONTAP mediante la recopilación de métricas de rendimiento, capacidad y hardware de FSx para los sistemas de archivos ONTAP. Grafana proporciona un panel de control donde se pueden mostrar las métricas de cosecha recopiladas.
- AWS CloudTrail— Se puede utilizar AWS CloudTrail para capturar todas las llamadas a la API de Amazon FSx como eventos. Estos eventos proporcionan un registro de las acciones realizadas por un usuario, rol o servicio AWS en Amazon FSx.

Temas

- Registro de llamadas a la API de FSx para ONTAP con AWS CloudTrail

Monitorización con Amazon CloudWatch

Puede supervisar los sistemas de archivos con Amazon CloudWatch, que recopila y procesa datos sin procesar de Amazon FSx para NetApp ONTAP para convertirlos en métricas legibles y prácticamente en tiempo real. Estas estadísticas se conservan durante un periodo de 15 meses, de forma que pueda acceder a la información histórica para determinar el rendimiento de su sistema de archivos. De forma predeterminada, los datos métricos de FSx for ONTAP se envían automáticamente CloudWatch en períodos de 1 minuto. Para obtener más información CloudWatch, consulta ¿Qué es Amazon CloudWatch? en la Guía del CloudWatch usuario de Amazon.

> **Note**
>
> De forma predeterminada, FSx for ONTAP envía los datos de las métricas CloudWatch en períodos de 1 minuto, excepto las siguientes métricas, que se envían en intervalos de 5 minutos:
>
> - `FileServerDiskThroughputBalance`
> - `FileServerDiskIopsBalance`

CloudWatch las métricas de FSx para ONTAP se organizan en cuatro categorías, que se definen mediante las dimensiones que se utilizan para consultar cada métrica. Para obtener más información sobre las dimensiones, consulta Dimensiones en la Guía del CloudWatch usuario de Amazon.

- Métricas del sistema de archivos: métricas de ile-system-level rendimiento y capacidad de almacenamiento.
- Métricas detalladas del sistema de archivos: F ile-system-level métricas de almacenamiento por nivel de almacenamiento (SSD y grupo de capacidad).
- Métricas de volumen: métricas de rendimiento y capacidad de almacenamiento por volumen.
- Métricas de volumen detalladas: métricas de capacidad de almacenamiento por volumen por nivel de almacenamiento o por tipo de datos (usuario, instantánea u otros).

Todas CloudWatch las métricas de FSx para ONTAP se publican en el espacio de nombres de`AWS/FSx`. CloudWatch

Temas

Cómo utilizar FSx para las métricas de ONTAP CloudWatch

Las CloudWatch métricas publicadas por Amazon FSx proporcionan información valiosa sobre sus FSx para los volúmenes y los sistemas de archivos de ONTAP.

Temas

Monitoreo de las métricas del sistema de archivos en la consola Amazon FSx

Puede utilizar el panel Monitoreo y rendimiento del panel de control del sistema de archivos de la consola de Amazon FSx para ver las métricas que se describen en la siguiente tabla. Para obtener más información, consulte Acceder a las CloudWatch métricas.

Monitoreo y rendimiento	¿Cómo...	Gráfico	Métricas relevantes
Resumen	... determinar la cantidad de capacidad de almacenamiento disponible en mi sistema de archivos?	Capacidad de almacenamiento principal	`StorageCapacity {SSD} - StorageUsed {SSD}`

Monitore y rendimie to	¿Cómo...	Gráfico	Métricas relevantes
		disponibl e (bytes)	
	... determinar el rendimiento total de los clientes de mi sistema de archivos?	Rendimien to total del cliente (bytes/se g)	SUMA (`DataReadBytes + DataWriteBytes`) / PERÍODO (en segundos)
	... determinar el total de IOPS de los clientes de mi sistema de archivos?	IOPS totales del cliente (operacio nes/ segundo)	SUMA (`DataRead0 perations + DataWrite0perations +Metadata0perations`) /PERÍODO (en segundos)
	... determinar la latencia media de las operaciones de lectura, escritura y metadatos de mi sistema de archivos?	Latencia promedio (ms/ opera ción)	Latencia de lectura promedio: `DataRead0 perationTime` * 1000/`DataRead0 perations` Latencia media de escritura : `DataWrite0peration Time` * 1000/`DataWrite 0perations` Latencia media de metadatos: `Metadata0 perationTime` * 1000/ `Metadata0perations`

Monitore y rendimie to	¿Cómo...	Gráfico	Métricas relevantes
	... determinar la distribución de la capacidad de almacenamiento utilizada y libre en mi sistema de archivos?	Distribuc ión de almacenam iento	Nivel principal disponible: `StorageCapacity {SSD} - StorageUsed {SSD}` Nivel principal utilizado: `StorageUsed {SSD}` Pool de capacidad utilizado: `StorageUsed {StandardCapacityPo ol }`
	... determinar los ahorros derivados de la eficiencia del almacenamiento (compresión, deduplicación y compactación)?	Ahorros en eficienci a de almacenam iento	`StorageEfficiencyS avings`
Almacen iento	... determinar cuánto almacenamiento principal está disponible?	Capacidad de almacenam iento principal disponibl e (bytes)	`StorageCapacity {SSD} - StorageUsed {SSD}`

Monitore y rendimie to	¿Cómo...	Gráfico	Métricas relevantes
	... determinar el porcentaje de almacenam iento principal utilizado para mi sistema de archivos?	Utilizaci ón de la capacidad de almacenam iento principal (porcenta je)	`StorageCapacity {SSD} * 100/StorageUsed {SSD}`
Rendimien to del servidor de archivos	... determinar si mi sistema de archivos se acerca al límite de rendimiento de la red?	Rendimien to de la red: utilización (porcenta je)	`NetworkThroughputU tilization`
	... determinar si mi sistema de archivos se acerca al límite de rendimiento del disco?	Rendimien to del disco: utilización (porcenta je)	`FileServerDiskThro ughputUtilization`
	... determinar si mi sistema de archivos ha agotado los créditos de ráfaga permitidos para el rendimiento del disco?	Rendimien to del disco: balance de ráfagas (porcenta je)	`FileServerDiskThro ughputBalance`

Monitore y rendimie to	¿Cómo...	Gráfico	Métricas relevantes
	... determinar si mi sistema de archivos se acerca al límite de IOPS de SSD de sus servidores de archivos?	IOPS de disco: utilización (porcenta je)	`FileServerDiskIops Utilization`
	... determinar si mi sistema de archivos ha agotado los créditos de ráfaga permitido s por sus servidores de archivos para las IOPS de las unidades SSD de disco?	IOPS de disco: balance de ráfaga (porcenta je)	`FileServerDiskIops Balance`
	... determinar la utilización media de la CPU del sistema de archivos?	Utilizaci ón de la CPU (porcenta je)	`CPUUtilization`
	... determinar si mi carga de trabajo hace un uso eficiente de la RAM y las cachés de lectura NVMe de mi sistema de archivos?	Porcentaj e de aciertos de caché	`FileServerCacheHit Ratio`
Desemp de disco	... determinar si mi sistema de archivos se acerca a la capacidad de IOPS de SSD aprovisionada actualmente?	IOPS de disco: utilizaci ón (SSD) (porcenta je)	`DiskIopsUtilization`

> **Note**
>
> Le recomendamos que mantenga una utilización media de la capacidad de rendimiento de cualquier dimensión relacionada con el rendimiento, como la utilización de la red, la utilización de la CPU y la utilización de IOPS de SSD por debajo del 50%. Esto garantiza que dispone de suficiente capacidad de rendimiento sobrante para los picos imprevistos de la carga de trabajo, así como para cualquier operación de almacenamiento en segundo plano (como la sincronización del almacenamiento, la organización de los datos en niveles o las copias de seguridad).

Monitoreo de las métricas de volumen en la consola de Amazon FSx

Puede ver el panel de Monitoring (Monitoreo) en el panel de control de su volumen en la consola de Amazon FSx para ver métricas de rendimiento adicionales. Para obtener más información, consulte Acceder a las CloudWatch métricas.

Monitore	¿Cómo...?	Gráfico	Métricas relevantes
	... determinar la capacidad de almacenamiento disponible de mi volumen?	Capacidad de almacenamiento disponible	`StorageCapacity`
	... determinar el rendimiento total de clientes de mi volumen?	Rendimiento total del cliente (bytes/seg)	SUMA (`DataReadBytes + DataWriteBytes`) / PERÍODO (en segundos)
	... determinar el total de IOPS de los clientes de mi volumen?	IOPS totales de los clientes (operacio	SUMA (`DataReadOperations + DataWriteOperations +MetadataOperations`

Monitore	¿Cómo...?	Gráfico	Métricas relevantes
		nes/ segundo)	) /PERÍODO (en segundos)
	... determinar cuántas operaciones de lectura y escritura provienen o van al nivel del pool de capacidad?	Pool de capacidad (IOPS) (operaciones/ segundo)	Operaciones de lectura: `CapacityPoolReadOperations` Operaciones de escritura: `CapacityPoolWriteOperations`
	... determinar la latencia media de las operaciones de lectura, escritura y metadatos de mi volumen?	Latencia promedio (ms/ operación)	Latencia de lectura promedio: `DataReadOperationTime * 1000/DataReadOperations` Latencia media de escritura: `DataWriteOperationTime * 1000/DataWriteOperations` Latencia media de metadatos: `MetadataOperationTime * 1000/MetadataOperations`
	... determinar la cantidad de archivos o inodos que están disponibles en mi volumen?	Archivos disponibles (inodos)	`FilesCapacity - FilesUsed`
	... determinar la distribución de la capacidad de almacenamiento usada y libre en mi volumen?	Distribución de almacenamiento	`StorageCapacity - StorageUsed`

Acceder a las CloudWatch métricas

Puede ver CloudWatch las métricas de Amazon para Amazon FSx de las siguientes maneras:

- La consola de Amazon FSx
- La CloudWatch consola Amazon
- El AWS Command Line Interface (AWS CLI) para CloudWatch
- La CloudWatch API

El siguiente procedimiento explica cómo ver las CloudWatch métricas del sistema de archivos con la consola Amazon FSx.

Para ver CloudWatch las métricas de su sistema de archivos mediante la consola Amazon FSx

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación izquierdo, elija Sistemas de archivos y, a continuación, elija el sistema de archivos cuyas métricas desee ver.
3. En la página Summary (Resumen), seleccione Monitoring & performance (Monitoreo y rendimiento) en el segundo panel para ver los gráficos de las métricas de su sistema de archivos.

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

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

El siguiente procedimiento explica cómo ver las CloudWatch métricas de su volumen con la consola Amazon FSx.

Para ver CloudWatch las métricas de su volumen mediante la consola Amazon FSx

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación izquierdo, elija Volúmenes y, a continuación, elija el volumen cuyas métricas desee ver.
3. En la página Summary (Resumen), seleccione Monitoring (Monitoreo) (la pestaña predeterminada) en el segundo panel para ver los gráficos de las métricas del volumen.

El siguiente procedimiento explica cómo ver las CloudWatch métricas del sistema de archivos con la CloudWatch consola de Amazon.

Para ver las métricas con la CloudWatch consola de Amazon

1. En la página de Summary (Resumen) de su sistema de archivos, seleccione Monitoring & performance (Monitoreo y rendimiento) en el segundo panel para ver los gráficos de las métricas de su sistema de archivos.
2. Selecciona Ver en métricas en el menú de acciones de la parte superior derecha del gráfico que quieres ver en la CloudWatch consola de Amazon. Se abrirá la página de métricas en la CloudWatch consola de Amazon.

El siguiente procedimiento explica cómo añadir las métricas del sistema de archivos FSx for ONTAP a un panel de control de la consola de Amazon. CloudWatch

Para añadir métricas a una CloudWatch consola de Amazon

1. Elija el conjunto de métricas (Resumen, Almacenamiento o Rendimiento) en el panel Monitoring & performance (Monitoreo y rendimiento) de la consola Amazon FSx.
2. Seleccione Añadir al panel de control en la parte superior derecha del panel. Esto abre la CloudWatch consola de Amazon.
3. Selecciona un CloudWatch panel de control existente de la lista o crea uno nuevo. Para obtener más información, consulta Uso de los CloudWatch paneles de Amazon en la Guía del CloudWatch usuario de Amazon.

En el siguiente procedimiento se explica cómo acceder a las métricas del sistema de archivos con AWS CLI.

Para acceder a las métricas desde AWS CLI

- Utilice el comando CloudWatch CLI list-metrics con el `--namespace "AWS/FSx"` parámetro. Para obtener más información, consulte Referencia de comandos de la AWS CLI.

El siguiente procedimiento explica cómo acceder a las métricas del sistema de archivos con la CloudWatch API.

Para acceder a las métricas desde la CloudWatch API

- Llame a la operación de la API GetMetricStatistics. Para obtener más información, consulta la referencia de la CloudWatch API de Amazon.

Métricas del sistema de archivos

Las métricas del sistema de archivos de Amazon FSx para NetApp ONTAP se clasifican como métricas del sistema de archivos o métricas detalladas del sistema de archivos.

- Las Métricas del sistema de archivos son métricas agregadas de rendimiento y almacenamiento para un único sistema de archivos que ocupan una única dimensión, `FileSystemId` Estas métricas miden el rendimiento de la red y el uso de la capacidad de almacenamiento de su sistema de archivos.
- Las Métricas detalladas del sistema de archivos miden la capacidad de almacenamiento de su sistema de archivos y el almacenamiento utilizado en cada nivel de almacenamiento (por ejemplo, el almacenamiento en SSD y el almacenamiento en grupos de capacidad). Cada métrica incluye una dimensión `FileSystemId`, `StorageTier` y `DataType`.

Tenga en cuenta lo siguiente sobre cuándo Amazon FSx publica puntos de datos para estas métricas: CloudWatch

- Para las métricas de uso (cualquier métrica cuyo nombre termine en Utilización, por ejemplo`NetworkThroughputUtilization`), se emite un punto de datos en cada período por cada servidor de archivos o agregado activo. Por ejemplo, Amazon FSx emite una métrica de un minuto por servidor de archivos activo y una métrica de un minuto por `FileServerDiskIopsUtilization` agregado de. `DiskIopsUtilization`
- Para todas las demás métricas, se emite un único punto de datos en cada período, que corresponde al valor total de la métrica en todos los servidores de archivos activos (por

ejemplo, en el caso de las métricas de servidores de archivos) o en todos los agregados (`DataReadBytes`por ejemplo, en el caso de las métricas de almacenamiento). `DiskReadBytes`

Temas

Métricas de E/S de red

Todas estas métricas tienen una dimensión, `FileSystemId`.

Métrica	Descripción
`NetworkThroughputUtilization`	Porcentaje de utilización del rendimiento de la red del sistema de archivos. La estadística `Average` es la utilización media del rendimiento de red del sistema de archivos durante un período específico. La estadística `Minimum` es la utilización más baja del rendimiento de red del sistema de archivos durante un período específico. La estadística `Maximum` es la utilización máxima del rendimiento de red del sistema de archivos durante un período específico. Unidades: porcentaje Estadísticas válidas: `Average`, `Minimum` y `Maximum`.

Métrica	Descripción
`NetworkSentBytes`	El número de bytes (E/S de red) enviados por el sistema de archivos. La estadística `Sum` es el número total de bytes enviados por el sistema de archivos durante un período específico. Para calcular el rendimiento enviado (bytes por segundo) de cualquier estadística, divídala por los segundos del periodo especificado. Unidades: bytes Estadísticas válidas: `Sum`
`NetworkReceivedBytes`	El número de bytes (E/S de red) recibidos por el sistema de archivos. La estadística `Sum` es el número total de bytes recibidos por el sistema de archivos durante un período específico. Para calcular el rendimiento recibido (bytes por segundo) de cualquier estadística, divídala por los segundos del periodo especificado. Unidades: bytes Estadísticas válidas: `Sum`

Métrica	Descripción
`DataReadBytes`	El número de bytes (E/S de red) que los clientes leen en el sistema de archivos. La estadística `Sum` es el número total de bytes asociados a operaciones de lectura durante el periodo especificado. Para calcular el rendimiento medio (bytes por segundo) de un periodo, divida la estadística `Sum` por el número de segundos del periodo especificado. Unidades: bytes Estadísticas válidas: `Sum`
`DataWriteBytes`	El número de bytes (E/S de red) que los clientes escriben en el sistema de archivos. La estadística `Sum` es el número total de bytes asociados a operaciones de escritura durante el periodo especificado. Para calcular el rendimiento medio (bytes por segundo) de un periodo, divida la estadística `Sum` por el número de segundos del periodo especificado. Unidades: bytes Estadísticas válidas: `Sum`

Métrica	Descripción
`DataReadOperations`	El recuento de operaciones de lectura (E/S de red) desde las lecturas realizadas por los clientes al sistema de archivos. La estadística `Sum` es el número total de operaciones de E/S que se produjeron durante un período específico. Para calcular la media de operaciones de lectura por segundo de un periodo, divida la estadística `Sum` por el número de segundos del periodo especificado. Unidades: recuento Estadísticas válidas: `Sum`
`DataWriteOperations`	El recuento de operaciones de escritura (E/S de red) realizadas por los clientes en el sistema de archivos. La estadística `Sum` es el número total de operaciones de E/S que se produjeron durante un período específico. Para calcular la media de operaciones de escritura por segundo de un periodo, divida la estadística `Sum` por el número de segundos del periodo especificado. Unidades: recuento Estadísticas válidas: `Sum`

Métrica	Descripción
`MetadataOperations`	El recuento de operaciones de metadatos (E/S de red) realizadas por los clientes al sistema de archivos. La estadística `Sum` es el número total de operaciones de E/S que se produjeron durante un período específico. Para calcular la media de operaciones de metadatos por segundo durante un periodo, divida la estadística `Sum` por el número de segundos del periodo especificado. Unidades: recuento Estadísticas válidas: `Sum`
`DataReadOperationTime`	La suma del tiempo total empleado en el sistema de archivos para las operaciones de lectura (E/S de red) de los clientes que acceden a los datos del sistema de archivos. La estadística `Sum` es el número total de segundos empleados por las operaciones de lectura durante el periodo especificado. Para calcular la latencia de lectura media de un período, divida la estadística `Sum` entre la `Sum` de la métrica `DataReadOperations` del mismo período. Unidades: segundos Estadísticas válidas: `Sum`

Métrica	Descripción
`DataWriteOperationTime`	La suma del tiempo total empleado en el sistema de archivos para realizar las operacion es de escritura (E/S de red) de los clientes que acceden a los datos del sistema de archivos. La estadística `Sum` es el número total de segundos empleados por las operaciones de escritura durante el periodo especificado. Para calcular la latencia de escritura media de un período, divida la estadística `Sum` entre `Sum` y la métrica `DataWriteOperations` del mismo período. Unidades: segundos Estadísticas válidas: `Sum`
`CapacityPoolReadBytes`	El número de bytes leídos (E/S de red) desde el nivel del pool de capacidad del sistema de archivos. Para garantizar la integridad de los datos, ONTAP realiza una operación de lectura en el pool de capacidad inmediatamente después de realizar una operación de escritura. La estadística `Sum` es el número total de bytes leídos desde el nivel del pool de capacidad del sistema de archivos durante un período específico. Para calcular los bytes del pool de capacidad por segundo, divida la estadística `Sum` entre los segundos de un período específic o. Unidades: bytes Estadísticas válidas: `Sum`

Métrica	Descripción
`CapacityPoolReadOperations`	El número de operaciones de lectura (E/S de red) desde el nivel del pool de capacidad del sistema de archivos. Esto se traduce en una solicitud de lectura del pool de capacidad. Para garantizar la integridad de los datos, ONTAP realiza una operación de lectura en el pool de capacidad inmediatamente después de realizar una operación de escritura. La estadística `Sum` es el número total de operaciones de lectura del pool de capacidad del sistema de archivos durante un período específico. Para calcular las solicitudes de pool de capacidad por segundo, divida la estadística `Sum` entre los segundos de un período específico. Unidades: recuento Estadísticas válidas: `Sum`

Métrica	Descripción
`CapacityPoolWriteBytes`	El número de bytes escritos (E/S de red) en el nivel del pool de capacidad del sistema de archivos. Para garantizar la integridad de los datos, ONTAP realiza una operación de lectura en el pool de capacidad inmediatamente después de realizar una operación de escritura. La estadística `Sum` es el número total de bytes escritos en el nivel del pool de capacidad del sistema de archivos durante un período específico. Para calcular los bytes del pool de capacidad por segundo, divida la estadística `Sum` entre los segundos de un período específico. Unidades: bytes Estadísticas válidas: `Sum`

Métrica	Descripción
`CapacityPoolWriteOperations`	El número de operaciones de escritura (E/S de red) en el sistema de archivos desde el nivel del pool de capacidad. Esto se traduce en una solicitud de escritura. Para garantizar la integridad de los datos, ONTAP realiza una operación de lectura en el pool de capacidad inmediatamente después de realizar una operación de escritura. La estadística `Sum` es el número total de operaciones de escritura en el nivel del pool de capacidad del sistema de archivos durante un período específico. Para calcular las solicitud es de pool de capacidad por segundo, divida la estadística `Sum` entre los segundos de un período específico. Unidades: recuento Estadísticas válidas: `Sum`

Métricas del servidor de archivos

Todas estas métricas ocupan una dimensión, `FileSystemId`.

Métrica	Descripción
`CPUUtilization`	El porcentaje de utilización de los recursos de CPU del sistema de archivos. La estadística `Average` es el uso medio de la CPU del sistema de archivos durante un período específico.

Métrica	Descripción
	La estadística `Minimum` es la utilización más baja de la CPU del sistema de archivos durante un período específico. La estadística `Maximum` es la utilización máxima de la CPU del sistema de archivos durante un período específico. Unidades: porcentaje Estadísticas válidas: `Average`, `Minimum` y `Maximum`.
`FileServerDiskThroughputUtilization`	El rendimiento del disco entre el servidor de archivos y el nivel principal, expresado en porcentaje del límite aprovisionado determinado por la capacidad de rendimiento. La estadística `Average` es el porcentaje medio de utilización del rendimiento del disco de los servidores de archivos durante un período específico. La estadística `Minimum` es el porcentaje más bajo de utilización del rendimiento del disco de los servidores de archivos durante un período específico. La estadística `Maximum` es la utilización máxima del rendimiento del disco de los servidores de archivos durante un período específico. Unidades: porcentaje Estadísticas válidas: `Average`, `Minimum` y `Maximum`.

Métrica	Descripción
`FileServerDiskThroughputBalance`	El porcentaje de créditos de ráfaga disponibles para el rendimiento de disco entre el servidor de archivos y el nivel primario. Esto es válido para los sistemas de archivos que se aprovisio nan con una capacidad de rendimiento de 512 MBps o menos. La estadística `Average` es el balance medio de ráfagas disponible durante un período específic o. La estadística `Minimum` es el saldo de ráfagas mínimo disponible durante un período específic o. La estadística `Maximum` es el saldo máximo de ráfagas disponible durante un período específic o. Unidades: porcentaje Estadísticas válidas: `Average`, `Minimum` y `Maximum`.

Métrica	Descripción
`FileServerDiskIopsBalance`	El porcentaje de créditos de ráfaga disponibles para las IOPS de disco entre el servidor de archivos y el nivel principal. Esto es válido para los sistemas de archivos aprovisionados con una capacidad de rendimiento de 512 MBps o menos. La estadística `Average` es el balance medio de ráfagas disponible durante un período específico. La estadística `Minimum` es el saldo de ráfagas mínimo disponible durante un período específico. La estadística `Maximum` es el saldo máximo de ráfagas disponible durante un período específico. Unidades: porcentaje Estadísticas válidas: `Average`, `Minimum` y `Maximum`.

Métrica	Descripción
`FileServerDiskIopsUtilization`	El porcentaje de IOPS de utilización de la capacidad de IOPS de disco disponible para el servidor de archivos. La estadística `Average` es la utilización media de las IOPS de disco del sistema de archivos durante un período específico. La estadística `Minimum` es la utilización mínima de IOPS de disco del sistema de archivos durante un período específico. La estadística `Maximum` es la utilización máxima de IOPS de disco del sistema de archivos durante un período específico. Unidades: porcentaje Estadísticas válidas: `Average`, `Minimum` y `Maximum`.

Métrica	Descripción
`FileServerCacheHitRatio`	El porcentaje de todas las solicitudes de lectura que se atienden mediante datos en las cachés RAM y NVMe del sistema de archivos. Un porcentaje más alto significa que las cachés de lectura del sistema de archivos atienden más lecturas. Unidades: porcentaje La estadística `Average` es el porcentaje medio de visitas a la memoria caché del sistema de archivos durante un período específico. La estadística `Minimum` es el porcentaje más bajo de visitas a la memoria caché del sistema de archivos durante un período específico. La estadística `Maximum` es el porcentaje más alto de aciertos de caché del sistema de archivos durante un período específico. Estadísticas válidas: `Average`, `Minimum` y `Maximum`

Métricas de E/S de disco

Todas estas métricas tienen una dimensión, `FileSystemId`.

Métrica	Descripción
`DiskReadBytes`	La cantidad de bytes (E/S de disco) de cualquier disco se lee en el nivel principal del sistema de archivos.

Métrica	Descripción
	La estadística `Sum` es el número total de bytes leídos del sistema de archivos durante un período específico. Para calcular el rendimiento de lectura en disco (bytes por segundo) de cualquier estadística `Sum`, divídala por los segundos del periodo especificado. Unidades: bytes Estadísticas válidas: `Sum`
`DiskWriteBytes`	El número de bytes (E/S de disco) de cualquier disco que se graba en el nivel principal del sistema de archivos. La estadística `Sum` es el número total de bytes escritos desde el sistema de archivos durante un período específico. Para calcular el rendimiento del disco de escritura (bytes por segundo) de cualquier estadística, divida la estadística `Sum` entre los segundos del período especificado. Unidades: bytes Estadísticas válidas: `Sum`

Métrica	Descripción
`DiskIopsUtilization`	Las IOPS de disco entre el servidor de archivos y los volúmenes de almacenamiento, como porcentaje del límite de IOPS de disco aprovisionado en los niveles principales. La estadística `Average` es la utilización media de las IOPS de disco del sistema de archivos durante un período específico. La estadística `Minimum` es la utilización mínima de IOPS de disco del sistema de archivos durante un período específico. La estadística `Maximum` es la utilización máxima de IOPS de disco del sistema de archivos durante un período específico. Unidades: porcentaje Estadísticas válidas: `Average`, `Minimum` y `Maximum`.
`DiskReadOperations`	El número de operaciones de lectura (E/S de disco) desde el nivel principal del sistema de archivos. La estadística `Sum` es el número total de operaciones de lectura del nivel principal durante un período específico. Unidades: recuento Estadísticas válidas: `Sum`

Métrica	Descripción
`DiskWriteOperations`	El número de operaciones de escritura (E/S de disco) en el nivel principal del sistema de archivos. La estadística `Sum` es el número total de operaciones de escritura en el nivel principal durante un período específico. Unidades: recuento Estadísticas válidas: `Sum`

Métricas de capacidad de almacenamiento

Todas estas métricas tienen una dimensión, `FileSystemId`.

Métrica	Descripción
`StorageEfficiencySavings`	Los bytes ahorrados gracias a las funciones de eficiencia del almacenamiento (compresión, deduplicación y compactación). La estadística `Average` es el ahorro medio de eficiencia del almacenamiento durante un período específico. Para calcular los ahorros en eficiencia del almacenamiento como un porcentaje de todos los datos almacenados, durante un período de un minuto, divida `StorageEfficiencySavings` entre la suma de `StorageEfficiencySavings` y la métrica del sistema de archivos `StorageUsed`, utilizando la estadística de `Sum` para `StorageUsed`.

Métrica	Descripción
	La estadística `Minimum` es el ahorro mínimo en eficiencia de almacenamiento durante un período específico. La estadística `Maximum` es el ahorro máximo en eficiencia de almacenamiento durante un período específico. Unidades: bytes Estadísticas válidas: `Average`, `Minimum` y `Maximum`
`StorageUsed`	La cantidad total de datos físicos almacenados en el sistema de archivos, tanto en el nivel principal (SSD) como en el nivel del pool de capacidad. Esta métrica incluye los ahorros derivados de las características de eficiencia del almacenamiento, como la compresión y la deduplicación de datos. Unidades: bytes Estadísticas válidas: `Average`, `Minimum` y `Maximum`

Métrica	Descripción
`LogicalDataStored`	La cantidad total de datos lógicos almacenados en el sistema de archivos, teniendo en cuenta tanto el nivel de SSD como el nivel del pool de capacidad. Esta métrica incluye el tamaño lógico total de las instantáneas FlexClone s, pero no incluye los ahorros en eficienci a de almacenamiento logrados mediante la compresión, la compactación y la deduplica ción. Para calcular el ahorro en bytes en términos de eficiencia de almacenamiento, tome el `Average` de `StorageUsed` durante un período determinado y réstelo del `Average` de `LogicalDataStored` durante el mismo período. Para calcular los ahorros en la eficiencia del almacenamiento como un porcentaje del tamaño total de los datos lógicos, tome el `Average` de `StorageUsed` durante un período determinado y réstelo del `Average` de `LogicalDataStored` durante el mismo período. A continuación, divida la diferencia entre `Average` de `LogicalDataStored` durante el mismo período. Unidades: bytes Estadísticas válidas: `Average`, `Minimum` y `Maximum`

Métricas detalladas del sistema de archivos

Las métricas detalladas del sistema de archivos son métricas detalladas de uso del almacenamiento para cada uno de sus niveles de almacenamiento. Todas las métricas detalladas del sistema de archivos tienen las dimensiones `FileSystemId`, `StorageTier` y `DataType`.

- La dimensión `StorageTier` indica el nivel de almacenamiento que mide la métrica, con valores posibles de `SSD` y `StandardCapacityPool`.
- La dimensión `DataType` indica el tipo de datos que mide la métrica, con el valor posible `All`.

Hay una fila para cada combinación única de un par clave-valor métrico y dimensional determinado, con una descripción de lo que mide esa combinación.

Métrica	Descripción
`StorageCapacityUtilization`	El uso de la capacidad de almacenamiento de cada uno de los agregados del sistema de archivos. Se emite una métrica por minuto para cada uno de los agregados del sistema de archivos. La `Average` estadística es la cantidad media de utilización de la capacidad de almacenam iento para el nivel de rendimiento del sistema de archivos durante el período especificado. La `Minimum` estadística es la cantidad más baja de utilización de la capacidad de almacenamiento para el nivel de rendimien to del sistema de archivos durante el período especificado. La `Maximum` estadística es la cantidad máxima de utilización de la capacidad de almacenam iento para el nivel de rendimiento del sistema de archivos durante el período especificado. Unidades: bytes

Métrica	Descripción
	Estadísticas válidas: `Average`, `Minimum` y `Maximum`
`StorageCapacity`	La capacidad de almacenamiento total del nivel principal (SSD). Unidades: bytes Estadísticas válidas: `Maximum`

Métrica	Descripción
`StorageUsed`	La capacidad de almacenamiento físico utilizada en bytes, específica del nivel de almacenamiento. Este valor incluye los ahorros derivados de las características de eficienci a del almacenamiento, como la compresión y la deduplicación de datos. Los valores de dimensión válidos para `StorageTier` son `SSD` y `StandardCapacityPool` , correspon dientes al nivel de almacenamiento que mide esta métrica. Esta métrica también requiere la dimensión `DataType` con el valor `All`. Las estadísticas `Average`, `Minimum` y `Maximum` representan el consumo de almacenamiento por nivel en bytes durante un período determinado. Para calcular la utilización de la capacidad de almacenamiento de su nivel de almacenam iento principal (SSD), divida cualquiera de estas estadísticas entre `Maximum` `StorageCa pacity` al mismo período, con la dimensión `StorageTier` igual a `SSD`. Para calcular la capacidad de almacenam iento libre de su nivel de almacenamiento principal (SSD) en bytes, reste cualquiera de estas estadísticas del `Maximum` `StorageCa pacity` durante el mismo período y obtenga la dimensión `StorageTier` igual a `SSD`. Unidades: bytes Estadísticas válidas: `Average`, `Minimum` y `Maximum`

Métricas del sistema de archivos escalables

Se proporcionan las siguientes métricas para FSx para sistemas de archivos ONTAP con dos o más pares de alta disponibilidad (HA). Para las métricas, se emite un punto de datos para cada par de HA y para cada agregado (para las métricas de uso del almacenamiento).

> **Note**
>
> Si tiene un sistema de archivos con varios pares de HA, también puede utilizar las métricas del sistema de archivos de un solo par de HA y las métricas de volumen.

Temas

Métricas de E/S de red

Todas estas métricas tienen dos dimensiones, `FileSystemId` y `FileServer`.

- `FileSystemId`— El ID de AWS recurso de su sistema de archivos.
- `FileServer`— El nombre de un servidor de archivos (o nodo) de ONTAP (por ejemplo,`FsxId01234567890abcdef-01`). Los servidores de archivos con números impares son los servidores de archivos preferidos (es decir, prestan servicio al tráfico a menos que el sistema de archivos se haya transferido por error al servidor de archivos secundario), mientras que los servidores de archivos con números pares son servidores de archivos secundarios (es decir, solo atienden el tráfico cuando su socio no está disponible). Por este motivo, los servidores de archivos secundarios suelen utilizar menos que los servidores de archivos preferidos.

Métrica	Descripción
`NetworkThroughputUtilization`	Utilización del rendimiento de la red como porcentaje del rendimiento de la red disponibl e para el sistema de archivos. Esta métrica

Métrica	Descripción
	equivale al máximo `NetworkSentBytes` y `NetworkReceivedBytes` a un porcentaje de la capacidad de rendimiento de la red de un par de alta disponibilidad para su sistema de archivos. En esta métrica se tiene en cuenta todo el tráfico, incluidas las tareas en segundo plano (como SnapMirror la organización en niveles y las copias de seguridad). Se emite una métrica por minuto para cada uno de los servidores de archivos del sistema de archivos. La `Average` estadística es la utilización media del rendimiento de la red para un servidor de archivos determinado durante el período especificado. La `Minimum` estadística es la utilización más baja del rendimiento de la red para un servidor de archivos determinado en un minuto, durante el período especificado. La `Maximum` estadística es la utilización máxima del rendimiento de la red para un servidor de archivos determinado durante un minuto, durante el período especificado. Unidades: porcentaje Estadísticas válidas: `Average`, `Minimum` y `Maximum`.

Métrica	Descripción
`NetworkSentBytes`	El número de bytes (E/S de red) enviados por el sistema de archivos. En esta métrica se tiene en cuenta todo el tráfico, incluidas las tareas en segundo plano (como SnapMirror la organizac ión en niveles y las copias de seguridad). Se emite una métrica por minuto para cada uno de los servidores de archivos del sistema de archivos. La `Sum` estadística es el número total de bytes enviados a través de la red por el servidor de archivos en cuestión durante el período especificado. La `Average` estadística es el número medio de bytes enviados a través de la red por el servidor de archivos determinado durante el período especificado. La `Minimum` estadística es el número más bajo de bytes enviados a través de la red por el servidor de archivos en cuestión durante el período especificado. La `Maximum` estadística es el número máximo de bytes enviados a través de la red por el servidor de archivos en cuestión durante el período especificado. Para calcular el rendimiento enviado (bytes por segundo) de cualquier estadística, divídala por los segundos del periodo especificado. Unidades: bytes

Métrica	Descripción
	Estadísticas válidas:`Sum`, `AverageMinimum`, y `Maximum`

Métrica	Descripción
`NetworkReceivedBytes`	El número de bytes (E/S de red) que recibe el sistema de archivos. En esta métrica se tiene en cuenta todo el tráfico, incluidas las tareas en segundo plano (como SnapMirror la organizac ión en niveles y las copias de seguridad). Se emite una métrica por minuto para cada uno de los servidores de archivos del sistema de archivos. La `Sum` estadística es el número total de bytes recibidos a través de la red por el servidor de archivos en cuestión durante el período especificado. La `Average` estadística es el número medio de bytes recibidos a través de la red por un servidor de archivos determinado cada minuto durante el período especificado. La `Minimum` estadística es el número más bajo de bytes recibidos a través de la red por el servidor de archivos determinado cada minuto durante el período especificado. La `Maximum` estadística es el número más alto de bytes recibidos a través de la red por el servidor de archivos determinado cada minuto durante el período especificado. Para calcular el rendimiento recibido (bytes por segundo) de cualquier estadística, divida la estadística por los segundos del período. Unidades: bytes

Métrica	Descripción
	Estadísticas válidas:`Sum`,, y `Average` `Minimum` `Maximum`

Métricas del servidor de archivos

Todas estas métricas tienen dos dimensiones, `FileSystemId` y `FileServer`.

Métrica	Descripción
`CPUUtilization`	El porcentaje de utilización de los recursos de CPU del sistema de archivos. Se emite una métrica por minuto para cada uno de los servidores de archivos de su sistema de archivos. La estadística `Average` es el uso medio de la CPU del sistema de archivos durante un período específico. La `Minimum` estadística es la utilización más baja de la CPU para el servidor de archivos determinado durante el período especificado. La `Maximum` estadística es la utilización máxima de la CPU para el servidor de archivos determinado durante el período especificado. Unidades: porcentaje Estadísticas válidas: `Average`, `Minimum` y `Maximum`.
`FileServerDiskThroughputUtilization`	El rendimiento del disco entre el servidor de archivos y el conjunto, expresado como un porcentaje del límite aprovisionado determinado por la capacidad de rendimiento. En esta

Métrica	Descripción
	métrica se tiene en cuenta todo el tráfico, incluidas las tareas en segundo plano (como la organización en niveles SnapMirror y las copias de seguridad). Esta métrica equivale a la suma `DiskReadBytes` y `DiskWriteBytes` el porcentaje de la capacidad de rendimiento del disco del servidor de archivos de un par de alta disponibilidad para su sistema de archivos. Se emite una métrica por minuto para cada uno de los servidores de archivos del sistema de archivos. La `Average` estadística es la utilización media del rendimiento del disco del servidor de archivos en cuestión durante el período especificado. La `Minimum` estadística es la utilización más baja del rendimiento de disco del servidor de archivos para el servidor de archivos determina do durante el período especificado. La `Maximum` estadística es la utilización máxima del rendimiento de disco del servidor de archivos para el servidor de archivos determinado durante el período especificado. Unidades: porcentaje Estadísticas válidas: `Average`, `Minimum` y `Maximum`.

Métrica	Descripción
`FileServerDiskIopsUtilization`	El uso de IOPS de la capacidad de IOPS de disco disponible para el servidor de archivos, expresado como porcentaje del límite de IOPS de disco. Esto se diferencia de `DiskIopsUtilization` la utilización de las IOPS de disco por encima del máximo que puede gestionar el servidor de archivos, a diferenci a de las IOPS de disco aprovisionadas. En esta métrica se tiene en cuenta todo el tráfico, incluidas las tareas en segundo plano (como la organización en niveles SnapMirror y las copias de seguridad). Se emite una métrica por minuto para cada uno de los servidores de archivos del sistema de archivos. La `Average` estadística es la utilización media de IOPS de disco para el servidor de archivos determinado durante el período especificado. La `Minimum` estadística es la menor utilización de IOPS de disco para el servidor de archivos determinado durante el período especificado. La `Maximum` estadística es la mayor utilización de IOPS de disco para el servidor de archivos determinado durante el período especificado. Unidades: porcentaje Estadísticas válidas: `Average`, `Minimum` y `Maximum`.

Métrica	Descripción
`FileServerCacheHitRatio`	El porcentaje de todas las solicitudes de lectura atendidas por datos que residen en las memorias RAM o NVMe del sistema de archivos para cada uno de los pares de alta disponibilidad (por ejemplo, el servidor de archivos activo de un par de alta disponibi lidad). Un porcentaje más alto indica una mayor proporción entre las lecturas almacenadas en caché y el total de lecturas. Se tienen en cuenta todas las E/S, incluidas las tareas en segundo plano (como SnapMirror la organizac ión en niveles y las copias de seguridad). Se emite una métrica por minuto para cada uno de los servidores de archivos del sistema de archivos. Unidades: porcentaje La `Average` estadística es la tasa media de aciertos de caché de uno de los pares de alta disponibilidad del sistema de archivos durante el período especificado. La `Minimum` estadística es la tasa de aciertos de caché más baja de uno de los pares de alta disponibilidad del sistema de archivos durante el período especificado. La `Maximum` estadística es la tasa de aciertos de caché más alta de uno de los pares de alta disponibilidad del sistema de archivos durante el período especificado. Estadísticas válidas: `Average`, `Minimum` y `Maximum`

Métricas de E/S de disco

Todas estas métricas tienen dos dimensiones, `FileSystemId` y `Aggregate`.

- `FileSystemId`— El ID de AWS recurso de su sistema de archivos.
- `Aggregate`— El nivel de rendimiento de su sistema de archivos se compone de varios grupos de almacenamiento denominados agregados. Hay un agregado para cada par de alta disponibilidad. Por ejemplo, agregue los `aggr1` mapas al servidor de archivos `FsxId01234567890abcdef-01` (el servidor de archivos activo) y al servidor de archivos `FsxId01234567890abcdef-02` (el servidor de archivos secundario) en un par HA.

Métrica	Descripción
`DiskReadBytes`	El número de bytes (E/S de disco) de cualquier disco se lee de este agregado. En esta métrica se tiene en cuenta todo el tráfico, incluidas las tareas en segundo plano (como SnapMirro r la organización en niveles y las copias de seguridad). Se emite una métrica por minuto para cada uno de los agregados del sistema de archivos. La `Sum` estadística es el número total de bytes leídos por minuto del agregado dado durante el período especificado. La `Average` estadística es el número medio de bytes leídos por minuto del agregado dado durante el período especificado. La `Minimum` estadística es el número más bajo de bytes leídos por minuto del agregado dado durante el período especificado. La `Maximum` estadística es el número más alto de bytes leídos por minuto del agregado dado durante el período especificado.

Métrica	Descripción
	Para calcular el rendimiento del disco de lectura (bytes por segundo) de cualquier estadística, divida la estadística por los segundos del período. Unidades: bytes Estadísticas válidas:`Sum`,, y `Average` `Minimum` `Maximum`

Métrica	Descripción
`DiskWriteBytes`	El número de bytes (E/S de disco) de cualquier disco que se graba en este agregado. En esta métrica se tiene en cuenta todo el tráfico, incluidas las tareas en segundo plano (como SnapMirror la organización en niveles y las copias de seguridad). Se emite una métrica por minuto para cada uno de los agregados del sistema de archivos. La `Sum` estadística es el número total de bytes escritos en el agregado dado durante el período especificado. La `Average` estadística es el número promedio de bytes escritos en el agregado dado cada minuto durante el período especificado. La `Minimum` estadística es el número más bajo de bytes escritos en el agregado dado cada minuto durante el período especificado. La `Maximum` estadística es el número más alto de bytes escritos en el agregado dado cada minuto durante el período especificado. Para calcular el rendimiento del disco de escritura (bytes por segundo) de cualquier estadística, divida la estadística entre los segundos del período especificado. Unidades: bytes Estadísticas válidas:`Sum`, `Average` `Minimum`, y `Maximum`

Métrica	Descripción
`DiskIopsUtilization`	El uso de IOPS de disco de un agregado, expresado como porcentaje del límite de IOPS de disco del agregado (es decir, el total de IOPS del sistema de archivos dividido por el número de pares de alta disponibilidad del sistema de archivos). Esto se diferencia `FileServerDiskIopsUtilization` en que se trata de la utilización de las IOPS de disco aprovisionadas en relación con el límite de IOPS aprovisionadas, a diferenci a de las IOPS de disco máximas admitidas por el servidor de archivos (es decir, según la capacidad de rendimiento configurada por par de HA). En esta métrica se tiene en cuenta todo el tráfico, incluidas las tareas en segundo plano (como SnapMirror la organización en niveles y las copias de seguridad). Se emite una métrica por minuto para cada uno de los agregados del sistema de archivos. La `Average` estadística es la utilización media de las IOPS del disco para un agregado determinado durante el período especificado. La `Minimum` estadística es la utilización más baja de IOPS de disco para el agregado dado durante el período especificado. La `Maximum` estadística es la utilización más alta de IOPS de disco para el agregado dado durante el período especificado. Unidades: porcentaje Estadísticas válidas: `Average`, `Minimum` y `Maximum`.

Métrica	Descripción
`DiskReadOperations`	El número de operaciones de lectura (E/S de disco) de este agregado. En esta métrica se tiene en cuenta todo el tráfico, incluidas las tareas en segundo plano (como SnapMirro r la organización en niveles y las copias de seguridad). Se emite una métrica por minuto para cada uno de los agregados del sistema de archivos. La `Sum` estadística es el número total de operaciones de lectura realizadas por el agregado en cuestión durante el período especificado. La `Average` estadística es el número medio de operaciones de lectura realizadas cada minuto por un agregado determinado durante el período especificado. La `Minimum` estadística es el número más bajo de operaciones de lectura realizadas cada minuto por el agregado dado durante el período especificado. La `Maximum` estadística es el número más alto de operaciones de lectura realizadas cada minuto por el agregado dado durante el período especificado. Para calcular el promedio de IOPS de disco durante el período, utilice la `Average` estadísti ca y divida el resultado entre 60 (segundos). Unidades: recuento

Métrica	Descripción
	Estadísticas válidas:`Sum`,`Average`, y `Minimum` `Maximum`
`DiskWriteOperations`	El número de operaciones de escritura (E/S de disco) en este agregado. En esta métrica se tiene en cuenta todo el tráfico, incluidas las tareas en segundo plano (como SnapMirro r la organización en niveles y las copias de seguridad). Se emite una métrica por minuto para cada uno de los agregados del sistema de archivos. La `Sum` estadística es el número total de operaciones de escritura realizadas por un agregado determinado durante el período especificado. La `Average` estadística es el número medio de operaciones de escritura realizadas cada minuto por un agregado determinado durante el período especificado. Para calcular el promedio de IOPS de disco durante el período, utilice la `Average` estadísti ca y divida el resultado entre 60 (segundos). Unidades: recuento Estadísticas válidas: y `Sum` `Average`

Métricas detalladas del sistema de archivos

Las métricas detalladas del sistema de archivos son métricas detalladas de uso del almacenamiento para cada uno de sus niveles de almacenamiento. Las métricas detalladas del sistema de archivos tienen `DataType` las dimensiones `FileSystemId``StorageTier`, y o las `FileSystemId` `Aggregate` dimensiones `StorageTierDataType`, y.

- Si no se proporciona la `Aggregate` dimensión, las métricas son para todo el sistema de archivos. `StorageCapacity`Las métricas `StorageUsed` y tienen un único punto de datos por minuto que corresponde al almacenamiento total consumido del sistema de archivos (por nivel de almacenamiento) y a la capacidad de almacenamiento total (para el nivel SSD). Mientras tanto, la `StorageCapacityUtilization` métrica emite una métrica por minuto para cada agregado.
- Cuando se proporciona la `Aggregate` dimensión, las métricas son para cada agregado.

El significado de las dimensiones es el siguiente:

- `FileSystemId`— El ID de AWS recurso de su sistema de archivos.
- `Aggregate`— El nivel de rendimiento de su sistema de archivos se compone de varios grupos de almacenamiento denominados agregados. Hay un agregado para cada par de alta disponibilidad. Por ejemplo, agregue los `aggr1` mapas al servidor de archivos `FsxId01234567890abcdef-01` (el servidor de archivos activo) y al servidor de archivos `FsxId01234567890abcdef-02` (el servidor de archivos secundario) en un par HA.
- `StorageTier`— Indica el nivel de almacenamiento que mide la métrica, con valores posibles de `SSD` y`StandardCapacityPool`.
- `DataType`— Indica el tipo de datos que mide la métrica, con el valor posible`All`.

Hay una fila para cada combinación única de un par clave-valor métrico y dimensional determinado, con una descripción de lo que mide esa combinación.

Métrica	Descripción
`StorageCapacityUtilization`	El uso de la capacidad de almacenamiento de un conjunto de sistemas de archivos determina do. Se emite una métrica por minuto para cada uno de los agregados del sistema de archivos. La `Average` estadística es la cantidad promedio de utilización de la capacidad de almacenamiento para un agregado determina do durante el período especificado. La `Minimum` estadística es la cantidad mínima de utilización de la capacidad de almacenam

Métrica	Descripción
	iento para un agregado determinado durante el período especificado. La `Maximum` estadística es la cantidad máxima de utilización de la capacidad de almacenam iento para un agregado determinado durante el período especificado. Unidades: bytes Estadísticas válidas: `Average`, `Minimum` y `Maximum`
`StorageCapacity`	La capacidad de almacenamiento de un conjunto de sistemas de archivos determinado. Se emite una métrica por minuto para cada uno de los agregados del sistema de archivos. La `Average` estadística es la cantidad media de capacidad de almacenamiento de un agregado determinado durante el período especificado. La `Minimum` estadística es la cantidad mínima de capacidad de almacenamiento para un agregado determinado durante el período especificado. La `Maximum` estadística es la cantidad máxima de capacidad de almacenamiento para un agregado determinado durante el período especificado. Unidades: bytes Estadísticas válidas: `Average`, `Minimum` y `Maximum`

Métrica	Descripción
`StorageUsed`	La capacidad de almacenamiento físico utilizada en bytes, específica del nivel de almacenamiento. Este valor incluye los ahorros derivados de las características de eficienci a del almacenamiento, como la compresión y la deduplicación de datos. Los valores de dimensión válidos para `StorageTier` son `SSD` y `StandardCapacityPool` , correspon dientes al nivel de almacenamiento que mide esta métrica. Se emite una métrica por minuto para cada uno de los agregados del sistema de archivos. La `Average` estadística es la cantidad promedio de capacidad de almacenamiento físico consumida en un nivel de almacenam iento determinado por el agregado en cuestión durante el período especificado. La `Minimum` estadística es la cantidad mínima de capacidad de almacenamiento físico consumida en un nivel de almacenamiento determinado por el agregado en cuestión durante el período especificado. La `Maximum` estadística es la cantidad máxima de capacidad de almacenamiento físico consumida en un nivel de almacenamiento determinado por un agregado determinado durante el período especificado. Unidades: bytes Estadísticas válidas: `Average`, `Minimum` y `Maximum`

Métricas de volumen

Su sistema de archivos Amazon FSx para NetApp ONTAP puede tener uno o más volúmenes que almacenen sus datos. Cada uno de estos volúmenes tiene un conjunto de métricas, que se clasifican como Métricas de volumen o Métricas de volumen detalladas.

- Las Métricas de volumen son métricas de rendimiento y almacenamiento por volumen que tienen dos dimensiones, `FileSystemId` y `VolumeId`. `FileSystemId` se asigna al sistema de archivos al que pertenece el volumen.
- Las métricas de volumen detalladas son per-storage-tier métricas que miden el consumo de almacenamiento por nivel con la `StorageTier` dimensión (con valores posibles de `SSD` y`StandardCapacityPool`) y por tipo de datos con la `DataType` dimensión (con valores posibles de `UserSnapshot`, y`Other`). Estas métricas tienen las dimensiones `FileSystemId`, `VolumeId`, `StorageTier` y `DataType`.

Temas

Métricas de E/S de red

Todas estas métricas tienen dos dimensiones, `FileSystemId` y `VolumeId`.

Métrica	Descripción
`DataReadBytes`	El número de bytes (E/S de red) leídos del volumen por los clientes. La estadística `Sum` es el número total de bytes asociados a operaciones de lectura durante el periodo especificado. Para calcular el rendimiento medio (bytes por segundo) de un periodo, divida la estadística `Sum` por el número de segundos del periodo especificado. Unidades: bytes

Métrica	Descripción
	Estadísticas válidas: `Sum`
`DataWriteBytes`	El número de bytes (E/S de red) escritos en el volumen por los clientes. La estadística `Sum` es el número total de bytes asociados a operaciones de escritura durante el periodo especificado. Para calcular el rendimiento medio (bytes por segundo) de un periodo, divida la estadística `Sum` por el número de segundos del periodo especificado. Unidades: bytes Estadísticas válidas: `Sum`
`DataReadOperations`	El número de operaciones de lectura (E/S de red) en el volumen por parte de los clientes. La estadística `Sum` es el número total de operaciones de lectura durante el periodo especificado. Para calcular la media de operaciones de lectura por segundo de un periodo, divida la estadística `Sum` por el número de segundos del periodo especificado. Unidades: recuento Estadísticas válidas: `Sum`

Métrica	Descripción
`DataWriteOperations`	El número de operaciones de escritura (E/S de red) realizadas por los clientes en el volumen. La estadística `Sum` es el número total de operaciones de escritura durante el periodo especificado. Para calcular la media de operaciones de escritura por segundo de un periodo, divida la estadística `Sum` por el número de segundos del periodo especificado. Unidades: recuento Estadísticas válidas: `Sum`
`MetadataOperations`	Número de operaciones de E/S (E/S de red) desde las actividades de metadatos de los clientes hasta el volumen. La estadística `Sum` es el número total de operaciones de metadatos durante el período especificado. Para calcular la media de operaciones de metadatos por segundo durante un periodo, divida la estadística `Sum` por el número de segundos del periodo especificado. Unidades: recuento Estadísticas válidas: `Sum`

Métrica	Descripción
`DataReadOperationTime`	La suma del tiempo total dedicado dentro del volumen a las operaciones de lectura (E/S de red) de los clientes que acceden a los datos del volumen. La estadística `Sum` es el número total de segundos empleados por las operaciones de lectura durante el periodo especificado. Para calcular la latencia de lectura media de un período, divida la estadística `Sum` entre la `Sum` de la métrica `DataReadOperations` del mismo período. Unidades: segundos Estadísticas válidas: `Sum`
`DataWriteOperationTime`	La suma del tiempo total empleado dentro del volumen para realizar las operaciones de escritura (E/S de red) de los clientes que acceden a los datos del volumen. La estadística `Sum` es el número total de segundos empleados por las operaciones de escritura durante el periodo especificado. Para calcular la latencia de escritura media de un período, divida la estadística `Sum` entre `Sum` y la métrica `DataWriteOperations` del mismo período. Unidades: segundos Estadísticas válidas: `Sum`

Métrica	Descripción
`MetadataOperationTime`	La suma del tiempo total empleado dentro del volumen para realizar las operaciones de metadatos (E/S de red) de los clientes que acceden a los datos del volumen. La estadística `Sum` es el número total de segundos empleados por las operaciones de lectura durante el periodo especificado. Para calcular la latencia media de un período, divida la estadística `Sum` por la `Sum` del `MetadataOperations` durante el mismo periodo. Unidades: segundos Estadísticas válidas: `Sum`
`CapacityPoolReadBytes`	El número de bytes leídos (E/S de red) del nivel del pool de capacidad del volumen. Para garantizar la integridad de los datos, ONTAP realiza una operación de lectura en el pool de capacidad inmediatamente después de realizar una operación de escritura. La estadística `Sum` es el número total de bytes leídos del nivel del pool de capacidad del volumen durante un período específico. Para calcular los bytes del conjunto de capacidad por segundo, divida la estadística `Sum` entre los segundos de un período específico. Unidades: bytes Estadísticas válidas: `Sum`

Métrica	Descripción
`CapacityPoolReadOperations`	El número de operaciones de lectura (E/S de red) del nivel del pool de capacidad del volumen. Esto se traduce en una solicitud de lectura del pool de capacidad. Para garantizar la integridad de los datos, ONTAP realiza una operación de lectura en el pool de capacidad inmediatamente después de realizar una operación de escritura. La estadística `Sum` es el número total de operaciones de lectura del nivel del pool de capacidad del volumen durante un período específico. Para calcular las solicitudes de grupos de capacidad por segundo, divida la estadística `Sum` entre los segundos de un período específico. Unidades: recuento Estadísticas válidas: `Sum`

Métrica	Descripción
`CapacityPoolWriteBytes`	El número de bytes escritos (E/S de red) en el nivel del pool de capacidad del volumen. Para garantizar la integridad de los datos, ONTAP realiza una operación de lectura en el pool de capacidad inmediatamente después de realizar una operación de escritura. La estadística `Sum` es el número total de bytes escritos en el nivel del pool de capacidad del volumen durante un período específico. Para calcular los bytes del pool de capacidad por segundo, divida la estadística `Sum` entre los segundos de un período específico. Unidades: bytes Estadísticas válidas: `Sum`

Métrica	Descripción
`CapacityPoolWriteOperations`	El número de operaciones de escritura (E/S de red) en el volumen desde el nivel del pool de capacidad. Esto se traduce en una solicitud de escritura. Para garantizar la integridad de los datos, ONTAP realiza una operación de lectura en el pool de capacidad inmediatamente después de realizar una operación de escritura. La estadística `Sum` es el número total de operaciones de escritura en el nivel del pool de capacidad del volumen durante un período específico. Para calcular las solicitudes de pool de capacidad por segundo, divida la estadística `Sum` entre los segundos de un período específico. Unidades: recuento Estadísticas válidas: `Sum`

Métricas de capacidad de almacenamiento

Todas estas métricas tienen dos dimensiones, `FileSystemId` y `VolumeId`.

Métrica	Descripción
`StorageCapacity`	El tamaño del volumen en bytes. Unidades: bytes Estadísticas válidas: `Maximum`
`StorageUsed`	La capacidad de almacenamiento lógico utilizada del volumen.

Métrica	Descripción
	Unidades: bytes Estadísticas válidas: `Average`, `Minimum` y `Maximum`
`StorageCapacityUtilization`	La utilización de la capacidad de almacenam iento del volumen. Unidades: porcentaje Estadísticas válidas: `Average`
`FilesUsed`	Los archivos utilizados (número de archivos o inodos) en el volumen. Unidades: recuento Estadísticas válidas: `Average`, `Minimum` y `Maximum`
`FilesCapacity`	El número total de inodos que se pueden crear en el volumen. Unidades: recuento Estadísticas válidas: `Maximum`

Métricas de volumen detalladas

Las métricas de volumen detalladas tienen más dimensiones que las métricas de volumen, lo que permite realizar mediciones más detalladas de los datos. Todas las métricas de volumen detalladas tienen las dimensiones `FileSystemId`, `VolumeId`, `StorageTier`, y `DataType`.

- La dimensión `StorageTier` indica el nivel de almacenamiento que mide la métrica, con valores posibles de `All`, `SSD` y `StandardCapacityPool`.
- La dimensión `DataType` indica el tipo de datos que mide la métrica, con valores posibles de `All`, `User`, `Snapshot` y `Other`.

En la siguiente tabla se define lo que mide la métrica `StorageUsed` para las dimensiones enumeradas.

Métrica	Descripción
`StorageUsed`	La cantidad de espacio lógico utilizado, en bytes. Esta métrica mide diferentes tipos de consumo de espacio en función de las dimensiones utilizadas con esta métrica. Cuando se establece `StorageTier` en `SSD` o `StandardCapacityPool` y se establece `DataType` en`All`, esta métrica mide el uso del espacio lógico de este volumen para los niveles de SSD y de pool de capacidad, respectiv amente. Cuando se establece la dimensión `DataType` en `User`, `Snapshot` o `Other` y se establece `StorageTier` en `All`, esta métrica mide el uso del espacio lógico para cada tipo de datos respectivo. El consumo de datos `Snapshot` incluye la reserva de instantáneas, que es el 5% del tamaño del volumen de forma predeterminada. Unidades: bytes Estadísticas válidas: `Average`, `Minimum` y `Maximum`
`StorageCapacityUtilization`	El porcentaje del espacio en disco físico utilizado por el volumen. Unidades: porcentaje Estadísticas válidas: `Maximum`

Advertencias y recomendaciones de rendimiento

FSx for ONTAP muestra una advertencia para CloudWatch las métricas 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 de Monitoring & performance (Monitoreo y rendimiento). Todas las advertencias de rendimiento activas o recientes de Amazon FSx y cualquier CloudWatch alarma configurada 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.

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

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. Estas recomendaciones describen cómo puede abordar un posible cuello de botella en el rendimiento. Puede tomar las medidas recomendadas si espera que la actividad 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 o la capacidad de almacenamiento del sistema de archivos, tal y como se describe en la siguiente tabla.

Sección de panel	Si hay una advertencia para esta métrica	Haga lo siguiente
Almacenamiento	Utilización de la capacidad de almacenamiento principal	Aumente la capacidad de almacenamiento principal de su sistema de archivos si su sistema de archivos aún no tiene la capacidad máxima de almacenamiento en SSD. Para obtener más información, consulte Modificación de la capacidad de almacenamiento de la SSD y las IOPS aprovisionadas. Si su sistema de archivos tiene varios pares de alta disponibilidad y la utilización de la capacidad de

Sección de panel	Si hay una advertencia para esta métrica	Haga lo siguiente
		almacenamiento principal solo es mayor para un subconjunto de los agregados del sistema de archivos (los grupos de almacenamiento que componen el nivel de almacenamiento principal), también puede reequilibrar la carga de trabajo para que la utilizaci ón de la capacidad de almacenamiento principal se distribuya de manera más uniforme en todo el sistema de archivos. Para obtener más información sobre cómo reequilibrar las cargas de trabajo, consulte. Supervisi ón de FSx para el equilibrio de la carga de trabajo de ONTAP
Rendimien to del servidor de archivos	Network throughput Rendimiento del disco IOPS de disco Utilización de la CPU	Aumente la capacidad de rendimiento de su sistema de archivos si su sistema de archivos aún no está al máximo de su capacidad de rendimiento. Para obtener más información sobre la actualización de la capacidad de rendimiento, consulte. Cómo modificar la capacidad de rendimiento Si su sistema de archivos tiene varios pares de alta disponibilidad y la utilización es alta solo para un subconjunto de servidores de archivos, también puede reequilibrar la carga de trabajo para que la carga de trabajo sea más uniforme y utilice las capacidad es de rendimiento de cada uno de los pares de alta disponibilidad del sistema de archivos. Para obtener más información sobre cómo reequilibrar las cargas de trabajo, consulte. Supervisión de FSx para el equilibrio de la carga de trabajo de ONTAP

Sección de panel	Si hay una advertencia para esta métrica	Haga lo siguiente
Desempeño de disco	IOPS de disco	Aumente las IOPS de SSD si su sistema de archivos aún no está al máximo de IOPS de SSD para la capacidad de rendimiento actual de su sistema de archivos. Para obtener más información sobre la actualización de las IOPS aprovisionadas del sistema de archivos, consulte. Modificación de la capacidad de almacenamiento de la SSD y las IOPS aprovisionadas Si su sistema de archivos tiene varios pares de alta disponibilidad y la utilización de las IOPS del disco solo es mayor para un subconjunto de los agregados del sistema de archivos (los grupos de almacenamiento que componen el nivel de almacenamiento principal), también puede reequilibrar la carga de trabajo para que las IOPS de disco se utilicen de manera más uniforme en todo el sistema de archivos. Para obtener más información sobre cómo reequilibrar las cargas de trabajo, consulte. Supervisión de FSx para el equilibrio de la carga de trabajo de ONTAP

Para obtener más información sobre el rendimiento del sistema de archivos, consulte Amazon FSx para NetApp el rendimiento de ONTAP.

Creación de CloudWatch alarmas de Amazon para monitorizar Amazon FSx

Puede crear una CloudWatch alarma que envíe un mensaje de Amazon Simple Notification Service (Amazon SNS) cuando la alarma cambie de estado. Una alarma vigila una métrica determinada durante el periodo especificado. Si es necesario, la alarma lleva a cabo una o más acciones basadas en el valor de la métrica en relación con un umbral dado durante una serie de períodos de tiempo. La acción es una notificación que se envía a un tema de Amazon SNS o a una política de Auto Scaling.

Las alarmas invocan acciones únicamente en caso de cambios de estado sostenidos. CloudWatch las alarmas no invocan acciones solo porque se encuentran en un estado determinado; el estado

debe haber cambiado y se ha mantenido durante un número específico de períodos. Puede crear una alarma desde la consola Amazon FSx o la consola Amazon CloudWatch .

Los siguientes procedimientos describen cómo crear alarmas utilizando la consola de Amazon FSx, AWS Command Line Interface (AWS CLI) y API.

Para configurar alarmas utilizando la consola de Amazon FSx

1. Abra la consola de Amazon FSx en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación izquierdo, elija Sistemas de archivos y, a continuación, elija el sistema de archivos para el que desee crear la alarma.
3. En la página Summary (Resumen), seleccione Monitoring & performance (Monitoreo y rendimiento) en el segundo panel.
4. Seleccione la pestaña de CloudWatch alarmas.
5. Selecciona Crear CloudWatch alarma. Se lo redirigirá a la consola de CloudWatch.
6. Elija Seleccionar métrica.
7. En la sección de Métricas, elija FSx.
8. Seleccione una categoría de métrica:
   - Métricas del sistema de archivos
   - Métricas detalladas del sistema de archivos
   - Métricas de volumen
   - Métricas de volumen detalladas
9. Seleccione la métrica para la que desea configurar la alarma y, a continuación, seleccione Seleccionar métrica.
10. En la sección Condiciones, elija las condiciones que desee para la alarma y, a continuación, elija 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, consulta Cómo CloudWatch las alarmas tratan los datos faltantes en la Guía del CloudWatch usuario de Amazon.

11. Si CloudWatch quieres enviarte un correo electrónico o una notificación de Amazon SNS cuando el estado de alarma inicie la acción, selecciona un estado de alarma para Activar el estado de alarma.

    En Enviar una notificación al siguiente tema de SNS, elija una opción. Si elige Create topic (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.

    > **Note**
    >
    > 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 recibirán ninguna notificación.

12. Rellene los campos Nombre de la alarma y Descripción de la alarma y, a continuación, seleccione Siguiente.
13. En la página Previsualizar y crear, revisa la alarma que vas a crear y, a continuación, selecciona Crear alarma.

Para configurar las alarmas mediante la consola CloudWatch

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. Seleccione Crear alarma para iniciar el Asistente de creación de alarma.
3. Siga el procedimiento descrito en Para configurar alarmas con la consola Amazon FSx, empezando por el paso 6.

Para configurar una alarma mediante el AWS CLI

- Llame al comando put-metric-alarmCLI. Para obtener más información, consulte Referencia de comandos de la AWS CLI.

Para configurar una alarma mediante la CloudWatch API

- Llame a la operación de la API PutMetricAlarm. Para obtener más información, consulta la referencia de la CloudWatch API de Amazon.

Supervisión de FSx para el equilibrio de la carga de trabajo de ONTAP

Si tiene un sistema de archivos con varios pares de alta disponibilidad, su rendimiento y rendimiento se distribuyen entre cada uno de los pares de alta disponibilidad. FSx for ONTAP equilibra automáticamente los archivos a medida que se escriben en el sistema de archivos, pero en raras ocasiones es posible que los datos de la carga de trabajo o la E/S se desequilibren entre los pares de alta disponibilidad, lo que puede afectar al rendimiento general de la carga de trabajo. Puede supervisar su carga de trabajo para asegurarse de que se mantenga equilibrada en cada uno de los pares de alta disponibilidad de su sistema de archivos (y sus correspondientes servidores de archivos y agregados, es decir, los grupos de almacenamiento que constituyen el nivel de almacenamiento principal).

Temas

Equilibrio de utilización del almacenamiento principal

La capacidad de almacenamiento principal del sistema de archivos se divide en partes iguales entre cada uno de sus pares de alta disponibilidad en grupos de almacenamiento denominados agregados. Cada par de HA tiene un agregado. Le recomendamos que mantenga una utilización promedio no superior al 80% para su nivel de almacenamiento principal de forma continua. Para los sistemas de archivos con varios pares de alta disponibilidad, le recomendamos que mantenga una utilización promedio de hasta el 80% para cada agregado.

Mantener una utilización del 80% garantiza que haya espacio libre para los nuevos datos entrantes y mantiene una sobrecarga considerable para las operaciones de mantenimiento, que pueden ocupar temporalmente espacio libre en sus agregados.

Si observa que sus agregados están desequilibrados, puede aumentar la capacidad de almacenamiento principal del sistema de archivos (aumentando proporcionalmente la capacidad de almacenamiento de cada agregado) o puede mover los volúmenes entre los agregados mediante el comando volume move de la CLI de ONTAP.

Desequilibrio en la utilización del rendimiento del disco y del servidor de archivos

Las capacidades de rendimiento total del sistema de archivos (como el rendimiento de la red, el rendimiento del servidor de archivos a disco y las IOPS y las IOPS del disco) se dividen en partes iguales entre los pares de alta disponibilidad del sistema de archivos. Le recomendamos que mantenga una utilización media inferior al 50% (y una utilización máxima máxima inferior al 80%) para todos los límites de rendimiento de forma continua; esto se aplica tanto a la utilización general de los recursos del servidor de archivos de su sistema de archivos en todos los pares de alta disponibilidad como a la utilización por servidor de archivos.

Si observa que el uso del rendimiento de su servidor de archivos está desequilibrado (y los servidores de archivos en los que su carga de trabajo está desequilibrada tienen un uso continuo superior al 80%), puede utilizar la CLI y la API REST de ONTAP para diagnosticar con más detalle la causa del desequilibrio de rendimiento y corregirlo. A continuación se incluye una tabla con los posibles indicadores de desequilibrio y los pasos a seguir para un diagnóstico más detallado.

Si su sistema de archivos es...	Entonces...
El rendimiento del disco del servidor de archivos o las IOPS del disco del servidor de archivos están desequilibrados	Es posible que se esté produciendo un bloqueo de E/S en un subconjunto de pares de alta disponibilidad (un subconjunto de sus volúmenes que contiene una enorme cantidad de datos a los que se accede), lo que puede limitar el rendimiento general de la carga de trabajo, ya que se ve obstruida con respecto a un subconjunto de pares de alta disponibilidad. Para cada servidor de archivos muy utilizado, compruebe los volúmenes más utilizados para ver qué volúmenes tienen la mayor

Si su sistema de archivos es...	Entonces...
	actividad dentro de un agregado. Si necesita más información sobre este procedimiento, consulte Reequilibrar los volúmenes muy utilizados.
El rendimiento de la red está desequilibrado, pero el rendimiento del disco del servidor de archivos, las IOPS del disco del servidor de archivos o las IOPS del disco no están desequilibradas	Sus datos se distribuyen uniformemente entre los pares de alta disponibilidad, pero sus clientes no. En el caso de los servidores de archivos que utilizan más el rendimiento de la red que otros, compruebe cuáles son los principales clientes de cada servidor de archivos y, a continuación, reequilibre esos clientes separando los volúmenes de esos clientes y volviéndolos a montar utilizando un punto final diferente en un par HA diferente. Si necesita más información sobre este procedimiento, consulte Reequilibrar los clientes de alto tráfico.

Asignación de CloudWatch dimensiones a los recursos de la CLI y la API REST de ONTAP

Tu sistema de archivos escalable tiene CloudWatch métricas de Amazon con la dimensión `FileServer` o`Aggregate`. Para seguir diagnosticando los casos de desequilibrio, debe asignar estos valores de dimensión a servidores de archivos (o nodos) y agregados específicos en la CLI de ONTAP o la API REST.

- En el caso de los servidores de archivos, cada nombre de servidor de archivos se asigna a un nombre de servidor de archivos (o nodo) en ONTAP (por ejemplo,). `FsxId01234567890abcdef-01` Los servidores de archivos con números impares son los servidores de archivos preferidos (es decir, prestan servicio al tráfico a menos que el sistema de archivos se haya transferido por error al servidor de archivos secundario), mientras que los servidores de archivos con números pares son servidores de archivos secundarios (es decir, solo atienden el tráfico cuando su socio no está disponible). Por este motivo, los servidores de archivos secundarios suelen utilizar menos que los servidores de archivos preferidos.
- En el caso de los agregados, cada nombre de agregado se asigna a un agregado en ONTAP (por ejemplo,`aggr1`). Hay un agregado para cada par de alta disponibilidad, `aggr1` es decir, el agregado lo comparten los servidores de archivos `FsxId01234567890abcdef-01` (el

servidor de archivos activo) y `FsxId01234567890abcdef-02` (el servidor de archivos secundario) en un par de alta disponibilidad, el agregado `aggr2` lo comparten los servidores `FsxId01234567890abcdef-03` de archivos`FsxId01234567890abcdef-04`, etc.

Puede ver las asignaciones entre todos los agregados y servidores de archivos mediante la CLI de ONTAP.

1. Para conectarse mediante SSH a la NetApp CLI de ONTAP de su sistema de archivos, siga los pasos descritos en la Uso de la NetApp ONTAP CLI sección de la Guía del usuario de Amazon FSx para NetApp ONTAP.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Utilice el comando storage aggregate show y especifique el parámetro. `-fields node`

   ```
   ::> storage aggregate show -fields node
   aggregate                    node
   ---------------------------- -------------------------
   aggr1                        FsxId01234567890abcdef-01
   aggr2                        FsxId01234567890abcdef-03
   aggr3                        FsxId01234567890abcdef-05
   aggr4                        FsxId01234567890abcdef-07
   aggr5                        FsxId01234567890abcdef-09
   aggr6                        FsxId01234567890abcdef-11
   6 entries were displayed.
   ```

Reequilibrar los clientes de alto tráfico

Si se produce un desequilibrio de E/S en todos los servidores de archivos (específicamente, debido a la utilización del rendimiento de la red), la causa puede ser el elevado número de clientes de E/S. Para identificar los clientes de alto tráfico, utilice la CLI de ONTAP.

1. Para conectarse mediante SSH a la NetApp CLI de ONTAP de su sistema de archivos, siga los pasos descritos en la Uso de la NetApp ONTAP CLI sección de la Guía del usuario de Amazon FSx para NetApp ONTAP.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Para ver los clientes con mayor tráfico, utilice el comando STATISTICS top client show ONTAP CLI. Si lo desea, puede especificar el `-node` parámetro para ver solo los clientes principales de un servidor de archivos específico. Si está diagnosticando un desequilibrio en un servidor de archivos específico, utilice el `-node` parámetro y `node_name` sustitúyalo por el nombre del servidor de archivos (por ejemplo,`FsxId01234567890abcdef-01`).

   Si lo desea, puede añadir el `-interval` parámetro, proporcionando el intervalo durante el que se debe medir (en segundos) antes de que se genere cada informe. Al aumentar el intervalo (por ejemplo, hasta un máximo de 300 segundos), se obtiene una muestra a más largo plazo de la cantidad de tráfico dirigida a cada volumen. El valor predeterminado es 5 (segundos).

   ```
   ::> statistics top client show -node FsxId01234567890abcdef-01 [-interval [5,300]]
   ```

   En el resultado, los principales clientes se muestran por su dirección IP y puerto.

   ```
                                                    *Total     Total
               Client   Vserver          Node           Ops     (Bps)
   ------------------ --------- ------------------------- ------ ---------
    172.17.236.53:938 svm01     FsxId01234567890abcdef-01   2143 140443648
   172.17.236.160:898 svm02     FsxId01234567890abcdef-01    812  53215232
   ```

3. Puede reequilibrar un subconjunto de los clientes de alto tráfico de la lista con otros servidores de archivos. Para ello, separe el volumen del cliente y vuelva a montarlo con el nombre DNS del punto de conexión NFS/SMB del SVM. De este modo, se obtiene un punto final aleatorio correspondiente a un par HA aleatorio.

   Le recomendamos que vuelva a utilizar el nombre DNS, pero tiene la opción de elegir de forma explícita qué par de HA montará un cliente determinado. Para garantizar que está montando un cliente en un punto final diferente, puede especificar una dirección IP de punto final diferente a la que corresponde al nodo que está experimentando mucho tráfico. Para ello, ejecute el siguiente comando:

   ```
   ::> network interface show -vserver svm_name -lif nfs_smb_management* -fields
    address,curr-node
   vserver   lif                  address      curr-node
   --------- -------------------- ------------ -------------------------
   svm01 nfs_smb_management_1 172.31.15.89 FsxId01234567890abcdef-01
   svm01 nfs_smb_management_3 172.31.8.112 FsxId01234567890abcdef-03
   2 entries were displayed.
   ```

Según el resultado del ejemplo del `statistics top client show` comando, el cliente `172.17.236.53` dirige mucho tráfico a`FsxId01234567890abcdef-01`. El resultado del `network interface show` comando indica que esta es la dirección`172.31.15.89`. Para montarlo en un punto final diferente, seleccione cualquier otra dirección (en este ejemplo, la única otra dirección es `172.31.8.112` la correspondiente a`FsxId01234567890abcdef-03`).

Reequilibrar los volúmenes muy utilizados

Si experimenta un desequilibrio de E/S en sus volúmenes o agregados, puede reequilibrar los volúmenes para redistribuir el tráfico de E/S entre los volúmenes.

> **Note**
>
> Si experimenta un desequilibrio en la utilización del almacenamiento en todos sus conjuntos, por lo general no hay ningún impacto en el rendimiento, a menos que la alta utilización vaya acompañada de un desequilibrio de E/S. Si bien puede mover los volúmenes de un agregado a otro para equilibrar la utilización del almacenamiento, le recomendamos que solo mueva los volúmenes si observa un impacto en el rendimiento, ya que mover los volúmenes puede tener un impacto adverso en el rendimiento si no se tiene en cuenta también la E/S que implica cada volumen que está considerando trasladar.

1. Para conectarse mediante SSH a la NetApp CLI de ONTAP de su sistema de archivos, siga los pasos descritos en la Uso de la NetApp ONTAP CLI sección de la Guía del usuario de Amazon FSx para NetApp ONTAP.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Utilice el comando CLI statistics volume show ONTAP para ver los volúmenes de tráfico más altos de un agregado determinado, con los siguientes cambios:

   - Sustituya *`aggregate_name por el nombre`* del agregado (por ejemplo,). `aggr1`
   - Si lo desea, puede agregar el `-interval` parámetro, proporcionando el intervalo durante el cual se debe medir (en segundos) antes de que se genere cada informe. Al aumentar el intervalo (por ejemplo, hasta un máximo de 300 segundos), se obtiene una muestra a más largo plazo de la cantidad de tráfico dirigida a cada volumen. El valor predeterminado es 5 (segundos).

```
::> statistics volume show -aggregate aggregate_name -sort-key total_ops [-interval
 [5,300]]
```

Según el intervalo que elija, los datos pueden tardar hasta 5 minutos en mostrarse. El comando muestra todos los volúmenes del agregado, junto con la cantidad de tráfico que se dirige a cada agregado.

```
                           *Total Read Write Other      Read Write Latency
    Volume Vserver Aggregate    Ops  Ops   Ops   Ops     (Bps) (Bps)    (us)
---------- ------- --------- ------ ---- ----- ----- --------- ----- -------
vol1__0007    svm1     aggr1   4078 4078     0     0 267255808     0    1092
vol1__0005    svm1     aggr1   4078 4078     0     0 267255808     0    1086
vol1__0003    svm1     aggr1   4077 4077     0     0 267223040     0    1086
vol1__0001    svm1     aggr1   4077 4077     0     0 267239424     0    1087
vol1__0008    svm1     aggr2   2314 2314     0     0 151650304     0    1112
vol1__0006    svm1     aggr2   2144 2144     0     0 140509184     0    1104
vol1__0002    svm1     aggr2   2183 2183     0     0 143065088     0    1106
vol1__0004    svm1     aggr2   2183 2183     0     0 143065088     0    1103
```

Las estadísticas de volumen se muestran por componente (por ejemplo, `vol1__0015` es el decimoquinto componente de FlexGroup`vol1`). Como puede ver en el resultado del ejemplo, los componentes de `aggr1` se utilizan más que los componentes de. `aggr2` Para equilibrar el tráfico entre los agregados, puede mover los volúmenes constitutivos entre los agregados para que el tráfico se distribuya de manera más uniforme.

3. Para mover un volumen entre agregados, utilice el comando volume move start ONTAP CLI y sustituya los valores siguientes:

   - *Sustituya svm_name por el nombre* de la SVM que aloja el volumen que va a mover.
   - Sustituya *volume_name por el nombre* del componente del volumen (por ejemplo,). `vol1__0001`
   - Sustituya *aggregate_name por el nombre* del agregado de destino del volumen.

   > **Important**
   >
   > El movimiento del volumen consume recursos de red y disco para los servidores de archivos de origen y destino. Como resultado, cualquier movimiento de volumen en

curso puede afectar al rendimiento de la carga de trabajo. Además, hay una fase de interrupción del proceso de movimiento del volumen que detiene temporalmente la E/S para detectar cualquier tráfico que se dirija al volumen.

```
::> volume move start -vserver svm_name -volume volume_name -
destination aggregate_name -foreground false
[Job 1] Job is queued: Move "vol1__0001" in Vserver "svm01" to aggregate "aggr1".
Use the "volume move show -vserver svm01 -volume vol1__0001" command to view the
 status of this operation.
```

Para comprobar el estado de la operación de movimiento de volumen, utilice el comando `volume move show` ONTAP CLI.

```
::> volume move show -vserver svm_name -volume volume_name
                          Vserver Name: svm01
                           Volume Name: vol1__0001
                  Actual Completion Time: -
                         Bytes Remaining: 1.00TB
           Specified Action For Cutover: retry_on_failure
         Specified Cutover Time Window: 30
                 Destination Aggregate: aggr2
                      Destination Node: FsxId01234567890abcdef-03
                       Detailed Status: Transferring data: 12.23GB sent.
                    Percentage Complete: 1%
                             Move Phase: replicating
               Prior Issues Encountered: -
          Estimated Remaining Duration: 00:40:25
                Replication Throughput: 434.3MB/s
                      Duration of Move: 00:00:27
                      Source Aggregate: aggr2
                           Source Node: FsxId01234567890abcdef-01
                            Move State: healthy
```

Este comando muestra el tiempo estimado para completar el movimiento, en uno de los campos de información. Cuando finalice la operación, el mismo comando mostrará que el `Move Phase` campo está completo.

Debe asegurarse de que cada uno FlexGroup esté distribuido uniformemente entre sus agregados, idealmente con los 8 componentes recomendados por agregado. Si mueve un volumen constitutivo a otro agregado para un agregado que de otro modo estaría equilibradoFlexGroup, debería a su vez mover otro volumen constituyente (menos utilizado) al agregado de origen para mantener el equilibrio.

Monitorización de FSx para eventos ONTAP EMS

Puede monitorizar FSx para detectar eventos del sistema de archivos ONTAP mediante el sistema de gestión de eventos (EMS) nativo de NetAPP ONTAP. Puede ver estos eventos mediante la CLI de NetApp ONTAP.

Temas

- Información general sobre los eventos del EMS
- Visualización de eventos del EMS
- Reenvío de eventos EMS a un servidor Syslog

Información general sobre los eventos del EMS

Los eventos EMS son notificaciones generadas automáticamente que le avisan cuando se produce una condición predefinida en su sistema de archivos FSx for ONTAP. Estas notificaciones lo mantienen informado para que pueda prevenir o corregir problemas que pueden provocar problemas mayores, como problemas de autenticación de las máquinas virtuales de almacenamiento (SVM) o los volúmenes llenos.

De forma predeterminada, los eventos se registran en el registro del sistema de administración de eventos. Con EMS, puede monitorizar eventos como los cambios en la contraseña de un usuario, el hecho de que un componente esté FlexGroup a punto de alcanzar su capacidad máxima, la conexión o desconexión manual de un número de unidad lógica (LUN) o el redimensionamiento automático de un volumen.

Para obtener más información sobre los eventos EMS de ONTAP, consulte la referencia de EMS de ONTAP en el Centro de documentación de NetApp ONTAP. Para mostrar las categorías de eventos, utilice el panel de navegación izquierdo del documento.

> **Note**
>
> Solo algunos mensajes EMS de ONTAP están disponibles para FSx para los sistemas de archivos ONTAP.

Las descripciones de los eventos del EMS contienen los nombres, la gravedad, las posibles causas, los mensajes de registro y las acciones correctivas que pueden ayudarle a decidir cómo responder. Por ejemplo, un evento wafl.vol.autoSize.fail se produce cuando no se puede ajustar automáticamente el tamaño de un volumen. Según la descripción del evento, la acción correctiva consiste en aumentar el tamaño máximo del volumen y, al mismo tiempo, configurar el tamaño automático.

Visualización de eventos del EMS

Utilice el event log show comando CLI de NetApp ONTAP para mostrar el contenido del registro de eventos. Este comando está disponible si tiene el rol `fsxadmin` en su sistema de archivos. La sintaxis del comando es la siguiente:

```
event log show [event_options]
```

Se muestran primero los eventos más recientes. De forma predeterminada, este comando muestra los eventos del nivel de gravedad `EMERGENCY`, `ALERT` y `ERROR` con la siguiente información:

- Time: la hora del evento.
- Node: el nodo en el que se produjo el evento.
- Severity: el nivel de gravedad del evento. Para mostrar los eventos de nivel de gravedad `NOTICE`, `INFORMATIONAL` o `DEBUG`, utilice la opción `-severity`.
- Event: el nombre y el mensaje del evento.

Para mostrar información detallada sobre los eventos, utilice una o más de las opciones de eventos que se muestran en la tabla siguiente.

Opciones de eventos	Descripción
`-detail`	Muestra información adicional sobre el evento.

Opciones de eventos	Descripción
`-detailtime`	Muestra la información detallada de eventos en orden cronológico inverso.
`-instance`	Muestra información detallada sobre todos los campos.
`-node` *`nodename`*`|local`	Muestra una lista de eventos del nodo que especifiq ue. Utilice esta opción con `-seqnum` para mostrar información detallada.
`-seqnum` *`sequence_number`*	Selecciona los eventos de la secuencia que coinciden con este número. Utilice esta opción con `-node` para mostrar información detallada.

Opciones de eventos	Descripción

`-time` *`MM/DD/YYYY HH:MM:SS`*	Selecciona los eventos que ocurrieron en este momento específico. Utilice el formato: MM/DD/AAAA HH:MM:SS [+-HH:MM]. Puede especificar un intervalo de tiempo mediante el operador `..` entre dos marcas de tiempo.
	`event log show -time "04/17/2023 05:55:00".."04/17/2023 06:10:00"`
	Los valores de tiempo comparativos son relativos a la hora actual en la que se ejecuta el comando. En el ejemplo siguiente, se indica cómo mostrar únicamente los eventos que se produjeron en el último minuto:
	`event log show -time >1m`
	Los campos de mes y fecha de esta opción no están rellenados con ceros. Estos campos pueden ser de un solo dígito; por ejemplo, `4/1/2023 06:45:00`.

Opciones de eventos	Descripción
`-severity sev_level`	Selecciona los eventos que coinciden con el valor *sev_level* , que debe ser uno de los siguientes: • EMERGENCY : interrupción • ALERT: punto único de error • ERROR: degradación • NOTICE: información • INFORMATIONAL : información • DEBUG: información sobre depuración Para mostrar todos los eventos, especifique la gravedad de la siguiente manera: `event log show -severity <=DEBUG`

Opciones de eventos	Descripción
`-ems-severity` *ems_sev_level*	Selecciona los eventos que coinciden con el valor *ems_sev_level* , que debe ser uno de los siguientes: • `NODE_FAULT` : se detecta un daño en los datos o el nodo no puede proporcio nar el servicio de atención al cliente. • `SVC_FAULT` : se detecta una pérdida temporal de servicio (normalmente un error de software transitor io). • `NODE_ERROR` : se detecta un error de hardware que no es inmediatamente fatal. • `SVC_ERROR` : se detecta un error de software que no es inmediatamente fatal. • `WARNING`: un mensaje de alta prioridad que no indica ningún error. • `NOTICE`: un mensaje de prioridad normal que no indica ningún error. • `INFO`: un mensaje de baja prioridad que no indica ningún error. • `DEBUG`: un mensaje de depuración.

Opciones de eventos	Descripción
	• VAR: un mensaje de gravedad variable, seleccionado en tiempo de ejecución. Para mostrar todos los eventos, especifique la gravedad de la siguiente manera: `event log show -ems-severity <=DEBUG`
`-source` *`text`*	Selecciona los eventos que coinciden con el valor del *`texto`*. La fuente suele ser un módulo de software.
`-message-name` *`message_name`*	Selecciona los eventos que coinciden con el valor del *`message_name`* . Los nombres de los mensajes son descriptivos, por lo que filtrar la salida por nombre de mensaje muestra mensajes de un tipo específico.
`-event` *`text`*	Selecciona los eventos que coinciden con el valor del *`texto`*. El campo `event` contiene el texto completo del evento, incluidos los parámetros.

Opciones de eventos	Descripción
`-kernel-generation-num` *integer*	Selecciona los eventos que coinciden con el valor *entero*. Solo los eventos que provienen del núcleo tienen números de generación del núcleo.
`-kernel-sequence-num` *integer*	Selecciona los eventos que coinciden con el valor *entero*. Solo los eventos que provienen del núcleo tienen números de generación del núcleo.
`-action` *text*	Selecciona los eventos que coinciden con el valor del *texto*. El campo `action` describe qué medidas correctivas, si las hay, debe tomar para corregir la situación.
`-description` *text*	Selecciona los eventos que coinciden con el valor del *texto*. El campo `descripti on` describe por qué ocurrió el evento y qué significa.
`-filter-name` *filter_name*	Selecciona los eventos que coinciden con el valor del *filter_name* . Solo se muestran los eventos incluidos en los filtros existentes que coinciden con este valor.

Opciones de eventos	Descripción
`-fields` *`fieldname ,...`*	Indica que el resultado del comando también incluye el campo o los campos especificados. Puede utilizar `-fields ?` para elegir los campos que desee especific ar.

Para visualizar los eventos del EMS

1. Para conectarse mediante SSH a la NetApp CLI de ONTAP de su sistema de archivos, siga los pasos descritos en la Uso de la NetApp ONTAP CLI sección de la Guía del usuario de Amazon FSx para NetApp ONTAP.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Utilice el comando `event log show` para mostrar el contenido del registro de eventos.

   ```
   ::> event log show
   Time                Node          Severity      Event
   ------------------- ------------- ------------- -------------------------
   6/30/2023 13:54:19  node1         NOTICE        vifmgr.portup: A link up event was
    received on node node1, port e0a.
   6/30/2023 13:54:19  node1         NOTICE        vifmgr.portup: A link up event was
    received on node node1, port e0d.
   ```

Para obtener información sobre los eventos de EMS devueltos por el `event log show` comando, consulte la referencia de EMS de ONTAP en el centro de documentación de ONTAP. NetApp

Reenvío de eventos EMS a un servidor Syslog

Puede configurar los eventos de EMS para reenviar las notificaciones a un servidor Syslog. El reenvío de eventos de EMS se utiliza para supervisar en tiempo real el sistema de archivos a fin de determinar y aislar las causas fundamentales de una amplia gama de problemas. Si su entorno aún no contiene un servidor Syslog para las notificaciones de eventos, primero debe crear uno. El DNS debe estar configurado en el sistema de archivos para resolver el nombre del servidor Syslog.

Para configurar los eventos de EMS para que reenvíen las notificaciones a un servidor Syslog

1. Para conectarse mediante SSH a la NetApp CLI de ONTAP de su sistema de archivos, siga los pasos descritos en la Uso de la NetApp ONTAP CLI sección de la Guía del usuario de Amazon FSx para NetApp ONTAP.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Utilice el comando create destination destination create para crear un tipo de destino de notificación de eventos`syslog`, especificando los siguientes atributos:

   - *`dest_name`*— El nombre del destino de la notificación que se va a crear (por ejemplo,`syslog-ems`). El nombre del destino de una notificación de evento debe tener entre 2 y 64 caracteres. Los caracteres válidos son los siguientes caracteres ASCII: A-Z, a-z, 0-9, «_» y «-». El nombre debe empezar y terminar por: A-Z, a-z o 0-9.
   - *`syslog_name`*— El nombre de host del servidor Syslog o la dirección IP a la que se envían los mensajes de Syslog.
   - *`transport_protocol`*— El protocolo utilizado para enviar los eventos:
     - `udp-unencrypted`— Protocolo de datagramas de usuario sin seguridad. Este es el protocolo por defecto.
     - `tcp-unencrypted`— Protocolo de control de transmisión sin seguridad.
     - `tcp-encrypted`— Protocolo de control de transmisión con seguridad de capa de transporte (TLS). Cuando se especifica esta opción, FSx for ONTAP verifica la identidad del host de destino validando su certificado.
   - *`port_number`*— El puerto del servidor Syslog al que se envían los mensajes de Syslog. El `syslog-port` parámetro de valor predeterminado depende de la configuración del parámetro. `syslog-transport` Si `syslog-transport` se establece en`tcp-encrypted`, el valor `syslog-port` por defecto es`6514`. Si `syslog-transport` está establecido en`tcp-unencrypted`, `syslog-port` tiene el valor por defecto`601`. De lo contrario, el puerto predeterminado se establece en`514`.

   ```
   ::> event notification destination create -name dest_name -syslog syslog_name -
   syslog-transport transport_protocol -syslog-port port_number
   ```

3. Utilice el comando event notification create para crear una nueva notificación de un conjunto de eventos definidos por un filtro de eventos para el destino de la notificación creado en el paso anterior, especificando los siguientes atributos:

   - *node_name*— El nombre del filtro de eventos. Los eventos que se incluyen en el filtro de eventos se reenvían a los destinos especificados en el `-destinations` parámetro.
   - *dest_name*— El nombre del destino de notificación existente al que se envían las notificaciones de eventos.

```
::> event notification create -filter-name filter_name -destinations dest_name
```

4. Utilice el `event notification destination check` comando para generar un mensaje de prueba y comprobar que la configuración funciona. Especifique los siguientes atributos con el comando:

   - *node_name*— El nombre del nodo (por ejemplo,`FsxId07353f551e6b557b4-01`).
   - *dest_name*— El nombre del destino de notificación existente al que se envían las notificaciones de eventos.

```
::> set diag
::*> event notification destination check -node node_name -destination-
name dest_name
```

Monitoreo con Cloud Insights

NetApp Cloud Insights es un NetApp servicio que puede utilizar para monitorizar sus sistemas de archivos Amazon FSx para NetApp ONTAP junto con sus otras NetApp soluciones de almacenamiento. Con Cloud Insights, puedes supervisar las métricas de configuración, capacidad y rendimiento a lo largo del tiempo para comprender las tendencias de tu carga de trabajo y planificar las necesidades futuras de rendimiento y capacidad de almacenamiento. También puedes crear alertas basadas en condiciones métricas que se puedan integrar con tus flujos de trabajo y herramientas de productividad existentes.

> **Note**
>
> Cloud Insights no es compatible con los sistemas de archivos escalables.

Cloud Insights ofrece:

- Una variedad de métricas y registros: recopile métricas de configuración, capacidad y rendimiento. Conozca las tendencias de su carga de trabajo con paneles, alertas e informes predefinidos.
- Análisis de usuarios y protección contra el ransomware: con las instantáneas de Cloud Secure y ONTAP, puede auditar, detectar, detener y reparar los incidentes relacionados con errores de usuario y ransomware.
- SnapMirror elaboración de informes: comprenda sus SnapMirror relaciones y establezca alertas sobre los problemas de replicación.
- Planificación de la capacidad: comprenda los requisitos de recursos de las cargas de trabajo locales para ayudarlo a migrar su carga de trabajo a una configuración de FSx for ONTAP más eficiente. También puede utilizar esta información para planificar cuándo necesitará más rendimiento o capacidad para la implementación de FSx para ONTAP.

Para obtener más información sobre Cloud Insights, consulta NetApp Cloud Insights en NetApp Cloud Central.

Monitoreo de sistemas de archivos de FSx en ONTAP mediante Harvest y Grafana

NetApp Harvest es una herramienta de código abierto para recopilar métricas de rendimiento y capacidad de los sistemas ONTAP y es compatible con FSx para ONTAP. Puede usar Harvest with Grafana como una solución de monitoreo de código abierto.

Primeros pasos con Harvest y Grafana

La siguiente sección detalla cómo puede configurar Harvest y Grafana para medir sus FSx para el rendimiento y la utilización de la capacidad de almacenamiento del sistema de archivos ONTAP.

Puede monitorizar su sistema de archivos Amazon FSx para NetApp ONTAP mediante Harvest y Grafana. NetApp Harvest supervisa los centros de datos de ONTAP mediante la recopilación de

métricas de rendimiento, capacidad y hardware de FSx para los sistemas de archivos de ONTAP. Grafana proporciona un panel de control en el que se pueden mostrar las métricas recopiladas de Harvest.

Paneles de Harvest compatibles

Amazon FSx para NetApp ONTAP expone un conjunto de métricas diferente al de ONTAP local. NetApp Por lo tanto, actualmente solo los siguientes paneles de out-of-the-box Harvest etiquetados con `fsx` se admiten para su uso con FSx for ONTAP. Es posible que a algunos de los paneles de estos paneles les falte información que no es compatible.

- ONTAP: Conformidad
- ONTAP: Instantáneas de protección de datos
- ONTAP: Seguridad
- ONTAP: SVM
- ONTAP: Volumen

Plantilla de AWS CloudFormation

Para empezar, puede implementar una plantilla AWS CloudFormation que lance automáticamente una instancia de Amazon EC2 que ejecute Harvest y Grafana. Como entrada a la plantilla AWS CloudFormation, debe especificar el `fsxadmin` usuario y el punto de conexión de administración de Amazon FSx para el sistema de archivos, que se añadirán como parte de esta implementación. Una vez completada la implementación, puede iniciar sesión en el panel de control de Grafana para monitorear su sistema de archivos.

Esta solución se utiliza AWS CloudFormation para automatizar la implementación de las soluciones Harvest y Grafana. La plantilla crea una instancia de Linux Amazon EC2 e instala el software Harvest y Grafana. Para usar esta solución, descargue la plantilla .template. fsx-ontap-harvest-grafana AWS CloudFormation

> **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.

Tipos de instancias de Amazon EC2

Al configurar la plantilla, debe proporcionar el tipo de instancia Amazon EC2. NetAppLa recomendación para el tamaño de la instancia depende del número de sistemas de archivos que supervise y del número de métricas que decida recopilar. Con la configuración predeterminada, por cada 10 sistemas de archivos que supervise, NetApp recomienda:

- CPU: 2 núcleos
- Memoria: 1 GB
- Disco: 500 MB (utilizado principalmente por archivos de registro)

A continuación, se muestran algunos ejemplos de configuraciones y el tipo de instancia `t3` que puede elegir.

Sistemas de archivos	CPU	Disk	Tipo de instancia
Menos de 10	2 núcleos	500 MB	`t3.micro`
De 10 a 40	4 núcleos	1000 MEGABYTE	`t3.xlarge`
Más de 40	8 núcleos	2000 MB	`t3.2xlarge`

Para obtener más información sobre los tipos de instancia de Amazon EC2, consulte Instancias de uso general en la Guía del usuario de Amazon EC2 para instancias Linux.

Reglas de puertos de instancias

Al configurar la instancia de Amazon EC2, asegúrese de que los puertos 3000 y 9090 estén abiertos para el tráfico entrante del grupo de seguridad en el que se encuentra la instancia Harvest y Grafana de Amazon EC2.

Procedimiento de implementación

El siguiente procedimiento configura e implementa la solución Harvest/Grafana. Tarda aproximadamente cinco minutos en implementarse. Antes de empezar, debe tener un sistema de archivos de FSx para ONTAP que se ejecute en una Amazon Virtual Private Cloud (Amazon VPC) en su cuenta AWS y la información de los parámetros de la plantilla que se indica a continuación.

Para obtener más información sobre la creación de un sistema de archivos, consulte Creación de FSx para sistemas de archivos ONTAP.

Para iniciar la pila de soluciones Harvest/Grafana

1. Descarga la fsx-ontap-harvest-grafanaplantilla .template. AWS CloudFormation Para obtener más información sobre la creación de pilas AWS CloudFormation, consulte Crear pilas en la consola 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. Debe lanzar esta solución en un Región de AWS donde Amazon FSx esté disponible. Para obtener más información, consulte Puntos finales y cuotas de Amazon FSx en Referencia general de AWS.

2. En el caso de los Parámetros, revise los parámetros de la plantilla y modifíquelos para adaptarlos a las necesidades de su sistema de archivos. Esta solución utiliza los siguientes valores predeterminados.

Parámetro	Predeterminado	Descripción
InstanceType	`t3.micro`	El tipo de instancia de Amazon EC2. A continuac ión se muestran los tipos de instancias `t3`. • `t3.micro` • `t3.small` • `t3.medium` • `t3.large` • `t3.xlarge` • `t3.2xlarge` Para ver la lista completa de los valores de

Parámetro	Predeterminado	Descripción
		tipo de instancia de Amazon EC2 permitido s para este parámetro, consulte .template. fsx-ontap -harvest-grafana
KeyPair	Sin valor predeterminado	El par de claves que se usa para obtener acceso a la instancia de Amazon EC2.
SecurityGroup	Sin valor predeterminado	El ID del grupo de seguridad de la instancia de Harvest/ Grafana. Asegúrese de que los puertos de entrada 3000 y 9090 estén abiertos desde los clientes que desea utilizar para acceder a su panel de control de Grafana.
Tipo de subred	Sin valor predeterminado	Especifique el tipo de subred, ya sea `public` o `private`. Utiliza una subred `public` para los recursos que deban conectarse a Internet y una subred privada para los recursos que no vayan a conectars e a Internet. Para obtener más información, consulte Tipos de subred en la Guía del usuario de Amazon VPC.

Parámetro	Predeterminado	Descripción
Subred	Sin valor predeterminado	Especifique la misma subred que su Amazon FSx NetApp para la subred preferida del sistema de archivos ONTAP. Puede encontrar el ID de Subred preferido del sistema de archivos en la consola de Amazon FSx, en la pestaña Red y seguridad de la página de detalles del sistema de archivos de FSx for ONTAP
LatestLinuxAmiId	`/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2`	Es la última versión de la AMI de Amazon Linux 2 en un Región de AWS dado.
F SxEndPoint	Sin valor predeterminado	La dirección IP del punto de conexión de administración del sistema de archivos. Puede encontrar la dirección IP del punto de conexión de administración del sistema de archivos en la consola de Amazon FSx, en la pestaña Administración de la página de detalles del sistema de archivos de FSx for ONTAP.

Parámetro	Predeterminado	Descripción
SecretName	Sin valor predeterminado	AWS Secrets Manager nombre secreto que contiene la contraseña del usuario `fsxadmin` del sistema de archivos. Es la contraseña que proporcionó al crear el sistema de archivos.

3. Elija Siguiente.
4. En Opciones, elija Siguiente.
5. En la página Revisar, revise y confirme la configuración. Debe seleccionar la casilla de verificación que reconoce que la plantilla crea recursos IAM.
6. Elija Crear para implementar la pila.

Puede ver el estado de la pila en la consola de AWS CloudFormation en la columna Estado. Debería ver el estado CREATE_COMPLETE en aproximadamente cinco (5) minutos.

Iniciar sesión en Grafana

Una vez finalizada la implementación, utilice su navegador para iniciar sesión en el panel de control de Grafana en la IP y el puerto 3000 de la instancia de Amazon EC2:

```
http://EC2_instance_IP:3000
```

Cuando se le solicite, utilice el nombre de usuario (`admin`) y la contraseña (`pass`) predeterminados de Grafana. Le recomendamos que cambie la contraseña en cuanto inicie sesión.

Para obtener más información, consulte la página de NetApp Harvest en GitHub.

Solución de problemas de Harvest y Grafana

Si le falta algún dato mencionado en los paneles de Harvest y Grafana o tiene problemas para configurar Harvest y Grafana con FSx para ONTAP, consulte los siguientes temas para encontrar una posible solución.

Temas

Los paneles de SVM y de volumen están en blanco

Si la AWS CloudFormation pila se implementó correctamente y puede ponerse en contacto con Grafana, pero los paneles de SVM y volumen están en blanco, utilice el siguiente procedimiento para solucionar los problemas de su entorno. Necesitará acceso SSH a la instancia de Amazon EC2 en la que se implementan Harvest y Grafana.

1. Utilice SSH en la instancia de Amazon EC2 en la que se ejecutan sus clientes de Harvest y Grafana.

   ```
   [~]$ ssh ec2-user@ec2_ip_address
   ```

2. Utilice el siguiente comando para abrir el `harvest.yml` archivo y:

   - Compruebe que se haya creado una entrada para su instancia de FSx for ONTAP como. `Cluster-2`
   - Compruebe que las entradas del nombre de usuario y la contraseña coincidan con sus `fsxadmin` credenciales.

   ```
   [ec2-user@ip-ec2_ip_address ~]$ sudo cat /home/ec2-user/harvest_install/harvest/
   harvest.yml
   ```

3. Si el campo de contraseña está en blanco, abra el archivo en un editor y actualícelo con la `fsxadmin` contraseña, de la siguiente manera:

   ```
   [ec2-user@ip-ec2_ip_address ~]$ sudo vi /home/ec2-user/harvest_install/harvest/
   harvest.yml
   ```

4. Asegúrese de que las credenciales de `fsxadmin` usuario se almacenen en Secrets Manager *`fsxadmin_password`* con el siguiente formato para futuras implementaciones, sustituyéndolas por su contraseña.

   ```
   {"username" : "fsxadmin", "password" : "fsxadmin_password"}
   ```

CloudFormation la pila se revierte después de agotarse el tiempo de espera

Si no puede implementar la CloudFormation pila correctamente y se está revirtiendo con errores, utilice el siguiente procedimiento para resolver el problema. Necesitará acceso SSH a la instancia EC2 implementada por la CloudFormation pila.

1. Vuelva a implementar la CloudFormation pila y asegúrese de que la reversión automática esté desactivada.
2. Utilice SSH en la instancia de Amazon EC2 en la que se ejecutan sus clientes de Harvest y Grafana.

   ```
   [~]$ ssh ec2-user@ec2_ip_address
   ```

3. Compruebe que los contenedores docker se hayan iniciado correctamente mediante el siguiente comando.

   ```
   [ec2-user@ip-ec2_ip_address ~]$ sudo docker ps
   ```

   En la respuesta, deberías ver cinco contenedores de la siguiente manera:

   ```
   CONTAINER ID   IMAGE                  COMMAND                  CREATED
    STATUS                          PORTS                    NAMES
   6b9b3f2085ef   rahulguptajss/harvest   "bin/poller --config…"   8 minutes ago
    Restarting (1) 20 seconds ago                            harvest_cluster-2
   3cf3e3623fde   rahulguptajss/harvest   "bin/poller --config…"   8 minutes ago   Up
    About a minute                                           harvest_cluster-1
   708f3b7ef6f8   grafana/grafana         "/run.sh"                8 minutes ago   Up
    8 minutes                   0.0.0.0:3000->3000/tcp   harvest_grafana
   0febee61cab7   prom/alertmanager       "/bin/alertmanager -…"   8
    minutes ago   Up 8 minutes                    0.0.0.0:9093->9093/tcp
    harvest_prometheus_alertmanager
   1706d8cd5a0c   prom/prometheus         "/bin/prometheus --c…"   8 minutes ago   Up
    8 minutes                   0.0.0.0:9090->9090/tcp   harvest_prometheus
   ```

4. Si los contenedores docker no se están ejecutando, compruebe si hay errores en el `/var/log/cloud-init-output.log` archivo de la siguiente manera.

   ```
   [ec2-user@ip-ec2_ip_address ~]$ sudo cat /var/log/cloud-init-output.log
        PLAY [Manage Harvest]
    ***********************************************************
   ```

```
TASK [Gathering Facts] *********************************************************
ok: [localhost]

TASK [Verify images] ***********************************************************
failed: [localhost] (item=prom/prometheus) => {"ansible_loop_var": "item",
 "changed": false, "item": "prom/prometheus",
"msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104, 'Co
nnection reset by peer'))"}
failed: [localhost] (item=prom/alertmanager) => {"ansible_loop_var": "item",
 "changed": false, "item": "prom/alertmanage
r", "msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104,
'Connection reset by peer'))"}
failed: [localhost] (item=rahulguptajss/harvest) => {"ansible_loop_var": "item",
 "changed": false, "item": "rahulguptajs
s/harvest", "msg": "Error connecting: Error while fetching server API version:
 ('Connection aborted.', ConnectionResetEr
ror(104, 'Connection reset by peer'))"}
failed: [localhost] (item=grafana/grafana) => {"ansible_loop_var": "item",
 "changed": false, "item": "grafana/grafana",
"msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104, 'Co
nnection reset by peer'))"}

PLAY RECAP *********************************************************************
localhost                  : ok=1    changed=0    unreachable=0    failed=1
 skipped=0    rescued=0    ignored=0
```

5. Si hay errores, ejecute los siguientes comandos para implementar los contenedores Harvest y Grafana.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo su
     [ec2-user@ip-ec2_ip_address ~]$ cd /home/ec2-user/harvest_install
     [ec2-user@ip-ec2_ip_address ~]$ /usr/local/bin/ansible-playbook
 manage_harvest.yml
     [ec2-user@ip-ec2_ip_address ~]$ /usr/local/bin/ansible-playbook
 manage_harvest.yml --tags api
```

6. Valide que los contenedores se hayan iniciado correctamente ejecutándolos sudo docker ps y conectándose a su URL de Harvest y Grafana.

Registro de llamadas a la API de FSx para ONTAP con AWS CloudTrail

Amazon FSx está integrado con AWS CloudTrail, un servicio que proporciona un registro de las acciones realizadas por un usuario, rol o un servicio AWS en Amazon FSx. CloudTrail captura como eventos todas las llamadas a la API de Amazon FSx de Amazon FSx para NetApp ONTAP. Las llamadas capturadas incluyen llamadas de la consola de Amazon FSx y de llamadas de código a operaciones de la API de Amazon FSx.

Si crea un rastro, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos para Amazon FSx. Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Historial de eventos. Utilizando la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a Amazon FSx. También puede identificar la dirección IP desde la que se realizó la solicitud, quién realizó la solicitud, cuándo se realizó y detalles adicionales.

Para obtener más información acerca de CloudTrail, consulte la Guía del usuario de AWS CloudTrail.

Información de Amazon FSx en CloudTrail

CloudTrail se habilita en su cuenta de AWS cuando la crea. Cuando se produce una actividad de API en Amazon FSx, dicha actividad se registra en un evento de CloudTrail junto con otros eventos de servicio AWS en el Historial de eventos. Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte Ver eventos con el historial de eventos de CloudTrail.

Para un registro continuo de eventos en su cuenta AWS, incluyendo eventos para Amazon FSx, cree un rastro. 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:

- Creación de una traza para su Cuenta de AWS
- Integraciones de servicios de AWS con registros de CloudTrail

- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de registro de CloudTrail de varias regiones y Recibir archivos de registro de CloudTrail de varias cuentas

CloudTrail registra todas las llamadas a la API de Amazon FSx. Por ejemplo, las llamadas a las operaciones `CreateFileSystem` y `TagResource` generan entradas en los archivos de registro de CloudTrail.

Cada entrada de registro o evento contiene información acerca de quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

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

Para obtener más información, consulte el Elemento userIdentity de CloudTrail en la Guía del usuario de AWS CloudTrail.

Comprensión de las entradas del archivo de registro de Amazon FSx

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros a un bucket de Amazon S3 que usted especifique. Los archivos log de CloudTrail pueden contener una o varias entradas de log. Un evento representa una solicitud específica realizada desde un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

El siguiente ejemplo muestra una entrada de registro de CloudTrail que 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"
}
```

Cuotas

A continuación, puede obtener información sobre las cuotas al trabajar con Amazon FSx para NetApp ONTAP.

Temas

Cuotas que puede aumentar

A continuación, se muestran las cuotas de Amazon FSx para NetApp ONTAP por Región de AWS cada Cuenta de AWS cuota que puede aumentar.

Recurso	Predeterminado	Descripción
Sistemas de archivos ONTAP	100	El número máximo de sistemas de archivos Amazon FSx para NetApp ONTAP que puede crear en esta cuenta.
Capacidad de almacenamiento SSD de ONTAP	524.288	La cantidad máxima de capacidad de almacenamiento en SSD (en GiB) para todos los sistemas de archivos Amazon FSx for NetApp ONTAP que puede tener en esta cuenta.
Capacidad de rendimiento de ONTAP	10 240	La cantidad máxima de capacidad de procesamiento (en MBps) para todos los sistemas de archivos Amazon FSx NetApp para ONTAP que puede tener en esta cuenta.

Recurso	Predeterminado	Descripción
IOPS SSD DE ONTAP	1 000 000	La cantidad máxima de IOPS de SSD para todos los sistemas de archivos Amazon FSx NetApp for ONTAP que puede tener en esta cuenta.
Copias de seguridad de ONTAP por sistema de archivos	10 000	El número máximo de copias de seguridad en volumen iniciadas por el usuario para todos los sistemas de archivos Amazon FSx NetApp for ONTAP que puede tener en esta cuenta.

Cómo solicitar un aumento de cuota

1. Abra la página AWS Support, inicie sesión si es necesario y, a continuación, elija Create case (Crear caso).
2. Para Create case (Crear caso), seleccione Account and billing support (Soporte de cuentas y facturación).
3. En el panel de Detalles del caso, introduzca las siguientes entradas:
   - En Tipo, elija Cuenta.
   - En Categoría, seleccione Otros problemas con la cuenta.
   - En Asunto, escriba **`Amazon FSx for NetApp ONTAP service limit increase request`**.
   - Proporcione una Descripción detallada de su solicitud, que incluya:
     - La cuota FSx que quiere aumentar, y el valor al que desea aumentarla, si se conoce.
     - La razón por la que quiere el aumento de la cuota.
     - El identificador del sistema de archivos y la región de cada sistema de archivos para el que solicita un aumento.
4. Indique las Opciones de contacto que prefiera y pulse Enviar.

Cuotas de recursos para cada sistema de archivos

En la siguiente tabla se enumeran las cuotas de Amazon FSx para los recursos de NetApp ONTAP para cada sistema de archivos de un. Región de AWS

Recurso	El límite por sistema de archivos
Capacidad de almacenamiento SSD mínima	1024 GiB por par de alta disponibilidad (HA)
Capacidad de almacenamiento SSD máxima	• Escalabilidad horizontal: 512 TiB por par HA, hasta 1 PiB • Ampliación: 192 TiB
El máximo de IOPS de SSD	Escalamiento horizontal: • 200 000 por par de HA (hasta 12 pares) Ampliación: • 160 000 en la región de EE. UU. Este (Ohio), la región de EE. UU. Este (Virginia del Norte), la región de EE. UU. oeste (Oregón) y Europa (Irlanda) • 80.000 en todos los demás Regiones de AWS lugares en los que FSx para ONTAP esté disponible
La capacidad de rendimiento mínima	• Capacidad de ampliación: 3.072 MBps por par HA • Ampliación: 128 MBps
La capacidad de rendimiento máxima	Escalamiento horizontal: • 73.728 MBps 1

Recurso	El límite por sistema de archivos
	Ampliación: • 4.096 MBps [2] en la región EE.UU. Este (Ohio), la región EE.UU. Este (Norte de Virginia), la región EE.UU. Oeste (Oregón) y Europa (Irlanda) • 2.048 MBps en todos los demás Regiones de AWS lugares en los que FSx para ONTAP esté disponible
Número máximo de volúmenes	• Capacidad de ampliación: 1000 • Ampliación: 500
Número máximo de instantáneas	1.023 por volumen 3
Número máximo de copias de seguridad	4.091 por volumen 4

Recurso	El límite por sistema de archivos
Número máximo de SVM	Escalado horizontal: • 5 Ampliación: • 6 (capacidad de rendimiento de 128 MBps) • 6 (capacidad de rendimiento de 256 MBps) • 14 (capacidad de rendimiento de 512 MBps) • 14 (capacidad de rendimiento de 1.024 MBps) • 24 (capacidad de rendimiento de 2.048 MBps) • 24 (capacidad de rendimiento de 4.096 MBps)
Número máximo de etiquetas	50
Período máximo de retención para las copias de seguridad automatizadas	90 días
Periodo máximo de retención para las copias de seguridad iniciadas por el usuario	Sin límite de retención

Note

[1] En un sistema de archivos ampliable con 12 pares de alta disponibilidad (6.144 MBps por par de alta disponibilidad). Para obtener más información, consulte Pares de alta disponibilidad (HA).

[2] Para aprovisionar una capacidad de rendimiento de 4 GBps, su sistema de archivos escalable FSx for ONTAP requiere una configuración del máximo de IOPS de SSD (160

000) y un mínimo de 5 120 GiB de capacidad de almacenamiento SSD de forma compatible. Región de AWS Para obtener más información sobre cuáles admiten una capacidad de rendimiento de 4.096 MBps, consulte. Regiones de AWS Impacto de la capacidad de rendimiento en el rendimiento

[3] Puede almacenar hasta 1023 instantáneas por volumen en cualquier momento. Cuando alcance este límite, debe eliminar una instantánea existente antes de poder crear una nueva instantánea del volumen.

[4] Puede almacenar hasta 4.091 copias de seguridad por volumen en cualquier momento. Cuando alcance este límite, debe eliminar una copia de seguridad existente antes de poder crear una nueva copia de seguridad de su volumen.

Solución de problemas de Amazon FSx para ONTAP NetApp

Utilice las siguientes secciones para solucionar los problemas que puedan presentarse con FSx para ONTAP.

Temas

Mi sistema de archivos Multi-AZ está en un estado **`MISCONFIGURED`**

Existen varias causas posibles por las que un sistema de archivos se encuentra en un `MISCONFIGURED` estado, cada una con su propia resolución, como se indica a continuación.

Temas

La cuenta del propietario de la VPC ha deshabilitado el uso compartido de VPC Multi-AZ

Los sistemas de archivos Multi-AZ creados por un participante Cuenta de AWS en una subred de VPC compartida pasarán a `MISCONFIGURED` un estado por uno de los siguientes motivos:

- La cuenta propietaria que compartía la subred de la VPC ha desactivado la compatibilidad con el uso compartido de VPC Multi-AZ para FSx en los sistemas de archivos ONTAP.
- La cuenta propietaria ha dejado de compartir la subred de VPC.

Si la cuenta propietaria ha dejado de compartir la subred de VPC, verás el siguiente mensaje en la consola de ese sistema de archivos:

```
The vpc ID vpc-012345abcde does not exist
```

Debe ponerse en contacto con la cuenta propietaria que compartió la subred de VPC con usted para resolver el problema. Para obtener más información, consulte Creación de FSx para sistemas de archivos ONTAP en subredes compartidas para obtener más información.

No puede crear un SVM nuevo en un sistema de archivos Multi-AZ

En el caso de los sistemas de archivos Multi-AZ creados por un participante Cuenta de AWS en una VPC compartida, no podrá crear una nueva SVM por uno de los siguientes motivos:

- La cuenta propietaria que compartía la subred de la VPC ha desactivado la compatibilidad con el uso compartido de VPC Multi-AZ para FSx en los sistemas de archivos ONTAP.
- La cuenta propietaria ha dejado de compartir la subred de VPC.

Debe ponerse en contacto con la cuenta propietaria que compartió la subred de VPC con usted para resolver el problema. Para obtener más información, consulte Creación de FSx para sistemas de archivos ONTAP en subredes compartidas para obtener más información.

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.

Temas

- Se modificó o eliminó la interfaz de red elástica del sistema de archivos
- Se eliminó la dirección IP elástica que está adjunta a la interfaz de red elástica del sistema de archivos

- El grupo de seguridad de VPC del sistema de archivos carece de las reglas de entrada requeridas
- El grupo de seguridad de VPC de la instancia de procesamiento carece de las reglas de salida requeridas
- La subred de la instancia de cómputo no usa ninguna de las tablas de enrutamiento asociadas a su sistema de archivos
- Amazon FSx no puede actualizar la tabla de enrutamiento de los sistemas de archivos Multi-AZ creados con AWS CloudFormation
- No se puede acceder a un sistema de archivos a través de iSCSI desde un cliente de otra VPC
- La cuenta propietaria ha dejado de compartir la subred de VPC
- No se puede acceder a un sistema de archivos a través de NFS, SMB, la CLI de ONTAP o la API de REST de ONTAP desde un cliente de otra VPC o en las instalaciones

Se modificó o eliminó la interfaz de red elástica del sistema de archivos

No debe modificar ni eliminar ninguna de las interfaces 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 su nube privada virtual (VPC) y el sistema de archivos. Cree un nuevo sistema de archivos y no modifique ni elimine la interfaz de red de Amazon FSx. Para obtener más información, consulte Control de acceso al sistema de archivos con Amazon VPC.

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, que 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. Para obtener más información, consulte Clientes compatibles.

El grupo de seguridad de VPC del sistema de archivos carece de las reglas de entrada requeridas

Revise las reglas de entrada especificadas en Grupos de seguridad de Amazon VPC, y asegúrese de que el grupo de seguridad asociado al sistema de archivos tenga las reglas de entrada correspondientes.

El grupo de seguridad de VPC de la instancia de procesamiento carece de las reglas de salida requeridas

Revise las reglas de salida especificadas en Grupos de seguridad de Amazon VPC, y asegúrese de que el grupo de seguridad asociado a la instancia informática tenga las reglas de salida correspondientes.

La subred de la instancia de cómputo no usa ninguna de las tablas de enrutamiento asociadas a su sistema de archivos

FSx para ONTAP crea puntos de conexión para acceder al sistema de archivos en una tabla de enrutamiento de VPC. Le recomendamos que configure el sistema de archivos para que utilice todas las tablas de enrutamiento de VPC asociadas a las subredes en las que se encuentran sus clientes. De forma predeterminada, Amazon FSx usa la tabla de enrutamiento de la VPC. Si lo desea, puede especificar una o más tablas de enrutamiento para que Amazon FSx las utilice al crear el sistema de archivos.

Si puede hacer ping al punto de conexión entre clústeres del sistema de archivos, pero no puede hacer ping al punto de conexión de administración del sistema de archivos (consulte Recursos del sistema de archivos para obtener más información), es probable que su cliente no esté en una subred asociada a una de las tablas de enrutamiento del sistema de archivos. Para acceder al sistema de archivos, asocie una de las tablas de enrutamiento del sistema de archivos a la subred del cliente. Para obtener información sobre actualizar las tablas de enrutamiento de su sistema de archivos de Amazon VPC, consulte Actualización de un sistema de archivos.

Amazon FSx no puede actualizar la tabla de enrutamiento de los sistemas de archivos Multi-AZ creados con AWS CloudFormation

Amazon FSx administra las tablas de enrutamiento de VPC para sistemas de archivos Multi-AZ mediante la autenticación basada en etiquetas. Estas tablas de rutas están etiquetadas con. `Key: AmazonFSx; Value: ManagedByAmazonFSx` Al crear o actualizar FSx para sistemas de archivos Multi-AZ de ONTAP, le AWS CloudFormation recomendamos que añada la etiqueta manualmente. `Key: AmazonFSx; Value: ManagedByAmazonFSx`

Si no puede acceder a su sistema de archivos Multi-AZ, compruebe si las tablas de enrutamiento de VPC asociadas al sistema de archivos están etiquetadas con. `Key: AmazonFSx; Value: ManagedByAmazonFSx` Si no lo están, Amazon FSx no podrá actualizar esas tablas de

enrutamiento para enrutar las direcciones IP flotantes de los puertos de administración y datos al servidor de archivos activo cuando se produzca un evento de conmutación por error. Para obtener información sobre actualizar las tablas de enrutamiento de su sistema de archivos de Amazon VPC, consulte Actualización de un sistema de archivos.

No se puede acceder a un sistema de archivos a través de iSCSI desde un cliente de otra VPC

Para acceder a un sistema de archivos a través del protocolo de interfaz de sistemas informáticos pequeños de Internet (iSCSI) desde un cliente de otra VPC, puede configurar el emparejamiento de Amazon VPC o AWS Transit Gateway entre la VPC asociada a su sistema de archivos y la VPC en la que reside su cliente. Para obtener más información, consulte Crear y aceptar conexiones de emparejamiento de VPC en la guía Amazon Virtual Private Cloud.

La cuenta propietaria ha dejado de compartir la subred de VPC

Si creó su sistema de archivos en una subred de VPC que se ha compartido con usted, es posible que la cuenta propietaria haya dejado de compartir la subred de VPC.

Si la cuenta propietaria ha dejado de compartir la subred de VPC, verás el siguiente mensaje en la consola de ese sistema de archivos:

```
The vpc ID vpc-012345abcde does not exist
```

Deberás ponerte en contacto con la cuenta propietaria para que pueda volver a compartir la subred contigo.

No se puede acceder a un sistema de archivos a través de NFS, SMB, la CLI de ONTAP o la API de REST de ONTAP desde un cliente de otra VPC o en las instalaciones

Para acceder a un sistema de archivos a través del Network File System (NFS), el bloque de mensajes del servidor (SMB) o la CLI y la API REST de NetApp ONTAP desde un cliente de otra VPC o local, debe configurar el enrutamiento AWS Transit Gateway entre la VPC asociada al sistema de archivos y la red en la que reside el cliente. Para obtener más información, consulte Acceso a datos.

No puede unir una máquina virtual de almacenamiento (SVM) a Active Directory

Si no puede unir un SVM a un Active Directory (AD), compruebe primero Unir las SVM a Microsoft Active Directory. Los problemas más comunes que impiden que un SVM se una a Active Directory se enumeran en las siguientes secciones, incluidos los mensajes de error que se generan en cada caso.

Temas

El nombre de NetBIOS de SVM es el mismo que el nombre de NetBIOS del dominio principal.

Unir un SVM a su Active Directory autoadministrado falla con el siguiente mensaje de error:

Amazon FSx no puede establecer una conexión con su Active Directory. Esto se debe a que el nombre del servidor que especificó es el nombre NetBIOS del dominio principal. Para solucionar este problema, elija un nombre NetBIOS para su SVM que sea diferente del nombre NetBIOS del dominio principal. A continuación, vuelva a intentar unir el SVM a su Active Directory.

Para resolver este problema, siga el procedimiento descrito en Unir un SVM a un Active Directory mediante la API y AWS Management ConsoleAWS CLI para volver a intentar unir el SVM a su AD. Asegúrese de usar un nombre NetBIOS para la SVM que sea diferente del nombre NetBIOS del dominio principal de Active Directory.

El SVM ya está unido a otro Active Directory

Unir un SVM a un Active Directory falla con el siguiente mensaje de error:

Amazon FSx no puede establecer una conexión a su Active Directory. Esto se debe a que el SVM ya está unido a un dominio. Para unir esta SVM a un dominio diferente, puede usar la CLI de ONTAP o la API de REST para desunir esta SVM de Active Directory. A continuación, vuelva a intentar unir el SVM a un Active Directory diferente.

Para resolver este problema, haga lo siguiente:

1. Utilice la CLI de NetApp ONTAP para desunir el SVM de su Active Directory actual. Para obtener más información, consulte Separe un Active Directory de su SVM mediante la CLI de ONTAP NetApp .
2. Siga el procedimiento descrito en Unir un SVM a un Active Directory mediante la API y AWS Management ConsoleAWS CLI para volver a intentar unir el SVM a su AD nuevo.

Amazon FSx no puede conectarse a los controladores de dominio de Active Directory porque el nombre NetBIOS de la SVM ya está en uso

La creación de una SVM unida a su AD autoadministrado falla con el siguiente mensaje de error:

Amazon FSx no puede establecer una conexión con su Active Directory. Esto se debe a que el nombre de NetBIOS (equipo) que especificó ya está en uso en Active Directory. Para solucionar este problema, elija un nombre NetBIOS para su SVM que no esté en uso en su Active Directory, especifique un NetBIOS (computadora). Luego, vuelva a intentar unir su SVM a su Active Directory.

Para resolver este problema, siga el procedimiento descrito en Unir un SVM a un Active Directory mediante la API y AWS Management ConsoleAWS CLI para volver a intentar unir el SVM a su AD.

Asegúrese de usar un nombre NetBIOS para su SVM que sea único y que no esté en uso en su Active Directory.

Amazon FSx no puede comunicarse con sus controladores de dominio de Active Directory

Unir un SVM a su AD autoadministrado falla con el siguiente mensaje de error:

Amazon FSx no puede comunicarse con su Active Directory. Para solucionar este problema, asegúrese de que se permita el tráfico de red entre Amazon FSx y sus controladores de dominio. A continuación, vuelva a intentar unir el SVM a su Active Directory.

Para resolver este problema, siga estos pasos:

1. Revise los requisitos descritos en Requisitos de configuración de la red y realice los cambios necesarios para habilitar las comunicaciones de red entre Amazon FSx y su AD.
2. Una vez que Amazon FSx pueda comunicarse con su AD, siga el procedimiento descrito en Unir un SVM a un Active Directory mediante la API y AWS Management ConsoleAWS CLI y vuelva a intentar unir su SVM a su AD.

Amazon FSx no puede conectarse a su Active Directory debido a que no se cumplen los requisitos de puerto o los permisos de la cuenta de servicio

Unir un SVM a su AD autoadministrado falla con el siguiente mensaje de error:

Amazon FSx no puede establecer una conexión con su Active Directory. Esto se debe a que no se cumplen los requisitos de puerto de su Active Directory o a que la cuenta de servicio proporcionada no tiene permisos para unir la máquina virtual de almacenamiento al dominio de la unidad organizativa especificada. Para solucionar este problema, actualice la configuración de Active Directory de la máquina virtual de almacenamiento después de resolver cualquier problema de permisos con los puertos y las cuentas de servicio, tal y como se recomienda en la guía del usuario de Amazon FSx.

Para resolver este problema, siga estos pasos:

1. Revise los requisitos descritos en Requisitos de configuración de la red y realice los cambios necesarios para cumplir con los requisitos de red y asegurarse de que las comunicaciones estén habilitadas en los puertos necesarios

2. Revise los requisitos de la cuenta de servicio descritos en Requisitos de la cuenta de servicio de Active Directory. Asegúrese de que la cuenta de servicio tenga los permisos delegados necesarios para unir su SVM al dominio de AD mediante la unidad organizativa especificada.
3. Una vez que haya realizado cambios en los permisos del puerto o en la cuenta de servicio, siga el procedimiento descrito en Unir un SVM a un Active Directory mediante la API y AWS Management ConsoleAWS CLI y vuelva a intentar unir el SVM a su AD.

Amazon FSx no puede conectarse a los controladores de dominio de Active Directory porque las credenciales de la cuenta de servicio no son válidas

Unir un SVM a su Active Directory autoadministrado falla con el siguiente mensaje de error:

Amazon FSx no puede establecer una conexión con sus controladores de dominio de Active Directory porque las credenciales de la cuenta de servicio proporcionadas no son válidas. Para solucionar este problema, actualice la configuración de Active Directory de la máquina virtual de almacenamiento con una cuenta de servicio válida.

Para resolver este problema, utilice el procedimiento descrito en Actualización de una configuración de SVM de Active Directory existente mediante las AWS Management Console API, y AWS CLI para actualizar las credenciales de la cuenta de servicio de la SVM. Al introducir el nombre de usuario de la cuenta de servicio, asegúrese de incluir solo el nombre de usuario (por ejemplo, `ServiceAcct`) y no incluya ningún prefijo de dominio (por ejemplo, `corp.com\ServiceAcct`) ni sufijo de dominio (por ejemplo, `ServiceAcct@corp.com`). No utilice el nombre distintivo (DN) al introducir el nombre de usuario de la cuenta de servicio (por ejemplo, `CN=ServiceAcct,OU=example,DC=corp,DC=com`).

Amazon FSx no puede conectarse a los controladores de dominio de Active Directory porque las credenciales de la cuenta de servicio no son suficientes

Unir un SVM a su Active Directory autoadministrado falla con el siguiente mensaje de error:

Amazon FSx no puede establecer una conexión con sus controladores de dominio de Active Directory. Esto se debe a que no se han cumplido los requisitos de puerto para Active Directory o a que la cuenta de servicio proporcionada no tiene permiso para unir la máquina virtual de almacenamiento al dominio de la unidad organizativa especificada.

Para resolver este problema, asegúrese de haber delegado los permisos necesarios en la cuenta de servicio que proporcionó. La cuenta de servicio debe poder crear y eliminar objetos informáticos en la unidad organizativa del dominio al que vaya a unir el sistema de archivos. La cuenta de servicio también necesita, como mínimo, tener permisos para hacer lo siguiente:

- Restablecer contraseñas
- Impedir que las cuentas lean y escriban datos
- Capacidad validada para escribir en el nombre de host del DNS
- Capacidad validada para escribir en el nombre de entidad principal del servicio
- Capacidad para crear y eliminar objetos del equipo
- Capacidad validada para leer y escribir las restricciones de la cuenta

Para obtener más información acerca de la creación de una cuenta de servicio con los permisos correctos, consulte Requisitos de la cuenta de servicio de Active Directory y Delegación de privilegios a la cuenta de servicio Amazon FSx.

Amazon FSx no se puede comunicar con sus servidores DNS o controladores de dominio de Active Directory

Unir un SVM a su Active Directory autoadministrado falla con el siguiente mensaje de error:

Amazon FSx no puede comunicarse con su Active Directory. Esto se debe a que Amazon FSx no puede acceder a los servidores DNS proporcionados ni a los controladores de dominio de su dominio. Para solucionar este problema, actualice la configuración de Active Directory de la máquina virtual de almacenamiento con servidores DNS válidos y una configuración de red que permita que el tráfico fluya desde la máquina virtual de almacenamiento al controlador de dominio.

Para resolver este problema, siga estos pasos:

1. Si solo se puede acceder a algunos de los controladores de dominio de su Active Directory, por ejemplo, debido a limitaciones geográficas o a firewalls, puede agregar los controladores de dominio preferidos. Con esta opción, Amazon FSx intenta ponerse en contacto con los controladores de dominio preferidos. Agregue los controladores de dominio preferidos mediante el comando CLI de `vserver cifs domain preferred-dc add` NetApp ONTAP, de la siguiente manera:

a. Para acceder a la CLI de NetApp ONTAP, ejecute el siguiente comando para establecer una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP. Reemplace *management_endpoint_ip* con la dirección IP del puerto de gestión del sistema de archivos.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Para obtener más información, consulte Administración de sistemas de archivos con la ONTAP CLI.

b. Escriba el siguiente comando, donde:

- `-vserver vserver_name` especifica el nombre de la máquina virtual de almacenamiento (SVM).
- `-domain domain_name` especifica el nombre de autorizado de Active Directory (FQDN) del dominio a los que pertenecen los controladores especificados.
- `-preferred-dc IP_address,…` especifica una o más direcciones IP de los controladores de dominio preferidos, como una lista separada por comas, por orden de preferencia.

```
FsxId123456789::> vserver cifs domain preferred-dc add -vserver vserver_name -
domain domain_name -preferred-dc IP_address, …+
```

El siguiente comando agrega los controladores de dominio 172.17.102.25 y 172.17.102.24 a la lista de controladores de dominio preferidos que el servidor SMB de SVM vs1 utiliza para administrar el acceso externo al dominio cifs.lab.example.com.

```
FsxId123456789::> vserver cifs domain preferred-dc add -vserver vs1 -domain
 cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

2. Compruebe si su controlador de dominio se puede resolver con DNS. Utilice el comando CLI de `vserver services access-check dns forward-lookup` NetApp ONTAP para devolver la dirección IP de un nombre de host en función de la búsqueda en el servidor DNS especificado o de la configuración DNS del servidor virtual.

a. Para acceder a la CLI de NetApp ONTAP, ejecute el siguiente comando para establecer una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp

ONTAP. Reemplace *management_endpoint_ip* con la dirección IP del puerto de gestión del sistema de archivos.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Para obtener más información, consulte Administración de sistemas de archivos con la ONTAP CLI.

b. Acceda al modo avanzado de la CLI de ONTAP con el siguiente comando.

```
FsxId123456789::> set adv
```

c. Escriba el siguiente comando, donde:

- `-vserver vserver_name` especifica el nombre de la máquina virtual de almacenamiento (SVM).
- `-hostname host_name` especifica el nombre de host que se va a buscar en el servidor DNS.
- `-node node_name` especifica el nombre del nodo en el que se ejecuta el comando.
- `-lookup-type` especifica el tipo de dirección IP que se va a buscar en el servidor DNS; el valor predeterminado es `all`.

```
FsxId123456789::> vserver services access-check dns forward-lookup \
-vserver vserver_name -node node_name \
-domains domain_name -name-servers dns_server_ip_address \
-hostname host_name
```

3. Revise la información que debe tener al unir un SVM a un AD.
4. Revise los requisitos de red al unir un SVM a un AD.
5. Utilice el procedimiento descrito en Requisitos de configuración de la red para actualizar la configuración de AD de su SVM con las direcciones IP correctas para los servidores de DNS de AD.

Amazon FSx no puede comunicarse con Active Directory debido a un nombre de dominio de Active Directory no válido.

Unir un SVM a su Active Directory autoadministrado falla con el siguiente mensaje de error:

Amazon FSx ha detectado que el FQDN proporcionado no es válido. Para solucionar este problema, actualice la configuración de Active Directory de la máquina virtual de almacenamiento con un FQDN que cumpla con los requisitos de configuración.

Para resolver este problema, siga estos pasos:

1. Revise los requisitos de nombres de dominio de Active Directory en las instalaciones que se describen en Información necesaria para unir un SVM a un Active Directory. Asegúrese de que el AD al que intenta unirse cumpla con esos requisitos.
2. Utilice el procedimiento descrito en Unir un SVM a un Active Directory mediante la API y AWS Management ConsoleAWS CLI y vuelva a intentar unir su SVM a un AD. Asegúrese de usar el formato correcto para el FQDN del dominio de AD.

La cuenta de servicio no puede acceder al grupo de administradores especificado en la configuración de SVM Active Directory

Unir un SVM a su Active Directory autoadministrado falla con el siguiente mensaje de error:

Amazon FSx no puede aplicar su configuración de Active Directory. Esto se debe a que el grupo de administradores que proporcionó no existe o no es accesible para la cuenta de servicio que proporcionó. Para solucionar este problema, asegúrese de que la configuración de red permita el tráfico desde el SVM hacia los controladores de dominio y los servidores DNS de Active Directory. A continuación, actualice la configuración de Active Directory de su SVM, proporcionando los servidores DNS de Active Directory y especificando un grupo de administradores en el dominio al que pueda acceder la cuenta de servicio proporcionada.

Para resolver este problema, siga estos pasos:

1. Revise la información sobre cómo proporcionar un grupo de dominios para realizar acciones administrativas en su SVM. Asegúrese de que esté utilizando el nombre correcto del grupo de administradores de dominio de AD.
2. Utilice el procedimiento descrito en Unir un SVM a un Active Directory mediante la API y AWS Management ConsoleAWS CLI y vuelva a intentar unir su SVM a un AD.

Amazon FSx no puede conectarse a los controladores de dominio de Active Directory, porque la unidad organizativa especificada no existe o no es accesible

Unir un SVM a su Active Directory autoadministrado falla con el siguiente mensaje de error:

Amazon FSx no puede establecer una conexión con su Active Directory. Esto se debe a que la unidad organizativa que especificó no existe o no es accesible para la cuenta de servicio proporcionada. Para solucionar este problema, actualiza la configuración de Active Directory de la máquina virtual de almacenamiento y especifica una unidad organizativa a la que la cuenta de servicio tenga permisos para unirse.

Para resolver este problema, siga estos pasos:

1. Revise los requisitos previos para unir un SVM a un AD.
2. Revise la información que debe tener al unir un SVM a un AD.
3. Vuelva a intentar unir el SVM al AD mediante este procedimiento con la unidad organizativa correcta.

No puede eliminar una máquina virtual de almacenamiento o un volumen

Cada sistema de archivos de FSx para ONTAP puede contener una o más máquinas virtuales de almacenamiento (SVM) y cada SVM puede contener uno o más volúmenes. Al eliminar un recurso, primero debe asegurarse de que se hayan eliminado todos sus elementos secundarios. Por ejemplo, antes de eliminar una SVM, primero debe eliminar todos los volúmenes no raíz de la SVM.

> **Important**
>
> Solo puede eliminar máquinas virtuales de almacenamiento mediante la consola, la API y la CLI de Amazon FSx. Solo puede eliminar volúmenes mediante la consola, la API o la CLI de Amazon FSx si el volumen tiene habilitadas las copias de seguridad de Amazon FSx.

Para ayudar a proteger sus datos y su configuración, Amazon FSx impide la eliminación de SVM y volúmenes en determinadas circunstancias. Si intenta eliminar una SVM o un volumen y su solicitud

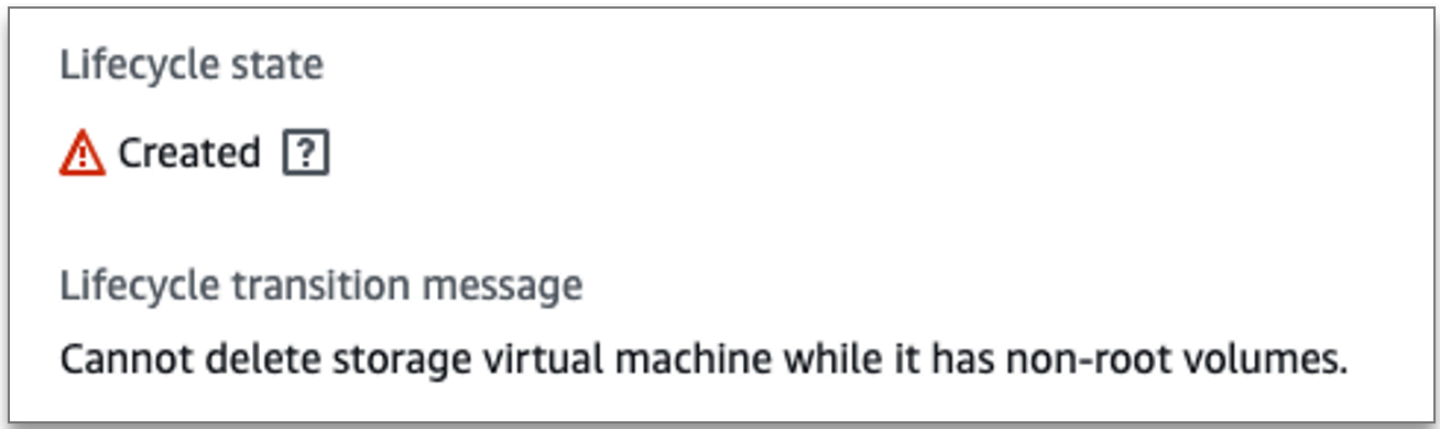
de eliminación no se realiza correctamente, Amazon FSx le proporciona información en AWS la consola AWS Command Line Interface ,AWS CLI() y en la API sobre el motivo por el que no se ha eliminado el recurso. Una vez que haya resuelto la causa del error de eliminación, puede volver a intentar la solicitud de eliminación.

Temas

Identificar las eliminaciones fallidas

Al eliminar un SVM o un volumen de Amazon FSx, normalmente verá la transición del estado de `Lifecycle` a `DELETING` del recurso hasta unos minutos antes de que el recurso desaparezca de la consola, la CLI y la API de Amazon FSx.

Si intenta eliminar un recurso y su estado `Lifecycle` pasa de `DELETING` y, después, vuelve a `CREATED`, este comportamiento indica que el recurso no se ha eliminado correctamente. En este caso, Amazon FSx muestra un icono de alerta en la consola junto al estado de ciclo de vida del `CREATED`. Al seleccionar el icono de alerta, aparecerá el motivo de la eliminación incorrecta, como se indica en el siguiente ejemplo.



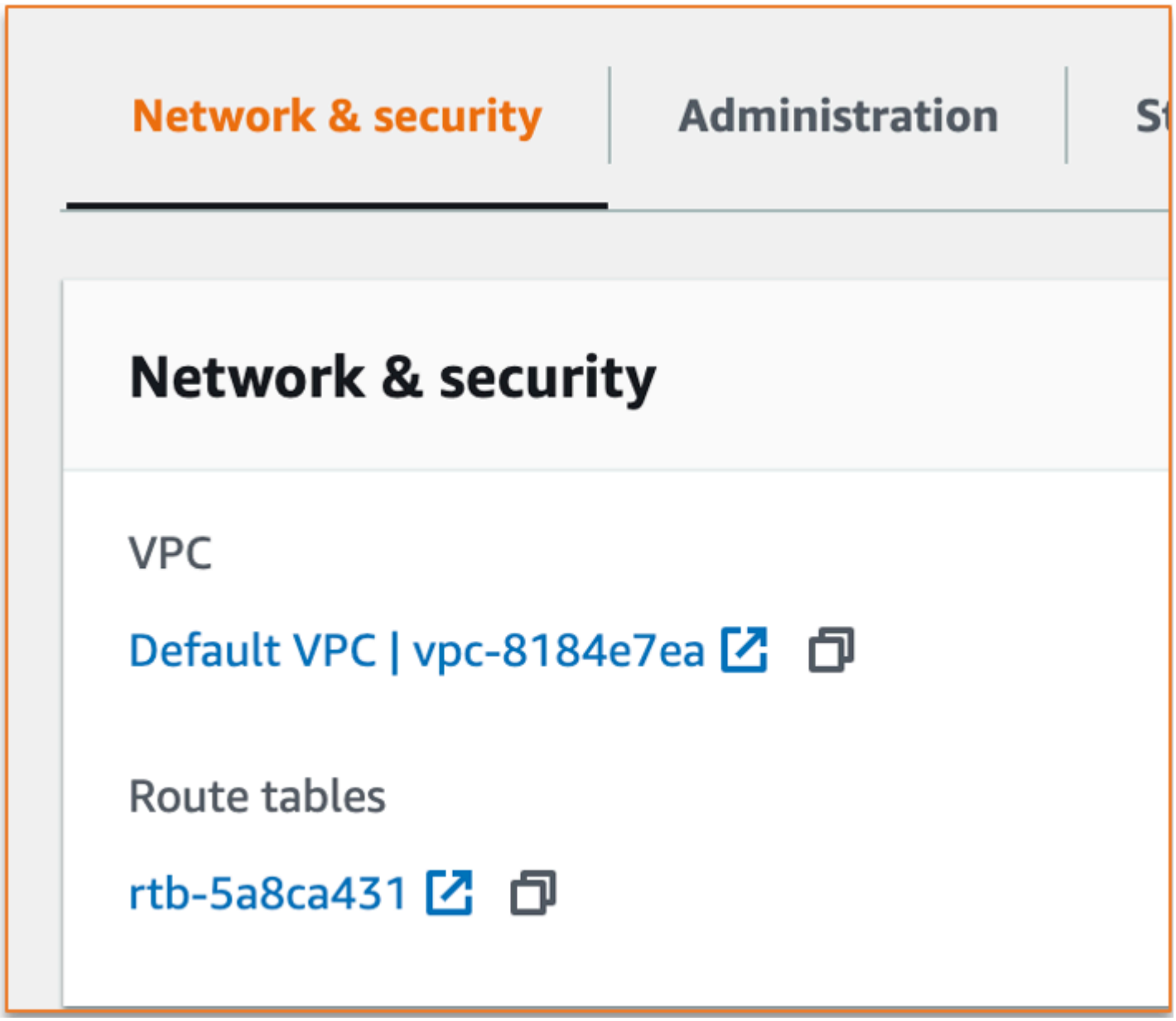
Los motivos más habituales por los que Amazon FSx impide la eliminación de volúmenes y SVM se indican en las siguientes secciones, con step-by-step instrucciones sobre cómo resolver estos problemas.

Eliminación de SVM: no se puede acceder a las tablas de enrutamiento

Cada sistema de archivos de FSx for ONTAP crea una o más entradas en la tabla de enrutamiento para proporcionar una conmutación por error automática y una recuperación por error en todas las zonas de disponibilidad. De forma predeterminada, estas entradas de la tabla de enrutamiento se crean en la tabla de enrutamiento predeterminada de la VPC. Si lo desea, puede especificar una o más tablas de enrutamiento no predeterminadas en las que se puedan crear FSx para las interfaces ONTAP. Amazon FSx etiqueta con una etiqueta `AmazonFSx` cada tabla de enrutamiento asociada a un sistema de archivos y, si se elimina esta etiqueta, puede impedir que Amazon FSx pueda eliminar recursos. Si se produce esta situación, verá el siguiente `LifecycleTransitionReason`:

```
Amazon FSx is unable to complete the requested storage virtual machine
operation because of an inability to access one or more of the route tables
associated with your file system. Please contact AWS Support.
```

Para encontrar las tablas de enrutamiento de su sistema de archivos en la consola de Amazon FSx, vaya a la página de resumen del sistema de archivos, en la pestaña Red y seguridad:



Si selecciona el enlace de las tablas de enrutamiento, accederá a sus tablas de enrutamiento. A continuación, compruebe que cada una de las tablas de enrutamiento asociadas a su sistema de archivos esté etiquetada con este par clave-valor:

```
Key: AmazonFSx
Value: ManagedByAmazonFSx
```

Si esta etiqueta no está presente, vuelva a crearla y, a continuación, intente eliminar el SVM de nuevo.

Eliminación de SVM: relación entre pares

Si intenta eliminar un SVM o un volumen que forma parte de una relación entre pares, primero debe eliminar la relación entre pares antes de eliminar el SVM o el volumen. Este requisito evita que las SVM emparejadas dejen de estar en mal estado. Si su SVM no se puede eliminar debido a una relación entre pares, verá el siguiente `LifecycleTransitionReason`:

Amazon FSx no puede eliminar la máquina virtual de almacenamiento porque forma parte de una relación entre pares de SVM o de pares de transición. Elimine la relación y vuelva a intentarlo.

Puede eliminar las relaciones entre pares de SVM a través de la CLI de ONTAP. Para acceder a la CLI de ONTAP, siga los pasos que se indican en Administración de sistemas de archivos con la ONTAP CLI. Con la CLI de ONTAP, lleve a cabo los pasos que se indican a continuación:

1. Compruebe las relaciones entre pares de SVM mediante el siguiente comando. Reemplace *svm_name* por el nombre de su SVM.

   ```
   FsxId123456789::> vserver peer show -vserver svm_name
   ```

   Si este comando se ejecuta correctamente, verá una salida similar a la siguiente:

   ```
               Peer        Peer                           Peering        Remote
   Vserver     Vserver     State        Peer Cluster      Applications   Vserver
   ----------- ----------- ------------ ----------------- -------------- ---------
   svm_name    test2       peered       FsxId02d81fef0d84734b6
                                                          snapmirror     fsxDest
   ```

```
svm_name    test3       peered       FsxId02d81fef0d84734b6
                                                  snapmirror     fsxDest
2 entries were displayed.
```

2. Elimine cada relación entre pares de SVM mediante el siguiente comando. Reemplace *svm_name* y *remote_svm_name* con sus valores reales.

```
FsxId123456789abcdef::> vserver peer delete -vserver svm_name -peer-
vserver remote_svm_name
```

Si este comando se ejecuta correctamente, verá la siguiente salida:

```
Info: 'vserver peer delete' command is successful.
```

Eliminación de SVM o volumen: SnapMirror

Del mismo modo que no se puede eliminar un SVM con una relación entre iguales sin eliminar primero la relación entre iguales (consulteEliminación de SVM: relación entre pares), tampoco se puede eliminar un SVM que tenga una SnapMirror relación sin eliminar primero la relación. SnapMirror Para eliminar la SnapMirror relación, utilice la CLI de ONTAP para realizar los siguientes pasos en el sistema de archivos que es el destino de la SnapMirror relación. Para acceder a la CLI de ONTAP, siga los pasos que se indican en Administración de sistemas de archivos con la ONTAP CLI.

> **Note**
>
> Las copias de seguridad de Amazon FSx se utilizan SnapMirror para crear point-in-time copias de seguridad incrementales de los volúmenes del sistema de archivos. No puede eliminar esta SnapMirror relación para las copias de seguridad en la CLI de ONTAP. Sin embargo, esta relación se elimina automáticamente al eliminar un volumen mediante la CLI, la API o la consola de AWS .

1. Enumere sus SnapMirror relaciones en el sistema de archivos de destino mediante el siguiente comando. Reemplace *svm_name* por el nombre de su SVM.

```
FsxId123456789abcdef::> snapmirror show -vserver svm_name
```

Si este comando se ejecuta correctamente, verá una salida similar a la siguiente:

```
Source            Destination    Mirror  Relationship   Total             Last
Path        Type  Path           State   Status         Progress  Healthy Updated
----------- ---- ------------    ------- -------------- --------- ------- --------
sourceSvm:sourceVol
            XDP  destSvm:destVol Snapmirrored
                                        Idle           -         true    -
```

2. Elimine la SnapMirror relación ejecutando el siguiente comando en el sistema de archivos de destino.

```
FsxId123456789abcdef::> snapmirror release -destination-path destSvm:destVol -
source-path sourceSvm:sourceVol -force true
```

Eliminación de SVM: LIF habilitado para Kerberos

Si intenta eliminar un SVM que tiene una interfaz lógica (LIF) con Kerberos activado, primero debe deshabilitar Kerberos en ese LIF antes de eliminar el SVM.

Puede deshabilitar Kerberos en un LIF a través de la CLI de ONTAP. Para acceder a la CLI de ONTAP, siga los pasos que se indican en Administración de sistemas de archivos con la ONTAP CLI.

1. Introduzca el modo de diagnóstico en la CLI de ONTAP mediante el siguiente comando.

```
FsxId123456789abcdef::> set diag
```

Cuando se le pida continuar, ingrese **y**.

```
Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y
```

2. Compruebe qué interfaces tienen activado Kerberos. Reemplace *svm_name* por el nombre de su SVM.

```
FsxId123456789abcdef::> kerberos interface show -vserver svm_name
```

Si este comando se ejecuta correctamente, verá una salida similar a la siguiente:

```
(vserver nfs kerberos interface show)
               Logical
Vserver        Interface     Address         Kerberos SPN
-------------- ------------ --------------- -------- ----------------------
svm_name       nfs_smb_management_1
                            10.19.153.48    enabled
5 entries were displayed.
```

3. Deshabilite el LIF de Kerberos mediante el siguiente comando. Reemplace *svm_name* por el nombre de su SVM. Deberá proporcionar el nombre de usuario y la contraseña de Active Directory que utilizó para unir este SVM a su Active Directory.

```
FsxId123456789abcdef::> kerberos interface disable -vserver svm_name -lif
 nfs_smb_management_1
```

Si este comando se ejecuta correctamente, verá la siguiente salida. Proporcione el nombre de usuario y la contraseña de Active Directory que utilizó para unir este SVM a su Active Directory. Cuando se le pida continuar, ingrese **y**.

```
(vserver nfs kerberos interface disable)
Username: admin
Password: *************

Warning: This command deletes the service principal name from the machine account
 on the KDC.
Do you want to continue? {y|n}: y

Disabled Kerberos on LIF "nfs_smb_management_1" in Vserver "svm_name".
```

4. Compruebe que Kerberos esté deshabilitado en la SVM mediante el siguiente comando. Reemplace *svm_name* por el nombre de su SVM.

```
FsxId123456789abcdef::> kerberos interface show -vserver svm_name
```

Si este comando se ejecuta correctamente, verá una salida similar a la siguiente:

```
(vserver nfs kerberos interface show)
               Logical
```

```
Vserver        Interface     Address          Kerberos SPN
-------------- ------------- ---------------- -------- ----------------------
svm_name       nfs_smb_management_1
                             10.19.153.48     disabled
5 entries were displayed.
```

5. Si la interfaz se muestra como`disabled`, intente volver a eliminar la SVM a través de la AWS CLI, la API o la consola.

   Si no ha podido eliminar el LIF mediante los comandos anteriores, puede forzar la eliminación del LIF de Kerberos mediante el siguiente comando. Reemplace *svm_name* por el nombre de su SVM.

   > **Important**
   >
   > El siguiente comando puede vincular el objeto informático de su SVM a su Active Directory.

   ```
   FsxId123456789abcdef::> kerberos interface disable -vserver svm_name -lif
    nfs_smb_management_1 -force true
   ```

   Si este comando se ejecuta correctamente, verá una salida similar a la siguiente. Cuando se le pida continuar, ingrese **y**.

   ```
   (vserver nfs kerberos interface disable)

   Warning: Kerberos configuration for LIF "nfs_smb_management_1" in Vserver
    "svm_name" will be deleted.
   The corresponding account on the KDC will not be deleted. Do you want to continue?
    {y|n}: y
   ```

Eliminación de SVM: otro motivo

Las SVM de FSx para ONTAP crean un objeto informático en su Active Directory cuando se unen a su Active Directory. En algunos casos, es posible que desee desunir manualmente un SVM de su Active Directory mediante la CLI de ONTAP. Para acceder a la CLI de ONTAP, siga los pasos que se indican en Administración de sistemas de archivos con la ONTAP CLI, inicie sesión en la CLI de

ONTAP a nivel del sistema de archivos con las credenciales de `fsxadmin`. Con la CLI de ONTAP, lleve a cabo los siguientes pasos para desunir un SVM de su Active Directory.

> **Important**
>
> Este procedimiento puede vincular el objeto informático de su SVM a su Active Directory.

1. Acceda al modo avanzado en la CLI de ONTAP mediante el siguiente comando.

   ```
   FsxId123456789abcdef::> set adv
   ```

   Después de ejecutar este comando, verá el resultado. Ingrese **y** para continuar.

   ```
   Warning: These advanced commands are potentially dangerous; use them only when
         directed to do so by NetApp personnel.
         Do you want to continue? {y|n}: y
   ```

2. Elimine el DNS de Active Directory mediante el siguiente comando. Reemplace *svm_name* por el nombre de su SVM.

   ```
   FsxId123456789abcdef::> vserver services name-service dns dynamic-update record
    delete -vserver svm_name -lif nfs_smb_management_1
   ```

   > **Note**
   >
   > Si el registro DNS ya se ha eliminado o si no se puede acceder al servidor DNS, se produce un error en este comando. Si eso ocurre, continúe con el siguiente paso.

3. Deshabilite el LIF de Kerberos mediante el siguiente comando. Reemplace *svm_name* por el nombre de su SVM.

   ```
   FsxId123456789abcdef::> vserver services name-service dns dynamic-update modify -
   vserver svm_name -is-enabled false -use-secure false
   ```

   Si este comando se ejecuta correctamente, verá la siguiente salida:

   ```
   Warning: DNS updates for Vserver "svm_name" are now disabled.
        Any LIFs that are subsequently modified or deleted
   ```

```
    can result in a stale DNS entry on the DNS server,
    even when DNS updates are enabled again.
```

4. Separe el dispositivo de Active Directory. Reemplace *svm_name* por el nombre de su SVM.

```
FsxId123456789abcdef::> vserver cifs delete -vserver svm_name
```

Tras ejecutar este comando, verá el siguiente resultado, en el que *CORP.EXAMPLE.COM* se sustituirá por el nombre de su dominio. Cuando se le solicite, escriba su nombre de usuario y contraseña. Cuando se le pregunte si desea eliminar el servidor, ingrese **y**.

```
In order to delete an Active Directory machine account for the CIFS server,
you must supply the name and password of a Windows account with sufficient
privileges to remove computers from the "CORP.EXAMPLE.COM" domain.
Enter the user name: admin
Enter the password:
Warning: There are one or more shares associated with this CIFS server
    Do you really want to delete this CIFS server and all its shares? {y|n}: y
Warning: Unable to delete the Active Directory computer account for this CIFS
 server.
    Do you want to continue with CIFS server deletion anyway? {y|n}: y
```

Eliminación de volumen: relación FlexCache

No puede eliminar los volúmenes que son los volúmenes de origen de una FlexCache relación a menos que elimine primero la relación de caché. Para determinar qué volúmenes tienen una FlexCache relación, puede utilizar la CLI de ONTAP. Para acceder a la CLI de ONTAP, siga los pasos que se indican en Administración de sistemas de archivos con la ONTAP CLI.

1. Compruebe las FlexCache relaciones mediante el siguiente comando.

```
FsxId123456789abcdef::> volume flexcache origin show-caches
```

2. Elimine cualquier relación de caché mediante el siguiente comando. Reemplace *dest_svm_name* y *dest_vol_name* con sus valores reales.

```
FsxId123456789abcdef::> volume flexcache delete -vserver dest_svm_name -
volume dest_vol_name
```

3. Una vez que haya eliminado la relación de caché, intente volver a eliminar su SVM a través de la CLI, la API o la consola de AWS .

Las copias de seguridad automáticas diarias fallan debido a una capacidad de volumen insuficiente

Las copias de seguridad automáticas diarias del volumen fallan y aparecen el siguiente mensaje:

```
Amazon FSx could not create a backup of your volume because the backup snapshot was
 deleted.
```

Las copias de seguridad diarias automáticas fallan porque no hay suficiente capacidad de almacenamiento libre en el volumen. Para mitigar esta situación, necesitará liberar capacidad de almacenamiento en el volumen. Para ello, puede utilizar una o más de las siguientes opciones, según su situación:

- Aumente la capacidad de almacenamiento del volumen
- Aumente la reserva de instantáneas del volumen
- Desactivar la eliminación automática de instantáneas
- No elimine la instantánea de respaldo mediante la CLI de ONTAP

Tiene una capacidad de volumen insuficiente

Si se está quedando sin espacio en sus volúmenes, puede utilizar los procedimientos que se muestran aquí para diagnosticar y resolver la situación.

Temas

- Determine cómo se utiliza la capacidad de almacenamiento de volúmenes
- Aumentar la capacidad de almacenamiento de un volumen
- Uso del ajuste automático del tamaño de los volúmenes
- El almacenamiento principal de su sistema de archivos está lleno
- Eliminación de instantáneas
- Aumentar la capacidad máxima de archivos de un volumen

Determine cómo se utiliza la capacidad de almacenamiento de volúmenes

Puede ver cómo se consume la capacidad de almacenamiento de su volumen mediante el comando CLI de `volume show-space` NetApp ONTAP. Esta información puede ayudarle a tomar decisiones sobre cómo recuperar o conservar la capacidad de almacenamiento en volumen. Para obtener más información, consulte Para supervisar la capacidad de almacenamiento de un volumen (consola).

Aumentar la capacidad de almacenamiento de un volumen

Puede aumentar la capacidad de almacenamiento de un volumen mediante la consola Amazon FSx y la API AWS CLI Amazon FSx. Para obtener más información sobre la actualización de un volumen con mayor capacidad, consulte Actualización de un volumen.

Como alternativa, puede aumentar la capacidad de almacenamiento de un volumen mediante el comando `volume modify` NetApp ONTAP CLI. Para obtener más información, consulte Para cambiar la capacidad de almacenamiento de un volumen (consola).

Uso del ajuste automático del tamaño de los volúmenes

Puede utilizar el ajuste automático del tamaño del volumen para que el volumen crezca automáticamente en una cantidad específica o hasta un tamaño específico cuando alcance un umbral de espacio utilizado. Puede hacerlo para los tipos de FlexVol volumen, que es el tipo de volumen predeterminado para FSx para ONTAP, mediante el comando CLI de ONTAP `volume autosize` NetApp . Para obtener más información, consulte Habilitar el ajuste automático del tamaño del volumen.

El almacenamiento principal de su sistema de archivos está lleno

Si el almacenamiento principal del sistema de archivos de FSx for ONTAP está lleno, no podrá añadir más datos a los volúmenes del sistema de archivos, aunque un volumen muestre que tiene suficiente capacidad de almacenamiento disponible. Puede ver la cantidad de capacidad de almacenamiento principal disponible en la pestaña Monitoreo y rendimiento de la página de detalles del sistema de archivos de la consola de Amazon FSx. Para obtener más información, consulte Supervisión del uso del almacenamiento SSD

Para resolver este problema, puede aumentar el tamaño del nivel de almacenamiento principal de su sistema de archivos. Para obtener más información, consulte Actualización del sistema de archivos, el almacenamiento SSD y las IOPS.

Eliminación de instantáneas

Las instantáneas están habilitadas de forma predeterminada en sus volúmenes, mediante la política de instantáneas predeterminada. Las instantáneas se almacenan en el directorio `.snapshot` de la raíz de un volumen. Puede administrar la capacidad de almacenamiento por volumen con respecto a las instantáneas de las siguientes maneras:

- Eliminar las instantáneas manualmente: recupere la capacidad de almacenamiento eliminando las instantáneas manualmente.
- Cree una política de eliminación automática de instantáneas: cree una política que elimine las instantáneas de forma más agresiva que la política de instantáneas predeterminada.
- Desactivar las instantáneas automáticas: conserve la capacidad de almacenamiento desactivando las instantáneas automáticas.

Para obtener más información sobre la eliminación de instantáneas y la administración de políticas de instantáneas para conservar la capacidad de almacenamiento, consulte Eliminación de instantáneas.

Aumentar la capacidad máxima de archivos de un volumen

Un volumen de FSx para ONTAP puede quedarse sin capacidad de archivo si se agota el número de inodos o punteros de archivo disponibles. De forma predeterminada, el número de inodos disponibles en un volumen es de 1 por cada 32 KB de tamaño de volumen. Para obtener más información, consulte Capacidad de archivos de volumen.

El número de inodos en un volumen aumenta proporcionalmente a la capacidad de almacenamiento del volumen, hasta un umbral de 648 GiB. De forma predeterminada, los volúmenes que tienen una capacidad de almacenamiento de 648 GiB o más tienen todos la misma cantidad de inodos, 21 251 126. Para ver la capacidad máxima de archivos de un volumen, consulte Visualización de la capacidad de archivos de un volumen.

Si crea un volumen superior a 648 GiB y desea tener más de 21 251 126 inodos, debe aumentar manualmente el número máximo de archivos del volumen. Si el volumen se está quedando sin capacidad de almacenamiento, puede comprobar su capacidad máxima de archivos. Si se acerca a su capacidad de archivos, puede aumentarla manualmente. Para obtener más información, consulte Para aumentar el número máximo de archivos en un volumen (ONTAPCLI).

Solución de problemas de red

Si tiene problemas de red, puede utilizar los procedimientos que se muestran aquí para diagnosticar el problema.

Desea capturar el rastreo de un paquete

El rastreo de paquetes es el proceso de verificar la ruta de un paquete a través de las capas hasta su destino. El proceso de rastreo de paquetes se controla con los siguientes NetApp comandos CLI de ONTAP:

- network tcpdump start: inicia el seguimiento de paquetes
- network tcpdump show: muestra los seguimientos de paquetes que se están ejecutando actualmente
- network tcpdump stop: detiene el rastreo de paquetes en ejecución

Estos comandos están disponibles para los usuarios que tienen la función de `fsxadmin` en su sistema de archivos.

Para capturar el rastreo de un paquete desde su sistema de archivos

1. Para conectarse mediante SSH a la NetApp CLI de ONTAP de su sistema de archivos, siga los pasos descritos en la Uso de la NetApp ONTAP CLI sección de la Guía del usuario de Amazon FSx para NetApp ONTAP.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Introduzca el nivel de privilegio de diagnóstico en la CLI de ONTAP mediante el siguiente comando.

   ```
   ::> set diag
   ```

   Cuando se le pida continuar, ingrese `y`.

   ```
   Warning: These diagnostic commands are for use by NetApp personnel only.
   Do you want to continue? {y|n}: y
   ```

3. Identifique la ubicación del sistema de archivos en la que desea guardar el rastreo de paquetes. El volumen debe estar en línea y debe estar montado en el espacio de nombres con una ruta de unión válida. Utilice el siguiente comando para comprobar si hay volúmenes que cumplan con esos criterios:

```
::*> volume show -junction-path !- -fields junction-path
vserver volume    junction-path
------- --------- -------------
fsx     test_vol1 /test_vol1
fsx     test_vol2 /test_vol2
fsx     test_vol2 /test_vol3
```

4. Inicie el rastreo con los argumentos mínimos requeridos. Sustituya lo siguiente:

   - Sustituya *node_name* por el nombre del nodo (por ejemplo,). `FsxId01234567890abcdef-01`
   - *Sustituya svm_name por el nombre* de la máquina virtual de almacenamiento (por ejemplo,). `fsx`
   - Sustituya *junction_path_name por el nombre del volumen* (por ejemplo,). `test-vol1`

```
::*> debug network tcpdump start -node node_name -ipspace Default -pass-through "-i
 e0e -w /clus/svm_name/junction_path_name"
Info: Started network trace on interface "e0e"
Warning: Snapshots should be disabled on the tcpdump destination volume while
 packet traces are occurring. Use the
"volume modify -snapshot-policy none -vserver fsx -volume test_vol1" command to
 disable Snapshots on the
tcpdump destination volume.
```

> **Important**
>
> Los rastros de paquetes solo se pueden capturar en la interfaz `e0e` y en el espacio IP `Default`. En FSx para ONTAP, todo el tráfico de red utiliza la interfaz `e0e`.

Cuando utilice el rastreo de paquetes, tenga en cuenta lo siguiente:

- *Al iniciar un rastreo de paquetes, debe incluir la ruta donde desea almacenar los archivos de rastreo, en este formato: /clus/svm_name/junction-path-name*
- Si lo desea, proporcione el nombre de archivo para el rastreo del paquete. *Si no se especifica el nombre_filtro, se genera automáticamente con el siguiente formato: node-name _ port-name _ yyyymmdd_hhmmss .trc*
- Si se especifican rastros rodantes, el filter_name tiene como sufijo un número que indica la posición en la secuencia de rotación.
- La CLI de ONTAP también acepta los siguientes argumentos -pass-through opcionales:

```
-B, --buffer-size=<KiB>
-c <number_of_packets>
-C <file_size-mB>
-F <filter_expression_filename>
-G <rotate_seconds>
--time-stamp-precision {micro|nano}
-Q, --direction {in|out|inout}
-s, --snapshot-length=<bytes>
-U, --packet-buffered
-W <rotate_file_count>
<filter-expression>
```

- Para obtener información sobre las expresiones de filtro, consulte la página de manual de pcap-filter(7).

5. Vea los rastreos en curso:

```
::*> debug network tcpdump show
Node                    IPspace  Port     Filename
----------------------  -------- -------- --------
FsxId123456789abcdef-01  Default  e0e      /clus/fsx/test_vol1/
FsxId123456789abcdef-01_e0e_20230605_181451.trc
```

6. Detenga el rastreo:

```
::*> debug network tcpdump stop -node FsxId123456789abcdef-01 -ipspace Default -
port e0e
Info: Stopped network trace on interface "e0e"
```

7. Vuelva al nivel de privilegios de administrador:

```
::*> set -priv admin
::>
```

8. Acceda a los rastros de paquetes.

   Los seguimientos de sus paquetes se almacenan en el volumen que especificó mediante el comando debug network tcpdump start y se puede acceder a ellos mediante la exportación a NFS o mediante un recurso compartido SMB que corresponda a ese volumen.

Para obtener más información sobre la captura de trazas de paquetes, consulte Cómo utilizar debug network tcpdump en ONTAP 9.10+ en la base de conocimientos. NetApp

Historial de documentos de Amazon FSx para ONTAP NetApp

- Versión de la API: 01-03-2018
- Última actualización de la documentación: 6 de febrero de 2024

En la siguiente tabla se describen los cambios importantes en la Guía del usuario de Amazon FSx NetApp ONTAP. Para obtener notificaciones sobre las actualizaciones de la documentación, puede suscribirse a la fuente RSS.

Cambio	Descripción	Fecha
Support agregado para 12 pares de alta disponibilidad en sistemas de archivos escalables	Amazon FSx para NetApp ONTAP agregó compatibilidad con 12 pares de alta disponibilidad en sistemas de archivos escalables. Los sistemas de archivos con 12 pares de alta disponibilidad pueden ofrecer hasta 72 GBps de capacidad de procesamiento y 2 400 000 IOPS de SSD en 12 pares de alta disponibilidad (HA). Para obtener más información, consulte Pares de alta disponibilidad (HA) y Amazon FSx NetApp para el rendimiento de ONTAP.	4 de marzo de 2024
Support agregado para el modo de escritura en la nube	Amazon FSx para NetApp ONTAP agregó compatibilidad con el modo de escritura en la nube para volúmenes. Para obtener más información, consulte Habilitar el modo	6 de febrero de 2024

	de escritura en la nube en un volumen.	
Support agregado para hacer copias de seguridad de FlexGroup volúmenes con AWS Backup	Ahora puede utilizarlos AWS Backup para realizar copias de seguridad y restaurar FlexGroup volúmenes en sus FSx para los sistemas de archivos ONTAP. Para obtener más información, consulte Uso AWS Backup con Amazon FSx.	11 de enero de 2024
Amazon FSx actualizó las políticas gestionadas de AmazonFSxFullAccess, AmazonFSxConsoleFullAccess, AmazonFSxReadOnlyAccess y SxConsoleReadOnlyAccess AmazonF SxServiceRolePolicy AWS	Amazon FSx actualizó las políticas de AmazonFSx FullAccess, AmazonFSx ConsoleFullAccess, AmazonFSxReadOnlyAccess y SxServiceRolePolicy AmazonF SxConsole ReadOnlyAccess para añadir el permiso. `ec2:GetSecurityGroupsForVpc` Para obtener más información, consulte Amazon FSx sobre las actualizaciones de las políticas AWS gestionadas.	9 de enero de 2024

Amazon FSx actualizó las políticas gestionadas de AmazonF SxFullAccess y AmazonF SxConsoleFullAccess AWS	Amazon FSx actualizó las SxConsoleFullAccess políticas de AmazonF SxFullAccess y AmazonF para añadir la acción. `ManageCrossAccountDataReplication` Para obtener más información, consulte Amazon FSx sobre las actualizaciones de las políticas AWS gestionadas.	20 de diciembre de 2023
Support agregado para métricas de escalamiento horizontal	FSx for ONTAP ahora proporciona CloudWatch métricas de Amazon para sistemas de archivos con varios pares de alta disponibilidad. Para obtener más información, consulte Métricas de sistemas de archivos escalables.	26 de noviembre de 2023
Support agregado para sistemas de archivos escalables	Amazon FSx para NetApp ONTAP agregó soporte para sistemas de archivos escalables que pueden ofrecer hasta 36 GBps de capacidad de procesamiento y 1 200 000 IOPS de SSD en seis pares de alta disponibilidad (HA). Para obtener más información, consulte Pares de alta disponibilidad (HA) y Amazon FSx NetApp para el rendimiento de ONTAP.	26 de noviembre de 2023

Support agregado para FlexGroup volúmenes	Amazon FSx para NetApp ONTAP agregó soporte para volúmenes. FlexGroup Para obtener más información, consulte Estilos de volumen.	26 de noviembre de 2023
Se agregó compatibilidad con VPC compartida para sistemas de archivos Multi-AZ	Las cuentas de los participantes ahora pueden crear sistemas de archivos Multi-AZ en una VPC que se haya compartido con ellos. Las cuentas de propietario pueden gestionar esta función en la consola, la CLI y la API de Amazon FSx. Para obtener más información, consulte Creación de FSx para sistemas de archivos ONTAP en subredes compartidas	26 de noviembre de 2023
Amazon FSx actualizó las políticas gestionadas de AmazonF SxFullAccess y AmazonF SxConsoleFullAccess AWS	Amazon FSx actualizó las SxConsoleFullAccess políticas de AmazonF SxFullAccess y AmazonF para añadir el permiso. `fsx:CopySnapshotAndUpdateVolume` Para obtener más información, consulte Amazon FSx sobre las actualizaciones de las políticas AWS gestionadas.	26 de noviembre de 2023

Amazon FSx actualizó las políticas gestionadas de AmazonF SxFullAccess y AmazonF SxConsoleFullAccess AWS	Amazon FSx actualizó las SxConsoleFullAccess políticas de AmazonF SxFullAccess y AmazonF para añadir los permisos y. `fsx:DescribeSharedVPCConfiguration` `fsx:UpdateSharedVPCConfiguration` Para obtener más información, consulte Amazon FSx sobre las actualizaciones de las políticas AWS gestionadas.	14 de noviembre de 2023
Soporte añadido para la creación de roles y usuarios ONTAP adicionales	Amazon FSx para NetApp ONTAP ahora admite la creación de funciones y usuarios de ONTAP adicionales para definir las capacidades y los privilegios de los usuarios al utilizar la CLI y la API REST de ONTAP. Para obtener más información, consulte Funciones y usuarios en Amazon FSx para NetApp ONTAP.	6 de septiembre de 2023

Support agregado para CloudWatch métricas adicionales y un panel de monitoreo mejorado	FSx para ONTAP proporciona ahora métricas de rendimiento adicionales y un panel de control de monitorización mejorado para una mayor visibilidad de la actividad del sistema de archivos. Para obtener más información, consulte Monitorear con CloudWatch.	17 de agosto de 2023
Amazon FSx actualizó la política gestionada de SxServiceRolePolicy AWS AmazonF	Amazon FSx actualizó el `cloudwatch:PutMetricData` permiso en AmazonF. SxServiceRolePolicy Para obtener más información, consulte Amazon FSx sobre las actualizaciones de las políticas AWS gestionadas.	24 de julio de 2023
Support agregado para usar NetApp System Manager directamente	Puede gestionar sus sistemas de archivos de FSx para ONTAP utilizando el System Manager directamente desde NetApp BlueXP. Para obtener más información, consulte Uso NetApp del administrador del sistema con BlueXP.	13 de julio de 2023

Soporte añadido para monitorizar eventos del EMS	Puede monitorizar FSx para detectar eventos del sistema de archivos ONTAP mediante el sistema de gestión de eventos (EMS) nativo de NetAPP ONTAP Events Management System (EMS). Puede ver los eventos de EMS mediante la CLI de NetApp ONTAP. Para obtener más información, consulte Monitorización de eventos FSx para ONTAP EMS.	13 de julio de 2023
Soporte añadido para SnapLock	FSx para ONTAP ahora admite volúmenes SnapLock. SnapLock le permite proteger sus archivos al pasarlos a un estado de escritura única y lectura múltiple (WORM), que impide su modificación o eliminación durante un periodo de conservación especificado. FSx for ONTAP admite los modos de retención empresarial y de conformidad con. SnapLock Para obtener más información, consulte Trabajar con. SnapLock	13 de julio de 2023

Soporte añadido para el cifrado de IPsec de datos en tránsito	FSx para ONTAP ahora admite el uso del cifrado de IPsec para cifrar los datos en tránsito entre los sistemas de archivos y los clientes conectados. Para más información, consulte Cifrado de datos en tránsito con cifrado IPsec.	13 de julio de 2023
Se ha incrementado el tamaño máximo del volumen	FSx para ONTAP actualizó el tamaño máximo de un volumen de 100 TB a 300 TB. Para obtener más informaci ón, consulte Activar el tamaño automático del volumen.	13 de julio de 2023
Amazon FSx actualizó la política gestionada de SxFullAccess AWS AmazonF	Amazon FSx actualizó la SxFullAccess política de AmazonF para eliminar el `fsx:*` permiso y añadir acciones específicas. `fsx` Para obtener más informaci ón, consulte la política de SxFullAccessAmazonF.	13 de julio de 2023
Amazon FSx actualizó la política gestionada de SxConsoleFullAccess AWS AmazonF	Amazon FSx actualizó la SxConsoleFullAccess política de AmazonF para eliminar el `fsx:*` permiso y añadir acciones específicas. `fsx` Para obtener más informaci ón, consulte la política de SxConsoleFullAcces sAmazonF.	13 de julio de 2023

Soporte añadido para unir máquinas virtuales de almacenamiento existentes a un Active Directory	Puede unir las máquinas virtuales de almacenam iento existentes a un Active Directory mediante la AWS Management Console API AWS CLI y. Para obtener más información, consulte Unir una SVM a un Active Directory.	13 de junio de 2023
Soporte añadido para caché de lectura NVMe para sistemas de archivos Single-AZ	La caché de lectura de NVMe ahora es compatible con los sistemas de archivos Single-AZ creados después del 28 de noviembre de 2022 con una capacidad de rendimien to de al menos 2 GBps en las regiones Este de EE. UU. (Ohio), Este de EE. UU. (Norte de Virginia), Oeste de EE. UU. (Oregón) y Europa (Irlanda). Para obtener más información, consulte Impacto del tipo de implementación en el rendimiento.	28 de noviembre de 2022
Soporte añadido para usar rangos de direcciones IP en la VPC para crear sistemas de archivos Multi-AZ	Ahora puede crear FSx Multi-AZ para los sistemas de archivos ONTAP especific ando los puntos de conexión que se encuentran dentro del rango de direcciones IP de su VPC. Para obtener más información, consulte Creación de FSx para sistemas de archivos ONTAP.	28 de noviembre de 2022

Soporte añadido para actualizar tablas de enrutamiento VPC en sistemas de archivos Multi-AZ	Ahora puede asociar (añadir) una nueva tabla de enrutamiento VPC a un sistema de archivos de FSx Multi-AZ para ONTAP existente o desasociar (eliminar) una tabla de enrutamiento VPC existente de un FSx Multi-AZ existente para ONTAP. Para obtener más información, consulte Actualización de un sistema de archivos.	28 de noviembre de 2022
Support agregado para el cifrado de datos en tránsito con AWS Nitro System	Los datos en tránsito se cifran automáticamente cuando se accede a ellos desde las instancias de Amazon EC2 compatibles en las regiones Este de EE. UU. (Ohio), Este de EE. UU. (Norte de Virginia), Oeste de EE. UU. (Oregón) y Europa (Irlanda). Para obtener más información, consulte Cifrar datos en tránsito con AWS Nitro System.	28 de noviembre de 2022

Soporte añadido para la creación de volúmenes DP	Ahora puede crear volúmenes DP (protección de datos) mediante la consola AWS CLI de Amazon FSx o la API de Amazon FSx. Puede utilizar los volúmenes DP como destino de una SnapVault relación NetApp SnapMirror o relación cuando desee migrar o proteger los datos de un solo volumen. Para obtener más información, consulte Tipos de volumen.	28 de noviembre de 2022
Soporte añadido para copiar etiquetas de volumen a copias de seguridad	Ahora puede habilitar `CopyTagsToBackups` en la AWS CLI o en la API de Amazon FSx para copiar automáticamente etiquetas de sus volúmenes a las copias de seguridad. Para obtener más información, consulte Copia de etiquetas en copias de seguridad.	28 de noviembre de 2022

Soporte añadido para elegir una política de instantáneas	Ahora puede elegir entre tres políticas de instantáneas integradas al crear o actualizar un volumen mediante la consola de Amazon FSx o la API AWS CLI de Amazon FSx. Además, puede seleccionar una política de instantáneas personalizada que se haya creado en la CLI de ONTAP o en la API de REST. Para obtener más información, consulte Políticas de instantáneas.	28 de noviembre de 2022
Soporte añadido para la opción de capacidad de rendimiento adicional del sistema de archivos	FSx para ONTAP admite ahora una capacidad de rendimiento de 4096 MBps para sistemas de archivos creados después del 28 de noviembre de 2022 en las regiones Este de EE. UU. (Ohio), Este de EE. UU. (Norte de Virginia), Oeste de EE. UU. (Oregón) y Europa (Irlanda). Para obtener más información, consulte Impacto de la capacidad de rendimiento en el rendimiento.	28 de noviembre de 2022

Soporte añadido para IOPS SSD adicionales	FSx para ONTAP admite ahora 160 000 IOPS SSD para sistemas de archivos creados después del 28 de noviembre de 2022 en las regiones Este de EE. UU. (Ohio), Este de EE. UU. (Norte de Virginia), Oeste de EE. UU. (Oregón) y Europa (Irlanda). Para obtener más información, consulte Impacto de la capacidad de rendimiento en el rendimiento.	28 de noviembre de 2022
Support agregado para usar FSx for ONTAP como almacén de datos externo para VMware Cloud on AWS	Puede usar FSx for ONTAP como almacén de datos externo para VMware Cloud on AWS Software-Defined Data Centers (SDDC). Este soporte adicional proporcio na flexibilidad para aumentar o reducir el almacenamiento independientemente de los recursos informáticos para las cargas de trabajo de VMware Cloud on. AWS Para obtener más información, consulte Uso de VMware Cloud con FSx para ONTAP.	30 de agosto de 2022

Aumente automáticamente la capacidad de almacenamiento de un sistema de archivos	Utilice una AWS CloudFormation plantilla personalizable AWS desarrollada por usted para aumentar automáticamente la capacidad de almacenamiento de su sistema de archivos cuando la cantidad de capacidad de almacenamiento SSD utilizada supere el umbral que especifique. Para obtener más información, consulte Aumento dinámico de la capacidad de almacenamiento SSD.	3 de junio de 2022
Amazon FSx ahora está integrado con AWS Backup	Ahora puede utilizarlos AWS Backup para realizar copias de seguridad y restaurar sus sistemas de archivos FSx, además de utilizar las copias de seguridad nativas de Amazon FSx. Para obtener más información, consulte Uso AWS Backup con Amazon FSx.	18 de mayo de 2022
Soporte añadido para implementaciones de sistemas de archivos ONTAP de una sola zona de disponibilidad	Puede crear FSx Single-AZ para sistemas de archivos ONTAP, que están diseñados para proporcionar alta disponibilidad y durabilidad dentro de una única zona de disponibilidad (AZ). Para obtener más información, consulte Elegir la implementación del sistema de archivos.	13 de abril de 2022

Support agregado para puntos finales AWS PrivateLink de VPC de interfaz	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
Soporte añadido para modificar la capacidad de rendimiento de los sistemas de archivos ONTAP existentes	Ahora puede modificar la capacidad de rendimiento disponible para sus sistemas de archivos ONTAP actuales. Para obtener más información, consulte Administración de la capacidad de rendimiento.	30 de marzo de 2022
Soporte añadido para la capacidad de almacenamiento SSD y la escalar de IOPS aprovisionadas	Ahora puede aumentar la capacidad de almacenamiento en SSD y las IOPS aprovisio nadas para los sistemas de archivos de FSx para ONTAP existentes a medida que evolucionan sus requisitos de almacenamiento e IOPS. Para obtener más informaci ón, consulte Administrar la capacidad de almacenamiento y las IOPS aprovisionadas.	25 de enero de 2022

Support añadido para las CloudWatch métricas de Amazon	Puede supervisar su sistema de archivos con Amazon CloudWatch, que recopila y procesa datos sin procesar de FSx para ONTAP para convertirlos en métricas legibles y prácticamente en tiempo real. Para obtener más información, consulta Monitoring with Amazon CloudWatch.	19 de enero de 2022
Soporte añadido para opciones adicionales de rendimiento del sistema de archivos	FSx para ONTAP ahora admite opciones de 128 MB/s y 256 MB/s para el rendimien to del sistema de archivos. Para obtener más informaci ón, consulte Impacto de la capacidad de rendimiento en el rendimiento.	30 de noviembre de 2021
Amazon FSx para NetApp ONTAP ya está disponible de forma general	FSx for ONTAP es un servicio totalmente gestionado que proporciona un almacenam iento de archivos altamente fiable, escalable, eficiente y rico en funciones integrado en el sistema de archivos ONTAP. NetApp Proporcio na las funciones, el rendimien to, las capacidades y las API habituales de los sistemas de NetApp archivos con la agilidad, la escalabilidad y la sencillez de un servicio totalmente gestionado. AWS	2 de septiembre de 2021

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.