



Guía del usuario de ONTAP

FSx para ONTAP



FSx para ONTAP: Guía del usuario de ONTAP

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

¿Qué es Amazon FSx for NetApp ONTAP?	1
Características de para FSx ONTAP	2
Seguridad y protección de datos	3
Herramientas de supervisión	4
Precios FSx para ONTAP	4
FSx para ONTAP en AWS re:Post	4
¿Es la primera vez que utilizas Amazon FSx ?	4
Funcionamiento	6
Sistemas de archivos	6
Máquinas virtuales de almacenamiento	6
Volúmenes	7
Niveles de almacenamiento	7
Organización de datos en niveles	8
Eficacia de almacenamiento	8
Acceso a sus datos	8
Gestión de los recursos de FSx ONTAP	9
Introducción	10
Configuración	10
Inscríbete en una Cuenta de AWS	10
Creación de un usuario con acceso administrativo	11
Siguiente paso	12
Cree su sistema de FSx archivos para ONTAP	13
Montaje del sistema de archivos	16
Limpieza de recursos	17
Regiones de AWS	20
Acceso a sus datos	24
Clientes compatibles	25
Uso de protocolos de almacenamiento en bloques	26
Acceder a los datos desde el Nube de AWS	27
Acceso a los datos desde la misma VPC	27
Acceder a los datos desde una VPC diferente	28
Acceso a los datos en las instalaciones	32
Acceso a NFS, SMB, la CLI de ONTAP y la API en las instalaciones	32
Acceso a los puntos de conexión entre clústeres en las instalaciones	33

Configurar el enrutamiento para acceder a sistemas de archivos Multi-AZ desde fuera de la VPC	34
Configurar el enrutamiento para acceder a sistemas de archivos Multi-AZ en las instalaciones	35
Montaje en clientes Linux	36
Usar /etc/fstab para montar automáticamente en el reinicio de la instancia	38
Montar en clientes de Windows	39
Requisitos previos	40
Montaje en clientes macOS	41
Aprovisionamiento de iSCSI para Linux	44
Antes de empezar	44
Instalar y configurar iSCSI en el host Linux	46
Configuración de iSCSI en el sistema de archivos FSx ONTAP	48
Monte un LUN iSCSI en su cliente Linux	50
Aprovisionamiento de iSCSI para Windows	56
Configurar iSCSI en el cliente de Windows	58
Configuración de iSCSI en el sistema de archivos FSx ONTAP	58
Montar un LUN iSCSI en el cliente de Windows	60
Validación de la configuración iSCSI	64
Aprovisionamiento de NVMe /TCP para Linux	65
Antes de empezar	66
Instale y configure NVMe en el host Linux	67
NVMe Configúrelo en el FSx sistema de archivos ONTAP	67
Monte un NVMe dispositivo en su cliente Linux	70
Aprovisionamiento NVMe/TCP para Windows	76
Acceso a los datos con otros servicios de AWS	76
Uso de Amazon WorkSpaces	76
Uso de Amazon ECS	83
Uso de Amazon EVS	86
Uso de la nube VMware	86
Opciones de disponibilidad, durabilidad e implementación	87
Selección de un tipo de implementación del sistema de archivos	87
Tipos de implementación Single-AZ	87
Tipos de implementación Multi-AZ	89
Selección de una generación del sistema de archivos	90
Proceso de conmutación por error FSx para ONTAP	92

Probar la conmutación por error en un sistema de archivos	93
Recursos de red	93
Subredes	93
Interfaces de red elástica del sistema de archivos	94
Rendimiento	96
Mida el desempeño	96
Latencia	96
Rendimiento e IOPS	96
Soporte para SMB, multicanal y NFS nconnect	97
Detalles de desempeño	97
Impacto del tipo de implementación en el rendimiento	99
Impacto de la capacidad de almacenamiento en el rendimiento	102
Impacto de la capacidad de rendimiento en el rendimiento	102
Ejemplo: capacidad de almacenamiento y capacidad de rendimiento	109
Administración de recursos	111
Administración de la capacidad de almacenamiento	111
Niveles de almacenamiento	112
Elegir la capacidad de almacenamiento del sistema de archivos	113
Capacidad de almacenamiento e IOPS del sistema de archivos	118
Capacidad de almacenamiento de volumen	139
Gestión de sistemas de archivos	166
Recursos del sistema de archivos	166
Creación de sistemas de archivos	169
Actualizar sistemas de archivos	183
Administración de pares de HA	187
Administrar la NVMe caché	196
Supervisión de detalles del sistema de archivos	196
Eliminación de sistemas de archivos	198
Administrar SVMs	199
Número máximo de archivos SVMs por sistema de archivos	199
Creando SVMs	200
Actualizando SVMs	206
Auditoría del acceso a archivos	208
Configuración de los grupos de trabajo	221
Supervisión de los detalles de la SVM	228
Eliminando SVMs	229

Gestión de volúmenes	230
Estilos de volumen	232
Tipos de volúmenes	234
Estilo de seguridad del volumen	234
Creación de volúmenes	235
Actualización de volúmenes	241
Movimiento de volúmenes	245
Supervisión de volúmenes	249
Eliminación de volúmenes	251
Creación de un iSCSI LUN	253
Pasos a seguir a continuación	255
Actualización de periodos de mantenimiento	255
Administración de la capacidad de rendimiento	257
Cuándo modificar la capacidad de rendimiento	258
¿Cómo se gestionan las solicitudes simultáneas?	259
Actualización de la capacidad de rendimiento	260
Monitoreo de los cambios en la capacidad de rendimiento	261
Gestión de recursos compartidos SMB	263
Administrar con NetApp aplicaciones	265
Registrarse en un NetApp inscrita	266
Utilización NetApp BlueXP	267
Uso de NetApp ONTAP CLI	268
Uso de ONTAP API de REST	272
Etiquetado de recursos	272
Conceptos básicos de etiquetas	273
Etiquetado de recursos	274
Copiar etiquetas en copias de seguridad	275
Restricciones de las etiquetas	276
Permisos y etiqueta	276
Protección de datos	278
Copia de seguridad de volúmenes	278
Cómo funcionan las copias de seguridad	280
Requisitos de almacenamiento	281
Copias de seguridad diarias automáticas	281
Copias de seguridad iniciadas por el usuario	282
Copiar etiquetas en copias de seguridad	282

Usando AWS Backup	283
Restauración de copias de seguridad	284
Rendimiento de las copias de seguridad	286
Copia de seguridad de volúmenes SnapLock	287
Crear copias de seguridad iniciadas por el usuario	287
Restauración de copias de seguridad	288
Restauración de un subconjunto de datos	292
Supervisión del progreso de la restauración del volumen	293
Eliminación de copias de seguridad	295
Uso de instantáneas de volumen	297
Políticas de instantáneas	298
Restauración de archivos a partir de instantáneas	299
Visualización de la instantánea común	300
Actualización del espacio de la reserva de instantáneas	301
Desactivación de las instantáneas automáticas	302
Eliminación de instantáneas	304
Eliminación de instantáneas	304
Reserva de instantáneas	306
Proteja los datos con la protección autónoma contra el ransomware	307
¿Cómo funciona ARP	307
¿Qué busca ARP	308
¿Cómo responder a un presunto ataque con ARP	308
Habilitar el ARP	309
Responder a las alertas de ARP	311
Comprenda las alertas de EMS para ARP	313
Proteja los datos con SnapLock	315
Cómo SnapLock funciona	316
Descripción SnapLock Conformidad	320
Descripción SnapLock Enterprise	321
Entender el SnapLock periodo de retención	323
Pasar archivos a WORM	325
Replicar sus datos con FlexCache	330
Cómo funciona FlexCache	331
FlexCachemodos de escritura	331
FlexCachedescripción general de la creación de volúmenes	332
Creación de un FlexCache	332

Utilización SnapMirror para la replicación programada	338
Utilización NetApp BlueXP para programar la replicación	339
Uso de ONTAP CLI para programar la replicación	339
Informes de facturación y uso	340
FSx para ver el informe de facturación de ONTAP	340
FSx para ver el informe de uso de ONTAP	344
Monitoreo de sistemas de archivos	349
Monitorización con CloudWatch	350
Acceder a las CloudWatch métricas	351
Monitorización en la FSx consola de Amazon	353
Métricas del sistema de archivos	366
Métricas del sistema de archivos de segunda generación	389
Métricas de volumen	408
Monitorización de eventos del EMS	418
Información general sobre los eventos del EMS	418
Visualización de eventos del EMS	419
Reenvío de eventos del EMS a un servidor Syslog	426
Supervisión con Data Infrastructure Insights	428
Monitoreo con Harvest y Grafana	429
Introducción a Harvest y Grafana	429
Paneles de Harvest compatibles	430
No se admite Harvest paneles	431
AWS CloudFormation plantilla	431
Tipos de EC2 instancias de Amazon	432
Procedimiento de implementación	432
Iniciar sesión en Grafana	436
Solución de problemas de Harvest y Grafana	436
Supervisión con AWS CloudTrail	440
FSx Información de Amazon en CloudTrail	440
Descripción de las entradas de los archivos de FSx registro de Amazon	441
Uso de Active Directory	444
Requisitos previos de Active Directory autoadministrado	445
Requisitos del Active Directory autoadministrado	445
Requisitos de configuración de la red	445
Requisitos de la cuenta de servicio de Active Directory	447
Las prácticas recomendadas del Active Directory autoadministrado	449

Delegar permisos a tu cuenta de FSx servicio de Amazon	449
Mantenga actualizada la configuración de AD	450
Limitar el tráfico dentro de una VPC con grupos de seguridad	451
Creación de reglas de grupos de seguridad de salida	451
Cómo funciona SVMs la unión a Active Directory	451
Información necesaria de Active Directory	452
Administración de las configuraciones del Active Directory de la SVM	454
Unirse SVMs a Active Directory	454
Actualización de configuraciones de Active Directory	457
Actualización de las configuraciones de Active Directory con la NetApp CLI	459
Migración a Amazon FSx	465
Migración mediante SnapMirror	465
Antes de empezar	467
Crear el volumen de destino	469
Registre el origen y el destino entre clústeres LIFs	470
Establezca el emparejamiento de clústeres entre el origen y el destino	471
Cree una relación de emparejamiento SVM	472
Cree la relación SnapMirror	473
Transfiera datos a su sistema de archivos FSx para ONTAP	474
Pasando a Amazon FSx	474
Migración de archivos con AWS DataSync	476
Requisitos previos	477
DataSync pasos básicos de migración	477
Seguridad	479
Protección de los datos	480
El cifrado de datos es FSx para ONTAP	481
Cifrado en reposo	481
Cifrado de datos en tránsito	484
Identity and Access Management	506
Público	507
Autenticación con identidades	507
Administración de acceso mediante políticas	511
FSx para ONTAP e IAM	514
Ejemplos de políticas basadas en identidades	520
Solución de problemas de IAM	523
Cómo utilizar roles vinculados a servicios	525

Uso de etiquetas con Amazon FSx	530
AWS políticas gestionadas	537
Amazon FSx ServiceRolePolicy	537
Amazon FSx DeleteServiceLinkedRoleAccess	537
Amazon FSx FullAccess	538
Amazon FSx ConsoleFullAccess	539
Amazon FSx ConsoleReadOnlyAccess	539
Amazon FSx ReadOnlyAccess	541
Actualizaciones de políticas	541
Control de acceso al sistema de archivos con Amazon VPC	553
Grupos de seguridad de Amazon VPC	554
Validación de la conformidad	557
Puntos de conexión de VPC de la interfaz	558
Consideraciones sobre los puntos de enlace de FSx VPC de la interfaz de Amazon	559
Creación de un punto de enlace de VPC de interfaz para la API de Amazon FSx	559
Creación de una política de puntos de conexión de VPC para Amazon FSx	560
Resiliencia	560
Copia de seguridad y restauración	561
Instantáneas	561
Zonas de disponibilidad	561
Seguridad de infraestructuras	562
Utilización de programas antivirus	563
Usuarios y roles de ONTAP	563
Roles y usuarios del administrador del sistema de archivos	564
Roles y usuarios de administrador de la SVM	565
Autenticación de usuarios de ONTAP con Active Directory	567
Creación de nuevos usuarios de ONTAP para la administración del sistema de archivos y la SVM	568
Creación de usuarios de ONTAP	569
Creación de roles de SVM	572
Configuración de la autenticación con Active Directory para usuarios de ONTAP	573
Configuración de la autenticación de clave pública	576
Actualización de los requisitos de contraseña	577
Se produce un error al actualizar la contraseña de la cuenta fsxadmin	578
Cuotas	580
Cuotas que puede aumentar	580

Cuotas de recursos para cada sistema de archivos	582
Solución de problemas	588
Sistemas de archivos mal configurados	588
El uso compartido de VPC está deshabilitado	588
No se puede crear un sistema de archivos Multi-AZ	589
El nivel de SSD está lleno en más del 90%	589
No puede acceder al sistema de archivos	590
Faltan etiquetas de tabla de rutas	591
Demasiadas rutas	591
Faltan rutas a los servidores	591
ENI modificado o eliminado	592
¿Se eliminó ENI	592
Faltan reglas de entrada	592
Faltan reglas de salida	592
La subred de la instancia de cómputo no usa ninguna de las tablas de enrutamiento asociadas a su sistema de archivos	592
No se puede actualizar la tabla de rutas Multi-AZ	593
No se puede acceder a iSCSI	593
Subred de VPC no compartida	594
No se puede acceder a NFS, SMB, CLI y API de ONTAP desde diferentes VPC y locales ..	594
SVM mal configurado	594
Su SVM tiene un volumen fuera de línea	594
Su SVM tiene un volumen fuera de línea con un LUN iSCSI o un espacio de nombres /TCP NVMe	595
No se puede unir SVM a AD	595
El nombre de NetBIOS de SVM es el mismo que el del dominio principal	596
SVM está unido a otro AD	596
Ya se ha utilizado el nombre de NetBIOS de SVM	597
FSx no puede acceder a los controladores de dominio de AD	597
La configuración de puertos o los permisos de la cuenta de servicio son insuficientes	598
Credenciales de cuenta de servicio inválidas	598
Amazon no FSx puede conectarse a los controladores de dominio de Active Directory porque las credenciales de la cuenta de servicio son insuficientes	599
No se puede acceder a los servidores DNS o controladores de dominio de AD	600
Nombre de dominio de AD no válido	602
La cuenta de servicio no puede acceder al grupo de administradores de AD	603

La OU especificada no es válida	603
No se puede eliminar el SVM o el volumen	604
Identificar las eliminaciones fallidas	605
Eliminación de SVM: no se puede acceder a las tablas de enrutamiento	605
Eliminación de SVM: relación entre pares	607
Eliminación de SVM o volumen: SnapMirror	608
Eliminación de SVM: LIF habilitado para Kerberos	609
Eliminación de SVM: otro motivo	611
Eliminación de volumen: relación FlexCache	613
Volumen mal configurado	614
El volumen está lleno en más del 98%	614
El volumen de almacenamiento en bloque está desconectado	614
Sin conexión FlexCache volumen de origen	615
Volumen fuera de línea con SnapMirror relación	615
El volumen de almacenamiento en bloque está restringido	616
Volumen de FlexCache origen restringido	616
Volumen restringido con SnapMirror relación	616
El volumen no tiene suficiente espacio de almacenamiento	617
Determine cómo se utiliza la capacidad de almacenamiento de volúmenes	617
Aumentar la capacidad de almacenamiento de un volumen	618
Uso del ajuste automático del tamaño de los volúmenes	618
El almacenamiento principal de su sistema de archivos está lleno	618
Eliminación de instantáneas	618
Aumentar la capacidad máxima de archivos de un volumen	619
Fallos en las copias de seguridad	620
Solución de problemas de red	620
Desea capturar el rastreo de un paquete	620
Historial de documentos	624
.....	dcxlvii

¿Qué es Amazon FSx for NetApp ONTAP?

Amazon FSx for 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 el popular sistema NetApp de archivos ONTAP. FSx for ONTAP combina las características habituales, el rendimiento, las capacidades y las operaciones de API de los sistemas de NetApp archivos con la agilidad, la escalabilidad y la sencillez de un sistema totalmente gestionado. Servicio de AWS

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

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

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

Para los clientes que utilizan NetApp ONTAP de forma local, ONTAP es la solución ideal FSx para migrar, crear copias de seguridad o agrupar 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.

Al tratarse de un servicio totalmente gestionado, FSx ONTAP facilita el lanzamiento y la ampliación de un almacenamiento de archivos compartido fiable, seguro y de alto rendimiento en la nube. Con FSx ONTAP, ya no tendrá que preocuparse por:

- 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) WorkSpaces, Amazon, AWS Key Management Service (AWS KMS) y. AWS CloudTrail

Temas

- [Características de para FSx ONTAP](#)
- [Seguridad y protección de datos](#)
- [Herramientas de supervisión](#)
- [Precios FSx para ONTAP](#)
- [FSx para ONTAP en AWS re:Post](#)
- [¿Es la primera vez que utilizas Amazon FSx ?](#)

Características de para FSx ONTAP

Con FSx ONTAP, dispondrá de 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 Network File System (NFS), Server Message Block (SMB), Internet Small Computer Systems Interface (iSCSI) y Non-Volatile Memory Express () NVMe
- [Opciones de implementación Multi-AZ y Single-AZ duraderas y de alta disponibilidad](#)
- 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
- Compatibilidad con NetApps [SnapMirror](#) función de replicación

- Compatibilidad con NetApp soluciones de almacenamiento en caché local: caché de archivos NetApp global y FlexCache
- Support para el acceso y la administración mediante aplicaciones nativas AWS o NetApp herramientas y operaciones de API
 - AWS Management Console, AWS Command Line Interface (AWS CLI) y SDKs
 - [NetApp CLI de ONTAP, API REST y BlueXP](#)

Seguridad y protección de datos

Se emplea el modelo de responsabilidad compartida en lo que respecta a. [Seguridad en Amazon FSx para NetApp ONTAP](#) Amazon FSx ofrece varios niveles de seguridad y [conformidad](#) para facilitar la protección de tus datos.

FSx for ONTAP admite las siguientes funciones de protección de datos, seguridad y control de acceso:

- [Cifrar los datos en reposo](#) para los datos del sistema de archivos y las copias de seguridad mediante AWS KMS keys
- Cifrar los datos en tránsito mediante:
 - [Kerberos para pequeñas y medianas empresas](#)
 - [IPSEC](#)
 - Cifrado basado en [Nitro](#)
- Escaneo [antivirus](#) bajo demanda
- Autenticación y autorización mediante [Microsoft Active Directory](#)
- [Auditoría de acceso a archivos](#)
- [NetAppSnapLock](#)WORM con modos de cumplimiento y retención empresarial

Para obtener más información, consulte [Protección de datos en Amazon FSx para NetApp ONTAP y Protección de datos](#).

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 puedes realizar copias de seguridad adicionales en cualquier momento. Para obtener más información, consulte [Protección de datos](#).

Herramientas de supervisión

Las herramientas de monitoreo incluyen [CloudWatchCloudTrail](#), [ONTAP eventos EMS](#), [NetApp Información sobre la infraestructura](#) de datos y [NetApp Cosecha](#).

Precios FSx para ONTAP

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

- Capacidad de almacenamiento en SSD (por gigabyte/mes o GB por mes)
- IOPS de SSD que aprovisiona por encima de tres IOPS/GB (por IOPS al mes)
- Capacidad de rendimiento (por megabytes por segundo [] -mes) MBps
- 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, consulta los [precios de Amazon FSx for NetApp ONTAP](#).

FSx para ONTAP en AWS re:Post

Si tienes problemas al usar Amazon FSx, úsala [AWS re:Post](#) para obtener respuestas a tus FSx preguntas sobre ONTAP.

¿Es la primera vez que utilizas Amazon FSx ?

Si es la primera vez que utilizas Amazon FSx, te recomendamos que leas las siguientes secciones en orden:

1. Si eres nuevo en esto AWS, consulta [Configuración FSx para ONTAP](#) para configurar un Cuenta de AWS.
2. Si estás listo para crear tu primer sistema de FSx archivos de Amazon, sigue las instrucciones que se indican en [Cómo empezar a usar Amazon FSx for NetApp ONTAP](#).
3. Para obtener más información acerca del rendimiento, consulte [Amazon FSx para el rendimiento de NetApp ONTAP](#).

4. Para conocer los detalles FSx de seguridad de Amazon, consulte [Seguridad en Amazon FSx para NetApp ONTAP](#).
5. Para obtener información sobre la FSx API de Amazon, consulta la [referencia de la FSx API de Amazon](#).

Cómo funciona Amazon FSx for 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 procedimientos de step-by-step configuración.

Temas

- [FSx para los sistemas de archivos ONTAP](#)
- [Máquinas virtuales de almacenamiento](#)
- [Volúmenes](#)
- [Niveles de almacenamiento](#)
- [Eficacia de almacenamiento](#)
- [Acceder a los datos almacenados en los sistemas de archivos de FSx ONTAP](#)
- [Gestión de los recursos de FSx ONTAP](#)

FSx para los sistemas de archivos ONTAP

Un sistema de archivos es el recurso principal FSx de ONTAP, de forma análoga a un clúster NetApp ONTAP local. 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 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 activa y en espera. Los sistemas de archivos ONTAP FSx de primera generación y los sistemas de archivos Multi-AZ de segunda generación admiten un par HA. Los sistemas de archivos Single-AZ de segunda generación admiten hasta 12 pares de HA. Para obtener más información, consulte [Administración de 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 del sistema de archivos FSx de ONTAP, sus clientes y estaciones de trabajo interactúan con un SVM mediante la dirección IP del punto final del SVM. Para obtener más información, consulte [Administrar SVMs](#).

Puede unirse SVMs a un Active Directory de Microsoft para autenticar y autorizar el acceso a los archivos. Para obtener más información, consulte [Cómo trabajar con Microsoft Active Directory en FSx ONTAP](#).

Volúmenes

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

Al crear un volumen, se establece el 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, ya sea 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 NetApp SnapMirror o SnapVault .

FSx en el caso de ONTAP, los volúmenes son de aprovisionamiento reducido, lo que significa que solo consumen capacidad de almacenamiento para los datos almacenados en ellos. Con volúmenes con aprovisionamiento ligero, 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 de los tres volúmenes no supere los 10 TiB en ningún momento. La cantidad de datos almacenados físicamente en un volumen se tiene en cuenta en el consumo total de capacidad de almacenamiento. Para obtener más información, consulte [Gestión de FSx volúmenes de ONTAP](#).

Niveles de almacenamiento

Un sistema de archivos FSx para ONTAP tiene dos niveles de almacenamiento: almacenamiento principal y almacenamiento agrupado de capacidades. 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 [FSx para los niveles de almacenamiento de ONTAP](#).

Organización de datos en niveles

La organización de datos en niveles es el proceso mediante el cual Amazon FSx for NetApp 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 (en frío). El periodo de enfriamiento de la política de estratificación de un volumen determina cuándo los datos se vuelven inactivos (en frío). Para obtener más información, consulte [Organización de datos de volumen en niveles](#).

Eficacia de almacenamiento

Amazon FSx for 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 [Eficacia de almacenamiento](#).

Acceder a los datos almacenados en los sistemas de archivos de FSx ONTAP

Puede acceder a los datos de los volúmenes ONTAP desde varios clientes Linux, Windows o macOS simultáneamente a través de los protocolos NFS (v3, v4, v4.1, v4.2) y SMB. FSx También puede acceder a los datos mediante el protocolo de bloques Non-Volatile Memory Express (NVMe) y la Interfaz de sistemas informáticos pequeños de Internet (iSCSI). Para obtener más información, consulte [Acceder a sus FSx datos de ONTAP](#).

Gestión de los recursos de FSx ONTAP

Existen varias formas de interactuar con el sistema de archivos FSx de ONTAP y gestionar sus recursos. Puede gestionar los recursos de ONTAP mediante ambas herramientas de gestión AWS y las herramientas de gestión de NetApp ONTAP: FSx

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

Para obtener más información, consulte [Administración de recursos](#).

Cómo empezar a usar Amazon FSx for NetApp ONTAP

Descubre cómo empezar a usar Amazon FSx para NetApp ONTAP. Este ejercicio introductorio incluye los siguientes pasos.

1. Inscribise en una cuenta Cuenta de AWS y cree un usuario administrativo en la cuenta.
2. Cree un sistema de archivos Amazon FSx for NetApp ONTAP mediante la FSx consola de Amazon.
3. Monta tu sistema de archivos desde una instancia de Amazon EC2 Linux.
4. Limpie los recursos de que ha creado.

Temas

- [Configuración FSx para ONTAP](#)
- [Cree un sistema de archivos Amazon FSx for NetApp ONTAP](#)
- [Montaje del sistema de archivos desde una instancia de Amazon EC2 Linux](#)
- [Limpieza de recursos](#)

Configuración FSx para ONTAP

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

1. [Inscríbete en una Cuenta de AWS](#)
2. [Creación de un usuario con acceso administrativo](#)

Temas

- [Inscríbete en una Cuenta de AWS](#)
- [Creación de un usuario con acceso administrativo](#)
- [Siguiente paso](#)

Inscríbete en una Cuenta de AWS

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

Para suscribirse a una Cuenta de AWS

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

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

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

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

Creación de un usuario con acceso administrativo

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

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión [AWS Management Console](#) como propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

Para obtener ayuda para iniciar sesión con el usuario raíz, consulte [Iniciar sesión como usuario raíz](#) en la Guía del usuario de AWS Sign-In .

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

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

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

Consulte las instrucciones en [Activar AWS IAM Identity Center](#) en la Guía del usuario de AWS IAM Identity Center .

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

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

Inicio de sesión como usuario con acceso de administrador

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

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

Concesión de acceso a usuarios adicionales

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

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

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

Para conocer las instrucciones, consulte [Add groups](#) en la Guía del usuario de AWS IAM Identity Center .

Siguiente paso

Para empezar a usar FSx ONTAP, consulta las instrucciones [Cómo empezar a usar Amazon FSx for NetApp ONTAP](#) para crear tus FSx recursos de Amazon.

Cree un sistema de archivos Amazon FSx for NetApp ONTAP

La FSx consola de Amazon 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 for NetApp ONTAP con la configuración recomendada por el servicio, utilice la opción de creación rápida.

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 volúmenes adicionales SVMs según sea necesario, incluido un SVM unido 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). También puede agregar pares de alta disponibilidad (HA) adicionales en función del tipo de implementación que elija y de la cantidad de pares de HA que agregue al crearla.

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 sistemas de archivos](#)

Cómo crear su sistema de archivos

1. Abra la FSx consola de Amazon 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 for 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 [Opciones de disponibilidad, durabilidad e implementación](#).

 Note

De forma predeterminada, se selecciona la última generación FSx del sistema de archivos ONTAP que esté disponible para usted. Región de AWS Puede especificar la generación de su sistema de archivos (si está disponible Regiones de AWS) con la opción de creación estándar. Para obtener más información, consulte [Creación de sistemas de archivos](#).

7. En Capacidad de almacenamiento en SSD, especifique la capacidad de almacenamiento del sistema de archivos en gibibytes (GiB). Introduzca cualquier número entero en el rango de 1024 a 1 048 576. Para obtener más información, consulte [Cómo 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 proporciona FSx automáticamente una capacidad de rendimiento recomendada en función del almacenamiento SSD. También puede elegir el rendimiento de su sistema de archivos (hasta 73 728, MBps según el tipo de implementación y la cantidad de pares de alta disponibilidad).
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:

- Rango de direcciones IP no asignadas de su VPC: elija esta opción para que FSx Amazon utilice las últimas 64 direcciones IP del rango CIDR principal de la VPC como rango de direcciones IP de punto final 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 direcciones IP SVMs 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.
- Rango de direcciones IP flotante fuera de la VPC: elija esta opción para que Amazon FSx utilice un rango de direcciones de 198.19.x.0/24 que no utilice 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. 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 y siempre que otro sistema de archivos no lo esté usando con la misma VPC y tablas de enrutamiento. Recomendamos usar un rango que esté dentro del rango de direcciones IP de la VPC.

 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 [Actualizar sistemas de archivos](#).

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 con la AWS KMS clave gestionada por el servicio predeterminada.

Montaje del sistema de archivos desde una instancia de Amazon EC2 Linux

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 tu sistema de archivos desde Amazon EC2

1. Abre la EC2 consola de Amazon en <https://console.aws.amazon.com/ec2/>.
2. Cree o seleccione una EC2 instancia de Amazon que ejecute Amazon Linux 2 y que esté en la misma nube privada virtual (VPC) que su sistema de archivos. Para obtener más información sobre el lanzamiento de una instancia, consulta el [paso 1: lanzar una instancia](#) en la Guía del EC2 usuario de Amazon.
3. Conéctate a tu instancia de Amazon EC2 Linux. Para obtener más información, consulta [Conéctate a tu instancia de Linux](#) en la Guía del EC2 usuario de Amazon.
4. Abre un terminal en tu EC2 instancia de Amazon mediante Secure Shell (SSH) e inicia sesión con las credenciales correspondientes.
5. Crea un directorio en tu EC2 instancia de Amazon para usarlo como punto de montaje del volumen con el siguiente comando. En el siguiente ejemplo, *mount-point* sustitúyalo por tu propia información.

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

6. Monta tu sistema de archivos Amazon FSx for NetApp ONTAP en el directorio que has 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 FSx consola de Amazon, seleccione Storage virtual machines y, a continuación, elija la SVM en la que se encuentra el volumen que va a montar. El nombre del DNS del sistema de archivos de red (NFS) se encuentra en el panel Puntos de conexión.
 - *volume-junction-path*: la ruta de unión del volumen que está montando. Puedes encontrar la ruta de unión de un volumen en la FSx consola de Amazon, en el panel Resumen de la página de detalles del volumen.
 - *mount-point*— El nombre del directorio que creaste en tu EC2 instancia 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 tienes problemas con tu EC2 instancia de Amazon (por ejemplo, si se agota el tiempo de espera de las conexiones), consulta [Solución de problemas de EC2 instancias](#) en la Guía del EC2 usuario de Amazon.

Limpieza de recursos

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

Cómo limpiar los recursos

1. En la EC2 consola de Amazon, cierra tu instancia. Para obtener más información, consulte [Finalizar su instancia](#) en la Guía del EC2 usuario de Amazon.
2. Abre la FSx consola de Amazon en <https://console.aws.amazon.com/fsx/>.
3. En la FSx consola de Amazon, elimine todos los volúmenes FSx de ONTAP que no sean volúmenes raíz de su SVM. Para obtener más información, consulte [Eliminación de volúmenes](#).
4. Elimina todos los tuyo FSx para ONTAP. SVMs Para obtener más información, consulte [Eliminación de máquinas virtuales de almacenamiento \(SVM\)](#).
5. En la FSx consola de Amazon, elimina tu 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 de control cambia a 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). Mantén seleccionada la casilla de verificación de las copias IDs de seguridad que desees eliminar y, a continuación, selecciona Eliminar copias de seguridad.

Tu sistema de FSx archivos de Amazon y todas las copias de seguridad automáticas relacionadas se eliminarán ahora, junto con las copias de seguridad manuales que hayas decidido eliminar.

Disponibilidad por Región de AWS

Los sistemas de archivos Amazon FSx for NetApp ONTAP están disponibles de la siguiente manera en las Regiones de AWS, con el soporte de tipo de implementación indicado para cada región:

Región de AWS	Single-AZ 1	Multi-AZ 1	Single-AZ 2	Multi-AZ 2		
Este de EE. UU. (Norte de Virginia)	✓	✓	✓	✓		
Este de EE. UU. (Ohio)	✓	✓	✓	✓		
Oeste de EE. UU. (Norte de California)	✓	✓	✓	✓		
Oeste de EE. UU. (Oregón)	✓	✓	✓	✓		
AWS GovCloud (Este de EE. UU.)	✓	✓				
AWS GovCloud (Estados Unidos-Oeste)	✓	✓				

Región de AWS	Single-AZ 1	Multi-AZ 1	Single-AZ 2	Multi-AZ 2		
Africa (Cape Town)	✓	✓				
Asia Pacific (Hong Kong)	✓	✓				
Asia-Pacífico (Tokio)	✓	✓	✓	✓		
Asia-Pacífico (Seúl)	✓	✓				
Asia-Pacífico (Osaka)	✓	✓				
Asia-Pacífico (Bombay)	✓	✓	✓	✓		
Asia-Pacífico (Hyderabad)	✓	✓				
Asia-Pacífico (Singapur)	✓	✓	✓	✓		
Asia-Pacífico (Sídney)	✓	✓	✓	✓		

Región de AWS	Single-AZ 1	Multi-AZ 1	Single-AZ 2	Multi-AZ 2		
Asia-Pacífico (Yakarta)	✓	✓				
Asia-Pacífico (Melbourne)	✓	✓				
Asia-Pacífico (Malasia)	✓	✓				
Asia-Pacífico (Tailandia)	✓	✓				
Canadá (centro)	✓	✓				
Oeste de Canadá (Calgary)	✓	✓				
Europa (Fráncfort)	✓	✓	✓	✓		
Europa (Zúrich)	✓	✓				
Europa (Estocolmo)	✓	✓	✓	✓		
Europa (Milán)	✓	✓				

Región de AWS	Single-AZ 1	Multi-AZ 1	Single-AZ 2	Multi-AZ 2		
Europa (España)	✓	✓				
Europa (Irlanda)	✓	✓	✓	✓		
Europa (Londres)	✓	✓				
Europa (París)	✓	✓				
Israel (Tel Aviv)	✓	✓				
México (central)	✓	✓				
Medio Oriente (EAU)	✓	✓				
Medio Oriente (Baréin)	✓	✓				
América del Sur (São Paulo)	✓	✓				

Acceder a sus FSx datos de ONTAP

Puede acceder a sus sistemas de FSx archivos de Amazon 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 para gestionar 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 de interfaz de sistemas informáticos pequeños de Internet (iSCSI) para soporte de almacenamiento en bloques compartido.
- **Nvme—** Para conectarse mediante la memoria no volátil Express (NVMe) o el soporte de almacenamiento en TCP/IP bloque compartido.
- **Management—** Para administrar SVMs mediante la CLI o API de NetApp ONTAP, o BlueXP NetApp

Note

El protocolo iSCSI está disponible en todos los sistemas de archivos que tienen 6 o menos [pares de alta disponibilidad \(HA\)](#). El NVMe/TCP protocolo está disponible en los sistemas de archivos de segunda generación que tienen 6 pares HA o menos.

Temas

- [Clientes compatibles](#)
- [Uso de protocolos de almacenamiento en bloques](#)
- [Acceder a los datos desde el Nube de AWS](#)
- [Acceso a los datos en las instalaciones](#)
- [Configurar el enrutamiento para acceder a sistemas de archivos Multi-AZ desde fuera de la VPC](#)
- [Configurar el enrutamiento para acceder a sistemas de archivos Multi-AZ en las instalaciones](#)
- [Montaje de volúmenes en clientes Linux](#)

- [Montaje de volúmenes en clientes de Microsoft Windows](#)
- [Montaje de volúmenes en clientes de macOS](#)
- [Aprovisionamiento de iSCSI para Linux](#)
- [Aprovisionamiento de iSCSI para Windows](#)
- [Aprovisionamiento de NVMe /TCP para Linux](#)
- [Aprovisionamiento NVMe/TCP para Windows](#)
- [Acceso a los datos con otros servicios de AWS](#)

Clientes compatibles

FSx para los sistemas de archivos ONTAP, permite acceder a los 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 desconecta FSx 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.

Se admiten las siguientes AWS instancias informáticas para su uso con ONTAP FSx :

- Instancias de Amazon Elastic Compute Cloud (Amazon EC2) que ejecutan Linux con compatibilidad con NFS o SMB, Microsoft Windows y macOS. Para obtener más información, consulte [Montaje de volúmenes en clientes Linux](#), [Montaje de volúmenes en clientes de Microsoft Windows](#) y [Montaje de volúmenes en clientes de macOS](#).
- Contenedores Docker de Amazon Elastic Container Service (Amazon ECS) en instancias de EC2 Amazon Windows y Linux. Para obtener más información, consulte [Uso de Amazon Elastic Container Service con FSx ONTAP](#).
- Amazon Elastic Kubernetes Service: para obtener más información, consulte el controlador [CSI de Amazon NetApp for ONTAP en la Guía del usuario de FSx 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 ONTAP](#).
- Instancias de Amazon AppStream 2.0.
- AWS Lambda — Para obtener más información, consulta la entrada del AWS blog [Habilitar el acceso de pequeñas y medianas empresas para cargas de trabajo sin servidor con Amazon](#). FSx
- Máquinas virtuales (VMs) que se ejecutan en la nube en entornos VMware . AWS Para obtener más información, consulte la [guía de implementación de Amazon FSx para NetApp ONTAP como almacenamiento externo y VMware Cloud on AWS con Amazon FSx for NetApp ONTAP](#).

Una vez montados, FSx los sistemas de archivos de 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.

Uso de protocolos de almacenamiento en bloques

Amazon FSx for NetApp ONTAP admite la interfaz de sistemas informáticos pequeños de Internet (iSCSI) y la memoria no volátil Express NVMe () sobre TCP NVMe/TCP) block storage protocols. In Storage Area Network (SAN) environments, storage systems are targets that have storage target devices. For iSCSI, the storage target devices are referred to as logical units (LUNs). For NVMe/TCP (los dispositivos de destino de almacenamiento se denominan espacios de nombres).

Se utiliza la interfaz lógica iSCSI (LIF) de un SVM para conectarse tanto NVMe al almacenamiento en bloques iSCSI.

El almacenamiento se configura creando LUNs para iSCSI y creando espacios de nombres para. NVMe LUNs y, a continuación, los hosts acceden a los espacios de nombres mediante protocolos iSCSI o TCP.

Para obtener más información sobre la configuración de iSCSI y el almacenamiento en NVMe/TCP bloque, consulte:

- [Aprovisionamiento de iSCSI para Linux](#)

- [Aprovisionamiento de iSCSI para Windows](#)
- [Aprovisionamiento de NVMe /TCP para Linux](#)
- [Aprovisionamiento NVMe/TCP para Windows](#)

 Note

El aprovisionamiento NVMe/TCP para Windows requiere el uso de un iniciador de terceros NVMe .

Acceder a los datos desde el Nube de AWS

Cada sistema de FSx archivos de Amazon está asociado a una Virtual Private Cloud (VPC). Puede acceder al sistema de archivos FSx de 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 otro VPCs que esté en AWS cuentas diferentes o. Regiones de AWS Además de los requisitos descritos en las siguientes secciones FSx para acceder a los recursos de ONTAP, también debe asegurarse de que el grupo de seguridad de VPC del sistema de archivos esté configurado de manera 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](#).

Acceso a los datos desde la misma VPC

Al crear el sistema de archivos Amazon FSx for NetApp ONTAP, selecciona la Amazon VPC en la que se encuentra. Todos SVMs los volúmenes asociados al sistema de archivos Amazon FSx for NetApp 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.

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 FSx consola de Amazon, elija Sistemas de archivos y, a continuación, elija el sistema de archivos ONTAP cuyo volumen vaya 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 los puntos finales FSx de un sistema de archivos ONTAP desde AWS ubicaciones fuera de la VPC de implementación del sistema de archivos.

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

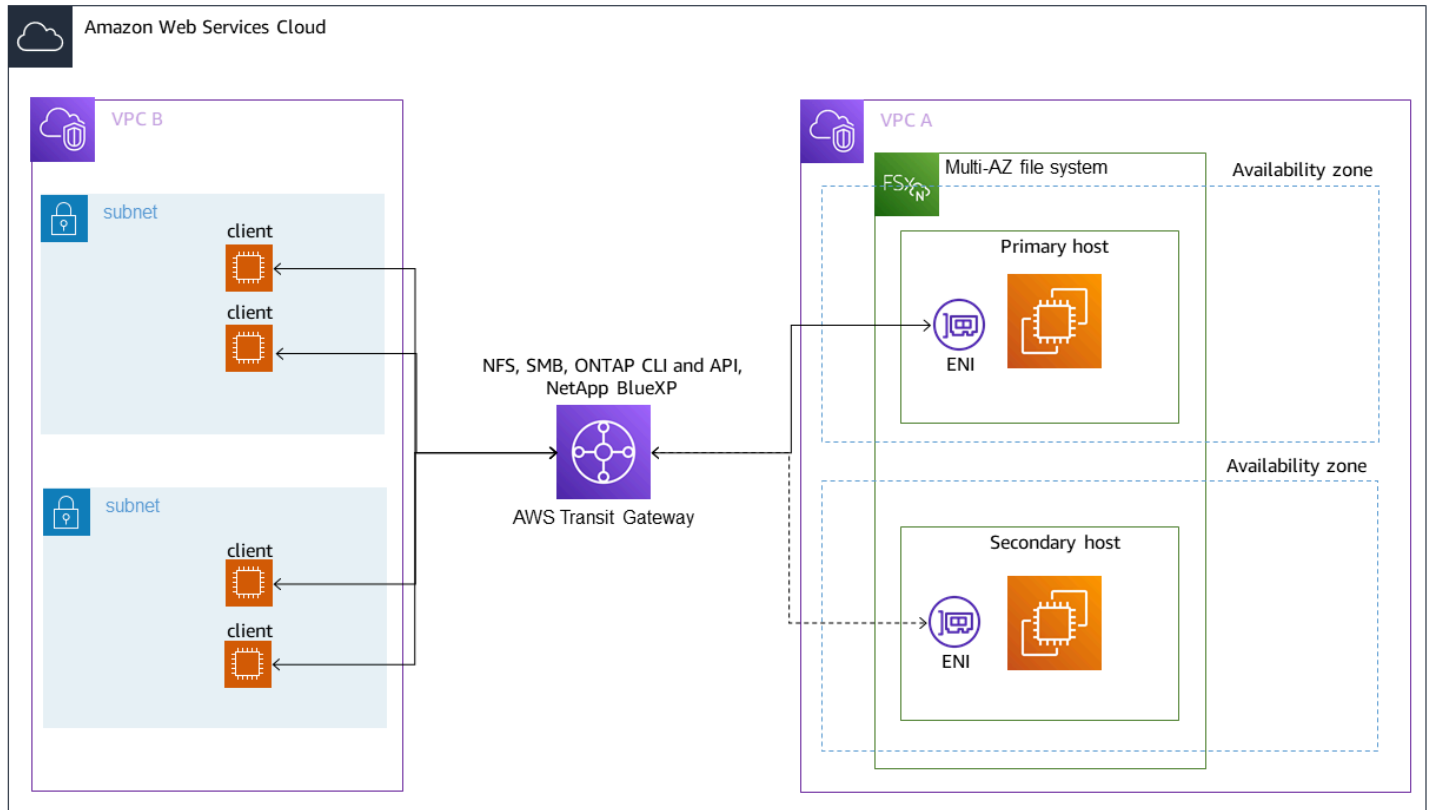
Los puntos finales de administración NFS, SMB y ONTAP de FSx Amazon NetApp para los sistemas de archivos Multi-AZ de ONTAP utilizan direcciones de protocolo de Internet (IP) flotantes para que los clientes conectados realicen una transición fluida entre el servidor de archivos preferido y el servidor 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 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:

- De forma predeterminada, los sistemas de archivos Multi-AZ creados con la FSx consola de Amazon utilizan las últimas 64 direcciones IP del rango CIDR principal de la VPC para el sistema de `EndpointIpAddressRange` archivos.
- Los sistemas de archivos Multi-AZ creados con la FSx API de Amazon AWS CLI o Amazon utilizan un rango de direcciones IP dentro del bloque de `198.19.0.0/16` direcciones de forma `EndpointIpAddressRange` predeterminada.
- También puedes especificar tu propio rango de direcciones IP cuando utilizas la opción de creación estándar. 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 y siempre que otro sistema de archivos no lo esté usando con la misma VPC y tablas de enrutamiento. Para esta opción, recomendamos usar un rango que esté dentro del rango de direcciones IP de la VPC.

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 [Actualizar sistemas de archivos](#).

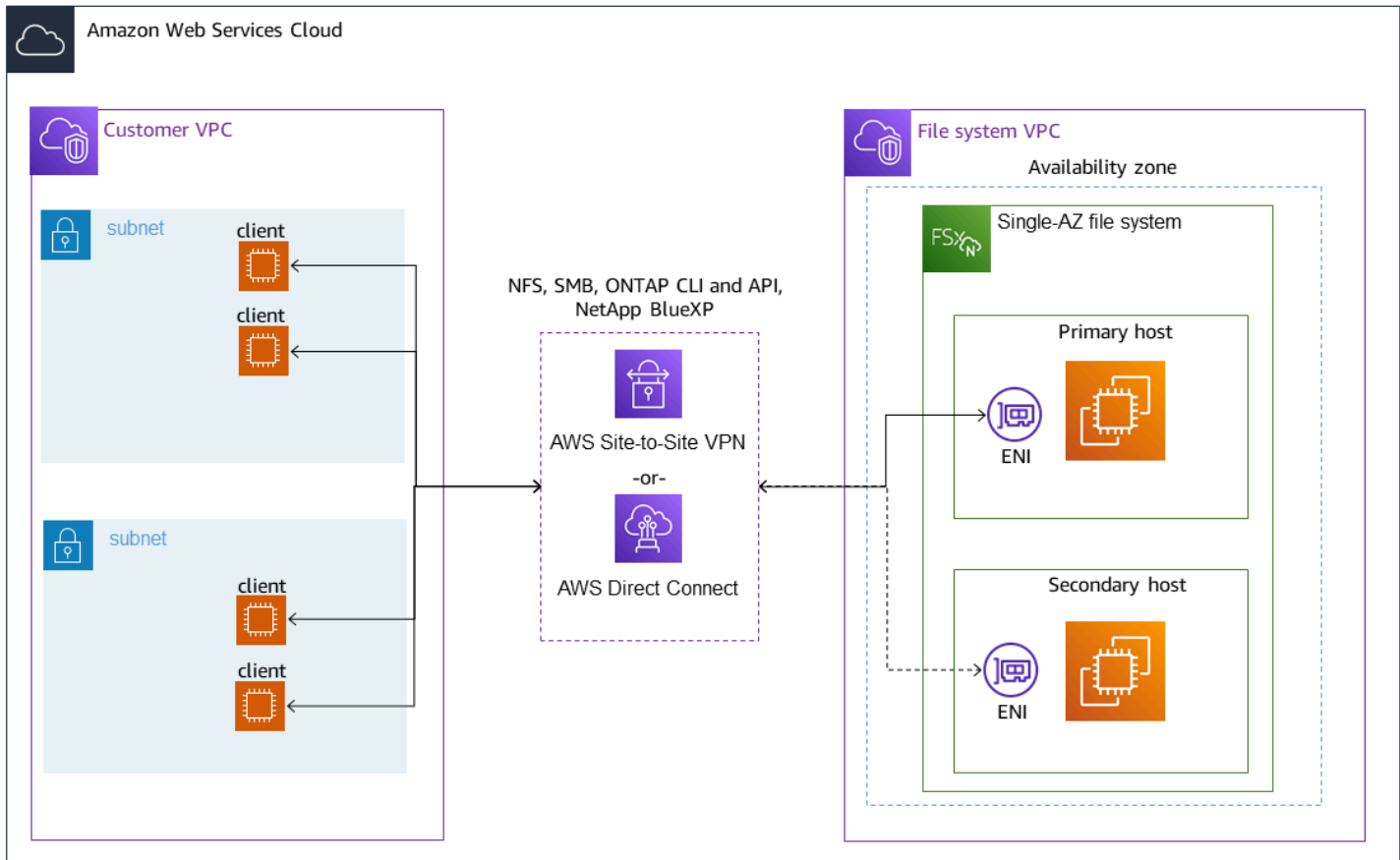
Para obtener información sobre cuándo debe utilizar Transit Gateway para acceder al sistema de archivos de ONTAP, consulte [¿Cuándo se requiere una puerta de enlace de tránsito?](#). FSx

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 se etiquetan con Key: AmazonFSx; Value: ManagedByAmazonFSx. Al crear o actualizar sistemas FSx de archivos Multi-AZ de ONTAP, le AWS CloudFormation recomendamos que añada la etiqueta manualmente. Key: AmazonFSx; Value: ManagedByAmazonFSx

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

Los puntos finales que se utilizan FSx para acceder a los sistemas de archivos Single-AZ de ONTAP a través de NFS o SMB, y para administrar los sistemas de archivos mediante la CLI o la API 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 través de NFS, SMB o la API REST, CLI o BlueXP de NetApp ONTAP	Solo si: • Accede desde una red emparejada (en las instalaciones, por ejemplo) y • No está accediendo a FSx través de una NetApp FlexCache instancia de Global File Cache o de Global File Cache
Acceso a los datos a través de iSCSI	No
Acceder a los datos mediante NVMe	No
Unión de una SVM a un Active Directory	No
SnapMirror	No
FlexCache Almacenamiento en caché	No
Caché de archivos global	No

Acceso a NVMe puntos finales iSCSI y entre clústeres fuera de la VPC de implementación

Puede usar el emparejamiento de VPC o AWS Transit Gateway para acceder a los puntos finales de su sistema de archivos, NVMe iSCSI y entre clústeres desde fuera de la VPC de implementación del sistema de archivos. Puede usar el emparejamiento de VPC para enrutar el tráfico NVMe iSCSI y entre clústeres. VPCs Una conexión de emparejamiento de VPC es una conexión de red entre dos VPCs y se utiliza para enrutar el tráfico entre ellas mediante direcciones privadas. IPv4 Puede utilizar el peering de VPC para conectarse VPCs 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 los sistemas de archivos de ONTAP desde las instalaciones locales utilizando [AWS VPN](#) o las [AWS Direct Connect](#) directrices FSx para casos de uso más específicos en las siguientes secciones. Además de los requisitos que se indican a continuación para acceder a diferentes FSx recursos de ONTAP desde 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 y la 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 los sistemas de archivos de ONTAP desde las redes locales FSx .

Acceso a sistemas de archivos Multi-AZ en las instalaciones

Amazon FSx requiere que utilices AWS Transit Gateway o configures una caché NetApp global de archivos remota o que accedas NetApp FlexCache a sistemas de archivos Multi-AZ desde una red local. Para admitir la conmutación por error entre zonas de disponibilidad para sistemas de archivos Multi-AZ, Amazon FSx utiliza direcciones IP flotantes para las interfaces utilizadas para los puntos de enlace de administración de NFS, SMB y ONTAP.

Dado que los puntos de enlace NFS, SMB y de administración utilizan direcciones IP flotantes, debe utilizarlas junto con estas interfaces AWS Direct Connect o AWS VPN para acceder a [AWS Transit Gateway](#) 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. `EndpointIpAddressRange` utiliza los siguientes rangos de direcciones, en función de cómo se cree el sistema de archivos:

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

- También puede especificar su propio rango de direcciones IP cuando usa la opción de creación estándar en la FSx consola de Amazon. 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 y siempre que no lo esté utilizando otro sistema de archivos con la misma VPC y tablas de enrutamiento. Para esta opción, recomendamos usar un rango que esté dentro del rango de direcciones IP de la VPC.

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 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.

Para obtener más información, consulte [Configurar el enrutamiento para acceder a sistemas de archivos Multi-AZ en las instalaciones](#).

Acceder a sistemas de archivos Single-AZ desde las instalaciones

Los sistemas de archivos AWS Transit Gateway Single-AZ no tienen el requisito de 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

FSx ya que los puntos finales entre clústeres de ONTAP están dedicados al tráfico de replicación entre los sistemas de archivos de NetApp ONTAP, incluidas las implementaciones locales, y en el caso de ONTAP. NetApp FSx El tráfico de replicación incluye SnapMirror y FlexClone las relaciones entre las máquinas virtuales de almacenamiento (SVMs) y los volúmenes de distintos sistemas de

archivos, y la caché de archivos global. FlexCache NetApp Los puntos de conexión entre clústeres también se utilizan para el tráfico de Active Directory.

Dado que los puntos de enlace 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 FSx para ONTAP, no es necesario que utilice una Transit Gateway para enrutar el tráfico entre clústeres entre el sistema local 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.

Para obtener más información, consulte [Configurar el enrutamiento para acceder a sistemas de archivos Multi-AZ en las instalaciones.](#)

Configurar el enrutamiento para acceder a sistemas de archivos Multi-AZ desde fuera de la VPC

Si tiene un sistema de archivos Multi-AZ con una dirección `EndpointIpAddressRange` que se encuentra fuera del rango de direcciones IP 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. Abre la FSx consola de Amazon en <https://console.aws.amazon.com/fsx/>.
2. Elija el FSx sistema de archivos de ONTAP para el que va a configurar el acceso desde una red interconectada.

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 al sistema de archivos FSx de ONTAP desde la red interconectada.

Para añadir la tabla de enrutamiento a su sistema de archivos, consulte [Actualizar sistemas 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.

Configurar el enrutamiento para acceder a sistemas de archivos Multi-AZ en las instalaciones

AWS Transit Gateway Para configurar el acceso a los sistemas de archivos Multi-AZ desde las instalaciones

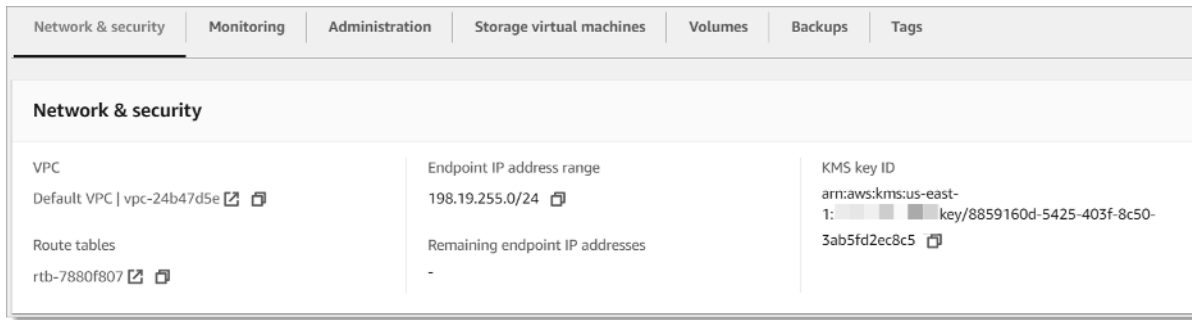
Si tienes un sistema de archivos Multi-AZ con un valor `EndpointIpAddressRange` que se encuentra fuera del rango de CIDR de tu VPC, debes configurar un enrutamiento adicional para acceder AWS Transit Gateway al sistema de archivos desde redes interconectadas o locales.

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. Abre la FSx consola de Amazon en <https://console.aws.amazon.com/fsx/>.

2. Elija el FSx sistema de archivos de ONTAP para el que va a configurar el acceso desde una red interconectada.
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 al sistema FSx de archivos de ONTAP desde la red interconectada.

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. Si tiene subredes de adjuntos de Transit Gateway independientes, también debe asociar las tablas de rutas de esas subredes a Amazon para FSx que se actualicen con las direcciones de los puntos de conexión de Amazon FSx .

Para agregar una tabla de enrutamiento a su sistema de archivos, consulte [Actualizar sistemas de archivos](#).

Montaje de volúmenes en clientes Linux

Recomendamos que los volúmenes que desea montar con clientes Linux tengan una configuración de estilo de seguridad de UNIX o mixed. Para obtener más información, consulte [Gestión de FSx volúmenes de ONTAP](#).

Note

De forma predeterminada, en el caso FSx de ONTAP, los montajes NFS son monturas. `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.

Cómo montar un volumen de ONTAP en un cliente Linux

1. Abre la EC2 consola de Amazon en <https://console.aws.amazon.com/ec2/>.
2. Cree o seleccione una EC2 instancia de Amazon 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 EC2 Linux, consulta el [paso 1: lanzar una instancia](#) en la Guía del EC2 usuario de Amazon.

3. Conéctate a tu instancia de Amazon EC2 Linux. Para obtener más información, consulta [Conéctate a tu instancia de Linux](#) en la Guía del EC2 usuario de Amazon.
4. Abre un terminal en tu EC2 instancia mediante un shell seguro (SSH) e inicia sesión con las credenciales adecuadas.
5. Cree un directorio en la EC2 instancia 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-01234567890abcdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /fsx
```

También puede utilizar la dirección IP del SVM en lugar de su nombre de DNS. Recomendamos usar el nombre del DNS para montar clientes en los sistemas de archivos de segunda generación, ya que ayuda a garantizar que los clientes estén equilibrados en 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 de segunda generación, el protocolo NFS paralelo (pNFS) está habilitado de forma predeterminada y se usa 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 su volumen FSx para ONTAP cuando se reinicie una instancia de Amazon EC2 Linux, 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

FSx para los sistemas de archivos ONTAP no admiten el montaje automático `/etc/fstab` en instancias de Amazon EC2 Mac.

Note

Antes de poder actualizar el `/etc/fstab` archivo de la EC2 instancia, asegúrese de que ya ha creado el sistema de archivos FSx para ONTAP. Para obtener más información, consulte [Creación de sistemas de archivos](#).

Para actualizar el archivo `/etc/fstab` de la instancia EC2

1. Conéctese a su EC2 instancia:

- 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, consulta los siguientes temas de la Guía del EC2 usuario de Amazon:

- [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 EC2 instancia ahora está configurada para montar el volumen ONTAP cada vez que se reinicie.

Montaje de volúmenes en clientes de Microsoft Windows

En esta sección se describe cómo acceder a los datos del sistema FSx de archivos de 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 FSx de máquinas virtuales de almacenamiento ONTAP](#). Para obtener más información sobre el uso de grupos de trabajo, consulte. [Configuración de un servidor SMB en un grupo de trabajo](#)
- El volumen que va a adjuntar tiene una configuración de estilo de seguridad de NTFS o mixed. Para obtener más información, consulte [Estilo de seguridad del volumen](#).

Para montar un volumen en un cliente de Windows mediante SMB y Active Directory

1. Abre la EC2 consola de Amazon en <https://console.aws.amazon.com/ec2/>.
2. Cree o seleccione una EC2 instancia de Amazon 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, consulta el [paso 1: lanzar una instancia](#) en la Guía del EC2 usuario de Amazon.

Para obtener más información sobre unir una SVM a un Active Directory, consulte [Administración FSx de máquinas virtuales de almacenamiento ONTAP](#).

3. Conéctese a su instancia de Amazon EC2 Windows. Para obtener más información, consulta Cómo [conectarse a tu instancia de Windows](#) en la Guía del EC2 usuario de Amazon.
4. Abra un símbolo del sistema.
5. Ejecute el siguiente comando. 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.
- Reemplace SHARE_NAME con el nombre de un recurso compartido SMB. 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 del DNS para montar clientes en los sistemas de archivos de segunda generación, ya que ayuda a garantizar que los clientes estén equilibrados en los pares de alta disponibilidad (HA) del sistema de archivos.

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

Montaje de volúmenes en clientes de macOS

En esta sección se describe cómo acceder a los datos del sistema FSx de archivos de 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. Abre la EC2 consola de Amazon en <https://console.aws.amazon.com/ec2/>.
2. Crea o selecciona 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, consulta el [paso 1: lanzar una instancia](#) en la Guía del EC2 usuario de Amazon.

3. Conéctate a tu instancia de Amazon EC2 Mac. Para obtener más información, consulta [Conéctate a tu instancia de Linux](#) en la Guía del EC2 usuario de Amazon.
4. Abre un terminal en tu EC2 instancia mediante un shell seguro (SSH) e inicia sesión con las credenciales adecuadas.
5. Cree un directorio en la EC2 instancia 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 del DNS para montar clientes en los sistemas de archivos de segunda generación, ya que ayuda a garantizar que los clientes estén equilibrados en 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](#).

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

1. Abra la EC2 consola de Amazon en <https://console.aws.amazon.com/ec2/>.
2. Cree o seleccione una EC2 instancia de Amazon 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 EC2 Linux, consulta el [paso 1: lanzar una instancia](#) en la Guía del EC2 usuario de Amazon.

3. Conéctate a tu instancia de Amazon EC2 Linux. Para obtener más información, consulta [Conéctate a tu instancia de Linux](#) en la Guía del EC2 usuario de Amazon.
4. FSx Para montar el volumen de ONTAP en la EC2 instancia de Linux, utilice un script de datos de usuario durante el lanzamiento de la instancia o ejecute 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-01234567890abcdef0.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. Recomendamos usar el nombre del DNS para montar clientes en los sistemas de archivos de segunda generación, ya que ayuda a garantizar que los clientes estén equilibrados en los pares de (HA) 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-01234567890abcdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /fsx
```

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

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

Aprovisionamiento de iSCSI para Linux

FSx para ONTAP es compatible con el protocolo iSCSI. Debe aprovisionar iSCSI tanto en el cliente Linux como en el sistema de archivos para poder usar el protocolo iSCSI para transportar datos entre los clientes y el sistema de archivos. El protocolo iSCSI está disponible en todos los sistemas de archivos que tienen 6 o menos [pares de alta disponibilidad \(HA\)](#).

El proceso de configuración de iSCSI en Amazon FSx for NetApp ONTAP consta de tres pasos principales, que se describen en los siguientes procedimientos:

1. Instale y configure el cliente iSCSI en el host de Linux.
2. Configure iSCSI en la SVM del sistema de archivos.
 - Cree un grupo de iniciadores iSCSI.
 - Asigne el grupo de iniciadores al LUN.
3. Monte un LUN iSCSI en el cliente Linux.

Antes de empezar

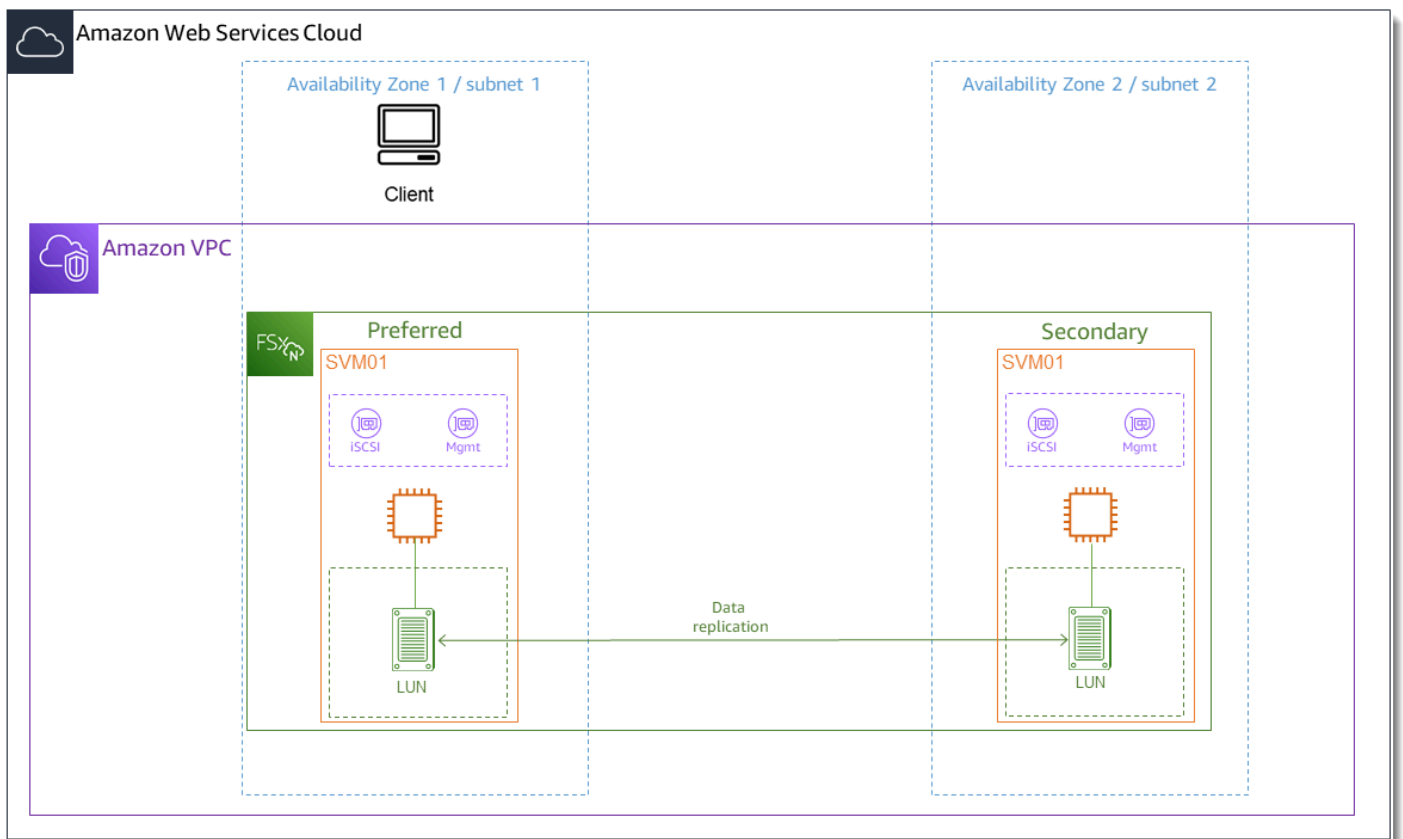
Antes de iniciar el proceso de configuración del sistema de archivos para iSCSI, debe completar los siguientes elementos.

- Cree un sistema de archivos FSx para ONTAP. Para obtener más información, consulte [Creación de sistemas de archivos](#).
- Cree un LUN iSCSI en el sistema de archivos. Para obtener más información, consulte [Creación de un iSCSI LUN](#).

- Cree una EC2 instancia que ejecute la Amazon Machine Image (AMI) de Amazon Linux 2 en la misma VPC que el sistema de archivos. Este es el host de Linux en el que configurará iSCSI y accederá a los datos de sus archivos.

Más allá del alcance de estos procedimientos, si el host está ubicado en otra VPC, puede utilizar la interconexión de VPC o conceder otro VPCs acceso AWS Transit Gateway a los puntos finales iSCSI del volumen. Para obtener más información, consulte [Acceso a los datos desde fuera de la VPC de implementación](#).

- Configure los grupos de seguridad de VPC del host Linux para permitir el tráfico entrante y saliente, como se describe en [Control de acceso al sistema de archivos con Amazon VPC](#).
- Obtenga las credenciales de ONTAP usuario con `fsxadmin` privilegios que utilizará para acceder al ONTAP CLI. Para obtener más información, consulte [Usuarios y roles de ONTAP](#).
- El host Linux que configurará para iSCSI y que utilizará FSx para acceder al sistema de archivos de ONTAP se encuentra en la misma VPC y. Cuenta de AWS
- Recomendamos que la EC2 instancia esté en la misma zona de disponibilidad que la subred preferida del sistema de archivos, como se muestra en el siguiente gráfico.



Si su EC2 instancia ejecuta una AML de Linux diferente a la de Amazon Linux 2, es posible que algunas de las utilidades utilizadas en estos procedimientos y ejemplos ya estén instaladas y que utilice comandos diferentes para instalar los paquetes necesarios. Además de instalar paquetes, los comandos que se utilizan en esta sección son válidos para otros EC2 Linux AMIs.

Temas

- [Instalar y configurar iSCSI en el host Linux](#)
- [Configuración de iSCSI en el sistema de archivos FSx ONTAP](#)
- [Monte un LUN iSCSI en su cliente Linux](#)

Instalar y configurar iSCSI en el host Linux

Cómo 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
```

Cómo 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 FSx ONTAP

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

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

2. Cree el grupo de iniciadores (igroup) mediante el comando NetApp [lun igroup create](#) CLI de ONTAP. Un grupo de iniciadores se asigna a LUNs iSCSI y controla a qué iniciadores (clientes) tienen acceso. 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 asignado a este igroup esté disponible 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 Current Is	Status	Network	Current

Vserver	Interface Port Home	Admin/Oper	Address/Mask	Node

<i>svm_name</i>				
	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

El proceso de montaje del LUN iSCSI en el cliente Linux consta de tres pasos:

1. Descubrimiento de los nodos iSCSI de destino
2. Partición del LUN iSCSI
3. Montaje del LUN iSCSI en el cliente

Analizamos los pasos en los siguientes procedimientos.

Descubrir los nodos iSCSI de destino

1. En su cliente Linux, utilice el siguiente comando para descubrir los nodos iSCSI de destino mediante `iscsi_1` la dirección IP. *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) Para lograr un rendimiento superior al del máximo de 5 Gbps (~625 MBps) para el LUN iSCSI para un cliente EC2 único de Amazon, siga los procedimientos descritos en [Ancho de banda de EC2 red de instancias de Amazon en la Guía del usuario de Amazon Elastic Compute Cloud](#) para instancias de Linux a fin de establecer sesiones adicionales para aumentar el rendimiento.

El siguiente comando establece 8 sesiones por iniciador por nodo ONTAP en cada zona de disponibilidad, lo que permite al cliente impulsar hasta 40 Gbps (5000 MBps) 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 iSCSI LUNs 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.

Cómo 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 FSx 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 NetApp ONTAP.
 - 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\t\talias "${ALIAS}"'\n\t\t}\n' $CONF
else
    printf "multipaths {\n\tmultipath {\n\t\t\twwid 3600a0980$SN\n\t\t\t\talias\n\t\t\t\t$ALIAS\n\t\t\t}\n}" >> $CONF
fi

```

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

```

~$ systemctl restart multipathd.service

```

Cómo 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. Puede crear varias particiones utilizando un valor menor que el último sector (20971519 en este ejemplo).

 Note

El valor `Last sector` variará según el tamaño del LUN iSCSI (10 GB en este ejemplo).

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

Se inicia el mensaje interactivo `fdisk`.

```
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. *partition_name* Tiene el formato. `<device_name> <partition_number>` 1 se usó como el número de partición utilizado en el `fdisk` comando del 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
```

Cómo 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) Si desea asignar a un usuario específico la propiedad del directorio de montaje, reemplace *username* con el nombre de usuario del propietario.

```
~$ 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.

Aprovisionamiento de iSCSI para Windows

FSx para ONTAP es compatible con el protocolo iSCSI. Debe aprovisionar iSCSI tanto en el cliente Windows como en la SVM y el volumen para usar el protocolo iSCSI para transportar datos entre los clientes y el sistema de archivos. El protocolo iSCSI está disponible en todos los sistemas de archivos que tienen 6 o menos [pares de alta disponibilidad \(HA\)](#).

Los ejemplos que se presentan en estos procedimientos muestran cómo aprovisionar el protocolo iSCSI en el cliente y FSx para el sistema de archivos ONTAP, y cómo utilizar la siguiente configuración:

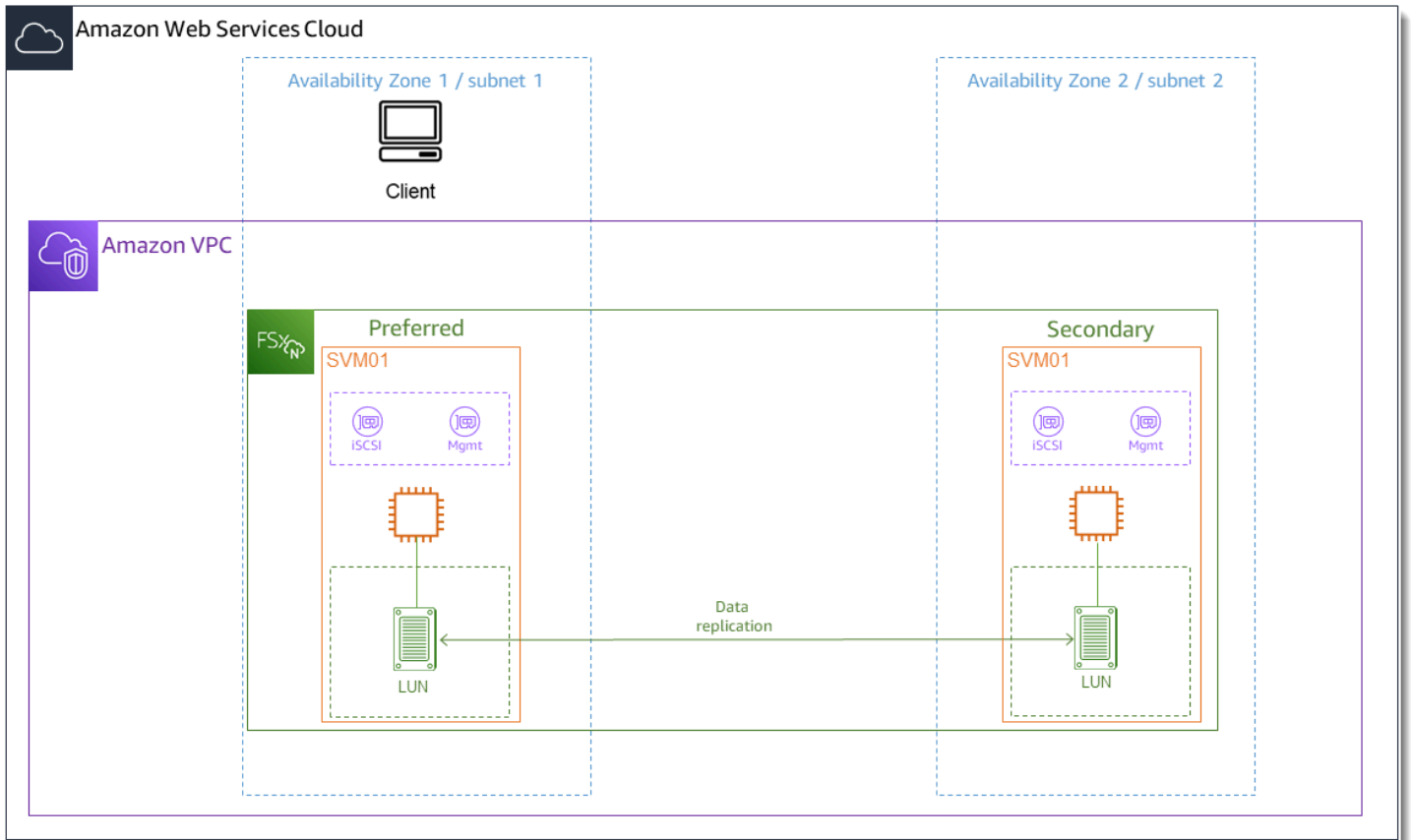
- El LUN iSCSI que se va a montar en un host de Windows ya está creado. Para obtener más información, consulte [Creación de un iSCSI LUN](#).
- El host de Microsoft Windows que monta el LUN iSCSI es una EC2 instancia de Amazon que ejecuta una Amazon Machine Image (AMI) de Microsoft Windows Server 2019. 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 la interconexión de VPC o conceder otro acceso AWS

Transit Gateway VPCs a los puntos finales iSCSI. Para obtener más información, consulte [Acceso a los datos desde fuera de la VPC de implementación](#).

Recomendamos que la EC2 instancia 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 FSx ONTAP](#)
- [Montar un LUN iSCSI en el cliente de Windows](#)
- [Validación de la configuración iSCSI](#)

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 de ONTAP mediante la CLI de NetApp ONTAP. FSx

```
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-I/O (MPIO) en su instancia de Windows. Utilice el siguiente comando :

```
PS C:\> Install-WindowsFeature Multipath-I0
```

5. Reinicia la instancia de Windows una vez finalizada la instalación de Multipath-I0. 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 FSx ONTAP

1. Para acceder al ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando. 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 [Administrar sistemas de archivos con el ONTAP CLI](#).

2. Uso de ONTAP CLI [lun igroup create](#), cree el grupo de iniciadores oigroup. Un grupo de iniciadores se asigna a LUNs iSCSI y controla a qué iniciadores (clientes) tienen acceso. 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
```

Para hacer que el LUNs mapeado a esto igroup esté disponible para varios hosts, puede especificar varios nombres de iniciadores separados por comas mediante [lun igroup create](#) ONTAP Comando CLI.

3. Confirme que igroup se creó correctamente mediante el [lun igroup show](#) ONTAP Comando de la CLI:

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

El sistema responde con lo siguiente:

Vserver	Igroup	Protocol	OS Type	Initiators
<i>svm_name</i>	<i>igroup_name</i>	iscsi	windows	iqn.1994-05.com.windows:abcdef12345

Una vez igroup creados, estará listo para crearlos 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
-----	-----	-----	-----	-----	-----
<i>svm_name</i>	/vol/ <i>vol_name</i> / <i>lun_name</i>	online	mapped	windows	10GB

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

- 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
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
-----	-----	-----	-----	-----	-----	-----
<i>svm_name</i>	<code>iscsi_1</code>	up/up	172.31.0.143/20	FSxId0123456789abcdef8-01	e0e	true
	<code>iscsi_2</code>	up/up	172.31.21.81/20	FSxId0123456789abcdef8-02	e0e	true
	<code>nfs_smb_management_1</code>	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

- En su instancia de Windows, abra un PowerShell terminal como administrador.
- Crearé 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 Gbps (5000 MBps) de rendimiento total al LUN iSCSI. Al disponer de 8 sesiones, se garantiza que un solo cliente pueda impulsar la capacidad total de 4000 para obtener el nivel más MBps alto de capacidad de rendimiento de ONTAP. FSx Si lo desea, puede cambiar el número de sesiones a un número de sesiones superior o inferior (cada sesión proporciona un rendimiento

MBps de hasta 625) modificando la variable. RecommendedConnectionCount Para obtener más información, consulte el ancho de [banda de la red de EC2 instancias](#) de Amazon 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 .ps1.

- 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.

```
Write-Host "Starting iSCSI connection setup..."
$TargetPortalAddresses = @("iscsi_1","iscsi_2"); $LocaliSCSIAddress = "ec2_ip"
$RecommendedConnectionCount = 8

Foreach ($TargetPortalAddress in $TargetPortalAddresses) {
    New-IscsiTargetPortal -TargetPortalAddress $TargetPortalAddress -
TargetPortalPortNumber 3260 -InitiatorPortalAddress $LocaliSCSIAddress
}

New-MSDSMSupportedHW -VendorId MSFT2005 -ProductId iSCSIBusType_0x9

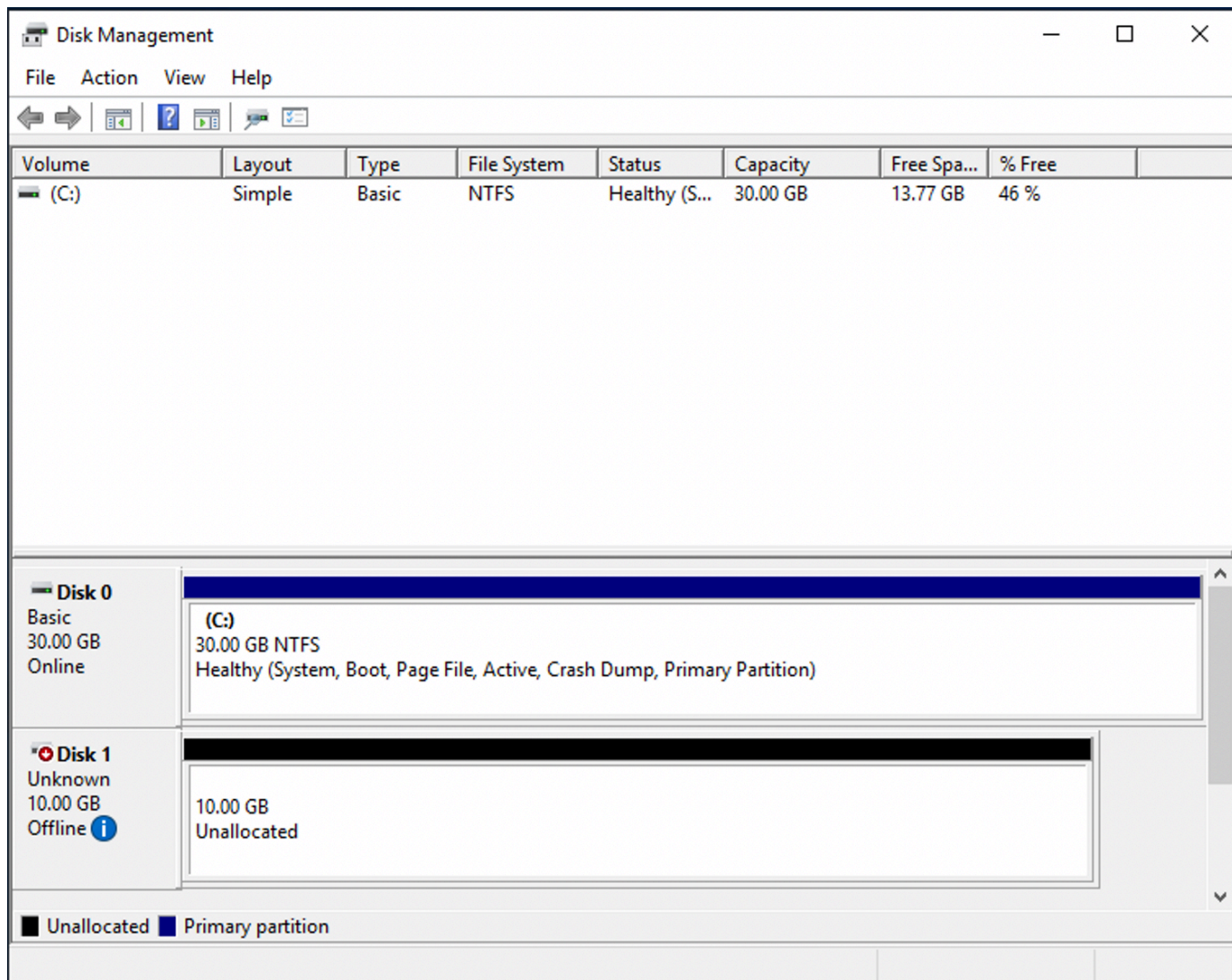
$currentMPIOSettings = Get-MPIOSetting
if ($currentMPIOSettings.PathVerificationState -ne 'Enabled') {
    Write-Host "Setting MPIO path verification state to Enabled"; Set-
MPIOSetting -NewPathVerificationState Enabled
} else { Write-Host "MPIO path verification state already Enabled" }

$portalConnectionCounts = @{}
foreach ($TargetPortalAddress in $TargetPortalAddresses)
{ $portalConnectionCounts[$TargetPortalAddress] = 0 }

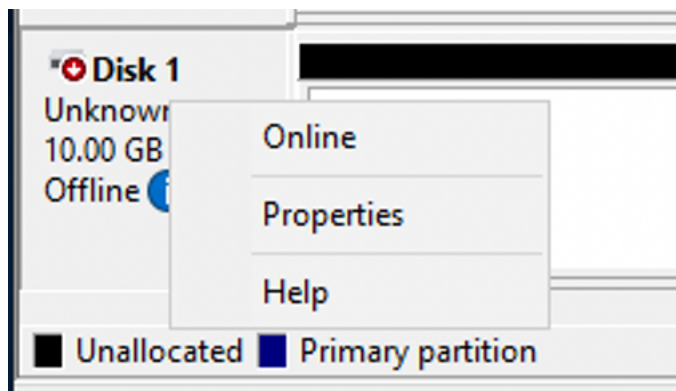
$sessions = Get-IscsiSession
if ($sessions) {
    foreach ($session in $sessions) {
        if ($session.IsConnected) {
            $targetPortal = (Get-IscsiTargetPortal -iSCSISession
$session).TargetPortalAddress
            if ($portalConnectionCounts.ContainsKey($targetPortal))
{ $portalConnectionCounts[$targetPortal]++ }
        }
    }
}
```

```
foreach ($TargetPortalAddress in $TargetPortalAddresses) {  
    $existingCount = $portalConnectionCounts[$TargetPortalAddress];  
    $remainingConnections = $RecommendedConnectionCount - $existingCount  
    Write-Host "Portal $TargetPortalAddress has $existingCount  
existing connections, $remainingConnections remaining (max recommended:  
$RecommendedConnectionCount)"  
    if ($remainingConnections -gt 0) {  
        Write-Host "Creating $remainingConnections connections for portal  
$TargetPortalAddress"  
        1..$remainingConnections | ForEach-Object {  
            Get-IscsiTarget | Connect-IscsiTarget -IsMultipathEnabled $true -  
TargetPortalAddress $TargetPortalAddress -InitiatorPortalAddress $LocaliSCSIAddress  
-IsPersistent $true  
        }  
    } else { Write-Host "Maximum connections (8) reached for portal  
$TargetPortalAddress" }  
}  
  
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.

Validación de la configuración iSCSI

Hemos incluido un script para comprobar que la configuración de iSCSI está correctamente configurada. El script examina parámetros, como el recuento de sesiones, la distribución de nodos y el estado de las E/S de varias rutas (MPIO). En la tarea siguiente, se explica cómo instalar y usar el script.

Cómo validar la configuración iSCSI

1. Abra una PowerShell ventana de Windows.
2. Descargue el script mediante el siguiente comando.

```
PS C:\> Invoke-WebRequest "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/samples/CheckiSCSI.zip" -OutFile "CheckiSCSI.zip"
```

3. Descomprima el archivo zip con el siguiente comando.

```
PS C:\> Expand-Archive -Path ".\CheckiSCSI.zip" -DestinationPath "./"
```

4. Ejecute el script mediante el siguiente comando.

```
PS C:\> ./CheckiSCSI.ps1
```

5. Revise el resultado para comprender el estado actual de la configuración. En el ejemplo siguiente, se muestra una configuración iSCSI correcta.

```
PS C:\> ./CheckiSCSI.ps1
```

```
This script checks the iSCSI configuration on the local instance.  
It will provide information about the number of connected sessions, connected file  
servers, and MPIO status.
```

```
MPIO is installed on this server.
```

```
MPIO Load Balance Policy is set to Round Robin (RR).  
Initiator: 'iqn.1991-05.com.microsoft:ec2amaz-d2cebnb'  
to Target: 'iqn.1992-08.com.netapp:sn.13266b10e61411ee8bc0c76ad263d613:vs.3'  
has 16 total sessions (16 active, 0 non-active)  
spread across 2 node(s).  
MPIO: Yes
```

Aprovisionamiento de NVMe /TCP para Linux

FSx para ONTAP es compatible con la memoria no volátil Express sobre TCP (NVMe/TCP) block storage protocol. With NVMe/TCP, se utiliza el ONTAP CLI para aprovisionar espacios de nombres y subsistemas y, a continuación, asignar los espacios de nombres a los subsistemas, de forma similar a como LUNs se aprovisionan y asignan a los grupos de iniciadores (iGroups) para iSCSI. [El protocolo NVMe /TCP está disponible en los sistemas de archivos de segunda generación que tienen 6 pares de alta disponibilidad \(HA\) o menos.](#)

Note

FSx para los sistemas de archivos ONTAP, utilice los puntos finales iSCSI de un SVM para los protocolos de almacenamiento en bloques NVMe iSCSI y /TCP.

El proceso de configuración de NVMe /TCP en Amazon FSx para NetApp ONTAP consta de tres pasos principales, que se describen en los siguientes procedimientos:

1. Instale y configure el NVMe cliente en el host Linux.
2. Configure NVMe en la SVM del sistema de archivos.

- Crea un NVMe espacio de nombres.
- Crea un subsistema NVMe .
- Asigne el espacio de nombres al subsistema.
- Agregue el nombre no calificado (NQN) del cliente al subsistema.

3. Monte un NVMe dispositivo en el cliente Linux.

Antes de empezar

Antes de comenzar el proceso de configuración del sistema de archivos para NVMe /TCP, debe completar los siguientes elementos.

- Cree un sistema de archivos FSx para ONTAP. Para obtener más información, consulte [Creación de sistemas de archivos](#).
- Cree una EC2 instancia que ejecute Red Hat Enterprise Linux (RHEL) 9.3 en la misma VPC que el sistema de archivos. Este es el host de Linux en el que configurará los datos de sus archivos NVMe y accederá a ellos mediante NVMe /TCP para Linux.

Más allá del alcance de estos procedimientos, si el host está ubicado en otra VPC, puede utilizar la interconexión de VPC o conceder otro VPCs acceso AWS Transit Gateway a los puntos finales iSCSI del volumen. Para obtener más información, consulte [Acceso a los datos desde fuera de la VPC de implementación](#).

- Configure los grupos de seguridad de VPC del host Linux para permitir el tráfico entrante y saliente, como se describe en [Control de acceso al sistema de archivos con Amazon VPC](#).
- Obtenga las credenciales de ONTAP usuario con `fsxadmin` privilegios que utilizará para acceder al ONTAP CLI. Para obtener más información, consulte [Usuarios y roles de ONTAP](#).
- El host Linux que configurará NVMe y utilizará para acceder al FSx sistema de archivos de ONTAP se encuentra en la misma Cuenta de AWS VPC y.
- Le recomendamos que la EC2 instancia esté en la misma zona de disponibilidad que la subred preferida de su sistema de archivos.

Si su EC2 instancia ejecuta una AMI de Linux diferente a la de RHEL 9.3, es posible que algunas de las utilidades utilizadas en estos procedimientos y ejemplos ya estén instaladas y que utilice comandos diferentes para instalar los paquetes necesarios. Además de instalar paquetes, los comandos que se utilizan en esta sección son válidos para otros EC2 sistemas Linux. AMIs

Temas

- [Instale y configure NVMe en el host Linux](#)
- [NVMe Configúrelo en el FSx sistema de archivos ONTAP](#)
- [Monte un NVMe dispositivo en su cliente Linux](#)

Instale y configure NVMe en el host Linux

Para instalar el NVMe cliente

1. Conexión a la instancia de Linux mediante un cliente SSH. Para obtener más información, consulte [Conéctese a la instancia de Linux desde Linux o macOS mediante SSH](#).
2. Instale `nvme-cli` con el siguiente comando:

```
~$ sudo yum install -y nvme-cli
```

3. Cargue el módulo `nvme-tcp` en el host:

```
$ sudo modprobe nvme-tcp
```

4. Obtenga el nombre NVMe cualificado (NQN) del host Linux mediante el siguiente comando:

```
$ cat /etc/nvme/hostnqn  
nqn.2014-08.org.nvmexpress:uuid:9ed5b327-b9fc-4cf5-97b3-1b5d986345d1
```

Registre la respuesta para su uso en un paso posterior.

NVMe Configúrelo en el FSx sistema de archivos ONTAP

Para configurar NVMe en el sistema de archivos

Conéctese a la NetApp CLI de ONTAP en el FSx sistema de archivos de ONTAP en el que planea crear los NVMe dispositivos.

1. Para acceder al ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando. 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 [Administrar sistemas de archivos con el ONTAP CLI](#).

2. Cree un volumen nuevo en el SVM que está utilizando para acceder a la interfaz. NVMe

```
::> vol create -vserver fsx -volume nvme_vol1 -aggregate aggr1 -size 1t
[Job 597] Job succeeded: Successful
```

3. Cree el espacio de NVMe nombres ns_1 mediante el comando CLI de [vserver nvme namespace create](#) NetApp ONTAP. Un espacio de nombres se asigna a los iniciadores (clientes) y controla qué iniciadores (clientes) tienen acceso a los dispositivos. NVMe

```
::> vserver nvme namespace create -vserver fsx -path /vol/nvme_vol1/ns_1 -size 100g
-ostype linux
Created a namespace of size 100GB (107374182400).
```

4. Cree el NVMe subsistema mediante el comando [vserver nvme subsystem create](#) NetApp CLI de ONTAP.

```
~$ vserver nvme subsystem create -vserver fsx -subsystem sub_1 -ostype linux
```

5. Asigne el espacio de nombres al subsistema que acaba de crear.

```
::> vserver nvme subsystem map add -vserver fsx -subsystem sub_1 -path /vol/
nvme_vol1/ns_1
```

6. Agregue el cliente al subsistema mediante el NQN que recuperó anteriormente.

```
::> vserver nvme subsystem host add -subsystem sub_1 -host-nqn
nqn.2014-08.org.nvmexpress:uuid:ec21b083-1860-d690-1f29-44528e4f4e0e -vserver fsx
```

Si desea que los dispositivos asignados a este subsistema estén disponibles para varios hosts, puede especificar varios nombres de iniciadores en una lista separados por comas. Para obtener más información, consulte [vserver nvme subsystem host add](#) en los documentos de ONTAP. NetApp

7. Confirme que el espacio de nombres existe con el comando [vserver nvme namespace show](#):

```
::> vserver nvme namespace show -vserver fsx -instance
```



```

Vserver Name: fsx
    Namespace Path: /vol/nvme_vol1/ns_1
        Size: 100GB
        Size Used: 90.59GB
        OS Type: linux
        Comment:
        Block Size: 4KB
        State: online
    Space Reservation: false
Space Reservations Honored: false
    Is Read Only: false
    Creation Time: 5/20/2024 17:03:08
    Namespace UUID: c51793c0-8840-4a77-903a-c869186e74e3
    Vdisk ID: 80d42c6f00000000187cca9
    Restore Inaccessible: false
    Inconsistent Filesystem: false
    Inconsistent Blocks: false
    NVFail: false
Node Hosting the Namespace: FsxId062e9bb6e05143fcb-01
    Volume Name: nvme_vol1
    Qtree Name:
    Mapped Subsystem: sub_1
    Subsystem UUID: db526ec7-16ca-11ef-a612-d320bd5b74a9
    Namespace ID: 00000001h
    ANA Group ID: 00000001h
    Vserver UUID: 656d410a-1460-11ef-a612-d320bd5b74a9
    Vserver ID: 3
    Volume MSID: 2161388655
    Volume DSID: 1029
    Aggregate: aggr1
    Aggregate UUID: cfa8e6ee-145f-11ef-a612-d320bd5b74a9
Namespace Container State: online
    Autodelete Enabled: false
    Application UUID: -
    Application: -
    Has Metadata Provisioned: true

```

1 entries were displayed.

8. Utilice el [network interface show -vserver](#) comando para recuperar las direcciones de las interfaces de almacenamiento en bloque de la SVM en la que ha creado sus dispositivos. NVMe

```

::> network interface show -vserver svm_name -data-protocol nvme-tcp

```

Vserver	Logical		Status	Network	Current
	Current Is	Interface			
	Port	Home	Admin/Oper	Address/Mask	Node

<i>svm_name</i>					
		iscsi_1	up/up	172.31.16.19/20	
FSxId0123456789abcdef8-01	e0e		true		
		iscsi_2	up/up	172.31.26.134/20	
FSxId0123456789abcdef8-02	e0e		true		
2 entries were displayed.					

Note

El `iscsi_1` LIF se utiliza tanto para NVMe iSCSI como para /TCP.

En este ejemplo, la dirección IP de `iscsi_1` es 172.31.16.19 y `iscsi_2` es 172.31.26.134.

Monte un NVMe dispositivo en su cliente Linux

El proceso de montaje del NVMe dispositivo en su cliente Linux consta de tres pasos:

1. Descubriendo los NVMe nodos
2. Particionar el dispositivo NVMe
3. Montaje del NVMe dispositivo en el cliente

Analizamos los pasos en los siguientes procedimientos.

Para descubrir los NVMe nodos de destino

1. En su cliente Linux, utilice el siguiente comando para descubrir los NVMe nodos de destino. Reemplace *iscsi_1_IP* por la dirección IP de `iscsi_1` y *client_IP* la dirección IP del cliente.

Note

`iscsi_1y iscsi_2` LIFs se utilizan tanto para iSCSI como para almacenamiento. NVMe

```
~$ sudo nvme discover -t tcp -w client_IP -a iscsi_1_IP
```

```
Discovery Log Number of Records 4, Generation counter 11
=====Discovery Log Entry 0=====
trtype: tcp
adrfam: ipv4
subtype: current discovery subsystem
treid: not specified
portid: 0
trsvcid: 8009
subnqn: nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:discovery
traddr: 172.31.26.134
eflags: explicit discovery connections, duplicate discovery information
sectype: none
=====Discovery Log Entry 1=====
trtype: tcp
adrfam: ipv4
subtype: current discovery subsystem
treid: not specified
portid: 1
trsvcid: 8009
subnqn: nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:discovery
traddr: 172.31.16.19
eflags: explicit discovery connections, duplicate discovery information
sectype: none
```

2. (Opcional) Para lograr un rendimiento superior al del cliente EC2 único de Amazon, máximo de 5 Gbps (~625 MBps) para su NVMe dispositivo de archivos, siga los procedimientos descritos en el [ancho de banda de la red de EC2 instancias de Amazon](#) en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux para establecer sesiones adicionales.
3. Inicie sesión en los iniciadores de destino con un tiempo de espera de pérdida del controlador de al menos 1800 segundos. De nuevo, use la dirección IP de `iscsi_1` para *iscsi_1_IP* y

la dirección IP del cliente para *client_IP*. NVMe Los dispositivos se presentan como discos disponibles.

```
~$ sudo nvme connect-all -t tcp -w client_IP -a iscsi_1 -l 1800
```

- Utilice el siguiente comando para comprobar que la NVMe pila ha identificado y fusionado las múltiples sesiones y ha configurado las múltiples rutas. Si la configuración fue correcta, el comando devuelve Y.

```
~$ cat /sys/module/nvme_core/parameters/multipath
Y
```

- Utilice los siguientes comandos para comprobar que la configuración NVMe -oF model esté establecida en NetApp ONTAP Controller y que el equilibrio de carga iopolicy esté establecido en la configuración correspondiente round-robin ONTAP espacios de nombres para distribuir la E/S en todas las rutas disponibles

```
~$ cat /sys/class/nvme-subsystem/nvme-subsys*/model
Amazon Elastic Block Store
NetApp ONTAP Controller
~$ cat /sys/class/nvme-subsystem/nvme-subsys*/iopolicy
numa
round-robin
```

- Use el siguiente comando para comprobar que los espacios de nombres se han creado y que se detectan correctamente en el host:

```
~$ sudo nvme list
```

Node	Generic Namespace	Usage	SN	Model	FW
Rev					

/dev/nvme0n1	/dev/ng0n1		vol05955547c003f0580	Amazon Elastic	
Block Store	0x1	25.77 GB / 25.77 GB		512 B + 0 B	
1.0					
/dev/nvme2n1	/dev/ng2n1		1WB12JWY/XLKAAAAAAAC	NetApp ONTAP	
Controller	0x1	107.37 GB / 107.37 GB		4 KiB + 0 B	
FFFFFFFF					

El nuevo dispositivo de la salida es `/dev/nvme2n1`. Este esquema de nombres puede variar en función de la instalación de Linux.

- Compruebe que el estado del controlador de cada ruta esté activo y que tenga el estado correcto de múltiples rutas de acceso asimétrico al espacio de nombres (ANA):

```
~$ nvme list-subsys /dev/nvme2n1
nvme-subsys2 -
  NQN=nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:subsystem.rhel
    hostnqn=nqn.2014-08.org.nvmexpress:uuid:ec2a70bf-3ab2-6cb0-
f997-8730057ceb24
    iopolicy=round-robin
\
+- nvme2 tcp
traddr=172.31.26.134,trsvcid=4420,host_traddr=172.31.25.143,src_addr=172.31.25.143
live non-optimized
+- nvme3 tcp
traddr=172.31.16.19,trsvcid=4420,host_traddr=172.31.25.143,src_addr=172.31.25.143
live optimized
```

En este ejemplo, la NVMe pila ha descubierto automáticamente el LIF alternativo del sistema de archivos, `172.31.26.134.iscsi_2`

- Compruebe que el NetApp el complemento muestra los valores correctos para cada ONTAP dispositivo de espacio de nombres:

```
~$ sudo nvme netapp ontapdevices -o column
Device          Vserver          Namespace Path
              NSID  UUID                      Size
-----
-----
-----
/dev/nvme2n1    fsx              /vol/nvme_vol1/ns_1
              1      0441c609-3db1-4b0b-aa83-790d0d448ece  107.37GB
```

Cómo particionar el dispositivo

- Use el siguiente comando para verificar que la ruta al nombre de dispositivo `nvme2n1` está presente.

```
~$ ls /dev/mapper/nvme2n1
/dev/nvme2n1
```

2. Particione el disco usando `fdisk`. Ingresará un mensaje interactivo. Ingrese las opciones en el orden que se muestra. Puede crear varias particiones utilizando un valor menor que el último sector (20971519 en este ejemplo).

 Note

El `Last sector` valor variará en función del tamaño del NVMe dispositivo (100 GiB en este ejemplo).

```
~$ sudo fdisk /dev/mapper/nvme2n1
```

Se inicia el mensaje interactivo `fdisk`.

```
Welcome to fdisk (util-linux 2.37.4).
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 (256-26214399, default 256):
Last sector, +sectors or +size{K,M,G,T,P} (256-26214399, default
26214399): 20971519
```

```
Created a new partition 1 of type 'Linux' and of size 100 GiB.
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/nvme2n1` estará disponible. `partition_name` Tiene el formato. `<device_name> <partition_number>` 1se utilizó como número de partición en el `fdisk` comando del paso anterior.

3. Cree su sistema de archivos con `/dev/nvme2n1` como ruta.

```
~$ sudo mkfs.ext4 /dev/nvme2n1
```

El sistema responde con lo siguiente:

```
mke2fs 1.46.5 (30-Dec-2021)
Found a dos partition table in /dev/nvme2n1
Proceed anyway? (y,N) y
Creating filesystem with 26214400 4k blocks and 6553600 inodes
Filesystem UUID: 372fb2fd-ae0e-4e74-ac06-3eb3eabd55fb
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000, 7962624, 11239424, 20480000, 23887872

Allocating group tables: done
Writing inode tables: done
Creating journal (131072 blocks): done
Writing superblocks and filesystem accounting information: done
```

Para montar el NVMe dispositivo en el cliente Linux

1. Cree un directorio `directory_path` como punto de montaje del sistema de archivos en la instancia de Linux.

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

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

```
~$ sudo mount -t ext4 /dev/nvme2n1 /directory_path/mount_point
```

3. (Opcional) Si desea asignar a un usuario específico la propiedad del directorio de montaje, reemplace `username` con el nombre de usuario del propietario.

```
~$ 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 NVMe dispositivo en su cliente de Linux.

Aprovisionamiento NVMe/TCP para Windows

FSx para ONTAP, es compatible con Non-Volatile Memory Express over TCP (NVMe/TCP) block storage protocol for Windows. With NVMe/TCP, se utiliza la ONTAP CLI para aprovisionar espacios de nombres y subsistemas y, a continuación, se asignan los espacios de nombres a los subsistemas, de forma similar a como se LUNs aprovisionan y asignan a los grupos de iniciadores (iGroups) para iSCSI. [El NVMe/TCP protocolo está disponible en los sistemas de archivos de segunda generación que tienen 6 o menos pares de alta disponibilidad \(HA\).](#) .

Para aprovisionar NVMe/TCP en un host Windows, tendrá que descargar un iniciador del proveedor que prefiera y seguir sus instrucciones para instalarlo y aprovisionarlo.

Acceso a los datos 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 ONTAP](#)
- [Uso de Amazon Elastic Container Service con FSx ONTAP](#)
- [Uso de Amazon Elastic VMware Service con FSx ONTAP](#)
- [FSx Uso de VMware Cloud con ONTAP](#)

Uso de Amazon WorkSpaces con FSx ONTAP

FSx for ONTAP se puede utilizar con Amazon WorkSpaces para proporcionar almacenamiento conectado a la red (NAS) compartido 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 al perfil móvil y a la carpeta principal y para proporcionar una carpeta de equipo compartida para WorkSpaces los usuarios de Windows y Linux. 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](#)
- [Proporcione una carpeta compartida para acceder a los archivos comunes](#)

Proporcione soporte para perfiles itinerantes

Puedes usar Amazon FSx para proporcionar soporte para perfiles de itinerancia a los usuarios de tu 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 FSx archivos de Amazon, lo que permite compartir los documentos y la configuración entre diferentes WorkSpaces instancias, y se hace una copia de seguridad automática mediante las copias de seguridad automáticas FSx diarias de Amazon.

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

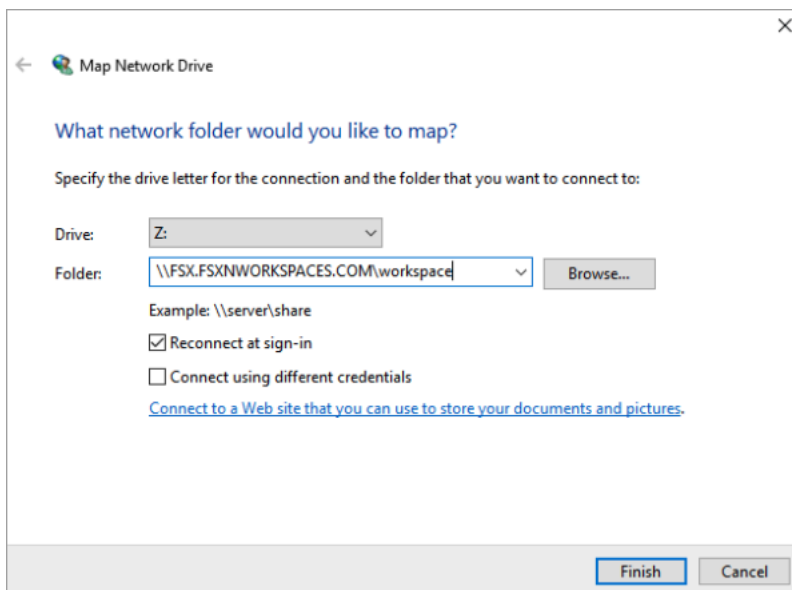
1. Cree un sistema de archivos FSx para ONTAP mediante la FSx consola de Amazon. Para obtener más información, consulte [Cómo crear un sistema de archivos \(consola\)](#).

Important

Cada sistema FSx de archivos de ONTAP tiene un rango de direcciones IP de punto final a partir del cual se crean los puntos finales asociados al sistema de archivos. En el caso de los sistemas de archivos Multi-AZ, FSx ONTAP elige un rango predeterminado de direcciones IP no utilizadas comprendido entre 198.19.0.0/16 como rango de direcciones IP de punto final. 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 Multi-AZ FSx para ONTAP WorkSpaces, 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 obtener más información, consulte [Cómo 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 obtener más información, consulte [Para crear un FlexVol volumen \(consola\)](#).
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 obtener más información, consulte [Gestión de recursos compartidos SMB](#).
5. Acceda a su Amazon FSx SVM desde una EC2 instancia de Amazon que ejecute Windows Server o desde un WorkSpace. Para obtener más información, consulte [Acceder a sus FSx datos de ONTAP](#).
6. Asigna tu recurso compartido a `Z:\` tu WorkSpaces instancia de Windows:



Paso 2: Vincular el archivo compartido FSx de ONTAP a las cuentas de usuario

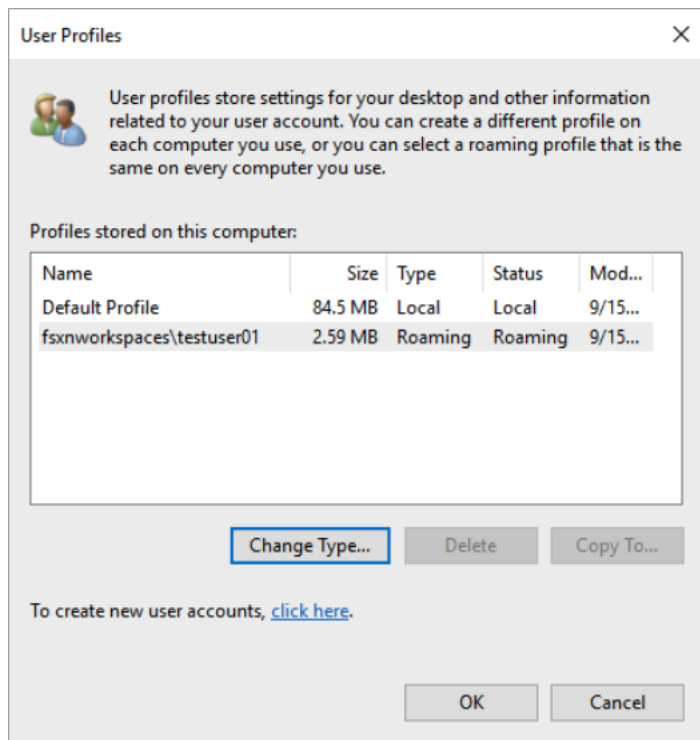
1. En la de su usuario de prueba Workspace, seleccione Windows > Sistema > Configuración avanzada del sistema.
2. En Propiedades del sistema, seleccione la pestaña Avanzadas y pulse el botón Configuración en la sección Perfiles de usuario. El usuario que haya iniciado sesión tendrá un tipo de perfil de Local.
3. Cierre la sesión del usuario de prueba en Workspace.
4. Configura al usuario de prueba para que tenga un perfil de itinerancia ubicado en tu sistema de FSx archivos de Amazon. En tu administrador WorkSpaces, abre una PowerShell consola y usa un comando similar al siguiente ejemplo (que usa la `profiles` carpeta que creaste anteriormente en el paso 1):

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

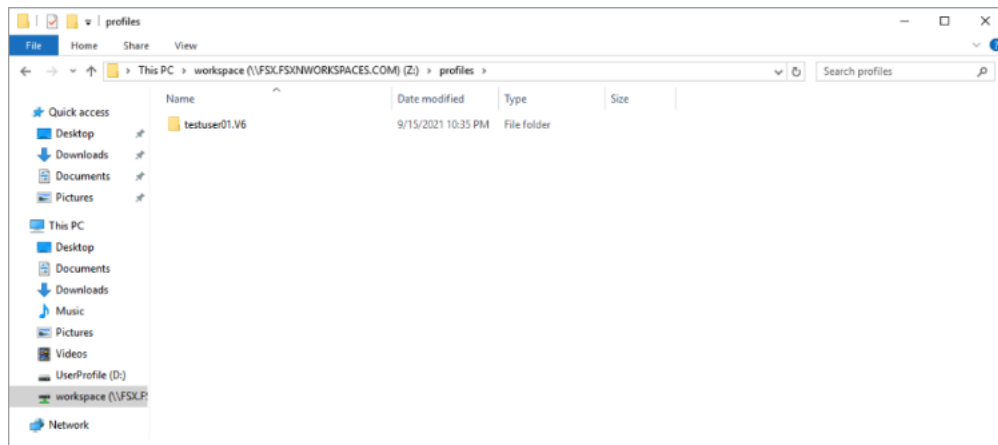
Por ejemplo:

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

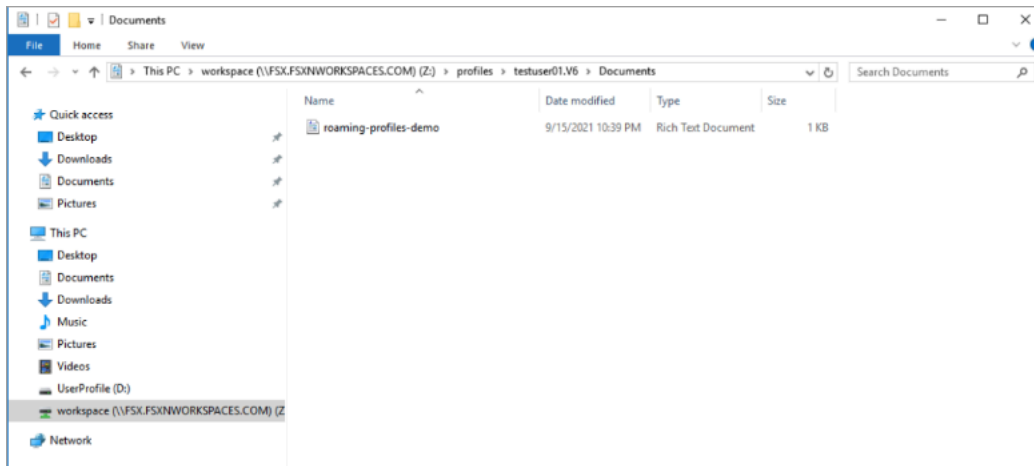
5. Inicie sesión con el usuario de prueba Workspace.
6. En Propiedades del sistema, seleccione la pestaña Avanzadas y pulse el botón Configuración en la sección Perfiles de usuario. El usuario que haya iniciado sesión tendrá un tipo de perfil de Roaming.



7. FSx Busque la carpeta compartida de 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.

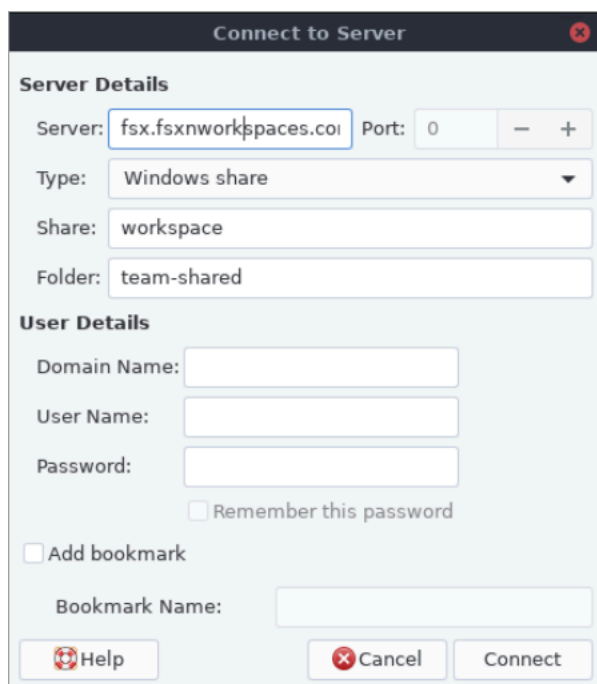


Proporcione una carpeta compartida para acceder a los archivos comunes

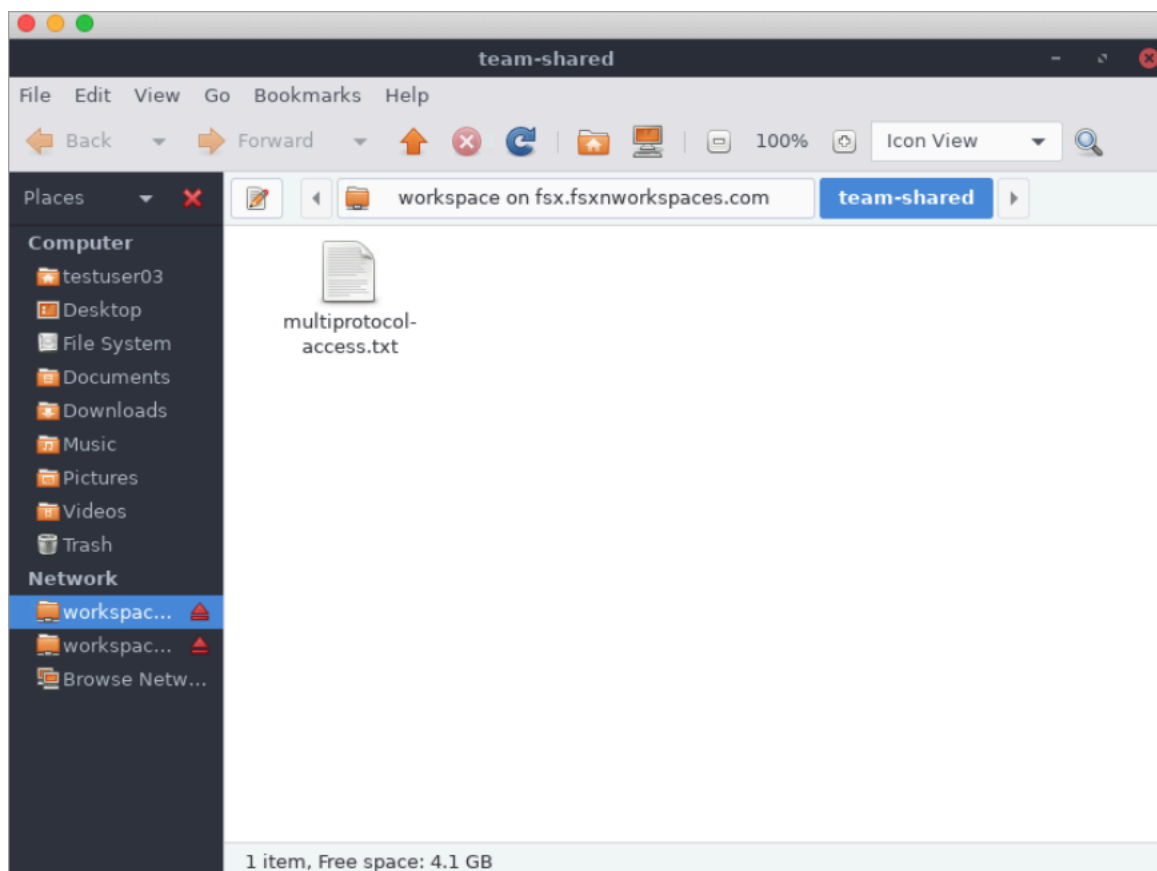
Puedes usar Amazon FSx para proporcionar una carpeta compartida a los usuarios de tu organización. Puede utilizar una carpeta compartida para almacenar los archivos que utilice su comunidad de usuarios, como archivos de demostración, ejemplos de código y manuales de instrucciones que necesiten todos 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 FSx compartida de Amazon que está disponible sin una carta de unidad, lo que te da una mayor flexibilidad a la hora de asignar recursos compartidos a los equipos.

Para 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 FSx recurso compartido de Amazon.
 - 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 ONTAP

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

Montaje en un contenedor de Amazon ECS Linux

1. Cree un clúster de ECS con la plantilla de clúster de 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 EC2 instancia para montar el volumen SVM de la siguiente manera:

```
sudo mkdir /fsxontap
```

3. Monte su volumen FSx para ONTAP en la EC2 instancia de Linux utilizando 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-01234567890abcdef0.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. `sourcePath` Sustitúyalos por el punto de montaje y el directorio del sistema de archivos FSx de 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 utilizando la plantilla de clúster de redes de EC2 Windows + 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 EC2 instancia de Windows unida a un dominio al clúster de Windows de ECS y asigne un recurso compartido SMB.

Inicie una EC2 instancia 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 EC2 instancia para poder asignar su recurso compartido de SMB a una unidad. Sustituya los valores que aparecen debajo del nombre netbios o DNS del sistema de FSx archivos y del nombre del recurso compartido. El volumen NFS vol1 que se montó en la EC2 instancia de Linux está configurado como un archivo compartido de CIFS fsxontap en el sistema de archivos. 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. Crea el mapeo global de SMB en la instancia mediante el EC2 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. `sourcePath` Sustitúyalos por el punto de montaje y el directorio del sistema de archivos FSx de ONTAP.

```
{
  "volumes": [
```

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

Uso de Amazon Elastic VMware Service con FSx ONTAP

Puede utilizar ONTAP como almacén de datos externo FSx para los centros de datos definidos por software VMware () de Amazon Elastic Service (Amazon EVS). SDDCs Para obtener más información, consulte [Ejecute cargas de trabajo de alto rendimiento con Amazon FSx for NetApp ONTAP](#). Para obtener instrucciones detalladas, consulte [Configurar Amazon FSx para NetApp ONTAP como almacén de datos NFS y Configurar Amazon FSx para NetApp ONTAP como almacén de datos iSCSI](#).

FSx Uso de VMware Cloud con ONTAP

Puede utilizar ONTAP como almacén de datos externo FSx para centros de datos AWS definidos por software en VMware la nube (). SDDCs Para obtener más información, consulte la [guía de implementación de Amazon FSx para NetApp ONTAP como almacenamiento externo y VMware Cloud on AWS con Amazon FSx for NetApp ONTAP](#).

Opciones de disponibilidad, durabilidad e implementación

Amazon FSx for NetApp ONTAP utiliza los tipos de despliegue Single-AZ y Multi-AZ. Puede elegir entre cuatro opciones: Single-AZ 1, Single-AZ 2, Multi-AZ 1 y Multi-AZ 2. 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 SLA (acuerdo de nivel de servicio) de disponibilidad del servicio, consulta el acuerdo de [nivel de FSx servicio de Amazon](#).

Temas

- [Selección de un tipo de implementación del sistema de archivos](#)
- [Selección de una generación del sistema de archivos](#)
- [Proceso de conmutación por error FSx para ONTAP](#)
- [Recursos de red](#)

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.

Tipos de implementación Single-AZ

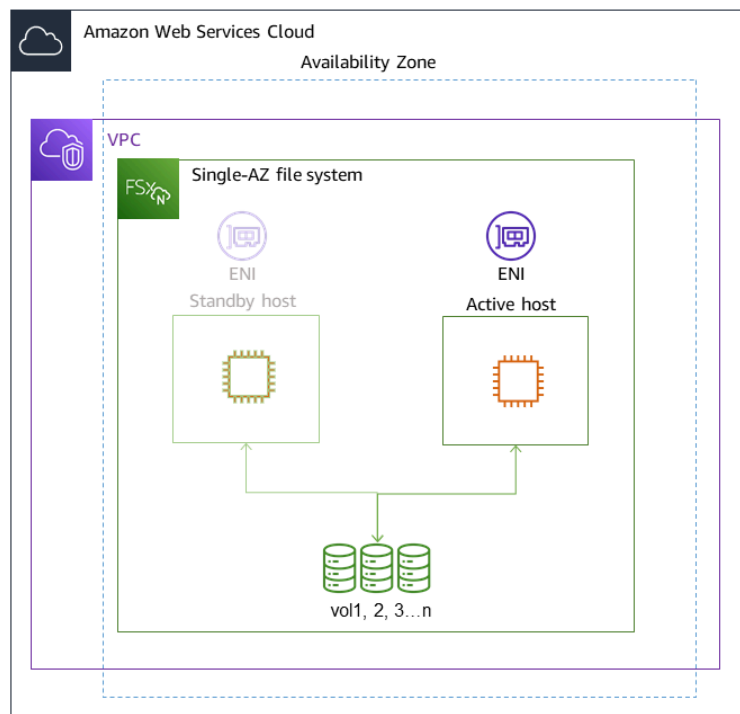
Puede elegir entre Single-AZ 1 y Single-AZ 2 para el sistema de archivos Single-AZ. Single-AZ 1 es un sistema de archivos de primera generación con un par de alta disponibilidad (HA), mientras que el Single-AZ 2 es un sistema de archivos de segunda generación con 1 a 12 pares de HA. Para obtener más información, consulte [Selección de una generación del sistema de archivos](#).

Al crear un sistema de archivos Single-AZ, Amazon aprovisiona FSx 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 error 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, usted seguirá teniendo acceso a los datos sin intervención manual.

Para garantizar una alta disponibilidad, Amazon monitorea FSx 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 replica FSx automáticamente sus datos dentro de una zona de disponibilidad para protegerlos de fallos de los 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. Ofrecen una solución rentable para casos de uso tales como entornos de desarrollo y pruebas, o para almacenar copias secundarias de datos que ya están almacenados in situ o en otros entornos Regiones de AWS, replicando únicamente los datos dentro de una única zona de disponibilidad.

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

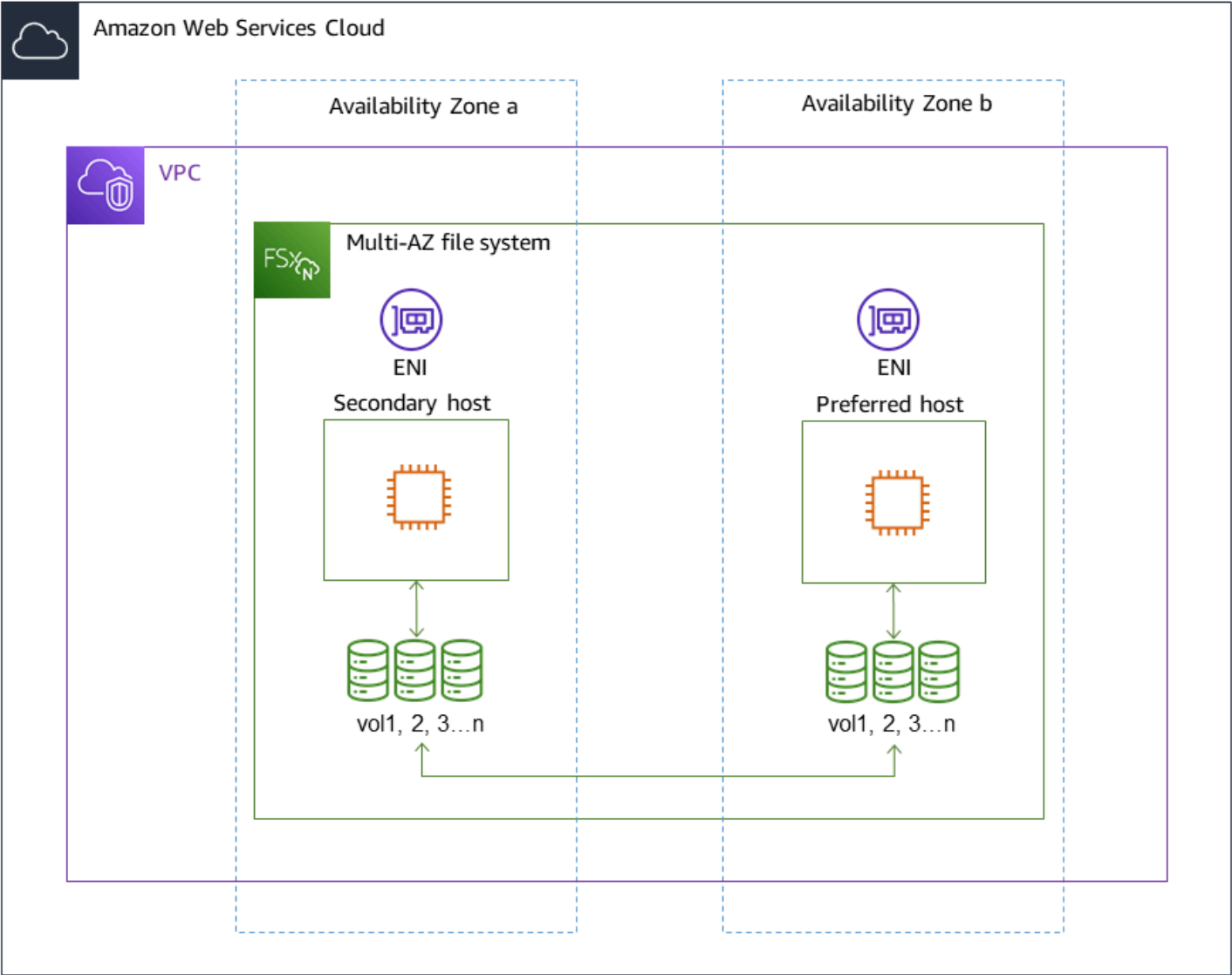


Tipos de implementación Multi-AZ

Puede elegir entre Multi-AZ 1 y Multi-AZ 2 para el sistema de archivos Multi-AZ. Multi-AZ 1 es un sistema de archivos de primera generación y Multi-AZ 2 es un sistema de archivos de segunda generación. Ambas opciones tienen un par de HA. Para obtener más información, consulte [Selección de una generación del sistema de archivos](#).

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 HA de servidores de archivos. El servidor de archivos en espera se implementa dentro de una zona de disponibilidad diferente a la del servidor de archivos activo dentro de la misma 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 Multi-AZ de primera generación FSx para ONTAP.



Selección de una generación del sistema de archivos

En la siguiente tabla se muestran las diferencias entre la primera y segunda generación de zonas de disponibilidad única y las zonas de disponibilidad múltiples para los sistemas de archivos ONTAP. FSx

FSx para las generaciones de sistemas de archivos ONTAP

Dimensión	Primera generación	Segunda generación (par de HA único)	Segunda generación (varios pares)
Tipo de implementación	SINGLE_AZ_1 MULTI_AZ_1	SINGLE_AZ_2 MULTI_AZ_2	SINGLE_AZ_2
Pares de HA	1 par de HA		1 a 12 pares de HA
Almacenamiento en SSD	Mínimo: 1 TiB Máximo: 192 TiB	Mínimo: 1 TiB Máximo: 512 TiB	Mínimo: 1 TiB (por par de HA) Máximo: 1 PiB (total)
IOPS en SSD	Mínimo: 3 IOPS/GIB de SSD Máximo: 160 000	Mínimo: 3 IOPS/GIB de SSD Máximo: 200 000	Mínimo: 3 IOPS/GIB de SSD Máximo: 2 400 000 (200 000 por par de HA)
Capacidad de rendimiento	128 MBps; 256; 512 MBps; 1.024 MBps; 2.048 MBps; 4.096 MBps MBps	384 MBps; 768; 1.536 MBps; 3.072; 6.144 MBps MBps MBps	1.536 MBps (por par de ha); 3.072 MBps (por par de ha); 6.144 MBps (por par de ha)

Note

No puede cambiar el tipo de implementación del sistema de archivos después de su creación. Si desea cambiar el tipo de implementación (por ejemplo, pasar de Single-AZ 1 a Single-AZ 2), puede hacer una copia de seguridad de los datos y restaurarlos en un nuevo sistema de archivos. También puede migrar sus datos con NetApp SnapMirror AWS DataSync, con o con una herramienta de copia de datos de terceros. Para obtener más información, consulte [Migración a ONTAP mediante FSx NetApp SnapMirror](#) y [Migración a FSx ONTAP mediante AWS DataSync](#).

Proceso de conmutación por error FSx para ONTAP

Los sistemas de archivos Single-AZ y Multi-AZ conmutan automáticamente por error al par de HA en cuestión desde el 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 de segunda generación con varios pares de HA, el comportamiento de conmutación por error de cada par de HA es independiente. Si el servidor de archivos preferido de 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 servidor de archivos nuevo que está activo comienza a atender todas las solicitudes de lectura y escritura del sistema de archivos a ese par de HA de manera automática. 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 recurre automáticamente a él por error y, por lo general, la recuperación se completa 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 sus FSx sistemas de archivos ONTAP Single-AZ y Multi-AZ, consulte. [Acceder a los datos desde el Nube de AWS](#)

Probar la conmutación por error en un sistema de archivos

Puede probar la conmutación por error en su sistema de archivos modificando su capacidad de rendimiento. Cuando modificas la capacidad de procesamiento de tu sistema de archivos, Amazon FSx cambia 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 reemplaza primero el servidor de archivos preferido. Una vez actualizado, el sistema de archivos regresa automáticamente al nuevo servidor principal y Amazon FSx reemplaza el servidor de archivos secundario.

Puede supervisar el progreso de la solicitud de actualización de la capacidad de rendimiento en la FSx consola de Amazon, 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 asocias a tu sistema de archivos. Para los sistemas de archivos Multi-AZ, Amazon FSx también proporciona dos ENIs, uno en cada una de las subredes que asocie a su sistema de archivos. Los clientes se comunican con tu sistema de FSx archivos de Amazon mediante la elastic network interface. Se considera que las interfaces de red están dentro del ámbito de servicio de Amazon FSx, a pesar de formar parte de la VPC de tu cuenta. Los sistemas de archivos Multi-AZ usan direcciones de protocolo de internet (IP) flotantes para que los clientes conectados puedan realizar una transición fluida entre servidores de archivos preferidos y 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.

En la siguiente tabla se resumen los recursos de subred, elastic network interface y dirección IP para cada uno de los tipos de implementación del FSx sistema de archivos ONTAP:

	Single-AZ de primera generación	Single-AZ de segunda generación	Multi-AZ
Número de subredes	1	1	2
Número de interfaces de red elásticas	2	2 por par de HA	2

	Single-AZ de primera generación	Single-AZ de segunda generación	Multi-AZ
Número de direcciones IP por ENI	1 + el número de SVMs en el sistema de archivos	Recuento de pares HA + recuento de pares HA multiplicado por el número de SVMs en el sistema de archivos	1 + el número de SVMs en el sistema de archivos
Número de rutas de VPC de tabla de enrutamiento	N/A	N/A	1 + el número de SVMs 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 desconecta FSx 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.

Amazon FSx para el rendimiento de NetApp ONTAP

A continuación se presenta un resumen del rendimiento del sistema de archivos Amazon FSx for NetApp ONTAP, con información sobre las opciones de rendimiento y rendimiento disponibles y consejos útiles sobre el rendimiento.

Temas

- [¿Cómo se mide el rendimiento de los sistemas de archivos FSx ONTAP](#)
- [Detalles de desempeño](#)
- [Impacto del tipo de implementación en el rendimiento](#)
- [Impacto de la capacidad de almacenamiento en el rendimiento](#)
- [Impacto de la capacidad de rendimiento en el rendimiento](#)
- [Ejemplo: capacidad de almacenamiento y capacidad de rendimiento](#)

¿Cómo se mide el rendimiento de los sistemas de archivos FSx ONTAP

El rendimiento del sistema de archivos se mide por su latencia, rendimiento y I/O operaciones por segundo (IOPS).

Latencia

Amazon FSx for 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 exprés no volátil) y en memoria, para ofrecer latencias aún más bajas cuando accedes a los datos que lees con más frecuencia.

Rendimiento e IOPS

Cada sistema de FSx archivos de Amazon proporciona hasta decenas GBps 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 configuración de la capacidad de rendimiento y de

la capacidad de almacenamiento total 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 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 SMB multicanal, consulte [Configuración de SMB multicanal 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 red disponible. NFSv3 y compatibilidad con 1.1+. NFSv4 nconnect [El ancho de banda de la red de EC2 instancias de Amazon](#) 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 el NetApp ONTAP soporte paranconnect, consulte el [ONTAPsoporte para NFSv4 .1](#).

Marcos gigantes

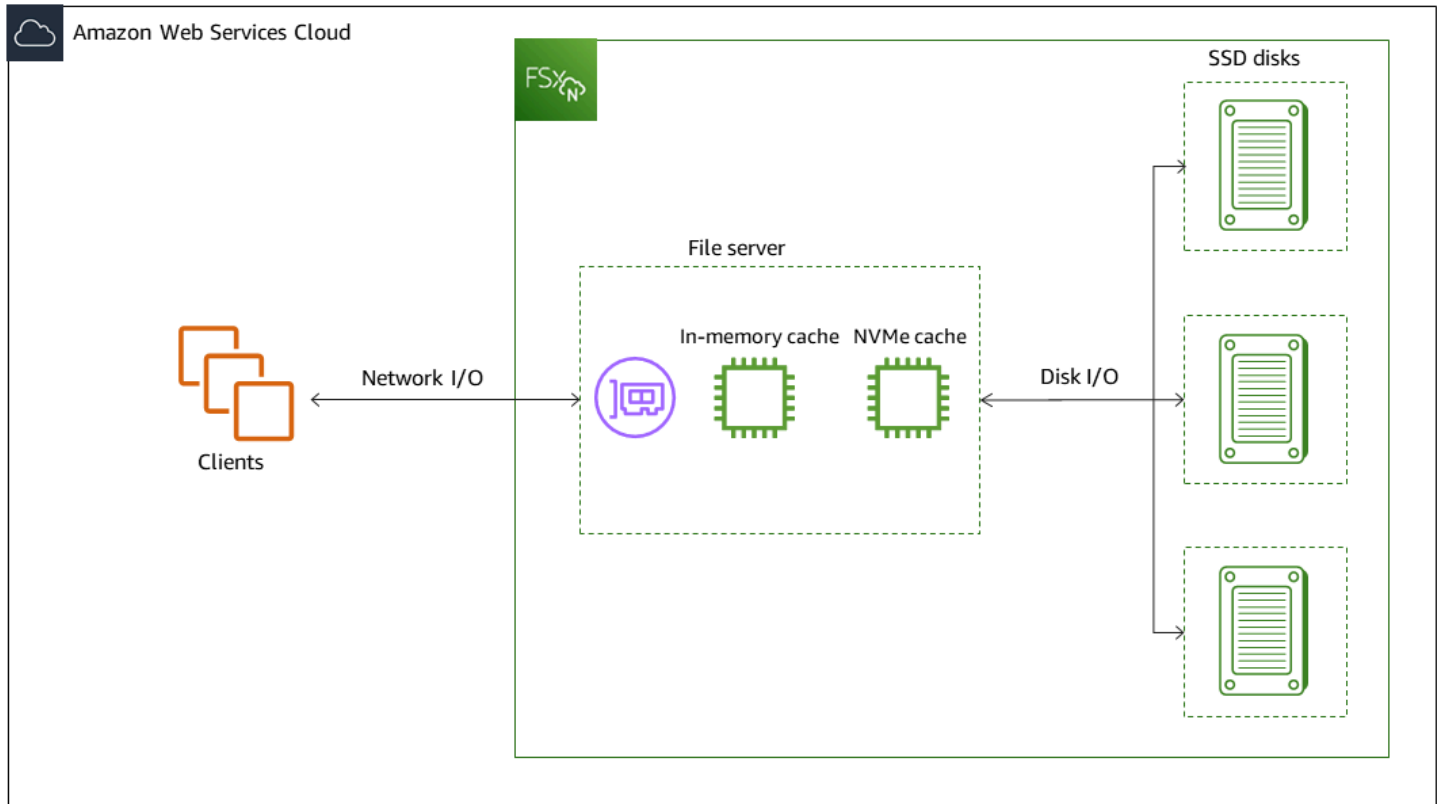
Para lograr el máximo rendimiento de lectura o escritura, te recomendamos habilitar tramas gigantes en todas las interfaces de red de la ruta de datos a tu sistema de FSx archivos de Amazon, incluidas las instancias de tus clientes EC2 . La configuración predeterminada de la unidad de transmisión máxima (MTU) para las interfaces de red del sistema de archivos de ONTAP es de 9 001 bytes. FSx

Detalles de desempeño

Para comprender en detalle el modelo de rendimiento de Amazon FSx for NetApp ONTAP, puede examinar los componentes arquitectónicos de un sistema de FSx archivos de Amazon. 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 interfaz de red elástica (ENI) de sistema de archivos hay un servidor de archivos de NetApp ONTAP que envía datos a través de la red a los clientes que acceden al sistema de archivos. Amazon FSx proporciona una caché rápida en memoria y una NVMe caché 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, NVMe caché en memoria, caché y volúmenes de almacenamiento).

- I/O Rendimiento de la red: throughput/IOPS de las solicitudes entre los clientes y el servidor de archivos (en conjunto)
- Tamaño de la memoria y de la NVMe caché del servidor de archivos: tamaño del conjunto de trabajo activo que se puede almacenar en caché
- I/O Rendimiento del disco: throughput/IOPS de las solicitudes entre el servidor de archivos y los discos de almacenamiento

Hay dos factores que determinan estas características de rendimiento del sistema de archivos: la cantidad total de IOPS del SSD y la capacidad de rendimiento que se configura para él. Las dos primeras características de rendimiento (el I/O rendimiento de la red y el tamaño en memoria y

NVMe caché) 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 del SSD.

Las cargas de trabajo basadas en archivos suelen tener picos de actividad y se caracterizan por períodos cortos e intensos de alta I/O tensión con 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 para las operaciones de red I/O y de disco I/O. Amazon FSx utiliza un mecanismo de I/O crédito 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 utilizarlos cuando realizan operaciones. I/O

Note

En el caso de los protocolos iSCSI y NVMe/TCP SAN, las operaciones del cliente de lectura secuencial pueden alcanzar el rendimiento máximo de I/O ráfaga de red o de referencia del sistema de archivos.

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 red.

Impacto del tipo de implementación en el rendimiento

Puede crear sistemas de archivos Single-AZ y Multi-AZ con ONTAP. FSx Los sistemas de archivos de primera generación (tanto Single-AZ como Multi-AZ) y los sistemas de archivos Multi-AZ de segunda generación funcionan con un par de alta disponibilidad (HA). Los sistemas de archivos Single-AZ de segunda generación funcionan con hasta 12 pares de HA. Para obtener más información, consulte [Administración de pares de alta disponibilidad \(HA\)](#).

FSx para ONTAP, los sistemas de archivos 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 grupos de almacenamiento de capacidad. Además, los sistemas de archivos que cumplen los siguientes requisitos proporcionan una caché de lectura

para reducir las latencias de NVMe lectura y aumentar las IOPS para los datos que se leen con frecuencia:

- Sistemas de archivos Multi-AZ 1 y Multi-AZ 2
- Sistemas de archivos Single-AZ (1) creados después del 28 de noviembre de 2022 con al menos un 2% de capacidad de rendimiento GBps
- Sistemas de archivos Single-AZ 2 con al menos un 6% GBps de capacidad de rendimiento por par

 Note

En el caso de los sistemas de archivos de segunda generación (Single-AZ 2 y Multi-AZ 2), el uso de una NVMe caché puede hacer que la carga de trabajo reduzca el rendimiento total en el caso de cargas de trabajo de E/S grandes o de alto rendimiento. Si tiene una carga de trabajo con un rendimiento limitado, le recomendamos que desactive la caché. NVMe Para obtener más información, consulte [Administrar la memoria caché NVMe](#).

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

First-generation file systems

Estas especificaciones de rendimiento se aplican a los sistemas de archivos Single-AZ y Multi-AZ de primera generación.

Rendimiento máximo del almacenamiento en SSD por par de HA para los sistemas de archivos de primera generación

Región Este de EE. UU. (Ohio), Región Este de EE. UU. (Norte de Virginia), Región Oeste de EE. UU. (Oregón) y Europa (Irlanda).		En todos los demás Regiones de AWS lugares donde está FSx disponible ONTAP	
Rendimiento de lectura () MBps	Rendimiento de escritura () MBps	Rendimiento de lectura () MBps	Rendimiento de escritura () MBps

	Región Este de EE. UU. (Ohio), Región Este de EE. UU. (Norte de Virginia), Región Oeste de EE. UU. (Oregón) y Europa (Irlanda).		En todos los demás Regiones de AWS lugares donde está FSx disponible ONTAP	
Single-AZ	4.096 ¹	1 000	2048	750
Multi-AZ	4.096 ¹	1800	2048	1300

 Note

¹ Para aprovisionar el 4% GBps de la capacidad de rendimiento, el sistema de archivos debe estar configurado con una capacidad mínima de almacenamiento SSD de 5.120 GiB y 160.000 IOPS de SSD.

Second-generation file systems

Estas especificaciones de rendimiento se aplican a los sistemas de archivos Single-AZ y Multi-AZ de segunda generación. Por lo general, los sistemas de archivos de segunda generación pueden ofrecer toda la capacidad aprovisionada para lecturas y hasta un tercio de la capacidad aprovisionada para escrituras. La excepción es la MB/s opción 6.144, que se muestra en esta tabla.

Rendimiento máximo del almacenamiento en SSD por par de HA para sistemas de archivos de segunda generación

	Rendimiento de lectura () MBps	Rendimiento de escritura () MBps
Single-AZ	6.144 ¹	1.024 ¹
Multi-AZ	6144	2048

Note

¹ por par HA (hasta 12). Para obtener más información, consulte [Administración de 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 proporcionado por los servidores de archivos, en función de la capacidad de rendimiento que seleccione para el 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 en SSD del sistema de archivos proporciona los siguientes niveles de rendimiento del disco e IOPS:

- Rendimiento de disco (MBps por TiB de almacenamiento): 768
- IOPS de disco (IOPs por TiB de almacenamiento): 3 072

Impacto de la capacidad de rendimiento en el rendimiento

Cada sistema de FSx archivos de Amazon tiene una capacidad de rendimiento que se configura al crear el sistema de archivos. La capacidad de rendimiento de su sistema de archivos determina el nivel de I/O rendimiento de la red o la velocidad a la que cada uno de los servidores de archivos que alojan su sistema de archivos puede entregar datos de archivos a través de la red a los clientes que acceden a ella. Los niveles más altos de capacidad de procesamiento incluyen más memoria y almacenamiento express (NVMe) de memoria no volátil para almacenar los datos en caché en cada servidor de archivos, y cada servidor de archivos admite niveles más altos de I/O rendimiento del 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.

First-generation Single-AZ file system

Estas especificaciones de rendimiento se aplican a los sistemas de archivos Single-AZ de primera generación creados después del 28 de noviembre de 2022 en las Regiones de AWS especificadas.

Las especificaciones de rendimiento de los sistemas de archivos Regiones de AWS son las siguientes: EE.UU. Este (Norte de Virginia), EE.UU. Este (Ohio), EE.UU. Oeste (Oregón) y Europa (Irlanda)

FSx capacidad de rendimiento (MBps)	Capacidad de rendimiento de la red (MBps)	IOPS de red	Almacenamiento en caché en memoria (GB)	Nivel de almacenamiento en caché de lectura (GB)	Rendimiento del disco (MBps)	IOPS de la unidad SSD *			
	Referencia	Ráfaga			Referencia	Ráfaga	Referencia	Ráfaga	
128	188	1500	Decenas de miles de referencia	16	–	128	1250	6000	40 000
256	375	1500		32	–	256	1250	12 000	40 000
512	750	1500	Cientos de miles de referencia	64	–	512	1250	20 000	40 000
1 024	1500	–		128	–	1 024	1250	40 000	–
2048	3.125	–		256	1900	2048	–	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 la memoria caché o caché del servidor de archivos. NVMe

Estas especificaciones de rendimiento se aplican a los sistemas de archivos Single-AZ de primera generación en todos los demás sitios en los que ONTAP esté Regiones de AWS disponible FSx .

Especificaciones de rendimiento para los sistemas de archivos en [todos los demás Regiones de AWS lugares donde ONTAP esté FSx disponible](#)

FSx	Capacidad de rendimiento de la red () MBps		IOPS de red	Almacenamiento en caché en memoria (GB)	Rendimiento del disco () MBps		IOPS de la unidad SSD *	
	Referencia	Ráfaga			Referencia	Ráfaga	Referencia	Ráfaga
128	150	1250	Decenas de miles de referencia	16	128	600	6000	18 750
256	300	1250		32	256	600	12 000	18 750
512	625	1250		64	512	600	18 750	–
1 024	1500	–	de miles	128	1 024	–	40 000	–
2048	3.125	–	de referencia	256	2048	–	80 000	–

Note

* Las IOPS de su SSD solo se utilizan cuando accede a datos que no están en caché en la memoria caché o caché del servidor de archivos. NVMe

Second-generation Single-AZ file system

Estas especificaciones de rendimiento se aplican a los sistemas de archivos Single-AZ de segunda generación.

Estas especificaciones de rendimiento para sistemas de archivos Single-AZ de segunda generación

FSx	Capacidad de almacenamiento de la red () MBps		IOPS de red	Almacenamiento en caché en memoria (GB)		NVMe almacenamiento en caché (GB)	Rendimiento del disco () MBps		IOPS de la unidad SSD *	
	Referencia	Ráfaga					Referencia	Ráfaga	Referencia	Ráfaga
384**	781	6.250	Cientos	16	–		384	3.125	12.500	65.000
768**	1.563	6.250	de miles	32	–		768	3.125	25 000	65.000
1536	3.125	6.250	de referenci	64	–		1536	3.125	50 000	65.000
3.072	6.250	–	a	128	–		3.072	–	100 000	–
6144	12.500	–		256	1900		6144	–	200.000	–

Note

* Las IOPS de su SSD solo se utilizan cuando accede a datos que no están en caché en la memoria caché o caché del servidor de archivos. NVMe

** Los sistemas de archivos Single-AZ de segunda generación admiten capacidades de rendimiento de 384 y 768, pero solo con un par de HA. Para añadir pares de alta disponibilidad, el sistema de archivos debe estar configurado con una capacidad de rendimiento mínima de 1.536 MBps .

First-generation Multi-AZ file system

Estas especificaciones de rendimiento se aplican a los sistemas de archivos Multi-AZ de primera generación creados después del 28 de noviembre de 2022 en las Regiones de AWS especificadas.

Las especificaciones de rendimiento de los sistemas de archivos Regiones de AWS son las siguientes: EE.UU. Este (Norte de Virginia), EE.UU. Este (Ohio), EE.UU. Oeste (Oregón) y Europa (Irlanda)

FSx	Capacidad de almacenamiento de la red () MBps		IOPS de red	Almacenamiento en caché en memoria (GB)		NVMe almacenamiento en caché (GB)	Rendimiento del disco () MBps		IOPS de la unidad SSD *	
	Referencia	Ráfaga					Referencia	Ráfaga	Referencia	Ráfaga
128	188	1500	Decenas de miles de referencia	16	238		128	1250	6000	40 000
256	375	1500		32	475		256	1250	12 000	40 000
512	750	1500	Cientos de miles de	64	950		512	1250	20 000	40 000
1 024	1500	–		128	1900		1 024	1250	40 000	–
2048	3.125	–		256	3800		2048	–	80 000	–

FSx	Capacidad de almacenamiento de la red () MBps		IOPS de red	Almacenamiento en caché en memoria (GB)	NVMe almacenamiento en caché en memoria (GB)	Rendimiento del disco () MBps		IOPS de la unidad SSD *	
4.096	6.250	–	referencia	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 la memoria caché o caché del servidor de archivos. NVMe

Estas especificaciones de rendimiento se aplican a los sistemas de archivos Multi-AZ de primera generación en todos los demás Regiones de AWS lugares FSx en los que ONTAP esté disponible.

Especificaciones de rendimiento para los sistemas de archivos en [todos los demás Regiones de AWS lugares donde ONTAP esté FSx disponible](#)

FSx	Capacidad de almacenamiento de la red () MBps		IOPS de red	Almacenamiento en caché en memoria (GB)	NVMe almacenamiento en caché en memoria (GB)	Rendimiento del disco () MBps		IOPS de la unidad SSD *	
	Referencia		Ráfaga			Referencia		Ráfaga	Ráfaga
128	150	1250	Decenas de	16	150	128	600	6000	18 750
256	300	1250		32	300	256	600	12 000	18 750

FSx	Capacidad de rendimiento de la red () MBps		IOPS de red	Almacenamiento en caché en memoria (GB)	NVMe almacenamiento en caché en memoria (GB)	Rendimiento del disco () MBps		IOPS de la unidad SSD *	
			miles de referencia						
512	625	1250	Cientos de miles de referencia	64	600	512	600	18 750	–
1 024	1500	–		128	1.200	1 024	–	40 000	–
2048	3.125	–		256	2400	2048	–	80 000	–

 Note

* Las IOPS de su SSD solo se utilizan cuando accede a datos que no están en caché en la memoria caché o caché del servidor de archivos. NVMe

Second-generation Multi-AZ file systems

Estas especificaciones de rendimiento se aplican a los sistemas de archivos Multi-AZ de segunda generación.

Estas especificaciones de rendimiento para sistemas de archivos Multi-AZ de segunda generación

FSx	Capacidad de almacenamiento de la red () MBps		IOPS de red	Almacenamiento en caché en memoria (GB)	NVMe almacenamiento en caché (GB)	Rendimiento del disco () MBps		IOPS de la unidad SSD *	
	Referencia	Ráfaga				Referencia	Ráfaga	Referencia	Ráfaga
384	781	6.250	Cientos de miles de referenci	16	237	384	3.125	12.500	65.000
768	1.563	6.250		32	474	768	3.125	25 000	65.000
1536	3.125	6.250		64	950	1536	3.125	50 000	65.000
3.072	6.250	–	a	128	1900	3.072	–	100 000	–
6144	12.500	–		256	3800	6144	–	200.000	–

 **Note**

* Las IOPS de su SSD solo se utilizan cuando accede a datos que no están en caché en la memoria caché o caché del servidor de archivos. 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 de primera generación que esté configurado con 2 TiB de capacidad de almacenamiento SSD y MBps 512 de capacidad de rendimiento tiene los siguientes niveles de rendimiento:

- Rendimiento de red: 625 de MBps referencia y 1250 MBps ráfagas (consulte la tabla de capacidad de rendimiento)
- Rendimiento de disco: 512 de MBps referencia y 600 ráfagas. MBps

Por lo tanto, su carga de trabajo al acceder al sistema de archivos podrá generar un rendimiento de hasta 625 bits de MBps referencia y 1250 en MBps ráfaga para las operaciones de archivos realizadas con datos a los que se accede activamente almacenados en caché en la memoria caché y en la caché del servidor de archivos. NVMe

Administración de FSx los recursos de ONTAP

Mediante la AWS Management Console CLI y la API de ONTAP, puede realizar las siguientes acciones administrativas FSx para los recursos de ONTAP: AWS CLI

- Crear, enumerar, actualizar y eliminar sistemas de archivos, máquinas virtuales de almacenamiento (SVMs), volúmenes, copias de seguridad y etiquetas.
- Administración del acceso, cuentas y contraseñas administrativas, requisitos de contraseñas, protocolos SMB e iSCSI, accesibilidad de red para los destinos de montaje de los sistemas de archivos existentes

Temas

- [Administración de la capacidad de almacenamiento](#)
- [Gestión de FSx sistemas de archivos ONTAP](#)
- [Administración FSx de máquinas virtuales de almacenamiento ONTAP](#)
- [Gestión de FSx volúmenes de ONTAP](#)
- [Creación de un iSCSI LUN](#)
- [Optimización del rendimiento con las ventanas FSx de mantenimiento de Amazon](#)
- [Administración de la capacidad de rendimiento](#)
- [Gestión de recursos compartidos SMB](#)
- [Gestión de FSx los recursos de ONTAP mediante NetApp aplicaciones](#)
- [Etiquetado de los recursos de Amazon FSx](#)

Administración de la capacidad de almacenamiento

Amazon FSx for 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

- [FSx para los niveles de almacenamiento de ONTAP](#)
- [Elegir la cantidad correcta de almacenamiento en SSD del sistema de archivos](#)
- [Capacidad de almacenamiento e IOPS del sistema de archivos](#)
- [Capacidad de almacenamiento de volumen](#)

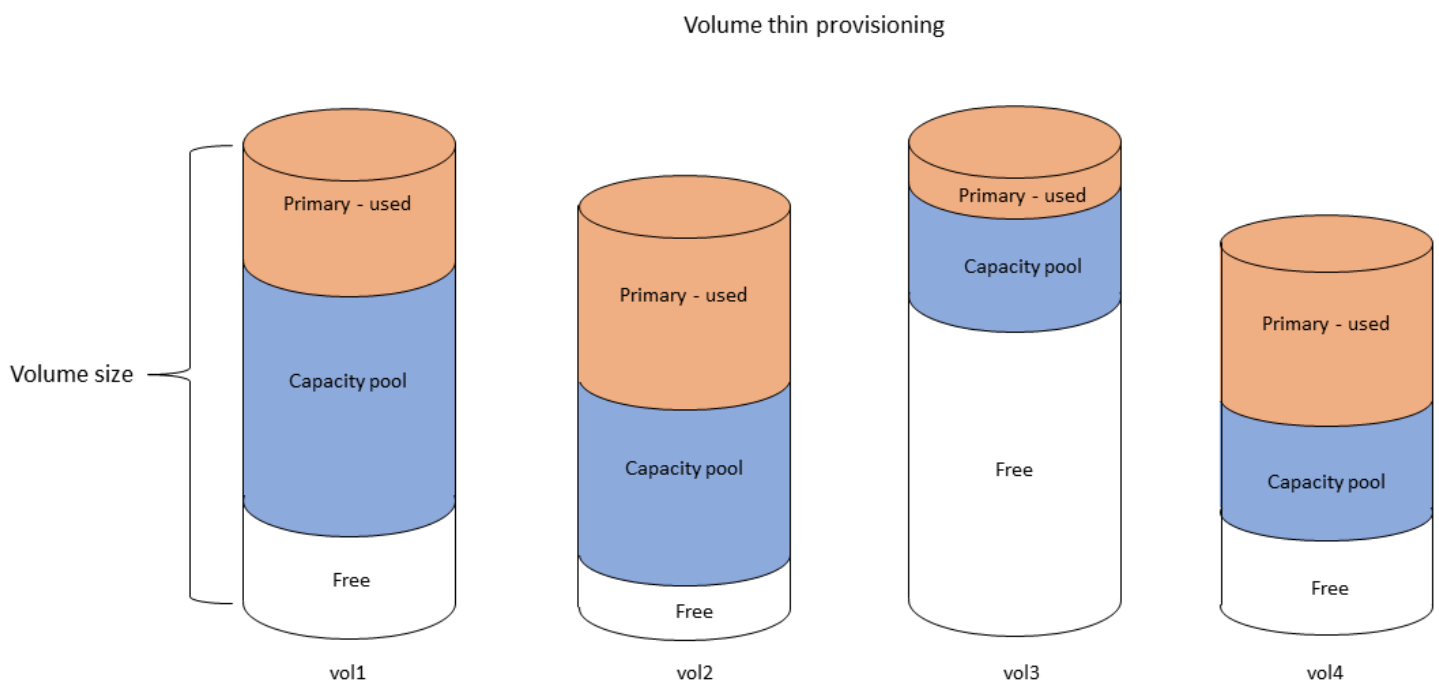
FSx para los niveles de almacenamiento de ONTAP

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

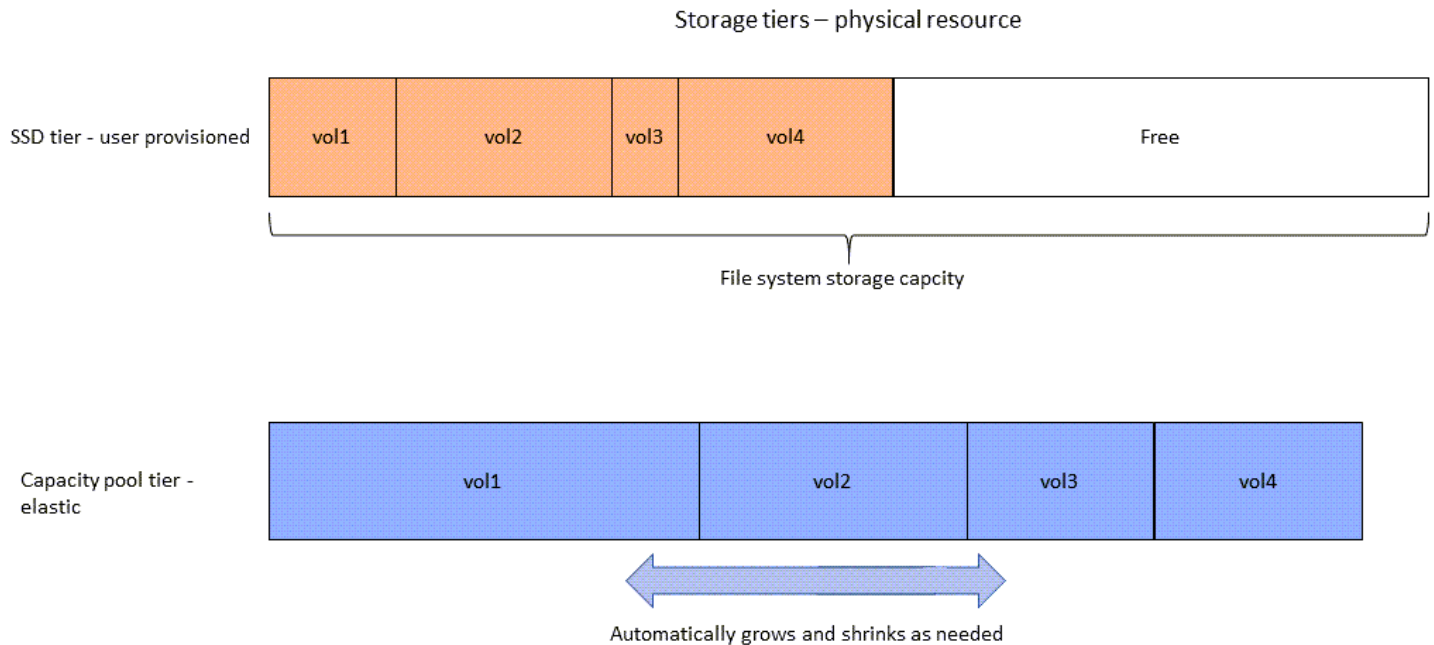
- Nivel SSD: almacenamiento en unidad de estado sólido (SSD) de alto rendimiento, aprovisionado por el usuario y diseñado específicamente para la parte activa del conjunto de datos.
- Nivel de reserva de capacidad: almacenamiento totalmente elástico que escala automáticamente a petabytes de tamaño y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

FSx Para ONTAP, un volumen 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. FSx en el caso de ONTAP, los volúmenes son de aprovisionamiento reducido y el almacenamiento del sistema de archivos no se reserva con antelación. 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 volúmenes de ONTAP FSx 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 FSx para su sistema de archivos 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 de software NetApp de 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 en 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	De 1 % a 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 que los datos se escriben directamente en el almacenamiento del pool de capacidad cuando se utilizan SnapMirror en 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 % del nivel de almacenamiento en SSD de forma continua. En el caso de los sistemas de archivos de segunda generación, 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 NetApp la recomendación 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](#).

Eficacia de almacenamiento

NetApp ONTAP ofrece funciones de eficiencia de almacenamiento a nivel de bloque a nivel de volumen que incluyen compresión, compactación y deduplicación. Estas características pueden

ahorrarle hasta un 65 % de la capacidad de almacenamiento en el caso de los archivos compartidos en general, sin sacrificar el rendimiento. Puede habilitar la eficiencia del almacenamiento por volumen. Estas funciones reducen la cantidad de capacidad de almacenamiento que consumen sus datos, lo que le permite consumir menos espacio de almacenamiento en las unidades SSD, el pool de capacidades y el almacenamiento de copias de seguridad. Puede habilitar la compresión y la deduplicación en cada volumen para los datos del almacenamiento en SSD. Los ahorros de almacenamiento derivados de la compresión y la deduplicación en el almacenamiento en SSD se mantienen cuando los datos se agrupan en niveles según el almacenamiento del grupo de capacidad. La eficiencia del almacenamiento siempre está habilitada para los datos de copias de seguridad, independientemente de la configuración de eficiencia de almacenamiento del sistema de archivos.

En la siguiente tabla, se muestran ejemplos de ahorros de almacenamiento típicos.

	Solo compresión	Solo deduplicación	Compresión y deduplicación
Recursos de archivos compartidos de uso general	50%	30%	65%
Servidores y escritorios virtuales	55%	70 %	70 %
Bases de datos	De 65 % a 70 %	0%	De 65 % a 70 %
Datos de ingeniería	55%	30%	75%
Datos geosísmicos	40%	3%	40%

Para la mayoría de las cargas de trabajo, habilitar la compresión y deduplicación no afectará negativamente al rendimiento del sistema de archivos. En la mayoría de las cargas de trabajo, la compresión aumenta el rendimiento general. Para permitir lecturas y escrituras rápidas desde la caché RAM, FSx los servidores de archivos ONTAP están equipados con niveles de ancho de banda de red más altos en las tarjetas de interfaz de red front-end (NICs) que los disponibles entre los servidores de archivos y los discos de almacenamiento. Dado que la compresión de datos reduce la cantidad de datos que se envían entre los servidores de archivos y los discos de almacenamiento, en la mayoría de las cargas de trabajo, verá un aumento en la capacidad de rendimiento general del

sistema de archivos al usar la compresión de datos. Los aumentos de la capacidad de rendimiento relacionados con la compresión de datos se limitarán una vez que se sature la NIC front-end del sistema de archivos.

Amazon FSx for NetApp ONTAP también es compatible con otras ONTAP funciones que le permiten ahorrar espacio, incluidas 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 la cantidad de ahorro de almacenamiento en un sistema de archivos con la eficiencia de almacenamiento habilitada, consulte [Supervisión del ahorro de eficiencia de almacenamiento](#).

Cálculo del ahorro de eficiencia de almacenamiento

Puede utilizar las métricas del sistema de CloudWatch archivos LogicalDataStored y StorageUsed FSx para ONTAP para calcular el ahorro de almacenamiento derivado de la compresión, la deduplicación, la compactación, las instantáneas y FlexClones. Estas métricas tienen una sola 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 periodo determinado y reste Average del LogicalDataStored mismo periodo. A continuación, divida la diferencia entre Average de LogicalDataStored durante el mismo periodo.

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 TiB) de los datos se agrupan automáticamente en el nivel del grupo de capacidad y el 20% restante (20 TiB) permanece

en el 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 aprovisiona 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 FSx para ONTAP, se especifica la capacidad de almacenamiento del nivel de SSD. En el caso de los sistemas de archivos Single-AZ de segunda generación, 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 aprovisiona, Amazon aprovisiona FSx automáticamente 3 operaciones de entrada/salida de SSD por segundo (IOPS) 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 Single-AZ de segunda generación, las IOPS en SSD se distribuyen de manera 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 ONTAP, consulte FSx [Impacto de la capacidad de rendimiento en el rendimiento](#)

Temas

- [Actualización del almacenamiento en SSD e IOPS del sistema de archivos](#)
- [Crear una alarma de utilización de la capacidad de almacenamiento para el sistema de archivos](#)
- [Actualización de la capacidad de almacenamiento y las IOPS aprovisionadas](#)
- [Actualización dinámica de la capacidad de almacenamiento](#)

- [Supervisión de la utilización del almacenamiento en SSD](#)
- [Supervisión del ahorro de eficiencia de almacenamiento](#)
- [Monitoreo de la capacidad de almacenamiento y las actualizaciones de IOPS](#)

Actualización del almacenamiento en SSD e IOPS del sistema de archivos

Cuando necesites almacenamiento adicional para la parte activa de tu conjunto de datos, puedes aumentar la capacidad de almacenamiento en SSD de tu sistema de archivos Amazon FSx for NetApp ONTAP. Usa la FSx consola de Amazon, la FSx API de Amazon o AWS Command Line Interface (AWS CLI) para aumentar la capacidad de almacenamiento de la SSD. Para obtener más información, consulte [Actualización de la capacidad de almacenamiento y las IOPS aprovisionadas](#).

Cuando aumentas la capacidad de almacenamiento SSD de tu sistema de FSx archivos de Amazon, 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, consulta 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 FSx consola, la CLI y la API de Amazon. 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 de la 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 ser como mínimo del 10 % de la capacidad de almacenamiento en SSD actual del sistema de archivos y debe llegar hasta la capacidad de almacenamiento en SSD máxima de la configuración del sistema de archivos.

- (Solo sistemas de archivos Single-AZ de segunda generación) Distribución de la capacidad de almacenamiento: la nueva capacidad de almacenamiento o IOPS en SSD que seleccione para el 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 escala FSx 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 FSx para su sistema de archivos 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, consulta los [precios de Amazon FSx for NetApp ONTAP](#).

¿Cuándo aumentar la capacidad de almacenamiento en 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 de segunda generación, 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](#).

Crear una alarma de utilización de la capacidad de almacenamiento para el sistema de archivos

Le recomendamos que no supere el 80 % de utilización media de la capacidad de almacenamiento en 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 de su sistema de archivos se acerca al 80%.

Cómo crear una alarma de utilización de la capacidad de almacenamiento del sistema de archivos

Puede utilizar la `StorageCapacityUtilization` métrica para crear una alarma que se active cuando uno o varios de sus sistemas de archivos FSx de ONTAP hayan alcanzado un umbral de utilización del almacenamiento.

1. Abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>
2. En el panel de navegación izquierdo, en Alarmas, seleccione Todas las alarmas. A continuación, seleccione Crear alarma. En el asistente de creación de alarmas, seleccione Seleccionar métrica.
3. En el explorador de gráficos, seleccione la pestaña Consulta de múltiples fuentes.

4. En el generador de consultas, seleccione lo siguiente:
 - Para Namespace, selecciona AWS/FSx> Métricas detalladas del sistema de archivos.
 - Para el nombre de la métrica, seleccione MAX (StorageCapacityUtilization).
 - En Filtrar por, si lo desea, puede incluir o excluir sistemas de archivos específicos por su identificador. Si deja la opción Filtrar por vacía, la alarma se activará cuando alguno de los sistemas de archivos supere el umbral de utilización de la capacidad de almacenamiento de la alarma.
 - Deje el resto de las opciones vacías y seleccione Consulta de gráficos.
5. Elija Seleccionar métrica. Al volver al asistente, en la sección Métricas, asigne una etiqueta a su métrica. Recomendamos mantener el periodo en 5 minutos.
6. En Condiciones, seleccione el Tipo de umbral estático siempre que la métrica sea Mayor o igual a 80.
7. Seleccione Siguiente para ir a la página Configurar acciones.

Cómo configurar acciones de alarma

Puede configurar una variedad de acciones para que la alarma se active cuando alcance el umbral que haya configurado. En este ejemplo, elegimos un tema del Simple Notification Service (SNS), pero puedes obtener más información sobre otras acciones en Uso de alarmas de [Amazon en la Guía del CloudWatch usuario](#) de Amazon. CloudWatch

1. En la sección Notificación, seleccione un tema del SNS al que desee enviar la notificación cuando la alarma tenga el estado ALARM. Puede elegir un tema existente o crear uno nuevo. Recibirá una notificación de suscripción que deberá confirmar antes de recibir las notificaciones de alarma en la dirección de correo electrónico.
2. Elija Siguiente.

Cómo finalizar la alarma

Sigue estas instrucciones para completar el proceso de creación de la CloudWatch alarma.

1. En la página Agregar nombre y descripción, asigne un nombre a la alarma y, si lo desea, una descripción y, a continuación, seleccione Siguiente.
2. Revise todo lo que ha configurado en la página Vista previa y creación y, a continuación, seleccione Crear alarma.

Actualización de la capacidad de almacenamiento 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 FSx consola Amazon, la y la API AWS CLI.

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

1. Abre la FSx consola de Amazon en <https://console.aws.amazon.com/fsx/>.
2. En el panel de navegación, elija Sistemas de archivos. En la lista de sistemas de archivos, seleccione el sistema de archivos ONTAP FSx para el que desee actualizar la capacidad de almacenamiento de la SSD y las IOPS de la SSD.
3. En Actions (Acciones), seleccione Update storage capacity (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 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 Porcentaje.
 - Para introducir el nuevo valor en GiB, elija 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 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 quieres que Amazon FSx escale automáticamente las IOPS de tu SSD para mantener 3 IOPS de SSD aprovisionadas por GiB de capacidad de almacenamiento SSD (hasta un máximo de 160 000), selecciona 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 FSx para su sistema de archivos de ONTAP, consulte. [Impacto de la capacidad de rendimiento en el rendimiento](#)

8. Elija Actualizar.

 Note

En la parte inferior de la petición, se muestra una vista previa de la configuración de la nueva capacidad de almacenamiento en SSD y de las IOPS en SSD. Para los sistemas de archivos de segunda generación, también se muestra el per-HA-pair valor.

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

Para actualizar la capacidad de almacenamiento de la SSD y las IOPS aprovisionadas FSx para un sistema de archivos compatible con ONTAP, utilice el AWS CLI comando [update-file-system](#) o la acción de API equivalente. [UpdateFileSystem](#) Establezca 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 en SSD, establezca `--storage-capacity` en un valor de capacidad de almacenamiento de destino que sea al menos un 10 % 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 IOPS valor debe ser superior o igual a tres veces la capacidad de almacenamiento de la SSD actual.
 - Si quieres que Amazon FSx aumente automáticamente las IOPS de tu SSD, usa `Mode=AUTOMATIC` y no uses el `Iops` parámetro. 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 FSx para su sistema de archivos ONTAP, consulte. [Impacto de la capacidad de rendimiento en el rendimiento](#)

En el siguiente ejemplo, se aumenta el almacenamiento en SSD del sistema de archivos a 2000 GiB y se establece la cantidad de IOPS en 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 [describe-file-systems](#) AWS CLI comando. Busque la sección `AdministrativeActions` en la salida.

Para obtener más información, consulte la referencia [AdministrativeAction](#) de la API de Amazon FSx for NetApp ONTAP.

Actualización dinámica de la capacidad de almacenamiento

Puede utilizar la siguiente solución para aumentar de forma dinámica la capacidad de almacenamiento en SSD de un FSx sistema de archivos de ONTAP cuando la cantidad de capacidad de almacenamiento en SSD utilizada supere el 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:

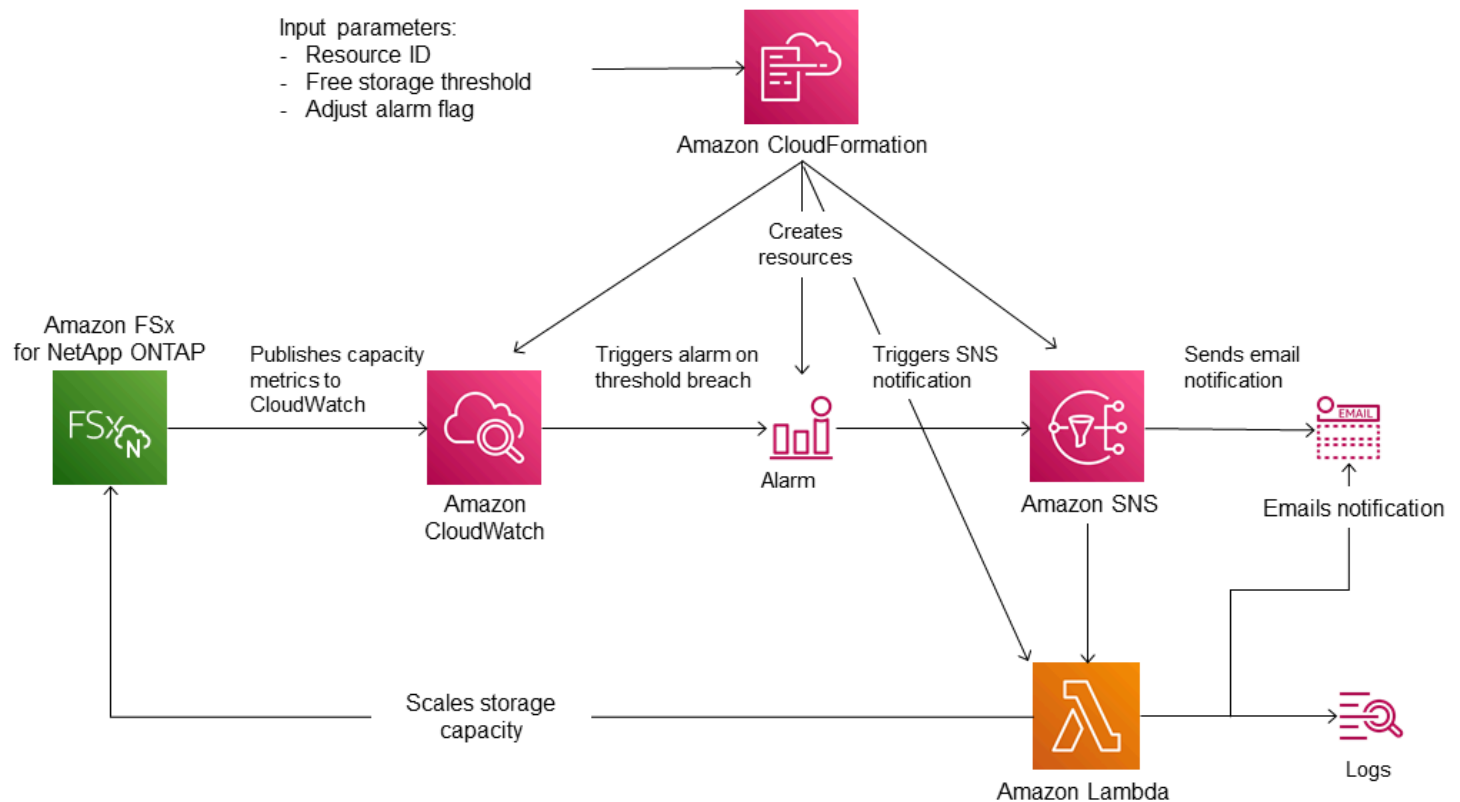
- Su ID FSx del sistema de archivos de ONTAP.
- El umbral de capacidad de almacenamiento de la SSD utilizada (valor numérico). Este es el porcentaje en el que se activará la CloudWatch alarma.
- El porcentaje en el que se va a aumentar la capacidad de almacenamiento (%).
- La dirección de correo electrónico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

Temas

- [Información general de la arquitectura](#)
- [AWS CloudFormation plantilla](#)
- [Despliegue automatizado con AWS CloudFormation](#)

Información general de la arquitectura

Al implementar esta solución, se crean 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 da permiso a la función Lambda para invocar las operaciones de la API de FSx Amazon.
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 el despliegue de los componentes que se utilizan para aumentar automáticamente la capacidad de almacenamiento de un FSx sistema de archivos de ONTAP. Para utilizar esta solución, descargue la [FSxOntapDynamicStorageScaling](#) AWS CloudFormation plantilla.

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.

Máximo FSx SizeinGi B

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 de 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 AWS CloudFormation usuario.

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 FSx archivos de Amazon que se ejecuta en la Amazon Virtual Private Cloud (Amazon VPC) en su. Cuenta de AWS Para obtener más información sobre la creación de FSx recursos de Amazon, consulte [Cómo empezar a usar Amazon FSx for NetApp ONTAP](#).

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

1. Descargue la plantilla de [FSxOntapDynamicStorageScaling](#) AWS CloudFormation .

Note

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

obtener más información, consulta los [FSx puntos de conexión y las cuotas de Amazon](#) en. Referencia general de AWS

2. En la AWS CloudFormation consola, selecciona 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.

Stack name

Stack name

FsxN-Storage-Scaling

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

Dynamic Storage Scaling Parameters

File system ID
Amazon FSx file system ID

fs-0123456789abcd

Threshold
Used storage capacity threshold (%)

70

Percentage Capacity Increase
The percentage increase in storage capacity when used storage exceeds LowFreeDataStorageCapacityThreshold. Minimum increase is 10 %

20

Email address
The email address for alarm notification.

storagescaler@example.com

Maximum supported file system storage capacity (DO NOT MODIFY)
Maximum size supported for the primary SSD storage tier.

196608

Cancel Previous **Next**

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 .

Supervisión de la utilización del almacenamiento en SSD

Puede monitorizar 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 almacenamiento en SSD e IOPS del sistema de archivos](#).

Puedes ver el almacenamiento SSD disponible de un sistema de archivos y la distribución general del almacenamiento en la FSx consola de Amazon. El gráfico de Capacidad de almacenamiento principal 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

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

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

1. Abre la FSx consola de Amazon en <https://console.aws.amazon.com/fsx/>.
2. Selecciona Sistemas de archivos en la columna de navegación de la izquierda y, a continuación, selecciona ONTAP sistema de archivos del que desea ver la información sobre la capacidad de almacenamiento. Aparece la página de detalles del sistema de archivos.
3. En el segundo panel, seleccione la pestaña Supervisión y rendimiento y, a continuación, seleccione Almacenamiento. Se muestran los gráficos de capacidad de almacenamiento principal disponible y de utilización de la capacidad de almacenamiento por agregado.

Supervisión del ahorro de eficiencia de almacenamiento

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

Cómo ver los ahorros en eficiencia de almacenamiento (consola)

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

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

2. Seleccione en la lista FSx de sistemas de archivos el sistema de archivos de ONTAP en el que desee ver la eficiencia de almacenamiento ahorrando.
3. Seleccione Resumen en la Supervisión y rendimiento en el 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 la eficiencia del almacenamiento (ONTAP CLI)

La eficiencia del almacenamiento se reduce simplemente con la compactación, la compresión y la deduplicación, sin los efectos de las instantáneas y FlexClones — ejecutando el comando mediante `storage aggregate show-efficiency` ONTAP CLI. Para obtener más información, consulte la sección sobre la [eficiencia de los agregados de almacenamiento](#) en NetApp ONTAP Centro de documentación.

1. Para acceder al ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando. 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 [Administrar sistemas de archivos con el ONTAP CLI](#).

2. El comando `storage aggregate show-efficiency` muestra información sobre la eficiencia del almacenamiento de todos los agregados. La eficiencia del almacenamiento se muestra en cuatro niveles diferentes:
 - Total
 - Agregado
 - Volumen
 - Instantánea y volumen FlexClone

```
::*> 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
```

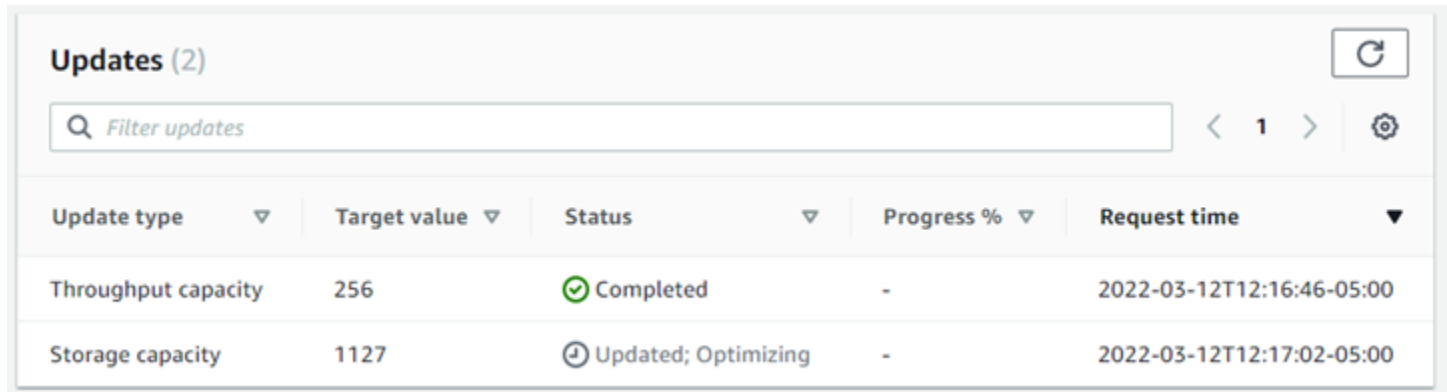
```
Number of Efficiency Disabled Volumes: 1
```

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 FSx consola, la CLI y la API de Amazon.

Cómo supervisar las actualizaciones del almacenamiento y de las IOPS (consola)

En la pestaña Actualizaciones de la página de detalles del sistema de archivos de su FSx sistema de archivos de ONTAP, puede ver las 10 actualizaciones más recientes de cada tipo de actualización.



Update type	Target value	Status	Progress %	Request time
Throughput capacity	256	Completed	-	2022-03-12T12:16:46-05:00
Storage capacity	1127	Updated; Optimizing	-	2022-03-12T12:17:02-05:00

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.

Estado

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

- **Pendiente:** Amazon FSx ha recibido 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 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.

Cómo supervisar las actualizaciones del almacenamiento y de las IOPS (CLI)

Puede ver y monitorear las solicitudes de aumento de la capacidad de almacenamiento SSD del sistema de archivos mediante el [describe-file-systems](#) AWS CLI comando y la operación de la [DescribeFileSystems](#) API. 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 FILE_SYSTEM_UPDATE acción y añade los nuevos discos de almacenamiento 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 STORAGE_OPTIMIZATION administrativa. 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"
    }
  }
]

```

Capacidad de almacenamiento de volumen

FSx en el caso de ONTAP, los volúmenes son recursos virtuales que se utilizan para agrupar los datos, determinar cómo se almacenan los datos y determinar el tipo de acceso a los mismos. 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 volúmenes FSx de ONTAP mediante la AWS Management Console API AWS CLI y 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](#)
- [Administración de la eficiencia de almacenamiento](#)
- [Habilitación del ajuste de tamaño automático](#)
- [Habilitación del modo de escritura en la nube](#)
- [Actualización de la capacidad de almacenamiento](#)
- [Actualización de una política de estratificación](#)
- [Actualización de días mínimos de enfriamiento](#)
- [Actualización de la política de recuperación de un volumen en la nube](#)
- [Actualización de la cantidad máxima de archivos en un volumen](#)
- [Supervisión de la capacidad de almacenamiento de volumen](#)
- [Supervisión de la capacidad de archivos de un volumen](#)

Organización de datos de volumen en niveles

Un sistema de archivos Amazon FSx for 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 periodo de enfriamiento y la configuración de los umbrales. En las siguientes secciones, se describen las políticas de estratificación del volumen y los umbrales de ONTAP que se usan para determinar cuándo se agrupan los datos según el grupo de capacidad.

Note

FSx for ONTAP permite agrupar los datos en niveles en el conjunto de capacidades de todos los SnapLock volúmenes, independientemente del tipo. SnapLock Para obtener más información, consulte [Cómo SnapLock funciona](#).

Políticas de estratificación del volumen

Para determinar cómo utilizar los niveles de almacenamiento del sistema de archivos de ONTAP, elija la política de estratificación de cada volumen del sistema de archivos. FSx Usted elige la política de organización en niveles al crear un volumen y puede modificarla en cualquier momento con la FSx consola de Amazon AWS CLI, la API o mediante [herramientas NetApp 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 FSx consola de Amazon.
- **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 FSx API de Amazon 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. Si la política Todo se aplica a un volumen que ya contiene datos, los datos existentes se agrupan en niveles desde el SSD hasta el grupo de capacidad. 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 estableces un volumen con esta política después de usar cualquier otra política, los datos existentes (incluidas las instantáneas) del volumen que estaba en el grupo de almacenamiento de capacidad se trasladan al almacenamiento SSD mediante un proceso en segundo plano. Esta migración de datos solo se produce cuando el uso de la SSD es inferior al 90% y la política de recuperación de datos en la nube está configurada en o. promote on-read Este proceso en segundo plano se puede acelerar leyendo los datos de forma intencionada. Para obtener más información, consulte [Políticas de recuperación en la nube](#).

Para obtener más información sobre cómo configurar o modificar la política de organización por niveles de un volumen, consulte [Actualización de una política de estratificación](#).

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 estratificación automática, los datos se almacenan en el nivel de almacenamiento en SSD durante un mínimo de 2 días (en función del periodo de refrigeración del volumen) antes de pasar al nivel del grupo de capacidad. ONTAP ejecuta periódicamente la deduplicación posterior al proceso de los datos almacenados en el nivel de almacenamiento en SSD. Para ello, se ajusta automáticamente la frecuencia en función de la velocidad de cambio de los datos en el volumen; las velocidades más altas provocan tareas de deduplicación posteriores al proceso con mayor frecuencia.

De forma predeterminada, la compresión posterior al proceso está desactivada en ONTAP debido al impacto que puede tener en el rendimiento de las cargas de trabajo continuas del sistema de archivos. Debe evaluar el impacto en el rendimiento de la carga de trabajo antes de habilitar la compresión posterior al proceso. Para habilitar la compresión posterior al proceso, asuma el nivel de privilegio de diagnóstico en la CLI de ONTAP y ejecute el siguiente comando:

```
::> volume efficiency inactive-data-compression modify -vserver svm-name -volume vol-name -is-enabled true
```

ONTAP ejecuta la compresión posterior al proceso para los datos que se retienen en el almacenamiento en SSD durante un mínimo de 14 días. En el caso de las cargas de trabajo en las

que es poco probable que se pueda acceder a los datos después de un periodo más corto, puede modificar la configuración de compresión posterior al proceso para ejecutarla antes. Por ejemplo, para aplicar los ahorros de compresión posterior al proceso a los datos a los que no se ha accedido durante 5 días, ejecute el siguiente comando de la CLI de ONTAP:

```
::> volume efficiency inactive-data-compression modify -vserver svm-name -volume vol-name -threshold-days 5 -threshold-days-min 2 -threshold-days-max 14
```

Para obtener más información sobre el comando, consulte [inactive-data-compression](#) [modificar la eficiencia del volumen](#)

Al retener los datos en la SSD, se maximizan las velocidades de transferencia de las copias de seguridad del volumen que se crean, ya que las velocidades de transferencia de datos son más altas en el almacenamiento en SSD.

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 [Actualización de 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 [Actualización de la política de recuperación de un volumen en la nube](#).

Umbrales de niveles

La utilización de la capacidad de almacenamiento en SSD de un sistema de archivos determina la forma en que ONTAP administra el comportamiento de estratificación 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 de 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 de segunda generación, 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 almacenamiento en SSD e IOPS del sistema de archivos](#).

FSx ya que 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 [Protección de los datos con instantáneas](#).

Capacidad de archivos de volumen

Los volúmenes de Amazon FSx for NetApp ONTAP tienen punteros de archivos que se utilizan para almacenar metadatos de 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. La cantidad de inodos en un volumen aumenta proporcionalmente a la capacidad de almacenamiento del volumen (y a la cantidad de componentes de volumen de los volúmenes FlexGroup). De forma predeterminada, los volúmenes FlexVol (o componentes FlexGroup) con una capacidad de almacenamiento de 648 GiB o más tienen todos la misma cantidad 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 cómo ver la cantidad máxima de archivos de un volumen, consulte [Supervisión 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 $\times$ (1 archivo $\div$ inode_size_in_bytes) = maximum_number_of_files

1 073 741 824 bytes $\times$ (1 archivo $\div$ 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 $\times$ (1 archivo $\div$ 4096 bytes) = 262 144 archivos

Un volumen FSx de ONTAP puede tener un máximo de 2 000 millones de inodos.

Para obtener información sobre cómo cambiar la cantidad máxima de archivos que puede almacenar un volumen, consulte [Actualización de la cantidad máxima de archivos en un volumen](#).

Administración de la eficiencia de almacenamiento

Al aumentar la eficiencia del almacenamiento en sus volúmenes FSx de ONTAP, puede optimizar la utilización del almacenamiento, reducir los costes de almacenamiento y mejorar el rendimiento general de su sistema de archivos.

ONTAP organiza los archivos en bloques de datos de 4 kibibytes (KiB). La eficiencia del almacenamiento se produce en el bloque de datos y no en archivos individuales. Cuando se habilita la eficiencia del almacenamiento, ONTAP emplea una combinación de técnicas de reducción de datos para eliminar los datos duplicados, reducir el tamaño de los datos y reorganizar el diseño de los datos para un uso óptimo del disco.

La eficiencia de almacenamiento se aplica de dos formas. Se aplican a los datos en línea (antes de que los datos se escriban en el disco, en la memoria) para generar ahorros de almacenamiento inmediatos. También se aplican a los datos en segundo plano (después de que se hayan escrito en el disco) en el nivel de almacenamiento en SSD mediante tareas periódicas de eficiencia para optimizar la utilización del almacenamiento a lo largo del tiempo. La eficiencia del almacenamiento en segundo plano no se basa en los datos una vez que están estratificados en el grupo de capacidad. Sin embargo, si los datos ahorraron espacio de almacenamiento mientras estaban en la SSD, estos ahorros se conservan cuando los datos se agrupan en niveles según el grupo de capacidad.

Note

ONTAP no permite aumentar la eficiencia del almacenamiento en los volúmenes de protección de datos (DP). Sin embargo, los ahorros de almacenamiento logrados en el

volumen de lectura y escritura (RW) de origen se conservan cuando los datos se replican en el volumen DP de destino.

Compresión de bloques de datos

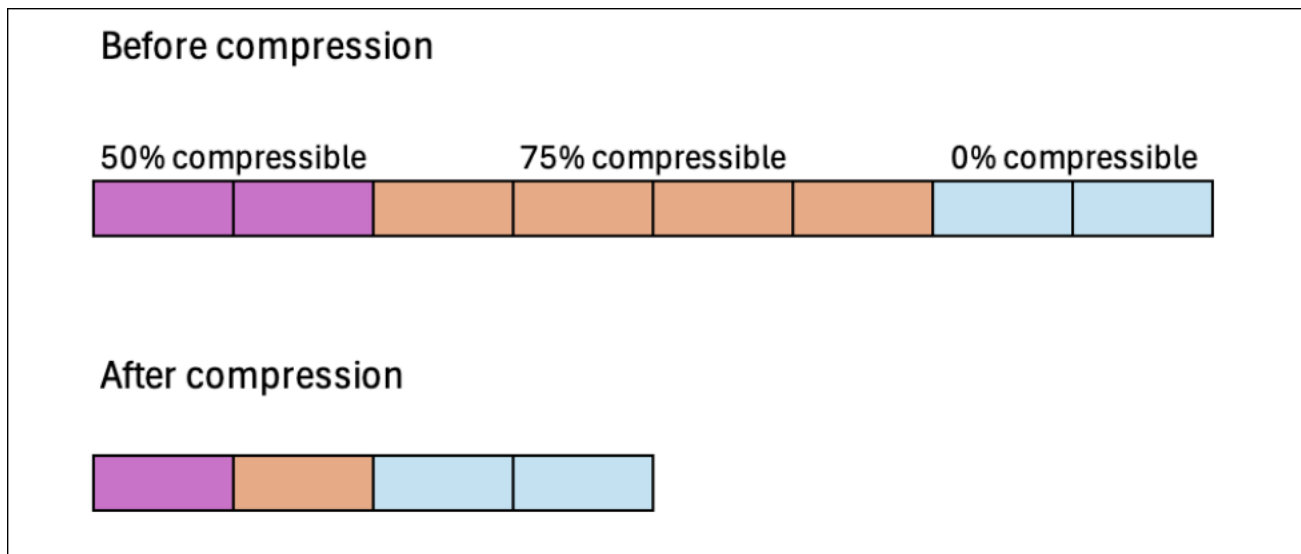
Los grupos de compresión son agrupaciones lógicas de datos que se administran y comprimen juntas como un solo bloque. ONTAP empaqueta automáticamente los bloques de datos en grupos de compresión, lo que reduce el espacio consumido en el disco. Para optimizar el rendimiento y la utilización del almacenamiento, ONTAP ofrece un enfoque equilibrado de la administración de datos mediante el ajuste del grado de compresión que se aplica a los datos en función de los patrones de acceso.

De forma predeterminada, los datos se comprimen en línea mediante grupos de compresión de 8 KB para garantizar un rendimiento óptimo al escribir datos en un volumen. Si lo desea, puede aplicar una compresión más intensa a los datos activando la compresión de datos inactivos en un volumen para comprimir aún más los datos en la SSD. La compresión de datos inactivos usa grupos de compresión de 32 KB en datos inactivos para ahorrar espacio de almacenamiento adicional. Para obtener más información, consulte el comando [volume efficiency inactive-data-compression modify](#) en el NetApp ONTAP Documentation Center.

Note

La compresión de datos inactivos consume IOPS adicionales de CPU y disco y puede ser una tarea que requiera muchos recursos. Le recomendamos que evalúe el impacto que tiene en el rendimiento la ejecución de una compresión de datos inactivos en la carga de trabajo antes de habilitar esta característica.

En la siguiente imagen, se ilustran los ahorros de almacenamiento que se pueden lograr al comprimir bloques de datos.



Desduplicación de bloques de datos

ONTAP detecta y elimina los bloques de datos duplicados para reducir las redundancias en los datos. Los bloques duplicados se sustituyen por referencias a bloques únicos compartidos.

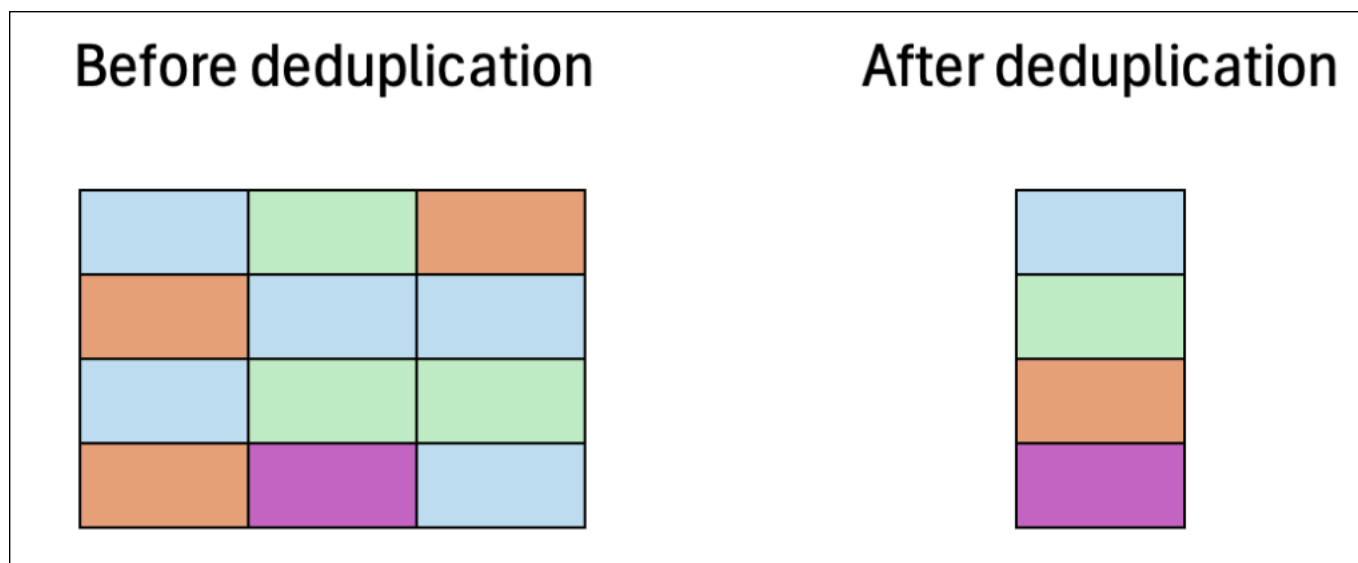
De forma predeterminada, los datos se deduplican en línea para reducir el espacio de almacenamiento antes de que los datos se escriban en el disco. ONTAP también ejecuta un escáner de deduplicación en segundo plano a intervalos específicos para identificar y eliminar los datos duplicados una vez escritos en el disco. Durante estos escaneos programados, ONTAP procesa un registro de cambios para identificar bloques de datos nuevos o modificados desde el último escaneo que aún no se han deduplicado. Cuando se encuentran duplicados, ONTAP actualiza los metadatos para que apunten a una sola copia de los bloques duplicados y marca los bloques redundantes como espacio libre listo para recuperarse.

Note

ONTAP aplica la deduplicación a 4 KB de escrituras entrantes a la vez, por lo que es posible que ahorre menos con la deduplicación al ejecutar cargas de trabajo con escrituras de menos de 4 KB.

FSx ya que ONTAP no admite la deduplicación entre volúmenes.

En la siguiente imagen, se ilustran los ahorros de almacenamiento que se pueden lograr con la deduplicación.

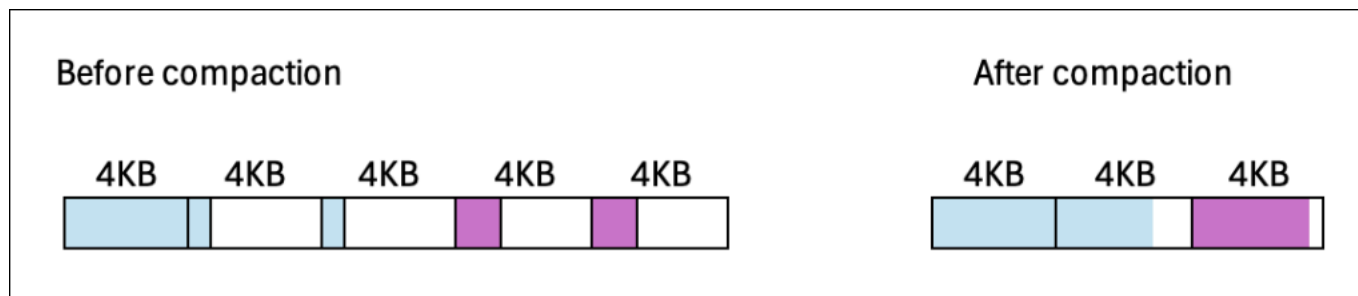


Compactación de bloques de datos

ONTAP consolida bloques de datos parcialmente ocupados de menos de 4 KB cada uno en un bloque de 4 KB usado de manera más eficiente.

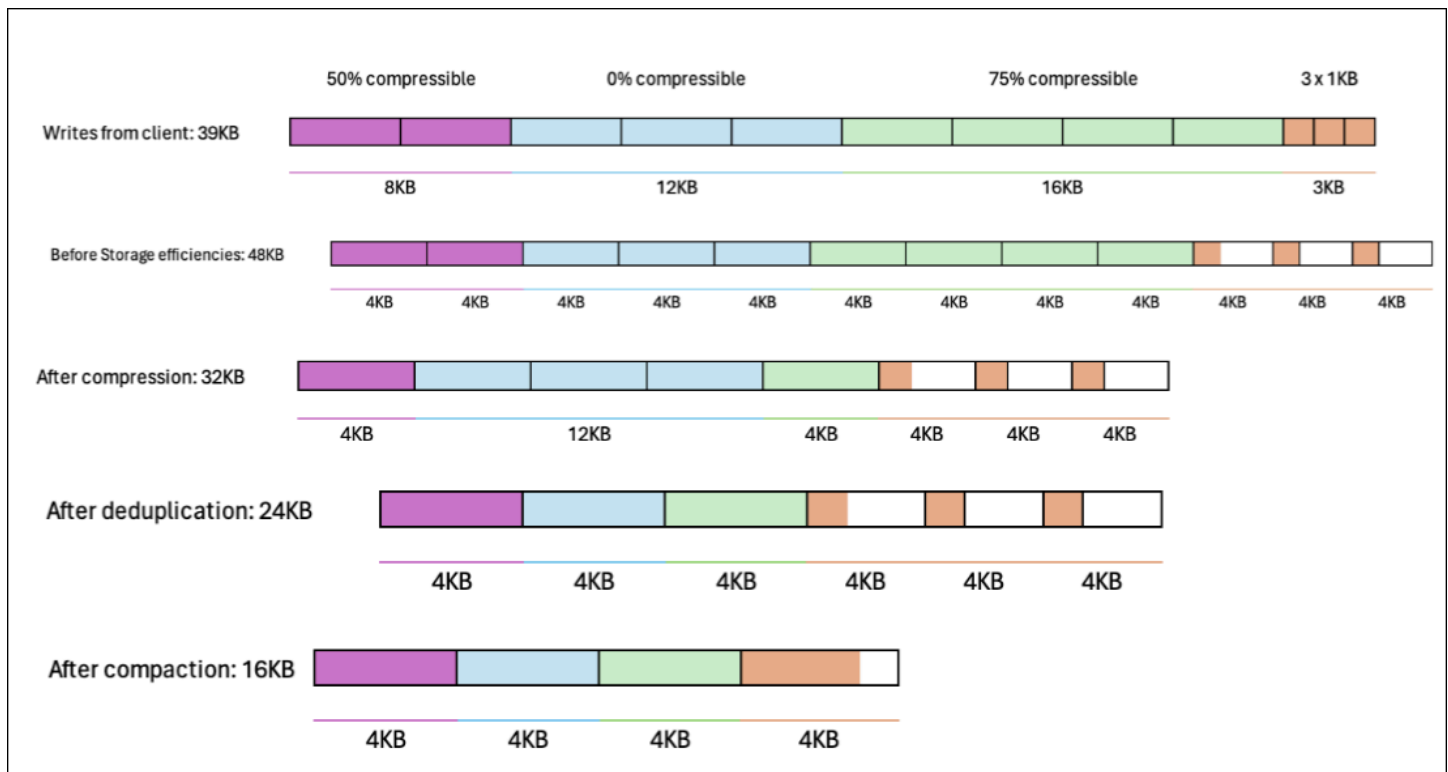
De forma predeterminada, los datos se compactan en línea para optimizar el diseño de los datos a medida que se escriben en el disco para minimizar la sobrecarga de almacenamiento, reducir la fragmentación y mejorar el rendimiento de lectura.

En la siguiente imagen, se ilustran los ahorros de almacenamiento que se pueden lograr con la compactación.



Ejemplo: eficiencia del almacenamiento

En la siguiente imagen, se ilustra cómo se aplican las eficiencias del almacenamiento a los datos.



Habilitación del ajuste de tamaño automático

Se usa el ajuste de tamaño automático de volumen para que este aumente automáticamente hasta un tamaño especificado cuando alcance un umbral de espacio usado. Puede hacerlo para los tipos de FlexVol volumen (el tipo de volumen predeterminado FSx para ONTAP) mediante el comando `volume autosize` CLI de ONTAP.

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

1. Para acceder a la ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando. 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 [Administrar sistemas de archivos con el 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.
- *min_size* Sustitúyalo por el tamaño mínimo al que se reducirá el volumen. Utilice el mismo formato que para *max_size*.
- *shrink_threshold* Sustitúyalo por el porcentaje de espacio utilizado al que el volumen se reducirá automáticamente.

```
::> 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
```

3. Para mostrar la configuración de tamaño automático actual, ejecute el siguiente comando. Reemplace el *svm_name* y el *vol_name* con su información.

```
::> volume autosize -vserver svm_name -volume vol_name
```

Habilitación del modo de escritura en la nube

Use el comando `volume modify` de la CLI de ONTAP para habilitar o deshabilitar el modo de escritura en la nube de 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 los siguientes:

- El volumen debe ser un volumen existente. Solo puede activar la característica en un volumen existente.
- El volumen debe ser de lectura y escritura (RW).
- El volumen debe tener la política de estratificación de todos. Para obtener más información sobre cómo modificar la política de estratificación de un volumen, consulte [Actualización de una política de estratificación](#).

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.

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

1. Para acceder a la ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando. 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 [Administrar sistemas de archivos con el 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. Use el siguiente comando para establecer el modo de escritura en la nube 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 el modo de escritura en la nube.
 - Sustituya el *vol_cw_mode* por `true` 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.
```

Actualización de la capacidad de almacenamiento

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.

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

- Puedes aumentar o disminuir la capacidad de almacenamiento de un volumen mediante la FSx consola y la API de Amazon. AWS CLI Para obtener más información, consulte [Actualización de volúmenes](#).

También puede usar la CLI de ONTAP para modificar la capacidad de almacenamiento de un volumen mediante el comando [volume modify](#).

Cómo modificar el tamaño de un volumen (CLI de ONTAP)

1. Para acceder a la ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando. 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 [Administrar sistemas de archivos con el ONTAP CLI](#).

2. Use el comando `volume modify` de la CLI de ONTAP para modificar la capacidad de almacenamiento de un volumen. Ejecute el siguiente comando usando los datos en lugar de los siguientes valores:
 - Reemplace *svm_name* con el nombre de la máquina virtual de almacenamiento (SVM) en el que se crea el volumen.
 - Reemplace *vol_name* con 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
```

Actualización de una política de estratificación

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

Cómo 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 FSx consola de Amazon 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 del volumen](#).
5. Seleccione Update (Actualizar) para aplicar la nueva política al volumen.

Cómo establecer la política de agrupamiento por nivel de un volumen (CLI)

- Modifique la política de estratificación de un volumen mediante el comando CLI [update-volume UpdateVolume](#) (es la acción equivalente de la API de FSx Amazon). 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"
  }
}

```

Cómo 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 [volume modify](#) de NetApp ONTAP.

1. Para acceder a la ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando. 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 [Administrar sistemas de archivos con el 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 del volumen](#).

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

Actualización de 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.

Cómo establecer los días mínimos de enfriamiento de un volumen (CLI)

- Modifique la configuración de un volumen mediante el comando [CLI update-volume](#) ([UpdateVolume](#) es la acción equivalente de la FSx API de Amazon). 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"
  }
}
```

Cómo 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 [volume modify](#) de documentación de NetApp ONTAP.

1. Para acceder a la ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando. 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 [Administrar sistemas de archivos con el 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.
```

Actualización de 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.

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

1. Para acceder a la ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando.

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 [Administrar sistemas de archivos con el 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.
```

Actualización de la cantidad máxima de archivos en un volumen

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

Cómo aumentar la cantidad máxima de archivos de un volumen (CLI de ONTAP)

Use el comando `volume modify` de la CLI de ONTAP para aumentar la cantidad máxima de archivos de un volumen. Para obtener más información, consulte [volume modify](#) en el centro de documentación de NetApp ONTAP.

1. Para acceder a la ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando. 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 [Administrar sistemas de archivos con el 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
```

Supervisión de la capacidad de almacenamiento de 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.

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

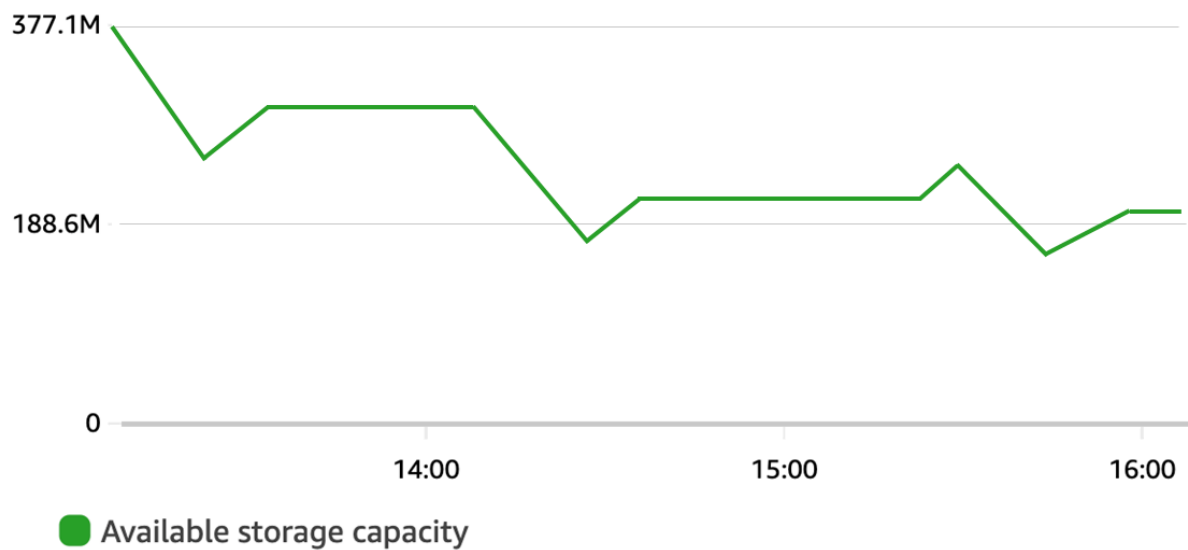
El gráfico de Almacenamiento disponible muestra la cantidad de capacidad de almacenamiento libre de un volumen a lo largo del tiempo. El gráfico Distribución del almacenamiento muestra cómo se distribuye actualmente la capacidad de almacenamiento de un volumen en 4 categorías:

- Datos de usuario
- Datos instantáneos
- Capacidad de volumen disponible
- Otros datos

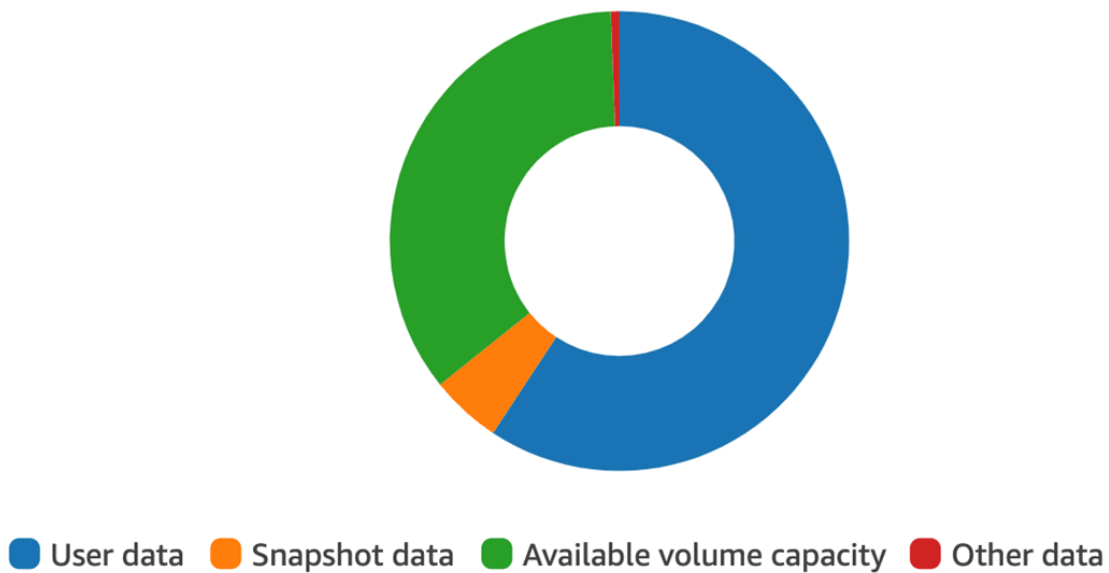
1. Abre la FSx consola de Amazon en <https://console.aws.amazon.com/fsx/>.
2. Seleccione Volumes (Volúmenes) en la columna de navegación de la izquierda y, a continuación, elija el volumen de ONTAP del que desee ver la información sobre la capacidad de almacenamiento. Aparece la página de detalles del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

Available storage capacity

No unit



Storage distribution



Cómo supervisar la capacidad de almacenamiento de un volumen (CLI de ONTAP)

Puede supervisar cómo se está consumiendo la capacidad de almacenamiento de su volumen usando el comando `volume show-space` de la CLI de ONTAP. Para obtener más información, consulte [volume show-space](#) en el centro de documentación de NetApp ONTAP.

1. Para acceder a la ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando. 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 [Administrar sistemas de archivos con el 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.

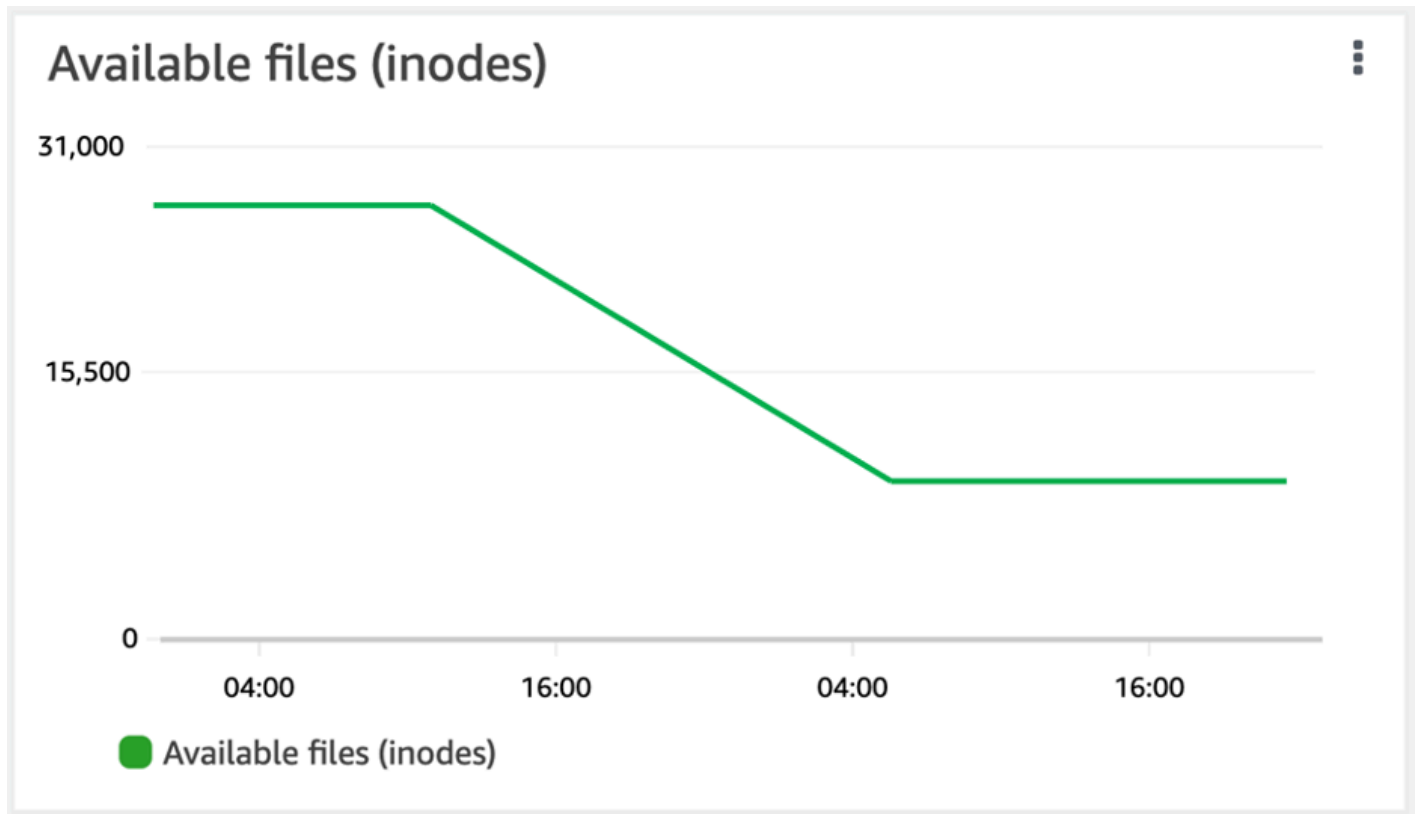
Para aumentar la cantidad de espacio disponible, puede [aumentar el tamaño](#) del volumen o [eliminar las instantáneas](#) que no esté utilizando, como se muestra en los procedimientos siguientes.

[Para los tipos de FlexVol volumen \(el tipo de volumen predeterminado FSx para los volúmenes de ONTAP\), 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.

Supervisión 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 métricas CloudWatch de volumen FilesCapacity y. FilesUsed
- En la FSx consola de Amazon, navega hasta el gráfico de archivos disponibles (inodos) en la pestaña Supervisión de tu volumen. La siguiente imagen muestra los archivos disponibles (inodos) en un volumen que disminuye con el tiempo.



Gestión de FSx sistemas de archivos ONTAP

Un sistema de archivos es el FSx recurso principal de Amazon, de forma análoga a un clúster ONTAP local. 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 de conexión de administración que puede usar para administrar recursos y datos con la CLI o la API de REST de ONTAP.

Recursos del sistema de archivos

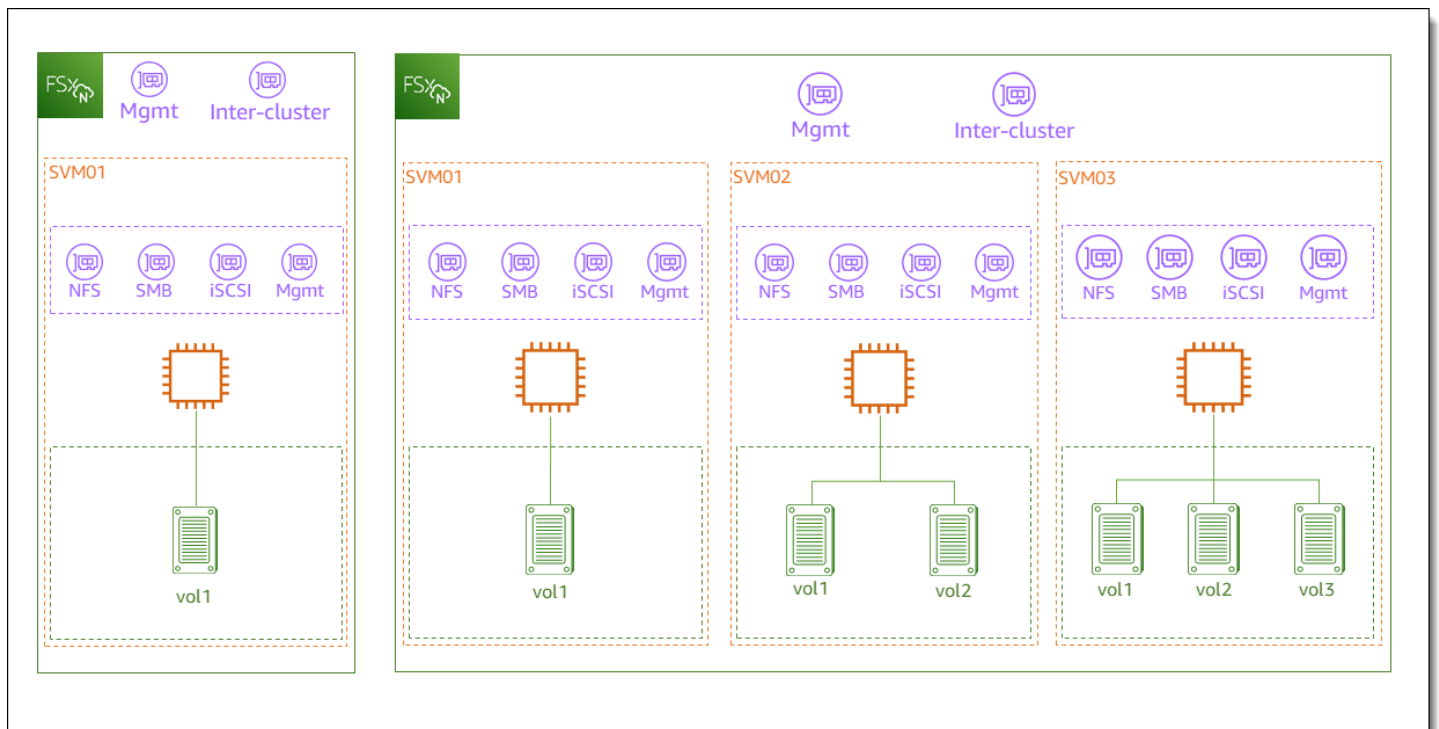
Un sistema de archivos de Amazon FSx for NetApp ONTAP se compone de los siguientes recursos principales:

- 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 (SVMs). Los sistemas de archivos de primera generación y los sistemas de archivos Multi-AZ de segunda generación tienen un par de HA, y los sistemas de

archivos Single-AZ de segunda generación tienen hasta 12 pares de HA. Cada par de HA tiene un grupo de almacenamiento denominado agregado. El conjunto de agregados de todos los pares de HA constituye el nivel de almacenamiento en SSD.

- Uno o varios SVMs que alojan los volúmenes del sistema de archivos y tienen sus propias credenciales y administración 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 sistema de archivos ONTAP de primera generación FSx con un par de alta disponibilidad y la relación entre sus recursos principales. El sistema FSx de archivos de ONTAP de la izquierda es el sistema de archivos más simple, con un SVM y un volumen. El sistema de archivos de la derecha tiene varios volúmenes SVMs, y algunos SVMs tienen varios volúmenes. SVMs Cada uno de los sistemas de archivos tiene varios puntos finales de administración y SVMs también puntos finales de acceso a los datos.



Al crear un sistema de archivos FSx para 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. Los sistemas de archivos Single-AZ de primera generación admiten un par de HA. Los sistemas de archivos Single-AZ de segunda generación admiten hasta 12 pares de HA. 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. Tanto los sistemas de archivos Multi-AZ de primera generación como los de segunda generación admiten un par de HA.

 Note

No puede cambiar el tipo de implementación del sistema de archivos después de su creación. Si desea cambiar el tipo de implementación (por ejemplo, pasar de Single-AZ 1 a Single-AZ 2), puede hacer una copia de seguridad de los datos y restaurarlos en un nuevo sistema de archivos. También puede migrar sus datos con NetApp SnapMirror AWS DataSync, con o con una herramienta de copia de datos de terceros. Para obtener más información, consulte [Migración a ONTAP mediante FSx NetApp SnapMirror](#) y [Migración a FSx ONTAP mediante AWS DataSync](#).

- Capacidad de almacenamiento: esta es la cantidad de almacenamiento en SSD, hasta 192 tebibytes (TiB) para los sistemas de archivos de primera generación, 512 TiB para los sistemas de archivos Multi-AZ de segunda generación y 1 pebibyte (PiB) para los sistemas de archivos Single-AZ de segunda generación.
- IOPS en SSD: de forma predeterminada, cada gigabyte de almacenamiento en SSD incluye tres IOPS en SSD (hasta el máximo admitido por 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 inactivos del sistema de archivos.
- 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 administrar los sistemas FSx de archivos de ONTAP mediante la NetApp CLI de ONTAP o la API REST. También puede configurar SnapMirror o establecer SnapVault relaciones entre un sistema de FSx archivos de Amazon y otro despliegue de ONTAP (incluido otro sistema de FSx archivos de Amazon). Cada sistema FSx de archivos de 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 FSx los recursos de ONTAP mediante NetApp aplicaciones](#) y [Replicar sus datos mediante NetApp SnapMirror](#).

Creación de sistemas de archivos

En esta sección se describe cómo crear un sistema de archivos FSx para ONTAP mediante la FSx consola de Amazon o la FSx API de Amazon. AWS CLI 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 ciertos aspectos al crear un sistema de archivos Multi-AZ en una VPC en la que participe. Estos aspectos se explican en este tema.

De forma predeterminada, al crear un nuevo sistema de archivos desde la FSx consola de Amazon, Amazon crea FSx automáticamente un sistema de archivos con una sola máquina virtual de almacenamiento (SVM) y un volumen, lo que permite un acceso rápido 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 volúmenes SVMs y adicionales según sea necesario.

Cómo crear un sistema de archivos (consola)

Este procedimiento utiliza la opción de creación estándar para crear un sistema de archivos FSx para ONTAP con una configuración que puede personalizar 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 [Cree un sistema de archivos Amazon FSx for NetApp ONTAP](#).

1. Abre la FSx consola de Amazon en <https://console.aws.amazon.com/fsx/>.
2. En el panel, 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 for NetApp ONTAP y, a continuación, elija Siguiente.
4. En la sección Método de creación, seleccione Crear estándar.

5. En la sección Información del sistema de archivos, proporcione 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: + - = . _ : /
- Para el tipo de implementación, elija Multi-AZ 2, Single-AZ 2, Multi-AZ 1 o Single-AZ 1.
 - 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. Multi-AZ 1 es una primera generación del sistema de archivos FSx ONTAP. Multi-AZ 2 es un sistema de archivos de segunda generación. Ambos admiten un par de alta disponibilidad (HA).
 - Los sistemas de archivos Single-AZ replican sus datos y ofrecen una conmutación por error automática dentro de una única zona de disponibilidad. El Single-AZ 1 es un sistema de archivos ONTAP FSx de primera generación que admite un par HA. Single-AZ 2 es un sistema de archivos de segunda generación que admite hasta 12 pares de HA. Para obtener más información, consulte [Administración de pares de alta disponibilidad \(HA\)](#).

Para obtener más información sobre los tipos de implementación, consulte [Opciones de disponibilidad, durabilidad e implementación](#).

 Note

No puede cambiar el tipo de implementación del sistema de archivos después de su creación. Si desea cambiar el tipo de implementación (por ejemplo, pasar de Single-AZ 1 a Single-AZ 2), puede hacer una copia de seguridad de los datos y restaurarlos en un nuevo sistema de archivos. También puede migrar sus datos con NetApp SnapMirror AWS DataSync, con o con una herramienta de copia de datos de terceros. Para obtener más información, consulte [Migración a ONTAP mediante FSx NetApp SnapMirror](#) y [Migración a FSx ONTAP mediante AWS DataSync](#).

- En SSD storage capacity, introduzca la capacidad de almacenamiento del sistema de archivos, en gibibytes (GiB). Introduzca cualquier número entero en el rango de 1024 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:
- Elige Automático (opción predeterminada) si quieres que Amazon FSx aprovisiona 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 en 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, tienes dos opciones para determinar tu capacidad de rendimiento en megabytes por segundo (): MBps
- Elige Capacidad de rendimiento recomendada si quieres que Amazon FSx elija automáticamente la capacidad de rendimiento en función de la cantidad de capacidad de almacenamiento que hayas elegido.
- Elija Especificar 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 implementación que haya elegido. También puede elegir el número de pares de HA (hasta 12). Para obtener más información, consulte [Administración de 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 el rendimiento de NetApp 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.
 - Para Grupos de seguridad de VPC, puede seleccionar un grupo de seguridad para asociar a la interfaz de red del sistema de archivos. Si no especificas ninguno, Amazon FSx asociará el grupo de seguridad predeterminado de la VPC a tu 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 rutas 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 rutas para sistemas de archivos Multi-AZ mediante la autenticación basada en etiquetas. Estas tablas de rutas se etiquetan con Key: AmazonFSx; Value: ManagedByAmazonFSx. Al crear sistemas de archivos Multi-AZ FSx para ONTAP, 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:

- Rango de direcciones IP no asignadas de su VPC: FSx Amazon elige las últimas 64 direcciones IP del rango CIDR principal de la VPC para usarlas como rango de direcciones IP de punto final para el 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 el 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 rutas 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:

- Rango de direcciones IP no asignadas de su VPC: FSx Amazon elige las últimas 64 direcciones IP del rango CIDR principal de la VPC para usarlas como rango de direcciones IP de punto final para el 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.

- Rango de direcciones IP flotante fuera de la VPC: Amazon FSx elige un rango de direcciones 198.19.x.0/24 que ningún otro sistema de archivos con la misma VPC y tablas de enrutamiento ya utiliza.
- 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 ONTAP: FSx

- 0.0.0.0/8
- 127.0.0.0/8
- 198.19.0.0/20
- 224.0.0.0/4

- 240.0.0.0/4
- 255.255.255.255/32

7. En la sección Seguridad y cifrado, en Clave de cifrado, elija la clave de cifrado de 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 [Administrar sistemas de archivos con el 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 [Administrar SVMs con el ONTAP CLI](#).

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.

- Para el estilo de seguridad del volumen, elija entre Unix (Linux) y NTFS para el volumen. Para obtener más información, consulte [Estilo de seguridad del volumen](#).
- En la sección Active Directory, puede unir un Active Directory a la SVM. Para obtener más información, consulte [Cómo trabajar con Microsoft Active Directory en FSx 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.
- Direcciones IP del servidor DNS: las IPv4 direcciones 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 FSx administradores AWS delegados, administradores AWS 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.

10. En la sección de Configuración del volumen predeterminado, proporcione la siguiente información para el volumen predeterminado creado con el sistema de archivos.

- En el campo Volume name, introduzca un nombre para el volumen. Puede usar hasta 203 caracteres alfanuméricos o de subrayado (_).
- (Sistemas de archivos con un solo par HA) Para el estilo de volumen, elija una de las siguientes opciones FlexVol o FlexGroup. FlexVol los volúmenes son volúmenes de uso general que pueden tener un tamaño de hasta 300 terabytes (TiB). FlexGroup los 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 20 a 314.572.800 mebibytes (MiB) para FlexVol volúmenes o 800 gibibytes (GiB): 2400 TiB por par HA para FlexGroup volúmenes. Por ejemplo, un sistema de archivos con 12 pares de HA tendría un tamaño de volumen mínimo de 9600 GiB y un tamaño máximo de 20 480 TiB.
- En el tipo de volumen, elija 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 un NetApp SnapMirror o SnapVault relación. 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 [Eficacia de almacenamiento](#).
- 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 [Crear una política de instantáneas](#) en el NetApp Documentación del producto 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 del volumen](#).

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 la sección SnapLock Configuración de volumen predeterminada, para SnapLock Configuración, elija entre Activado y Desactivado. Para obtener más información sobre la configuración de un SnapLock Volumen de conformidad o un SnapLock Volumen empresarial, consulte [Descripción SnapLock Conformidad](#) y [Descripción SnapLock Enterprise](#). Para obtener más información acerca de SnapLock, consulte [Proteja sus datos con SnapLock](#).
13. 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.
14. 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.

15. 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.
16. Elija Create file system.

Cómo crear un sistema de archivos (CLI)

- Para crear un sistema de archivos FSx para ONTAP, utilice el comando [create-file-system](#)CLI (o la operación [CreateFileSystem](#)API equivalente), como se muestra en el siguiente ejemplo.

Note

No puede cambiar el tipo de implementación del sistema de archivos después de su creación. Si desea cambiar el tipo de implementación (por ejemplo, pasar de Single-AZ 1 a Single-AZ 2), puede hacer una copia de seguridad de los datos y restaurarlos en un nuevo sistema de archivos. También puede migrar sus datos con NetApp SnapMirror AWS DataSync, con o con una herramienta de copia de datos de terceros. Para obtener más información, consulte [Migración a ONTAP mediante FSx NetApp SnapMirror](#) y [Migración a FSx ONTAP mediante AWS DataSync](#).

```
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
```

Tras 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` de la CLI y la operación de API `CreateFileSystem` no crean una SVM ni un volumen predeterminados. Para crear una SVM, consulte [Creación de máquinas virtuales de almacenamiento \(SVM\)](#); para crear un volumen, consulte [Creación de volúmenes](#).

Creación de sistemas de archivos FSx para ONTAP en subredes compartidas

El uso compartido de VPC permite Cuentas de AWS crear varios recursos en nubes privadas virtuales compartidas y administradas de forma centralizada (). VPCs 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 se 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 FSx permiso a Amazon para modificar las tablas de rutas de las subredes compartidas en nombre de la cuenta del participante. Para obtener más información, consulte [Administración de la compatibilidad de VPC compartidas con sistemas de archivos Multi-AZ](#).

 Note

Es responsabilidad de la cuenta de participante coordinar con el propietario de la VPC para evitar la creación de subredes de VPC posteriores que se superpongan con el enrutamiento de interdominios sin clases (CIDR) integrado en la VPC de los sistemas de archivos del participante. Si las subredes se superponen, el tráfico al sistema de archivos puede verse interrumpido.

Requisitos y consideraciones de la subred compartida

Al crear sistemas FSx de archivos de 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 participante no pueden inicializar recursos mediante grupos de seguridad que pertenezcan a otros participantes o al 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 de propietario desea eliminar o modificar estos grupos de seguridad, el participante que creó el grupo de seguridad debe realizar la acción.
- Las cuentas de participante pueden ver, crear, modificar y eliminar los sistemas de archivos Single-AZ y sus recursos asociados en subredes que la cuenta de propietario compartió con ellos.
- Las cuentas de participante pueden ver, crear, modificar y eliminar los sistemas de archivos Multi-AZ y sus recursos asociados en subredes que la cuenta de propietario compartió con ellos. Además, la cuenta del propietario también debe conceder al FSx servicio de Amazon permisos para modificar las tablas de rutas en las subredes compartidas en nombre de la cuenta del participante. Para obtener más información, consulte [Administración de la compatibilidad de VPC compartidas con sistemas de archivos Multi-AZ](#)
- El propietario de la VPC compartida no puede ver, modificar ni eliminar recursos que un participante cree 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 de los 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 se 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 subredes de forma segura con VPCs 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 cuentas VPCs con una cuenta de participante. Para obtener información, consulte [Compartir la VPC con otras cuentas](#) en la guía del usuario de la nube privada virtual de Amazon.
- Para crear cuentas de participantes FSx para los sistemas de archivos Multi-AZ de ONTAP, el propietario de la VPC también debe conceder al FSx servicio de Amazon permisos para crear y modificar tablas de rutas en las subredes compartidas en nombre de las cuentas de los participantes. Esto se debe a que, en FSx el caso de ONTAP, los sistemas de archivos Multi-AZ utilizan direcciones IP flotantes para que los clientes conectados puedan realizar una transición fluida entre el servidor de archivos preferido y el servidor en espera durante una 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 de la compatibilidad de VPC compartidas con sistemas de archivos Multi-AZ

Las cuentas de propietario pueden gestionar si las cuentas de los participantes pueden o no crear sistemas de archivos Multi-AZ FSx para ONTAP en subredes de VPC que el propietario haya compartido con los participantes mediante la API, y AWS Management Console AWS CLI, como se describe en las siguientes secciones.

Para administrar el uso compartido de VPC en sistemas de archivos Multi-AZ (consola)

Abre la FSx consola de Amazon en <https://console.aws.amazon.com/fsx/>.

1. En el panel de navegación, seleccione Configuración.
2. Ubique la configuración de VPC compartida de Multi-AZ en la página Configuración.

- Para habilitar el uso compartido de VPC en sistemas de archivos Multi-AZ en las subredes de VPC compartidas, seleccione **Habilitar actualizaciones de las tablas de enrutamiento** desde cuentas de participante.
- Para deshabilitar el uso compartido de VPC para los sistemas de archivos Multi-AZ en todos VPCs sus dominios, elija **Inhabilitar las actualizaciones de las tablas de enrutamiento** de las cuentas de los participantes. Se muestra 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 característica. Una vez que se desactive la característica, estos sistemas de archivos pasarán a un estado MISCONFIGURED y puede que dejen de estar disponibles.

3. Ingrese **confirm** y seleccione **Confirmar** para deshabilitar la característica.

Cómo administrar el uso compartido de VPC en 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-configuration](#) utilice el comando CLI o el comando API [DescribeSharedVpcConfiguration](#) equivalente, 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-configuration](#) CLI o el comando API [UpdateSharedVpcConfiguration](#) equivalente. En el siguiente ejemplo, se permite compartir VPC en 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 característica, configure `EnableFsxRouteTableUpdatesFromParticipantAccounts` 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"
}
```

Actualizar sistemas 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 FSx consola y la CLI de Amazon. Puede actualizar lo siguiente FSx para las propiedades del sistema de archivos de ONTAP mediante la FSx consola y la API de Amazon: AWS CLI

- 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, consulte [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, consulte [Optimización del rendimiento con las ventanas FSx de mantenimiento de Amazon](#).
- 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 [Administrar sistemas de archivos con el ONTAP CLI](#).

- Tablas de enrutamiento de Amazon VPC. Con Multi-AZ FSx para los sistemas de archivos ONTAP, los puntos de enlace que utiliza para acceder a los datos a través de NFS o SMB y los puntos de enlace de administración para acceder a la CLI, la API y BlueXP de ONTAP utilizan direcciones IP flotantes en las tablas de rutas de Amazon VPC que se asocian al 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 se etiquetan con `Key: AmazonFSx; Value: ManagedByAmazonFSx`. Al crear o actualizar sistemas FSx de archivos Multi-AZ de ONTAP, le AWS CloudFormation recomendamos que añada la etiqueta manualmente. `Key: AmazonFSx; Value: ManagedByAmazonFSx`

Cómo actualizar un sistema de archivos (consola)

Los siguientes procedimientos proporcionan instrucciones sobre cómo realizar actualizaciones en un sistema de archivos existente FSx para ONTAP mediante el AWS Management Console

Cómo actualizar las copias de seguridad diarias automáticas

1. Abre la FSx consola de Amazon en <https://console.aws.amazon.com/fsx/>.
2. Para mostrar la página de detalles del sistema de archivos, en el panel de navegación izquierdo, selecciona Sistemas de archivos y, a continuación, elige el FSx sistema de archivos de ONTAP que deseas 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.

Cómo actualizar el período de mantenimiento semanal

1. Abre la FSx consola de Amazon en <https://console.aws.amazon.com/fsx/>.
2. Para mostrar la página de detalles del sistema de archivos, en el panel de navegación izquierdo, selecciona Sistemas de archivos y, a continuación, elige el FSx sistema de archivos de ONTAP que deseas 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.

Cómo cambiar la contraseña administrativa del sistema de archivos

1. Abre la FSx consola de Amazon en <https://console.aws.amazon.com/fsx/>.
2. Para mostrar la página de detalles del sistema de archivos, en el panel de navegación izquierdo, selecciona Sistemas de archivos y, a continuación, elige el FSx sistema de archivos de ONTAP que deseas 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 mensaje de error que indica que la nueva contraseña no cumple los requisitos de contraseña, puede utilizar el [security login role config show](#) ONTAP Comando CLI para ver la configuración de requisitos de contraseña en el sistema de archivos. Para obtener más información e instrucciones sobre cómo cambiar la configuración de contraseña, consulte [Se produce un error al actualizar la contraseña de la cuenta fsxadmin](#).

Cómo actualizar tablas de enrutamiento de VPC en sistemas de archivos Multi-AZ

1. Abra la FSx consola de Amazon en <https://console.aws.amazon.com/fsx/>.
2. Para mostrar la página de detalles del sistema de archivos, en el panel de navegación izquierdo, selecciona Sistemas de archivos y, a continuación, elige el FSx sistema de archivos de ONTAP que deseas 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.

Cómo actualizar un sistema de archivos (CLI)

El siguiente procedimiento ilustra cómo realizar actualizaciones en un sistema de archivos existente FSx para ONTAP mediante el AWS CLI

1. Para actualizar la configuración de un sistema de archivos FSx para ONTAP, utilice el comando [update-file-system](#) CLI (o la operación [UpdateFileSystem](#) API 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 y automáticas, establezca la propiedad AutomaticBackupRetentionDays en 0.

```
aws fsx update-file-system \
  --file-system-id fs-0123456789abcdef0 \
  --ontap-configuration AutomaticBackupRetentionDays=0
```

Administración de pares de alta disponibilidad (HA)

Cada sistema FSx de archivos de ONTAP funciona con uno o más pares de servidores de archivos de alta disponibilidad (HA) en una configuración activa y 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. FSx en el caso de ONTAP, los sistemas de archivos de primera generación funcionan con un par HA, que ofrece hasta un 4% de la capacidad GBps de procesamiento y 160.000 unidades SSD. IOPs FSx en el caso de ONTAP, los sistemas de archivos Multi-AZ de segunda generación también funcionan con un par HA y ofrecen hasta un 6% de capacidad de procesamiento y 200 000 IOPS GBps de SSD. FSx para ONTAP, los sistemas de archivos Single-AZ de segunda generación funcionan con hasta 12 pares de HA, lo que puede ofrecer hasta el 72% de la capacidad de procesamiento y 2 400 000 IOPS GBps de SSD (el 6% GBps de la capacidad de rendimiento y 200 000 IOPS de SSD por par de HA).

Al crear el sistema de archivos desde la FSx consola de Amazon, Amazon FSx recomienda el número de pares de alta disponibilidad que debe utilizar en función del almacenamiento SSD que desee. También puede elegir manualmente la cantidad de pares de HA en función de los 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 hasta un 6% de capacidad GBps de rendimiento y 200 000 SSD) IOPs, y varios pares de alta disponibilidad si sus cargas de trabajo necesitan niveles más altos de escalabilidad del rendimiento.

Cada par de HA tiene un agregado, que es un conjunto lógico de discos físicos.

Note

Puede agregar pares de HA a los sistemas de archivos Single-AZ de segunda generación. Para obtener más información, consulte [Agregar pares de alta disponibilidad \(HA\)](#). De lo contrario, puede migrar los datos entre sistemas de archivos (con diferentes pares de alta disponibilidad) mediante SnapMirror AWS DataSync, o restaurando los datos de una copia de seguridad a un nuevo sistema de archivos.

Agregar pares de alta disponibilidad (HA)

FSx para ONTAP, los sistemas de archivos están compuestos por uno o más pares de servidores de archivos de alta disponibilidad. Los sistemas de archivos de primera generación y los sistemas de archivos Multi-AZ de segunda generación admiten un par de HA, mientras que los sistemas de

archivos Single-AZ de segunda generación admiten hasta 12 pares de HA. También puede agregar más pares de HA después de crear un sistema de archivos Single-AZ de segunda generación (hasta un máximo de 12). Agregar pares de HA no supone una interrupción y, por lo general, solo toma unos minutos.

Tenga en cuenta los siguientes aspectos cuando agregue pares de HA al sistema de archivos:

- Al agregar pares de HA al sistema de archivos, se introducen nuevos servidores de archivos con propio almacenamiento (o agregado). Los nuevos pares de HA tienen la misma capacidad de rendimiento y capacidad de almacenamiento que los pares de HA existentes en el sistema de archivos. Por ejemplo, supongamos que su sistema de archivos tiene dos pares de alta disponibilidad con un total de 12 GBps de capacidad de rendimiento y 2 tebibytes (TiB) de almacenamiento SSD. Si agrega un nuevo par HA, su sistema de archivos tendrá un 18% GBps de capacidad de procesamiento y 3 TiB de almacenamiento SSD.
- Para aprovechar el rendimiento adicional de los nuevos pares de HA, debe trasladar algunos de los volúmenes existentes a los nuevos pares de HA y volver a montar los clientes para conectarse a ellos. Para obtener más información, consulte [Equilibrar las cargas de trabajo entre pares de alta disponibilidad](#).
- No puede modificar la capacidad de rendimiento, la capacidad de almacenamiento en SSD ni las IOPS en SSD aprovisionadas del sistema de archivos cuando agrega pares de HA o mientras se esté realizando una actualización para agregar pares de HA.
- No puede eliminar los pares de HA después de agregarlos. Le recomendamos que escale la capacidad de rendimiento del sistema de archivos si necesita aumentar el rendimiento temporalmente (suponiendo que el sistema de archivos no tenga la máxima capacidad de rendimiento). Esto aumenta la capacidad de rendimiento de los pares de HA existentes del sistema de archivos.
- Para aumentar los pares de HA en un sistema de archivos de segunda generación de uno a dos o más, el sistema de archivos puede tener cinco SVM como máximo.
- El protocolo iSCSI está disponible en sistemas de archivos que tienen seis o menos pares de alta disponibilidad (pares de HA). El protocolo NVMe /TCP está disponible en los sistemas de archivos de segunda generación que tienen seis pares HA o menos. Para obtener más información, consulte [Acceder a sus FSx datos de ONTAP](#).
- Al añadir nuevos pares de alta disponibilidad al sistema de archivos, la NVMe memoria caché se habilita de forma predeterminada para los nuevos nodos del sistema de archivos. Recomendamos deshabilitarla para cargas de trabajo de alto rendimiento. Para obtener más información, consulte [Administrar la memoria caché NVMe](#).

Cómo agregar pares de HA

1. Abre la FSx consola de Amazon en <https://console.aws.amazon.com/fsx/>.
2. Para mostrar la página de detalles del sistema de archivos, en el panel de navegación izquierdo, selecciona Sistemas de archivos y, a continuación, elige el FSx sistema de archivos de ONTAP que deseas actualizar.
3. En el panel Resumen, en Cantidad de pares de HA, seleccione Actualizar.
4. En el menú desplegable Pares de HA, seleccione la cantidad de pares de HA que desee agregar al sistema de archivos.
5. Haga clic en el botón Actualizar.

Después de agregar los pares de HA, es importante reequilibrar los datos existentes para garantizar que las E/S se distribuyan uniformemente entre los pares de HA del sistema de archivos. Para obtener más información, consulte [Equilibrar las cargas de trabajo entre pares de alta disponibilidad](#).

Equilibrar las cargas de trabajo entre pares de alta disponibilidad

Si tiene un sistema de archivos con varios pares de alta disponibilidad (HA), su rendimiento y almacenamiento se distribuyen entre cada uno de sus pares de HA. FSx ya que ONTAP equilibra automáticamente los archivos a medida que se escriben en el sistema de archivos, pero los datos de la carga de trabajo y la E/S dejan de estar equilibrados una vez que se añaden los pares de alta disponibilidad. Además, en raras ocasiones, podría haber un desequilibrio de los datos de carga de trabajo o las E/S entre los pares de HA existentes del sistema de archivos, lo que puede afectar al rendimiento general de la carga de trabajo. Si la carga de trabajo se desequilibra alguna vez, puede volver a equilibrarla en cada uno de los pares de HA del sistema de archivos (y sus correspondientes servidores de archivos y agregados, es decir, los grupos de almacenamiento que componen el nivel de almacenamiento principal).

Temas

- [Equilibrio de utilización de almacenamiento principal](#)
- [Desequilibrio en la utilización del rendimiento del disco y del servidor de archivos](#)
- [Asignación de CloudWatch dimensiones a los recursos de la CLI y la API REST de ONTAP](#)
- [Reequilibrio de clientes](#)
- [Reequilibrio de volúmenes](#)

Equilibrio de utilización de almacenamiento principal

La capacidad de almacenamiento principal del sistema de archivos se divide en partes iguales entre cada uno de los pares de HA 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 el nivel de almacenamiento principal de forma continua. Para los sistemas de archivos con varios pares de HA, 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 los agregados.

Si observa que hay un desequilibrio en los agregados, 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 de un agregado a otro. Para obtener más información, consulte [Movimiento de volúmenes entre agregados](#).

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 del disco) se dividen en partes iguales entre los pares de HA del sistema de archivos. Le recomendamos que mantenga una utilización media inferior al 50 % (y una utilización 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 del sistema de archivos en todos los pares de HA como a la utilización por servidor de archivos.

Si observa que la utilización del rendimiento del servidor de archivos está desequilibrado (y los servidores de archivos en los que la carga de trabajo está desequilibrada tienen un uso continuo superior al 80 %), puede usar la CLI y la API de 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 por seguir para un diagnóstico más detallado.

Si en el sistema de archivos...	Entonces...
El rendimiento o las IOPS del disco del	Es posible que se esté produciendo un hotspot en la E/S en un subconjunto de pares de HA (un subconjunto de los volúmenes que contiene una enorme cantidad de datos a los que se accede), lo que

Si en el sistema de archivos...	Entonces...
servidor de archivos están desequilibrados	puede limitar el rendimiento general de la carga de trabajo, ya que se ve obstruida con respecto a un subconjunto de pares de HA. Por cada servidor de archivos con mucho uso, compruebe los volúmenes más usados para ver qué volúmenes tienen la mayor actividad dentro de un agregado. Si necesita más información sobre este procedimiento, consulte Reequilibrio de volúmenes .
El rendimiento de la red está desequilibrado, pero el rendimiento o las IOPS del disco del servidor de archivos o las IOPS del disco no están desequilibrados	Los datos se distribuyen uniformemente entre los pares de HA, pero los 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 sus volúmenes y júntelos de nuevo usando un punto de conexión diferente en un par de HA distinto. Si necesita más información sobre este procedimiento, consulte Reequilibrio de clientes .

Asignación de CloudWatch dimensiones a los recursos de la CLI y la API REST de ONTAP

Tu sistema de archivos de segunda generación tiene CloudWatch métricas de Amazon con la Aggregate dimensión FileServer o. 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 o la API de REST de ONTAP.

- 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 preferidos (es decir, prestan servicio al tráfico a menos que el sistema de archivos se haya transferido al servidor de archivos secundario), mientras que los servidores de archivos con números pares son secundarios (es decir, solo prestan servicio al tráfico cuando el socio no está disponible). Por este motivo, los servidores de archivos secundarios tienen menos utilización 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 HA, es decir, el agregado aggr1 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 HA; el agregado aggr2 lo comparten los servidores de archivos FsxId01234567890abcdef-03 y FsxId01234567890abcdef-04, y así sucesivamente.

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 NetApp ONTAP CLI](#) sección de la Guía del usuario de Amazon FSx for NetApp ONTAP.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. Use 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.
```

Reequilibrio de clientes

Después de agregar pares de HA o si hay un desequilibrio de E/S en los servidores de archivos (específicamente, debido a la utilización del rendimiento de la red), puede reequilibrar los clientes. Si va a reequilibrar los clientes después de agregar pares de HA, puede pasar a [Remontaje de clientes](#). De lo contrario, primero debe identificar los clientes con mucho tráfico que desee trasladar para reequilibrar la E/S de la carga de trabajo.

Si hay un desequilibrio de E/S en los servidores de archivos (específicamente, debido a la utilización del rendimiento de la red), la causa puede ser que los clientes tengan mucha E/S. Para identificar los clientes de alto tráfico, use la CLI de ONTAP.

Identificar clientes de alto tráfico

1. Para conectarse mediante SSH a la NetApp CLI de ONTAP de su sistema de archivos, siga los pasos descritos en la [Uso de NetApp ONTAP CLI](#) sección de la Guía del usuario de Amazon FSx for NetApp ONTAP.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. Para ver los clientes con mayor tráfico, use el comando [statistics top client show](#) de la CLI de ONTAP. Si lo desea, puede especificar el parámetro `-node` para ver solo los clientes principales de un servidor de archivos específico. Si está diagnosticando el desequilibrio en un servidor de archivos específico, use el parámetro `-node` y sustituya `node_name` por el nombre del servidor de archivos (por ejemplo, `FsxId01234567890abcdef-01`).

Si lo desea, puede agregar el parámetro `-interval` y proporcione 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 dirigido a cada volumen. El valor predeterminado es 5 (en 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.

Client	Vserver	Node	*Total Ops	Total (Bps)
172.17.236.53:938	svm01	FsxId01234567890abcdef-01	2143	140443648
172.17.236.160:898	svm02	FsxId01234567890abcdef-01	812	53215232

Remontaje de clientes

- Puede reequilibrar los clientes con otros pares de HA. Para ello, separe el volumen del cliente y vuelva a montarlo con el nombre del DNS del punto de conexión NFS/SMB de la SVM; de este modo, se obtiene un punto de conexión aleatorio correspondiente a un par de HA aleatorio.

Le recomendamos que vuelva a usar el nombre del 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 de conexión diferente, puede especificar la dirección IP de un punto de

conexión diferente a la que corresponde al servidor de archivos que tiene mucho tráfico. Puede hacerlo ejecutando 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 comando `statistics top client show`, el cliente `172.17.236.53` genera mucho tráfico hacia `FsxId01234567890abcdef-01`. El resultado del comando `network interface show` indica que esta es la dirección `172.31.15.89`. Para montarlo en un punto de conexión diferente, seleccione cualquier otra dirección (en este ejemplo, la única otra dirección es `172.31.8.112`, que corresponde a `FsxId01234567890abcdef-03`).

Reequilibrio de volúmenes

Si hay un desequilibrio de E/S en los volúmenes o agregados, puede reequilibrar los volúmenes para redistribuir el tráfico de E/S entre los volúmenes.

Note

Si hay un desequilibrio en la utilización del almacenamiento en todos los agregados, 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 entre agregados para equilibrar la utilización del almacenamiento, le recomendamos que solo mueva los volúmenes si observa un impacto en el rendimiento. Esto es así, 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 piensa 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 NetApp ONTAP CLI](#) sección de la Guía del usuario de Amazon FSx for NetApp ONTAP.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

- Use el comando [statistics volume show](#) de la CLI de ONTAP para ver los volúmenes con tráfico más alto de un agregado determinado, con los siguientes cambios:

- aggregate_name** Sustitúyalo por el nombre del agregado (por ejemplo,). aggr1
- Si lo desea, puede agregar el parámetro `-interval` y proporcione 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 dirigido a cada volumen. El valor predeterminado es 5 (en segundos).

```
::> statistics volume show -aggregate aggregate_name -sort-key total_ops [-interval [5,300]]
```

Según el intervalo que elija, la visualización de los datos puede tardar hasta 5 minutos. El comando muestra todos los volúmenes del agregado, junto con la cantidad de tráfico que se dirige a cada agregado.

Volume	Vserver	Aggregate	*Total Ops	Read Ops	Write Ops	Other Ops	Read (Bps)	Write (Bps)	Latency (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, si 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 de componentes entre los agregados para que el tráfico se distribuya de manera más uniforme.

- Si ha agregado nuevos pares de HA, debe mover los volúmenes existentes a nuevos agregados. Para obtener más información, consulte [Movimiento de volúmenes entre agregados](#).

Administrar la memoria caché NVMe

La NVMe memoria caché está habilitada de forma predeterminada en su sistema de archivos de segunda generación. Si su sistema de archivos de segunda generación tiene una carga de trabajo de alto rendimiento, puede deshabilitar la memoria caché para mejorar el NVMe rendimiento. El siguiente procedimiento explica cómo habilitar, deshabilitar y validar la memoria caché del sistema de archivos. NVMe

Para administrar la NVMe memoria caché

1. Utilice SSH en su ONTAP sistema de archivos. Para obtener más información, consulte [the section called “Uso de NetApp ONTAP CLI”](#).

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. Utilizar [system node external-cache modify](#) ONTAP Comando CLI. Elija entre **true** habilitar la NVMe caché o **false** deshabilitarla.

```
::> system node external-cache modify -node * -is-enabled [true|false]
```

3. Utilizar [system node external-cache show](#) ONTAP Comando CLI para comprobar si la NVMe caché está habilitada o deshabilitada.

```
::> system node external-cache show -node * -fields is-enabled
```

La NVMe caché se habilita o deshabilita por nodo. Al agregar nuevos pares de alta disponibilidad (HA) al sistema de archivos, cada nodo nuevo tiene el mismo comportamiento predeterminado que los nodos de un nuevo sistema de archivos. Por lo tanto, la NVMe caché se habilitaría para cualquier nodo nuevo de un sistema de archivos, incluso si los nodos existentes la tienen deshabilitada. Para obtener más información, consulte [Agregar pares de alta disponibilidad \(HA\)](#).

Supervisión de detalles del sistema de archivos

Puede ver la información de configuración detallada de su sistema FSx de archivos ONTAP mediante la FSx consola de Amazon, la API y la API AWS CLI, si es compatible AWS SDKs.

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.

En las siguientes pestañas, se proporciona 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 servidor de archivos y el disco

Para obtener más información, consulte [Monitorización con Amazon CloudWatch](#).

- Administración: muestra la siguiente información de administración del sistema de archivos:
 - La DNS nombres y IP direcciones de los puntos finales de administración del sistema de archivos y entre clústeres.
 - La ONTAP nombre de usuario del administrador.
 - La opción de actualizar el ONTAP contraseña de administrador.
- Lista del sistema de archivos SVMs
- Lista de los volúmenes del sistema de archivos
- Configuración de copia de seguridad: cambia la configuración de copia de seguridad diaria y 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, agregar o eliminar los pares clave:valor de la etiqueta.
- Uso de la CLI o la API: utilice el comando [describe-file-systems](#)CLI o la operación de [DescribeFileSystems](#)API.

FSx para el estado del sistema de archivos ONTAP

Puedes ver el estado de un sistema de FSx archivos de Amazon mediante la FSx consola de Amazon, el AWS CLI comando [describe-file-systems](#) o la operación de la API [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 va a eliminar un sistema de archivos existente.
MAL CONFIGURADO	El sistema de archivos está mal configurado pero es recuperable.
ERROR	1. El sistema de archivos ha fallado y Amazon no FSx puede recuperarlo. 2. Al crear un nuevo sistema de archivos, Amazon no FSx ha podido crear uno nuevo.

Eliminación de sistemas de archivos

Puede eliminar un sistema FSx de archivos de ONTAP mediante la FSx consola de Amazon AWS CLI, la y la FSx API de Amazon y SDKs.

Para eliminar un sistema de archivos:

- Usando la consola: siga el procedimiento descrito en [Limpieza de recursos](#).
- Mediante la CLI o la API: primero elimine todos los volúmenes y SVMs del sistema de archivos. A continuación, utilice el comando [delete-file-system](#) CLI o la operación [DeleteFileSystem](#) API.

Administración FSx de máquinas virtuales de almacenamiento ONTAP

En el FSx caso de ONTAP, los volúmenes se alojan en servidores de archivos virtuales denominados máquinas virtuales de almacenamiento (). SVMs 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 desde 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 final de la SVM (dirección IP). FSx

Amazon crea FSx automáticamente un SVM predeterminado en su sistema de archivos cuando crea un sistema de archivos con. AWS Management Console Puedes crear archivos adicionales SVMs en tu sistema de archivos en cualquier momento mediante la consola o la FSx API de Amazon y SDKs. AWS CLI No puede crear SVMs mediante la CLI de ONTAP o la API REST.

Puede unirlos SVMs a un Active Directory de Microsoft para autenticar y autorizar el acceso a los archivos. Para obtener más información, consulte [Cómo trabajar con Microsoft Active Directory en FSx ONTAP](#).

Número máximo de archivos SVMs por sistema de archivos

En la siguiente tabla se muestra el número máximo SVMs que se puede crear para un sistema de archivos. El número máximo SVMs depende de la cantidad de capacidad de rendimiento aprovisionada en megabytes por segundo (). MBps

Pares de alta disponibilidad (HA)	Cantidad de capacidad de rendimiento () MBps	Número máximo de SVMs por sistema de archivos
1 par de HA	128	6
	256	6
	384	6
	512	14
	768	14
	1 024	14

Pares de alta disponibilidad (HA)	Cantidad de capacidad de rendimiento () MBps	Número máximo de SVMs por sistema de archivos
	1536	14
	2048	24
	3.072	14
	4.096	24
	6144	24
2 a 12 pares de HA	Cualquiera	5

Temas

- [Creación de máquinas virtuales de almacenamiento \(SVM\)](#)
- [Actualización de máquinas virtuales de almacenamiento \(SVM\)](#)
- [Auditoría del acceso a archivos](#)
- [Configuración de un servidor SMB en un grupo de trabajo](#)
- [Supervisión de los detalles de configuración de la máquina virtual de almacenamiento \(SVM\)](#)
- [Eliminación de máquinas virtuales de almacenamiento \(SVM\)](#)

Creación de máquinas virtuales de almacenamiento (SVM)

Puede crear un SVM FSx para ONTAP mediante la AWS Management Console API, y. AWS CLI

La cantidad máxima SVMs que puede crear para un sistema de archivos depende del tipo de implementación del sistema de archivos y de la cantidad de capacidad de rendimiento aprovisionada. Para obtener más información, consulte [Número máximo de archivos SVMs por sistema de archivos](#).

Propiedades de SVM

Al crear una SVM, se definen las siguientes propiedades:

- El sistema FSx de archivos de 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 [Cómo trabajar con Microsoft Active Directory en FSx ONTAP](#).
- El estilo de seguridad del volumen raíz: defina el estilo de seguridad del volumen raíz (Unix o NTFS) para adaptarlo al tipo de clientes que utiliza para acceder a sus datos dentro de la 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 [Administrar SVMs con el ONTAP CLI](#).

Cómo crear una máquina virtual de almacenamiento (consola)

1. Abre la FSx consola de Amazon 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 [Administrar SVMs con el ONTAP CLI](#).

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 de los servidores DNS: las IPv4 direcciones de los servidores DNS de tu 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 FSx administradores AWS delegados, administradores AWS 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).

Cómo crear una máquina virtual de almacenamiento (CLI)

- FSx Para crear una máquina virtual de almacenamiento (SVM) para ONTAP, utilice el comando [create-storage-virtual-machine](#) CLI (o la operación [CreateStorageVirtualMachine](#) API 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
```

Tras 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",
        "IpAddresses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com",
        "IpAddresses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddresses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddresses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com",
        "IpAddresses": ["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 máquinas virtuales de almacenamiento (SVM)

Puede actualizar las siguientes propiedades de configuración de la máquina virtual de almacenamiento (SVM) mediante la FSx consola de Amazon y la FSx API de Amazon: AWS CLI

- 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 [Administración de las configuraciones del Active Directory de la SVM](#).

Cómo actualizar las credenciales de la cuenta de administrador de SVM (consola)

1. Abra la FSx consola de Amazon 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 SVMs disponibles Cuenta de AWS en la actualidad Región de AWS, expanda ONTAP y seleccione Almacenamiento de máquinas virtuales.
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.

Cómo actualizar las credenciales de la cuenta de administrador de SVM (CLI)

- Para actualizar la configuración de una SVM FSx para ONTAP, utilice el comando [update-storage-virtual-machine](#) CLI (o la operación [UpdateStorageVirtualMachine](#) API 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 \
```

Tras 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",
        "IpAddresses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com",
        "IpAddresses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddresses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddresses": ["198.19.0.5", "198.19.0.6"]
      }
    }
  }
}
```

```

    },
    "Iscsi": {
      "DnsName": "iscsi.svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com",
      "IpAddresses": ["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"
    }
  }
}

```

Auditoría del acceso a archivos

Amazon FSx for 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](#)
- [Descripción general de las tareas para configurar la auditoría de acceso a los archivos](#)

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	Acceso a archivos

ID de evento (EVT/ EVTX)	Evento	Descripción	Categoría
		directorio). ONTAP genera este evento cuando un cliente de Windows intenta eliminar el objeto (archivo o directorio)	



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 ONTAP FSx para la auditoría del 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. [Consulte los registros de eventos de auditoría](#) después de que ONTAP FSx 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 (ACEs) designadas como tipou, 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 los de auditoría. ACEs AI convertir ACLs a bits de modo, ACEs se omite la auditoría. Al convertir los bits de modo a ACLs, no ACEs se generan auditorías.

- 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 SVMs

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.

Cómo configurar las políticas de auditoría de NTFS (pestaña Seguridad de Windows)

Las políticas de auditoría de NTFS se configuran añadiendo entradas a NTFS SACLs 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 discrecionales (DACLS) para aplicar permisos de acceso a archivos y carpetas, SACLs para auditar archivos y carpetas, o ambas opciones y. SACLs DACLS

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. Seleccione 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. 4. Omite el resto de este procedimiento.

Si desea...	Haga lo siguiente:
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 abrirá el *object* cuadro Entrada de auditoría para.

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 Aplicar.
 13. Cuando termine de añadir, eliminar o editar las entradas de auditoría, pulse Aceptar.

object Se cierra el cuadro Entrada de auditoría para.

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 está configurando SACLs un solo archivo, el cuadro Reemplazar todas las entradas de auditoría heredables existentes en todos los descendientes por entradas de auditoría heredables de este objeto no aparece en el cuadro Auditoría.

15. Seleccione Aceptar.

Cómo 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 `ntfs sac1` add de [vserver security file-directory](#).

Por ejemplo, el siguiente comando crea una política de seguridad con el nombre del SVM denominado. `p1 vs0`

```
vserver security file-directory policy create -policy-name p1 -vserver vs0
```

A continuación, el siguiente comando aplica la política `p1` de seguridad al `vs0` SVM.

```
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 archivos y directorios de estilo de seguridad de UNIX, agregue auditorías ACEs (expresiones de control de acceso) a NFS ACLs v4.x (listas de control de acceso). 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, tanto la opción discrecional como la de sistema se almacenan en la misma ACL. ACEs Por lo tanto, debe tener cuidado al agregar la auditoría ACEs a una ACL existente para evitar sobrescribir y perder una ACL existente. No importa el orden en el que agregue la auditoría ACEs a una ACL existente.

Cómo 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 la auditoría ACEs deseada.
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.

Configuración de un servidor SMB en un grupo de trabajo

Puede configurar un servidor de bloque de mensajes de servidor (SMB) en un grupo de trabajo como alternativa a unir un [SVM a un Active Directory de Microsoft](#) cuando la infraestructura de dominio de Microsoft Active Directory no esté disponible. Un grupo de trabajo es una peer-to-peer red que usa el protocolo SMB y solo tiene cuentas y grupos locales.

El proceso de configuración de un servidor SMB como miembro de un grupo de trabajo consiste en lo siguiente:

- Crear el servidor SMB en una máquina virtual de almacenamiento (SVM).
- Creación de usuarios y grupos locales.
- Agregar usuarios o grupos locales como miembros del grupo de trabajo.

Tenga en cuenta que los servidores SMB en modo de grupo de trabajo no admiten las siguientes funciones SMB:

- SMB3 Protocolo testigo
- SMB3 CA comparte
- SQL sobre SMB
- Redirección de carpetas
- Perfiles de itinerancia
- Objeto de política de grupo (GPO)
- Servicio de instantáneas de volúmenes (VSS)

Además, un servidor SMB en modo de grupo de trabajo solo admite la autenticación NTLM y no admite la autenticación Kerberos.

Los siguientes procedimientos explican el proceso de configuración de un servidor SMB en una SVM de un grupo de trabajo, la creación de cuentas locales y la adición de estas cuentas a los miembros del grupo de trabajo. Utilizará la NetApp ONTAP CLI desde el sistema de archivos o desde la interfaz de administración de SVM para implementar estos procedimientos. Para obtener más información, consulte [Uso de NetApp ONTAP CLI](#).

Temas

- [Crear un servidor SMB en un grupo de trabajo](#)
- [Crear una cuenta de usuario local en el servidor SMB](#)
- [Crear grupos locales en el servidor SMB](#)
- [Agregar usuarios locales al grupo local](#)

Crear un servidor SMB en un grupo de trabajo

Puede utilizar el [vserver cifs create](#) ONTAP CLI comando para crear un servidor SMB en el SVM y especificar el grupo de trabajo al que pertenece.

Antes de empezar

El SVM y los volúmenes (e interfaces) que utiliza para entregar los datos deben estar configurados para permitir el protocolo SMB.

LIFs Deben poder conectarse a los servidores DNS que están configurados en el SVM. Es posible que se requiera una licencia CIFS en el sistema de archivos; sin embargo, no se requiere una licencia CIFS si el servidor SMB se utilizará únicamente para la autenticación.

Para crear un servidor SMB en un grupo de trabajo

1. Para acceder a la ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando. 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 [Administrar sistemas de archivos con el ONTAP CLI](#).

2. Cree el servidor SMB en un grupo de trabajo:

```
FSxIdabcde123456::> vserver cifs create -vserver vserver_name -cifs-  
server cifs_server_name -workgroup workgroup_name [-comment workgroup_description]
```

El siguiente comando crea el servidor SMB smb_server01 en el grupo de trabajo: workgroup01

```
FSxIdabcde123456::> vserver cifs create -vserver svm1 -cifs-server SMB_SERVER01 -  
workgroup workgroup01
```

Si está conectado al puerto de administración de la SVM, no necesita especificar un. -vserver

3. Compruebe la configuración del servidor SMB mediante el `vserver cifs show` comando.

En el siguiente ejemplo, el resultado del comando muestra que se smb_server01 creó un servidor SMB con el nombre SVM svm1 del grupo de trabajo: workgroup01

```
FSxIdabcde123456::> vserver cifs show -vserver svm1

                                Vserver: svm1
                                CIFS Server NetBIOS Name: SMB_SERVER01
                                NetBIOS Domain/Workgroup Name: workgroup01
                                Fully Qualified Domain Name: -
                                Organizational Unit: -
                                Default Site Used by LIFs Without Site Membership: -
```

```
Workgroup Name: workgroup01
Authentication Style: workgroup
CIFS Server Administrative Status: up
CIFS Server Description:
List of NetBIOS Aliases: -
```

Crear una cuenta de usuario local en el servidor SMB

Puede crear una cuenta de usuario local que se pueda utilizar para autorizar el acceso a los datos contenidos en el SVM a través de una conexión SMB. También puede usar cuentas de usuario locales para la autenticación al crear una sesión SMB. La funcionalidad de usuario local está habilitada de forma predeterminada cuando se crea la SVM. Al crear una cuenta de usuario local, debe especificar un nombre de usuario y debe especificar el SVM al que desea asociar la cuenta.

Para crear cuentas de usuario locales en el servidor SMB

1. Cree el usuario local mediante el comando [vserver cifs users-and-groups local-user create](#)ONTAPCLI:

```
vserver cifs users-and-groups local-user create -vserver svm_name -user-  
name user_name optional_parameters
```

Los siguientes parámetros opcionales pueden resultar útiles:

- `-full-name`— El nombre completo del usuario.
- `-description`— Una descripción para el usuario local.
- `-is-account-disabled {true|false}`— Especifica si la cuenta de usuario está habilitada o deshabilitada. Si no se especifica este parámetro, el valor predeterminado es habilitar la cuenta de usuario.

El comando solicita la contraseña del usuario local.

2. Introduzca una contraseña para el usuario local y, a continuación, confírmela.
3. Compruebe que el usuario se ha creado correctamente:

```
vserver cifs users-and-groups local-user show -vserver svm_name
```

El siguiente ejemplo crea un usuario local `SMB_SERVER01\sue`, con un nombre completo `Sue Chang`, asociado a SVM: `svm1`

```
FSxIdabcde123456::> vservers cifs users-and-groups local-user create -vservers svm1
-user-name SMB_SERVER01\sue -full-name "Sue Chang"
```

Enter the password:
Confirm the password:

```
FSxIdabcde123456::> vservers cifs users-and-groups local-user show
```

Vserver	User Name	Full Name	Description
svm1	SMB_SERVER01\Administrator		Built-in administrator account
svm1	SMB_SERVER01\sue	Sue Chang	

Crear grupos locales en el servidor SMB

Puede crear grupos locales que se puedan utilizar para autorizar el acceso a los datos asociados al SVM a través de una conexión SMB. También puede asignar privilegios que definan los derechos de usuario o las capacidades que tiene un miembro del grupo.

La funcionalidad de grupo local está habilitada de forma predeterminada cuando se crea la SVM. Al crear un grupo local, debe especificar un nombre para el grupo y debe especificar la SVM a la que desea asociarlo. Puede especificar un nombre de grupo con o sin el nombre de dominio local y, si lo desea, puede especificar una descripción para el grupo local. No puede agregar un grupo local a otro grupo local.

Para crear un grupo local en el servidor SMB

1. cree el grupo local mediante el comando [vservers cifs users-and-groups local-group create](#) ONTAPCLI.

```
vservers cifs users-and-groups local-group create -vservers svm_name -group-
name group_name [-description local_group_description]
```

Es útil incluir una descripción del grupo local.

2. Compruebe que el grupo se ha creado correctamente:

```
vservers cifs users-and-groups local-group show -vservers svm_name
```

El siguiente ejemplo crea un grupo local SMB_SERVER01\engineering asociado a SVM: svm1

```
FSxIdabcde123456:> vservers cifs users-and-groups local-group create -vservers svm1 -
group-name SMB_SERVER01\engineering
```

```
FSxIdabcde123456:> vservers cifs users-and-groups local-group show -vservers svm1
```

Vserver	Group Name	Description
svm1	BUILTIN\Administrators	Built-in Administrators group
svm1	BUILTIN\Backup Operators	Backup Operators group
svm1	BUILTIN\Guests	Built-in Guests group
svm1	BUILTIN\Power Users	Restricted administrative privileges
svm1	BUILTIN\Users	All users
svm1	SMB_SERVER01\engineering	

Agregar usuarios locales al grupo local

Puede administrar la pertenencia a grupos locales agregando y quitando usuarios locales o de dominio, o agregando y quitando grupos de dominio. Esto resulta útil si desea controlar el acceso a los datos en función de los controles de acceso establecidos en el grupo o si desea que los usuarios tengan privilegios asociados a ese grupo. Si ya no desea que un usuario local, un usuario de dominio o un grupo de dominios tengan derechos o privilegios de acceso en función de su pertenencia a un grupo, puede eliminar al miembro del grupo.

Al añadir miembros a un grupo local, tenga en cuenta lo siguiente:

- No puede añadir usuarios al grupo especial Todos.
- No puede añadir un grupo local a otro grupo local.
- Para agregar un usuario o grupo de dominio a un grupo local, ONTAP debe poder resolver el nombre en un SID.

Al eliminar miembros de un grupo local, tenga en cuenta lo siguiente:

- No puedes eliminar miembros del grupo especial Todos.
- Para eliminar a un miembro de un grupo local, ONTAP debe poder resolver su nombre en un SID.

Debe tener la `fsxadmin` función necesaria para ejecutar los comandos utilizados en este procedimiento. Para obtener más información, consulte [Usuarios y roles de ONTAP](#).

Para administrar la pertenencia a un grupo local

- Agregue o elimine un miembro de un grupo mediante los comandos CLI [vserver cifs users-and-groups local-group add-members](#) y [vserver cifs users-and-groups local-group ONTAP remove-members](#).

- Para añadir miembros a un grupo de trabajo:

```
vserver cifs users-and-groups local-group add-members -vserver svm_name -group-name group_name -member-names name[,...]
```

Puede especificar una lista delimitada por comas de usuarios locales, usuarios de dominio o grupos de dominios para añadirlos al grupo local especificado.

- Para ver los miembros de un grupo de trabajo:

```
vserver cifs users-and-groups local-group show-members -vserver svm_name -group-name group_name
```

- Para eliminar miembros de un grupo de trabajo:

```
vserver cifs users-and-groups local-group remove-members -vserver svm_name -group-name group_name -member-names name[,...]
```

Puede especificar una lista delimitada por comas de usuarios locales, usuarios de dominio o grupos de dominios para eliminarlos del grupo local especificado.

En el siguiente ejemplo, se agrega un usuario local `SMB_SERVER01\sue` al grupo `SMB_SERVER01\engineering` local de SVM: `svm1`

```
FSxIdabcde123456:> vserver cifs users-and-groups local-group add-members -vserver svm1 -group-name SMB_SERVER01\engineering -member-names SMB_SERVER01\sue
```

El siguiente ejemplo elimina el usuario local `SMB_SERVER01\sue` y el grupo local `SMB_SERVER01\james` de `SMB_SERVER01\engineering` `svm1` SVM:

```
FSxIdabcde123456::> vservers cifs users-and-groups local-group remove-  
members -vservers svm1 -group-name SMB_SERVER01\engineering -member-names  
SMB_SERVER01\sue,SMB_SERVER01\james
```

En el siguiente ejemplo, se enumeran los miembros del grupo SMB_SERVER01\engineering local:

```
FSxIdabcdef01234::> vservers cifs users-and-groups local-group show-members -  
vservers svm_name -group-name group_name
```

```
Vserver: svm1  
Domain Name: SMB_SERVER01  
Group Name: SMB_SERVER01\engineering  
Member Name: SMB_SERVER01\anita  
SMB_SERVER01\james  
SMB_SERVER01\liang
```

Supervisión de los detalles de configuración de la máquina virtual de almacenamiento (SVM)

Puede ver las máquinas virtuales FSx de almacenamiento de ONTAP que se encuentran actualmente en su sistema de archivos mediante la FSx consola de Amazon, la API de Amazon y la FSx API de Amazon. AWS CLI

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-machines](#) CLI o la operación de [DescribeStorageVirtualMachines](#) API.

La respuesta del sistema es una lista de descripciones completas de SVMs todo lo que contiene tu cuenta Región de AWS.

Eliminación de máquinas virtuales de almacenamiento (SVM)

Solo puede eliminar un SVM FSx de ONTAP mediante la FSx consola de Amazon AWS CLI, la y la API. 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.

Cómo eliminar una máquina virtual de almacenamiento (consola)

1. Abra la FSx consola de Amazon 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 SVMs disponibles, expanda ONTAP y seleccione 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 volúmenes](#).
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).

Cómo eliminar una máquina virtual de almacenamiento (CLI)

- Para eliminar una FSx máquina virtual de almacenamiento ONTAP, utilice el comando [delete-storage-virtual-machine](#)CLI (o la operación [DeleteStorageVirtualMachine](#)API equivalente), como se muestra en el siguiente ejemplo.

```
aws fsx delete-storage-virtual-machine --storage-virtual-machine-id svm-  
abcdef0123456789d
```

Gestión de FSx volúmenes de ONTAP

Cada máquina virtual de almacenamiento (SVM) de un sistema de archivos FSx de ONTAP puede tener uno o más volúmenes. Un volumen es un contenedor de datos aislado para archivos, directorios o unidades lógicas de almacenamiento iSCSI (LUNs). 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 por NFS y SMB) al mismo volumen.

Puede crear volúmenes mediante la AWS Management Console, AWS CLI, la FSx API de Amazon o NetApp BlueXP. También puede utilizar el terminal administrativo del sistema de archivos o del SVM para crear, actualizar y eliminar volúmenes mediante el NetApp CLI de ONTAP o API REST.

Note

Puede crear 500 volúmenes por par de alta disponibilidad, hasta 1000 volúmenes en todos los pares de alta disponibilidad. FlexGroup Los volúmenes constitutivos se tienen en cuenta para este límite. De forma predeterminada, hay ocho volúmenes constitutivos por agregado, por FlexGroup.

Al crear un volumen, se definen las siguientes propiedades:

- Estilo de volumen: el [estilo de volumen](#) puede ser uno de los dos FlexVol o FlexGroup.
- Nombre de 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 un NetApp SnapMirror o SnapVault relación.
- 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 de almacenamiento: las características de [eficiencia de almacenamiento](#), que incluyen compactación, compresión y deduplicación de datos, proporcionan un ahorro de almacenamiento típico del 65 % para cargas de trabajo de uso compartido de archivos y de uso general.
- [Estilo de seguridad](#) del volumen (Unix o NTFS): determina qué tipo de permisos se usan para acceder a los datos del volumen al autorizar a los usuarios.
- Estratificación de datos: la [política de estratificación](#) define qué datos se almacenan en el nivel del grupo de capacidad rentable.
- [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 usar una política personalizada que se haya creado mediante la CLI de ONTAP o la API de 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. Puedes configurar esta opción mediante la FSx API AWS CLI o Amazon.

Temas

- [Estilos de volumen](#)
- [Tipos de volúmenes](#)
- [Estilo de seguridad del volumen](#)
- [Creación de volúmenes](#)
- [Actualización de volúmenes](#)

- [Movimiento de volúmenes entre agregados](#)
- [Supervisión de volúmenes](#)
- [Eliminación de volúmenes](#)

Estilos de volumen

FSx for ONTAP ofrece dos estilos de volúmenes que puede utilizar para distintos fines. Puede crear uno FlexVol o varios FlexGroup volúmenes mediante la FSx consola de Amazon AWS CLI, la y la FSx API de Amazon.

- **FlexVol** Los volúmenes ofrecen la experiencia más sencilla para los sistemas de archivos con un par de alta disponibilidad (HA), por lo que son el estilo de volumen predeterminado para los sistemas de archivos de primera generación y los sistemas de archivos de segunda generación con un par de HA. El tamaño mínimo de un FlexVol el volumen es de 20 mebibytes (MiB) y el tamaño máximo es de 314.572.800 MiB.
- **FlexGroup** los volúmenes se componen de varios componentes FlexVol volúmenes, lo que les permite ofrecer un rendimiento y una escalabilidad de almacenamiento superiores a FlexVol volúmenes para sistemas de archivos con varios pares de alta disponibilidad. FlexGroup los volúmenes son el estilo de volumen predeterminado para los sistemas de archivos de segunda generación con más de un par de alta disponibilidad. El tamaño mínimo de un FlexGroup el volumen es de 100 gibibytes (GiB) por componente y el tamaño máximo es de 20 pebibytes (PiB).

Puede convertir un volumen con FlexVol estilo al FlexGroup estilo con el ONTAP CLI, que crea un FlexGroup con un solo constituyente. Sin embargo, le recomendamos que lo utilice AWS DataSync para mover datos entre un FlexVol volumen y un nuevo FlexGroup volumen para garantizar que los datos se distribuyan uniformemente en el FlexGroup's electores. Para obtener más información, consulte [FlexGroup constituyentes](#).

Note

Si desea utilizar el ONTAP CLI para convertir un FlexVol volumen a FlexGroup volumen, asegúrese de eliminar todas las copias de seguridad del FlexVol volumen antes de convertirlo. ONTAP no reequilibra automáticamente los datos como parte de la conversión, por lo que es posible que los datos estén desequilibrados en el FlexGroup electores.

FlexGroup constituyentes

A FlexGroup el volumen está formado por componentes, que son FlexVol volúmenes. De forma predeterminada, en el FSx caso de ONTAP, se asignan ocho componentes a un FlexGroup volumen por par de HA.

Cuando crea su FlexGroup volumen, su tamaño se divide uniformemente entre sus componentes. Por ejemplo, si crea un disco de 800 gigabytes (GB) FlexGroup volumen con ocho componentes, cada componente tiene un tamaño de 100 GB. A FlexGroup el 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 un volumen con ocho componentes tiene un tamaño mínimo de 800 GB y un tamaño máximo de 20 PiB.

ONTAP distribuye los datos en el archivo entre los componentes. Puede almacenar hasta dos mil millones de archivos en cada componente de su FlexGroup volumen.

Cuando actualizas el tamaño de tu FlexGroup volumen, el nuevo tamaño se distribuye uniformemente entre sus componentes existentes.

También puede añadir más componentes a su FlexGroup volumen utilizando el ONTAP CLI o API REST. Sin embargo, le recomendamos que solo lo haga si necesita capacidad de almacenamiento adicional y todos los componentes ya tienen su tamaño máximo (300 TiB por componente). El agregado 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 sistema balanceado FlexGroup volumen. Cuando se escriben nuevos datos en el FlexGroup volumen, ONTAP prioriza su distribución entre los nuevos componentes hasta que los componentes estén equilibrados. Si añade nuevos componentes, le recomendamos que elija un número par y que no supere los ocho por agregado.

Note

Si añade nuevos componentes, las instantáneas existentes se convierten en instantáneas parciales; por lo tanto, no se pueden utilizar para restaurarlas por completo FlexGroup volumen a un estado anterior. Las instantáneas anteriores no pueden ofrecer una point-in-time imagen completa de su FlexGroup volumen porque los nuevos constituyentes aún no existían. Sin embargo, las instantáneas parciales se pueden usar para restaurar archivos y directorios individuales, crear un volumen nuevo o replicar con SnapMirror.

Tipos de volúmenes

FSx for ONTAP ofrece dos tipos de volúmenes que puede crear mediante la FSx consola de Amazon AWS CLI, la y la FSx API de Amazon.

- Los volúmenes de lectura y escritura (RW) se usan 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 un NetApp SnapMirror o SnapVault relación. Debe utilizar los volúmenes DP cuando desee [migrar](#) o [proteger los datos de un único](#) volumen.

FlexVol y FlexGroup los volúmenes pueden ser RW o DP.

Note

No es posible actualizar un tipo de volumen después de su creación.

Estilo de seguridad del volumen

Al crear un volumen FSx para ONTAP, puede elegir entre dos estilos de seguridad: Unix y NTFS. Cada estilo de seguridad tiene un efecto diferente en la forma en que se administran 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 ONTAP utiliza FSx para controlar el acceso a los datos y qué tipo de cliente puede modificar estos permisos.

Los dos factores que se usan para determinar el estilo de seguridad de un volumen son el tipo de administrador que gestiona el sistema de archivos y el tipo de usuario o servicio que accede a los datos del volumen.

Al crear un volumen en la FSx consola, la CLI y la API de Amazon, 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, consulta [Actualización de volúmenes](#).

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. Solo los clientes Linux pueden modificar los permisos con el estilo de seguridad de Unix, y los tipos de permisos que se utilizan en los archivos y directorios son mode-bits o NFS v4.x. ACLs
- **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. Solo los clientes de Windows pueden modificar los permisos con el estilo de seguridad NTFS, y los tipos de permisos que se utilizan en los archivos y directorios son NTFS. ACLs

Creación de volúmenes

Puede crear una FSx para ONTAP FlexVol o FlexGroup volumen mediante la FSx consola de Amazon AWS CLI, la y la FSx API de Amazon, además de la NetApp Interfaz de línea de comandos (CLI) de ONTAP y API REST.

Para crear un FlexVol volumen (consola)

Note

El estilo de seguridad del volumen se establece automáticamente en el estilo de seguridad del volumen raíz.

1. Abra la FSx consola de Amazon 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, selecciona Amazon FSx for NetApp ONTAP.
5. En la sección Información 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, selecciona FlexVol.
7. En la sección Detalles del volumen, proporcione la siguiente información:
 - En el campo Volume name, introduzca un nombre para el volumen. Puede usar 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, elija 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 un NetApp SnapMirror o SnapVault relación. 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 Activado para activar las características de eficiencia del almacenamiento de ONTAP (desduplicación, compresión y compactación) de este volumen. Para obtener más información, consulte [Eficacia de almacenamiento](#).
 - Para el estilo de seguridad del volumen, elija entre Unix (Linux) y NTFS 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 [Crear una política de instantáneas](#) en la NetApp Documentación del producto ONTAP.

8. En la sección Estratificación del almacenamiento, proporcione la siguiente información:

- En Política de estratificación del grupo de capacidad, seleccione la política de estratificación del grupo de almacenamiento para el volumen, que puede ser automática (la predeterminada), solo instantáneas, todas o ninguna. Para obtener más información, consulte [Políticas de estratificación del volumen](#).
 - Si selecciona automática o solo instantáneas, puede establecer el periodo de enfriamiento de la política de estratificación para definir la cantidad de días 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 comprendido entre 2 y 183 días. El valor predeterminado es de 31 días.
9. En la sección Avanzadas, para SnapLock Configuración, elija entre Activado y Desactivado. Para obtener más información sobre la configuración de un SnapLock Volumen de conformidad o un SnapLock Volumen empresarial, consulte [Descripción SnapLock Conformidad](#) y [Descripción SnapLock Enterprise](#). 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 Estado del panel Volúmenes. El volumen está listo para su uso cuando su estado es Creado.

Para crear un FlexGroup volumen (consola)

 Note

Solo puedes crear FlexGroup volúmenes para sistemas de archivos con varios pares de alta disponibilidad mediante la FSx consola de Amazon. Para crear FlexVol para volúmenes para sistemas de archivos con varios pares de alta disponibilidad, utilice la AWS CLI FSx API de Amazon o las herramientas NetApp de administración.

1. Abre la FSx consola de Amazon 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, selecciona Amazon FSx for NetApp ONTAP.
5. En la sección Información 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, seleccione FlexGroup.
7. En la sección Detalles del volumen, proporcione la siguiente información:
- En el campo Volume name, introduzca un nombre para el volumen. Puede usar hasta 203 caracteres alfanuméricos o de subrayado (_).
 - En Tamaño de volumen, introduzca cualquier número entero en el rango de 800 gibibytes (GiB) a 2400 tebibytes (TiB) por par de HA. Por ejemplo, un sistema de archivos con 12 pares de alta disponibilidad (HA) tendría un tamaño de volumen mínimo de 9600 GiB y un tamaño máximo de 20 480 TiB.
 - Para el tipo de volumen, elija Lectura/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 utilizarse como destino de un NetApp SnapMirror o SnapVault relación. 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 [Eficacia de almacenamiento](#).
 - Para el estilo de seguridad del volumen, elija entre Unix (Linux) y NTFS 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 [Crear una política de instantáneas](#) en la NetApp Documentación del producto ONTAP.

8. En la sección Estratificación del almacenamiento, proporcione la siguiente información:
 - En Política de estratificación del grupo de capacidad, seleccione la política de estratificación del grupo de almacenamiento para el volumen, que puede ser automática (la predeterminada), solo instantáneas, todas o ninguna. Para obtener más información, consulte [Políticas de estratificación del volumen](#).
 - Si selecciona automática o solo instantáneas, puede establecer el periodo de enfriamiento de la política de estratificación para definir la cantidad de días 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 comprendido entre 2 y 183 días. El valor predeterminado es de 31 días.
9. En la sección Avanzadas, para SnapLock Configuración, elija entre Activado y Desactivado. Para obtener más información sobre la configuración de un SnapLock Volumen de conformidad o un SnapLock Volumen empresarial, consulte [Descripción SnapLock Conformidad](#) y [Descripción SnapLock Enterprise](#). 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 Estado del panel Volúmenes. El volumen está listo para su uso cuando su estado es Creado.

Cómo crear un volumen (CLI)

- Para crear un volumen FSx para ONTAP, utilice el comando CLI [create-volume](#) (o la operación API [CreateVolume](#) 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 la copia de seguridad de un volumen en un volumen nuevo. Para obtener más información, consulte [Restauración de copias de seguridad en un volumen nuevo](#).

Actualización de volúmenes

Puede actualizar la configuración de un volumen FSx para ONTAP mediante la FSx consola de Amazon AWS CLI, la y la FSx API de Amazon, además de la NetApp Interfaz de línea de comandos (CLI) de ONTAP y API REST. Puede modificar las siguientes propiedades de un volumen existente FSx para ONTAP:

- 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 las copias de seguridad (mediante la FSx API AWS CLI y Amazon)

Para obtener más información, consulte [Gestión de FSx volúmenes de ONTAP](#).

Cómo actualizar la configuración de un volumen (consola)

1. Abre la FSx consola de Amazon 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, puedes aumentar o disminuir el tamaño del volumen dentro del rango especificado en la FSx consola de Amazon. En FlexVol volúmenes, el tamaño máximo es de 300 TiB. En FlexGroup volúmenes, el tamaño máximo es de 300 TiB multiplicado por el número total de volúmenes constitutivos que su FlexGroup tiene, hasta un máximo de 20 PiB.

8. En [Eficiencia de almacenamiento](#), seleccione Activado para activar las características de eficiencia de almacenamiento de ONTAP (desduplicación, compresión y compactación) del volumen o seleccione 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 del volumen](#).
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 NTFS o UNIX ACLs 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 [Crear una política de instantáneas en](#) el NetApp Documentación del producto 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.

Cómo 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 API [UpdateVolume](#) 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
```

Expansión FlexGroup volumes

Puede añadir volúmenes constitutivos adicionales a su FlexGroup volumen con el `volume expand` comando de ONTAP CLI. Esta es una práctica recomendada después de agregar pares de alta disponibilidad (HA) al sistema de archivos, ya que garantiza que FlexGroup el volumen se mantiene equilibrado.

Antes de expandir tu FlexGroup volumen, tenga en cuenta los siguientes puntos:

- Todo de un FlexGroup's los volúmenes constitutivos tienen la misma capacidad de almacenamiento. Cuando amplías tu FlexGroup volumen con componentes adicionales, cada componente es del mismo tamaño que los componentes existentes. Por lo tanto, corrobore que cada agregado tenga suficiente espacio disponible antes de agregar los componentes.
- AWS recomienda mantener ocho volúmenes de componentes por agregado para cada uno FlexGroup volumen. Ocho volúmenes constitutivos por agregado maximizan el paralelismo de FlexGroup volúmenes y ofrece el rendimiento más óptimo para su carga de trabajo. Por lo general, solo recomendamos ampliar su FlexGroup volumen con componentes adicionales si agrega pares de HA. Este es el único escenario en el que tendría que agregar componentes para mantener ocho componentes por agregado.
- Si las recetas FlexGroup el volumen está en un SnapMirror relación, entonces tanto el origen como el destino FlexGroup los volúmenes deben tener el mismo número de componentes. De lo contrario, SnapMirror las transferencias fallarán. SnapMirror opera a nivel de constituyente y transfiere datos entre cada constituyente individual. Por lo tanto, si expande un FlexGroup volumen con volúmenes constitutivos adicionales, también debe expandir manualmente cualquier volumen que se encuentre en un SnapMirror relación con él.
- Cuando expandes un FlexGroup volumen con componentes adicionales, todas sus copias instantáneas existentes se convierten en copias «parciales». Las copias parciales no se pueden restaurar, pero se pueden examinar y se pueden restaurar los archivos individuales. Además, esto se traduce en la pérdida de cualquier incrementalidad de las copias de FSx seguridad, AWS copias de seguridad o SnapMirror relaciones.
- No puede eliminar los volúmenes de componentes una vez que los haya agregado.

Sumar FlexGroup componentes de volumen

Puede utilizar el ONTAP CLI para añadir los volúmenes constitutivos a su FlexGroup volumen.

Para añadir FlexGroup componentes de volumen

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 [Administrar sistemas de archivos con el ONTAP CLI](#).

2. [Utilice la opción de expansión de volumen](#) ONTAP Comando CLI para expandir su FlexGroup volumen con componentes adicionales. Reemplace los siguientes valores:
- *svm_name* con el nombre de la máquina virtual de almacenamiento (SVM) que aloja su FlexGroup volumen (por ejemplo, *svm1*).
 - *vol_name* con el nombre del FlexGroup volumen que desea expandir (por ejemplo, *vol1*).
 - *aggregates* con una lista de los agregados separados por comas que desee añadir FlexGroup los volúmenes constitutivos en. Por ejemplo, *aggr1* para un único agregado o *aggr1, aggr2* para varios agregados.
 - *constituent_per_aggregate* con el número de componentes adicionales que desee agregar a cada uno de los *aggregates* especificados. Solo debe añadir los componentes suficientes para garantizar que su FlexGroup el volumen tiene un número equilibrado de componentes en todos los agregados en los que reside.

```
::> volume expand -vserver svm_name -volume vol_name -aggr-list aggregates -aggr-list-multiplier constituents_per_aggregate
```

Important

No puedes eliminar FlexGroup los componentes después de añadirlos, así que compruebe las entradas antes de ejecutar el comando anterior.

Movimiento de volúmenes entre agregados

Cuando agrega pares de alta disponibilidad (HA) al sistema de archivos, necesita reequilibrar los datos existentes moviendo los volúmenes a los nuevos agregados. Para mover un volumen entre agregados, puede usar el comando `volume move` de la CLI de ONTAP.

Antes de usar el comando `volume move`, tenga en cuenta los siguientes aspectos:

- El uso del comando `volume move` puede afectar al rendimiento porque consume recursos de red y disco del sistema de archivos. Por lo tanto, recomendamos mover los volúmenes entre agregados durante los periodos de baja actividad. Como alternativa, puede reducir la utilización del rendimiento de la red y el del disco en el sistema de archivos a no más del 50 % mientras mueve los volúmenes.
- Para reducir el impacto en el rendimiento del sistema de archivos, le recomendamos mover un solo volumen entre dos pares de HA y agregados por la vez. Por ejemplo, si el sistema de archivos tiene cuatro pares de HA, le recomendamos mover dos volúmenes por la vez (suponiendo que los movimientos del volumen no se realicen desde o hacia los mismos pares de HA). ONTAP permite mover hasta ocho volúmenes de cada par de HA por vez, pero si hay más movimientos de volumen simultáneos, se reducirá el rendimiento tanto de las operaciones de E/S del cliente como de cualquier movimiento de volumen en curso.
- Todos los datos almacenados en el nivel de SSD del volumen afectado se transfieren físicamente a un conjunto diferente de discos en un servidor de archivos distinto. Esta operación se realiza en segundo plano y lleva tiempo. La velocidad de la transferencia depende de la capacidad de rendimiento y de la cantidad de actividad del sistema de archivos. Sin embargo, el movimiento del volumen se puede limitar. Para obtener más información, consulte [Limitación de los movimientos de volumen](#).
- Los datos almacenados en el nivel de capacidad no se mueven físicamente porque los pares de HA comparten el mismo almacenamiento del grupo de capacidad. Como resultado, será más rápido mover los volúmenes con la mayoría de los datos agrupados en niveles. Tenga en cuenta que los metadatos de los archivos siempre se almacenan en el nivel de SSD. Para obtener más información, consulte [Organización de datos de volumen en niveles](#).

Fases del movimiento de un volumen

La operación de traslado de un volumen consta de dos fases: la fase de replicación y la fase de transición. Durante la fase de replicación, los datos existentes se replican en el nuevo agregado del volumen. Durante la fase de transición, ONTAP intenta realizar una transferencia rápida final al

nuevo agregado del volumen. Esto incluye transferir cualquier dato que se haya escrito durante la fase de transferencia y redirigir el tráfico nuevo al agregado del volumen recién creado. De forma predeterminada, el periodo de transición es de 30 segundos y detiene todas las E/S del volumen. Si ONTAP no puede realizar todos estos pasos durante el periodo de transición, se producirá un error. De forma predeterminada, ONTAP intentará transferir tres veces consecutivas. Si los tres intentos consecutivos fallan, ONTAP lo volverá a intentar una vez cada hora hasta que lo consiga. Puede reducir la carga del sistema de archivos para garantizar que la fase de transición se realice correctamente reduciendo o pausando el tráfico de E/S del volumen antes de que comience la fase de transición.

Inicio de movimientos de volumen

Cómo iniciar un movimiento de volumen

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 [Administrar sistemas de archivos con el ONTAP CLI](#).

2. Ejecute el comando [volume move start](#) de la CLI de ONTAP. Reemplace los siguientes valores:
 - `vserver_name` con el nombre de la SVM que aloja el volumen que se va a mover.
 - `volume_name` con el nombre del componente del volumen (por ejemplo, `vol1__0001`).
 - `aggregate_name` con el nombre del agregado de destino del volumen.
 - `-enforce-network-throttling` para limitar el rendimiento total del movimiento de volumen. Es opcional.

```
::> volume move start -vserver svm_name -volume volume_name --destination-  
aggregate 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.
```

Important

El traslado de volúmenes consume recursos de red y disco para los servidores de archivos de origen y destino. Por lo tanto, el rendimiento de la carga de trabajo puede verse afectado por cualquier movimiento de volumen que se esté realizando. Además, el tráfico de E/S al volumen se detendrá temporalmente durante la fase de transición del movimiento del volumen.

Supervisión de movimientos de volumen

Cómo supervisar un movimiento de volumen

- Para comprobar el estado de la operación de movimiento de volumen, use el comando `volume move show` de la CLI de ONTAP.

```
::> 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: FsxD01234567890abcdef-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: aggr1
Source Node: FsxD01234567890abcdef-01
Move State: healthy
```

El resultado del comando muestra el tiempo estimado para completar el movimiento. Cuando haya terminado, la `Move phase` mostrará el estado `completed`.

Mantener el equilibrio FlexGroup volumes

Para que su carga de trabajo funcione de manera óptima, su FlexGroup los volúmenes deben abarcar todos los agregados y tener un número par de volúmenes constitutivos por agregado. Recomendamos tener ocho componentes por agregado. Tenga en cuenta los siguientes escenarios al reequilibrar FlexGroup volúmenes:

- En movimiento FlexGroup componentes entre los agregados existentes: si mueve un FlexGroup's volumen constitutivo a otro agregado de un volumen que de otro modo estaría equilibrado FlexGroup, a continuación, debe mover otro componente que se utilice menos al agregado original. Esto asegura que su FlexGroup tiene un número par de componentes por agregado.

¿Se mueve FlexGroup los componentes se convierten en nuevos agregados después de agregar pares de HA: si mueve un FlexGroup's los volúmenes constitutivos a nuevos agregados después de añadir los pares de HA, debería expandir el FlexGroup con componentes adicionales en los agregados que perdieron componentes. Esto asegura que su FlexGroup tiene un número par de componentes por agregado. Para obtener más información, consulte [the section called "Expanding FlexGroup volumes"](#).

Limitación de los movimientos de volumen

Si desea limitar el ancho de banda de un movimiento de volumen en el sistema de archivos, puede agregar la opción `-enforce-network-throttling` al principio de la operación.

Note

El uso de esta opción afecta a los entrantes SnapMirror transferencias de datos de replicación para el sistema de archivos. Lleve un registro de cómo configura las opciones de replicación del sistema de archivos porque no podrá verlas después de configurarlas.

Cómo limitar un movimiento de volumen

1. El límite usa el límite de replicación global. Para configurar el acelerador de replicación global, utilice el siguiente comando en ONTAP CLI.

```
::> options -option-name replication.throttle.enable on
```

2. Especifique el ancho de banda total máximo que puede usar la replicación y sustituya la siguiente opción:
 - `kbs_throttle` con el rendimiento máximo deseado para usarlo en cualquier replicación (incluyendo SnapMirror y el volumen se mueve), en kilobytes por segundo.

```
::> options -option-name replication.throttle.incoming.max_kbs kbs_throttle
::> options -option-name replication.throttle.outgoing.max_kbs kbs_throttle
```

Supervisión de volúmenes

Puede ver los volúmenes que se encuentran actualmente en su sistema de archivos mediante la FSx consola de Amazon AWS CLI, la y la FSx API de Amazon y SDKs.

Para supervisar los volúmenes del 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 [DescribeVolumes](#) la operación de API.

```
$ aws fsx describe-volumes
{
  "Volumes": [
    {
      "CreationTime": "2024-03-04T20:17:44+00:00",
      "FileSystemId": "fs-abcdef0123a0bb087",
      "Lifecycle": "CREATED",
      "Name": "SVM8_ext_root",
      "OntapConfiguration": {
        "FlexCacheEndpointType": "NONE",
        "JunctionPath": "/",
        "SecurityStyle": "NTFS",
        "SizeInMegabytes": 1024,
        "StorageEfficiencyEnabled": false,
        "StorageVirtualMachineId": "svm-01234567890abcdef",
        "StorageVirtualMachineRoot": true,
        "TieringPolicy": {
```

```

        "Name": "NONE"
      },
      "UUID": "42ce3de0-da64-11ee-a22d-7f7cdfb8d381",
      "OntapVolumeType": "RW",
      "SnapshotPolicy": "default",
      "CopyTagsToBackups": false,
      "VolumeStyle": "FLEXVOL",
      "AggregateConfiguration": {
        "Aggregates": [
          "aggr1"
        ]
      },
      "SizeInBytes": 1073741824
    },
    "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcdef0123a0bb087/fsvol-abcdef0123456789a",
    "VolumeId": "fsvol-abcdef0123456789a",
    "VolumeType": "ONTAP"
  }
]
}

```

Visualización de volúmenes sin conexión

No puede crear ni eliminar copias de seguridad de volúmenes cuando el volumen de origen está desconectado. Puede utilizar el [volume show](#) ONTAP Comando CLI para determinar el estado actual de un volumen.

```
volume show -vserver svm-name
```

Para obtener información sobre cómo acceder al ONTAP CLI en su sistema de archivos, consulte [Uso de NetApp ONTAP CLI](#).

```
FsxIdabc12345::> volume show -vserver vs1
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used%
vs1	vol1	aggr1	online	RW	2GB	1.9GB	5%
vs1	vol1_dr	aggr0_dp	online	DP	200GB	160.0GB	20%
vs1	vol2	aggr0	online	RW	150GB	110.3GB	26%
vs1	vol2_dr	aggr0_dp	online	DP	150GB	110.3GB	26%
vs1	vol3	aggr1	online	RW	150GB	120.0GB	20%

vs1	vol3_dr	aggr1_dp	online	DP	150GB	120.0GB	20%
vs1	vol4	aggr1	online	RW	200GB	159.8GB	20%

7 entries were displayed.

Para volver a poner en línea un volumen sin conexión, utilice la [volume online](#) ONTAP Comando CLI, como se muestra en el siguiente ejemplo. Si solo existe un SVM (Vserver), no es necesario que especifique el `-vserver` parámetro.

```
FsxID-abcdef123456:> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

Eliminación de volúmenes

Puede eliminar un volumen FSx de ONTAP mediante la FSx consola de Amazon AWS CLI, la y la FSx API de Amazon, además de NetApp Interfaz de línea de comandos (CLI) de ONTAP y API REST.

Antes de eliminar un volumen, asegúrese de que ninguna aplicación esté accediendo a los datos del volumen que desea eliminar.

Important

Solo puede eliminar volúmenes mediante la FSx consola, la API o la CLI de Amazon si el volumen tiene habilitadas las FSx copias de seguridad de Amazon.

Realizar una copia de seguridad final del volumen

Cuando eliminas un volumen con la FSx consola de Amazon, tienes la opción de realizar una copia de seguridad final del volumen. Como práctica recomendada, te recomendamos que optes por realizar una copia de seguridad final. 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.

Para obtener más información sobre las copias de seguridad por volumen, consulte [Protección de datos con copias de seguridad de volúmenes](#).

Cómo eliminar un volumen (consola)

1. Abra la FSx consola de Amazon 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. (SnapLock Enterprise (solo volúmenes) Para Bypass SnapLock Enterprise Retention, seleccione Sí.
7. 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.
8. Para confirmar la eliminación del volumen, escriba delete en el campo Confirmar eliminación.
9. Seleccione Eliminar volúmenes.

Cómo eliminar un volumen (CLI)

- Para eliminar un FSx volumen de ONTAP, utilice el comando CLI [delete-volume](#) (o la operación API [DeleteVolume](#) equivalente), como se muestra en el siguiente ejemplo.

```
aws fsx delete-volume --volume-id fsvol-1234567890abcde
```

Eliminación SnapLock volumes

En esta sección se explica cómo eliminar un SnapLock volumen.

Puede eliminar un SnapLock Volumen de cumplimiento si los períodos de retención de todos los archivos de escritura única y lectura múltiple (WORM) que contiene han caducado.

 Note

Al cerrar un archivo Cuenta de AWS que contenga SnapLock Enterprise o Compliance volúmenes AWS y, FSx para ONTAP, suspenda su cuenta durante 90 días dejando sus datos intactos. Si no vuelve a abrir su cuenta durante esos 90 días, AWS eliminará sus datos, incluidos los datos de SnapLock volúmenes independientemente de tu configuración de retención.

Puede eliminar un SnapLock Un volumen empresarial en cualquier momento si dispone de los permisos necesarios. Para eliminar un SnapLock Volumen empresarial mediante ONTAP CLI, usted debe tener la `fsxadmin` función. Para obtener más información, consulte [Roles y usuarios del administrador del sistema de archivos](#).

Para eliminar un SnapLock Para un volumen empresarial que contenga datos de WORM con una política de retención activa mediante la FSx consola de Amazon, la CLI o la FSx API de Amazon, debe tener el permiso de `fsx:BypassSnapLockEnterpriseRetention` IAM.

 Warning

El período mínimo de retención de un SnapLock el volumen del registro de auditoría es de seis meses. Hasta que finalice este período de retención, no podrá eliminar el SnapLock el volumen del registro de auditoría, la máquina virtual de almacenamiento (SVM) o el sistema de archivos asociado a la SVM, incluso si el volumen se creó en SnapLock Modo empresarial. Para obtener más información, consulte [SnapLock auditar volúmenes de registro](#).

Creación de un iSCSI LUN

En este proceso se describe cómo crear un LUN iSCSI en un sistema de archivos de Amazon FSx for NetApp ONTAP mediante el NetApp ONTAP `lun create` Comando CLI. Para obtener más información, consulte [lun create](#) en la NetApp ONTAP Centro de documentación.

 Note

El protocolo iSCSI no es compatible con sistemas de archivos con más de seis pares de HA.

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 al ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando. 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 [Administrar sistemas de archivos con el ONTAP CLI](#).

2. Cree un LUN mediante el `lun create` NetApp CLI comando, sustituyendo los siguientes valores:
 - **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
<i>svm_name</i>	<i>/vol/vol_name/lun_name</i>	online	unmapped	windows_2008	10GB

Pasos a seguir a continuación

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 [Aprovisionamiento de iSCSI para Linux](#) o [Aprovisionamiento de iSCSI para Windows](#).

Optimización del rendimiento con las ventanas FSx de mantenimiento de Amazon

Al tratarse de un servicio totalmente gestionado, FSx 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 es posible que notes un impacto breve (menos de 60 segundos) en el rendimiento cuando se realiza el mantenimiento; Amazon FSx 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. Cuando se aplican parches, se aplican parches a cada uno de los servidores de archivos del sistema de archivos de a uno y, por lo general, se tarda hasta una hora en aplicar parches a cada servidor de archivos. Antes de aplicar parches a un servidor de archivos dentro de un par de HA, el sistema de archivos se desplaza automáticamente al socio de HA de los servidores de archivos, lo que puede provocar una breve pausa de E/S (menos de 60 segundos) para cualquier E/S dirigida a ese par de HA. A continuación, el sistema de archivos se recuperará, lo que puede provocar otra breve pausa de E/S (menos de 60 segundos). El inicio del periodo de mantenimiento se elige durante la creación del sistema de archivos. Si no selecciona el periodo, se le asigna uno automáticamente.

Important

Para garantizar que el sistema de archivos se pueda parchear correctamente, FSx ONTAP pondrá en línea todos los volúmenes que estén fuera de línea mientras dure el proceso de aplicación de parches. Los clientes no podrán acceder FSx a los volúmenes que Amazon vuelva a poner en línea.

FSx for ONTAP le permite ajustar el período de mantenimiento según sea necesario para adaptarse a su carga de trabajo y sus requisitos operativos. Puede cambiar el periodo de mantenimiento con la frecuencia que necesite, siempre que se realice uno al menos una vez cada 14 días. Si se publica un parche y no se aplica ningún período de mantenimiento en un plazo de 14 días, FSx ONTAP procederá al mantenimiento del sistema de archivos para garantizar su seguridad y fiabilidad.

Note

Para garantizar la integridad de los datos durante las actividades de mantenimiento, FSx ONTAP cierra todos los bloqueos oportunistas y completa cualquier operación de escritura pendiente en los volúmenes de almacenamiento subyacentes que alojan el sistema de archivos antes de que comience el mantenimiento.

Puede utilizar la Amazon FSx Management Console AWS CLI, la AWS API o alguna de las AWS SDKs para cambiar el período de mantenimiento de sus sistemas de archivos.

Cómo cambiar el período de mantenimiento semanal (consola)

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

2. Seleccione File systems (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 Update (Actualizar) para que aparezca la ventana Change maintenance window (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-system](#) CLI, consulte [Cómo actualizar un sistema de archivos \(CLI\)](#).

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 rendimiento de su sistema de archivos en cualquier momento. Tenga en cuenta que su sistema de archivos requiere una configuración específica para alcanzar la máxima capacidad de rendimiento. Por ejemplo, para aprovisionar el 4% GBps de la capacidad de rendimiento de un sistema de archivos de primera generación, el sistema de archivos requiere una configuración con una capacidad mínima de almacenamiento SSD de 5.120 GiB y 160.000 IOPS de SSD. Para obtener 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 obtener más información, consulte [Rendimiento](#).

Cuando modificas la capacidad de procesamiento de tu sistema de archivos, Amazon FSx cambia el servidor de archivos que alimenta tu 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 ONTAP cierra todos los bloqueos oportunistas y completa cualquier operación de escritura pendiente 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 obtener más información, consulte [the section called “Actualización de periodos de mantenimiento”](#).

Temas

- [Cuándo modificar la capacidad de rendimiento](#)
- [¿Cómo se gestionan las solicitudes simultáneas?](#)
- [Actualización de la capacidad de rendimiento](#)
- [Monitoreo de los cambios en la capacidad de rendimiento](#)

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 obtener más información, consulte [the section called “Monitorización en la FSx consola de Amazon”](#).

¿Cómo se gestionan las solicitudes simultáneas?

En el caso de sistemas de archivos de primera generación, 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 en 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 envías una SSD/IOPS update and throughput capacity update at the same time, both requests are accepted. The SSD/IOPS actualización, se prioriza antes que la actualización de la capacidad de rendimiento.
- Si envía una actualización de la capacidad de rendimiento mientras SSD/IOPS update is in progress, the throughput capacity update request is accepted and queued to occur after the SSD/IOPS update. The throughput capacity update starts after SSD/IOPS se actualiza una (hay nuevos valores disponibles) y durante el paso de optimización. Esto normalmente dura menos de 10 minutos.
- Si envía una solicitud de actualización SSD/IOPS update while a throughput capacity update is in progress, the SSD/IOPS de almacenamiento, se acepta y se pone en cola para comenzar una vez que se haya completado la actualización de la capacidad de rendimiento (hay una nueva capacidad de rendimiento disponible). Esto normalmente dura 20 minutos.

Tenga en cuenta los siguientes aspectos al solicitar una actualización de la capacidad de rendimiento para los sistemas de archivos de segunda generación:

- Debe esperar un mínimo de seis horas entre actualizaciones de la capacidad de rendimiento de los sistemas de archivos de segunda generación.
- El periodo de recuperación de la capacidad de rendimiento se comparte con el escalado de SSD/IOPS.
- El escalado de la capacidad de rendimiento y el escalado de SSD/IOPS no se pueden realizar de forma simultánea ni ponerse en cola mientras uno está en curso.
- No puede añadir pares de alta disponibilidad (HA) junto con el escalado o escalado de la capacidad de rendimiento y el escalado de la capacidad de rendimiento. SSD/IOPS scaling are in progress. However, adding HA pairs doesn't share a cooldown with SSD/IOPS Para obtener más información, consulte [Agregar pares de alta disponibilidad \(HA\)](#).

Para obtener más información sobre el almacenamiento en SSD y las actualizaciones de IOPS aprovisionadas, consulte [Administración de la capacidad de almacenamiento](#).

Actualización de la capacidad de rendimiento

Puedes modificar la capacidad de procesamiento de un sistema de archivos mediante la FSx consola de Amazon, la AWS Command Line Interface (AWS CLI) o la FSx API de Amazon.

Note

Debe esperar un mínimo de seis horas entre actualizaciones de la capacidad de rendimiento de los sistemas de archivos de segunda generación.

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

1. Abre la FSx consola de Amazon 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.
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).

Puedes supervisar el progreso de la actualización mediante la FSx consola de Amazon AWS CLI, la y la API. Para obtener más información, consulte [Monitoreo de los cambios en la capacidad de rendimiento](#).

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

Para modificar la capacidad de procesamiento de un sistema de archivos, usa el AWS CLI comando [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.

Puedes supervisar el progreso de la actualización mediante la FSx consola de Amazon AWS CLI, la y la API. Para obtener más información, consulte [Monitoreo de los cambios en la capacidad de rendimiento](#).

Monitoreo de los cambios en la capacidad de rendimiento

Puede supervisar el progreso de una modificación de la capacidad de rendimiento mediante la FSx consola de Amazon, la API y el 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.

Estado

El estado actual de la actualización. Para las actualizaciones de capacidad de rendimiento, los valores posibles son los siguientes:

- Pendiente: Amazon FSx ha recibido la solicitud de actualización, pero no ha empezado a procesarla.
- En curso: Amazon FSx está procesando la solicitud de actualización.
- Finalizado: la actualización de la capacidad de rendimiento se completó correctamente.
- Error: se produjo un error en la actualización de la capacidad de rendimiento. Elija el signo de interrogación (?) para ver detalles sobre el motivo por el que se produjo un error en la actualización del rendimiento.

Tiempo de solicitud

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

Supervisar los cambios con la API AWS CLI y

Puede ver y supervisar las solicitudes de modificación de la capacidad de rendimiento del sistema de archivos mediante el comando [describe-file-systems](#) CLI y la acción de la [DescribeFileSystems](#) API. 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 MBps y una capacidad de rendimiento objetivo de 256 MBps

```
.  
.   
.   
  "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.

Gestión de recursos compartidos SMB

Para gestionar los archivos compartidos SMB en su sistema de FSx archivos de Amazon, 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 administrar los recursos compartidos de archivos SMB mediante el Administrador del NetApp sistema. Para obtener más información, consulte [Utilización NetApp System Manager con BlueXP](#).

Para conectar carpetas compartidas a tu sistema de FSx archivos de Amazon

1. Lanza tu EC2 instancia de Amazon y conéctala al Active Directory de Microsoft al que está unido tu sistema de FSx archivos de Amazon. Para ello, elija uno de los procedimientos siguientes de la Guía de administración AWS Directory Service :
 - [Únase sin problemas a una EC2 instancia de Windows](#)
 - [Cómo unir manualmente una instancia de Windows](#)

2. Conéctese a la instancia con un usuario que sea miembro del grupo de administradores del sistema de archivos. Para obtener más información, consulte [Conectarse a su instancia de Windows](#) en la Guía del EC2 usuario de Amazon.
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 FSx consola de Amazon, elija Storage virtual machines, elija su SVM y, a continuación, desplácese hacia abajo hasta Endpoints hasta encontrar el nombre DNS SMB. También puede obtener el nombre DNS en la respuesta a la operación de la API. [DescribeStorageVirtualMachines](#)

6. Seleccione Aceptar. A continuación, aparecerá una entrada para tu sistema de FSx archivos de Amazon en la lista de la herramienta Carpetas compartidas.

Ahora que Shared Folders está conectado a tu sistema de FSx archivos de Amazon, puedes 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.

- Crear un nuevo recurso compartido de archivos: en la herramienta Carpetas compartidas, selecciona Shares en el panel izquierdo para ver los recursos compartidos activos de tu sistema de FSx archivos de Amazon. 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

La eliminación de archivos compartidos de la GUI solo es posible si se ha conectado a fsmgmt.msc con el nombre DNS del sistema de archivos de 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.

Gestión de FSx los recursos de ONTAP mediante NetApp aplicaciones

Además de la AWS Management Console AWS CLI, y la AWS API y SDKs, también puede utilizar estas NetApp herramientas y aplicaciones de administración para administrar sus recursos FSx de ONTAP:

Temas

- [Registrarse en un NetApp inscrita](#)
- [Utilización NetApp BlueXP](#)
- [Uso de NetApp ONTAP CLI](#)
- [Uso de ONTAP API de REST](#)

 Important

Amazon FSx se sincroniza periódicamente con 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, AWS CLI, API y SDKs.

Registrarse en un NetApp inscrita

Para descargar algunos NetApp software, como BlueXP, SnapCenter, y el ONTAP Conector antivirus, es necesario tener un NetApp account. Para suscribirse a un NetApp lleve a cabo los siguientes pasos:

1. Ve a la [NetApp](#) Página de registro de usuarios y regístrese para obtener una nueva NetApp cuenta de usuario.
2. Complete los formularios con su información. Asegúrese de seleccionar la NetApp Nivel de acceso de cliente/usuario final. En el campo NÚMERO DE SERIE, copie y pegue el ID del sistema de archivos del sistema de archivos FSx de ONTAP. Vea el siguiente ejemplo:

USER ACCESS LEVEL

- ☐ Guest User ☒ NetApp Customer / End User
- ☐ NetApp Reseller / Service Provider / System Integrator / Partner

Product Information (Optional)

Please enter a Serial Number or System ID to help us validate your access level.

Please note: Not providing a Serial Number or System ID may delay processing of your request.

SERIAL NUMBER

fs-0de9123abcf12368a

(Either a NetApp hardware Serial Number, often located on back of unit; or a NetApp software Serial Number.)

OR

SYSTEM ID

(Run a "sysconfig -a" command on your NetApp product. The output should list the System ID.)

NETAPP TOKEN

Qué esperar después de registrarse

Cientes con NetApp los productos pasarán de tener acceso a la cuenta de NSS al nivel de cliente en el plazo de un día laborable. Clientes nuevos en NetApp se incorporarán siguiendo las prácticas comerciales estándar, además de tener su cuenta de NSS nivelada con el acceso a nivel de cliente. Proporcionar el identificador del sistema de archivos ayudará 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.

Utilización 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 FSx Amazon NetApp for ONTAP](#).

 Note

NetApp BlueXP no es compatible con los sistemas de archivos de segunda generación con más de un par de alta disponibilidad (HA).

Utilización NetApp System Manager con BlueXP

Puede gestionar sus sistemas de archivos de Amazon FSx for NetApp ONTAP mediante System Manager directamente desde BlueXP. BlueXP le permite utilizar la misma interfaz de System Manager a la que está acostumbrado, para 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 de segunda generación con más de un par de alta disponibilidad.

Uso de NetApp ONTAP CLI

Puede gestionar sus recursos de Amazon FSx for NetApp ONTAP mediante el NetApp ONTAP CLI. Puede administrar los recursos en el sistema de archivos (de forma análoga a NetApp A nivel de ONTAP (clúster) y a nivel de SVM).

Administrar sistemas de archivos con el ONTAP CLI

Puede ejecutar ONTAP Comandos CLI en FSx el sistema de archivos ONTAP, similares a ejecutarlos en un NetApp ONTAP clúster. Puede acceder al ONTAP CLI en su sistema de archivos mediante el establecimiento de una conexión shell segura (SSH) con el punto final de administración del sistema de archivos e iniciando sesión con el `fsxadmin` nombre de usuario y la contraseña. Tiene la opción de establecer la `fsxadmin` contraseña al crear un 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, la `fsxadmin` contraseña no estaba configurada, por lo que tendrá que establecer una para iniciar sesión en el ONTAP CLI. Para obtener más información sobre cómo configurar la contraseña del sistema de `fsxadmin` archivos, consulte [Actualizar sistemas de archivos](#). Puede encontrar el nombre DNS y la dirección IP del terminal de administración de su sistema de archivos en la FSx consola de Amazon, en la pestaña Administración de la página de detalles del FSx sistema de archivos de ONTAP.

Para conectarse al punto final de administración del sistema de archivos con SSH, primero inicie sesión en una EC2 instancia en la misma VPC que el sistema de archivos de FSx ONTAP. Una vez que haya iniciado sesión en la EC2 instancia, utilice el `fsxadmin` usuario y la contraseña para utilizar SSH en la dirección IP del punto de administración del sistema de archivos o en el nombre de DNS, como en los ejemplos siguientes.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

El comando SSH con valores de muestra:

```
ec2user $ ssh fsxadmin@198.51.100.0
```

El comando SSH utilizando el nombre DNS del punto de conexión de gestión:

```
ec2user $ ssh fsxadmin@file-system-management-endpoint-dns-name
```

El comando SSH con un nombre DNS de ejemplo:

```
ec2user $ ssh fsxadmin@management.fs-0abcdef123456789.fsx.us-east-2.aws.com
Password: fsxadmin_password
```

```
This is your first recorded login.
FsxId0abcdef123456789::>
```

Alcance de ONTAP Comandos CLI disponibles para **fsxadmin**

La `fsxadmin` vista administrativa se encuentra en el nivel del sistema de archivos, que incluye todos los volúmenes SVMs y todos los volúmenes del sistema de archivos. La `fsxadmin` función desempeña la función de ONTAP administrador de clústeres. Como los sistemas de archivos de Amazon FSx for NetApp ONTAP están totalmente gestionados, la `fsxadmin` función puede ejecutar un subconjunto de los disponibles ONTAP Comandos de la CLI.

Para ver una lista de los comandos que se `fsxadmin` pueden ejecutar, utilice lo siguiente [security login role show](#) ONTAP Comando de la CLI:

```
FsxId0abc123def456::> security login role show -role fsxadmin -access !none
```

Vserver	Role Name	Command/Directory	Access 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
		.	
		.	
		.	

378 entries were displayed.

Administrar SVMs con el ONTAP CLI

Puede acceder al ONTAP CLI en su SVM mediante el establecimiento de una conexión shell segura (SSH) al punto final de administración de la SVM mediante el nombre de `vsadmin` usuario y la contraseña. Puede encontrar el nombre DNS y la dirección IP del punto de conexión de la SVM en la FSx consola de Amazon, en el panel Endpoints de la página de detalles de las máquinas virtuales de almacenamiento, que se muestra en el siguiente gráfico.

Endpoints	
Management DNS name svm-06bd701ce68090281.fs-0f17f52f84f11b409.fsx.us-east-2.aws.com	Management IP address 198.19.254.86
NFS DNS name svm-06bd701ce68090281.fs-0f17f52f84f11b409.fsx.us-east-2.aws.com	NFS IP address 198.19.254.86
iSCSI DNS name iscsi.svm-06bd701ce68090281.fs-0f17f52f84f11b409.fsx.us-east-2.aws.com	iSCSI IP addresses 172.31.23.54, 172.31.0.124

Para conectarse al punto final de administración de la SVM mediante SSH, puede utilizar el nombre de usuario y la `vsadmin` contraseña. Si no estableció una contraseña para el usuario de `vsadmin` cuando se creó la SVM, puede configurar la contraseña de `vsadmin` en cualquier momento. Para obtener más información, consulte [Actualización de máquinas virtuales de almacenamiento \(SVM\)](#). 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-abcdef0123456789fs-0abcdef123456789.fsx.us-east-2.aws.com
```

Password: **vsadmin-password**

This is your first recorded login.

```
FsxId0abcdef123456789::>
```

Amazon FSx for NetApp ONTAP es compatible con NetApp ONTAP Comandos de la CLI.

Para obtener una referencia completa de NetApp ONTAP Comandos CLI, consulte la [página Comandos de ONTAP: manual de referencia](#).

Uso de ONTAP API de REST

Al acceder al sistema FSx de archivos de ONTAP mediante el ONTAP Utilice las `fsxadmin` credenciales para la API REST y realice una de las siguientes acciones:

- Desactive la validación de TLS.
- O
- Confíe en las AWS autoridades de certificación (CAs): el CAs paquete de certificados de cada región se encuentra en la URLs siguiente dirección:
 - `https://fsx-aws-certificates.s3.amazonaws.com/bundle- aws-region .pem` para públicoRegiones de AWS
- `https://fsx-aws-us-gov-certificates.s3.us-gov-west-1.amazonaws.com/bundle- aws-region .pem` para AWS GovCloud regiones
- `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 NetApp ONTAP Los comandos de la API REST, consulte la [NetApp ONTAP Referencia en línea de la API REST](#).

Etiquetado de los recursos de Amazon FSx

Para ayudarte a gestionar tus sistemas de archivos y otros FSx recursos de Amazon, puedes asignar tus propios metadatos a cada recurso en forma de etiquetas. Con las etiquetas, puede clasificar sus AWS recursos de diferentes maneras, por ejemplo, por propósito, 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 recursos](#)
- [Copiar etiquetas en copias de seguridad](#)
- [Restricciones de las etiquetas](#)
- [Permisos y etiqueta](#)

Conceptos básicos de etiquetas

Una etiqueta es una etiqueta que se asigna a un AWS recurso. 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 AWS los recursos de diferentes maneras, por ejemplo, por propósito, propietario o entorno. Por ejemplo, puedes definir un conjunto de etiquetas para los sistemas de FSx archivos de Amazon de tu cuenta que te ayuden a rastrear el 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 de más fácilmente. Puede buscar y filtrar los recursos en función de las etiquetas que agregue. Para obtener más información sobre cómo implementar una estrategia de etiquetado de recursos eficaz, consulta Cómo [etiquetar AWS los recursos](#) en. Referencia general de AWS

Algunos comportamientos de etiquetado para considerar:

- Las etiquetas no tienen ningún significado semántico para Amazon FSx y se interpretan estrictamente como una cadena 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 utilizas la FSx API de Amazon, el AWS Command Line Interface (AWS CLI) o un AWS SDK, puedes 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 elimina 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 anula 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

Se requieren ciertos permisos AWS Identity and Access Management (IAM) para que los usuarios etiqueten los recursos al crearlos. Para obtener más información, consulte [Conceder permisos para etiquetar recursos durante la creación](#).

Etiquetado de recursos

Puedes etiquetar FSx los recursos de Amazon que existen en tu cuenta. Si utilizas la FSx consola de Amazon, puedes aplicar etiquetas a los recursos mediante la pestaña Etiquetas de la pantalla de recursos correspondiente. 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 Name, esta clave no tiene ningún significado semántico para el FSx servicio de Amazon.

Para implementar un control detallado sobre los usuarios y grupos que pueden etiquetar los recursos en el momento de la creación, puedes aplicar permisos a nivel de recursos basados en etiquetas

en tus políticas de IAM a las acciones de la FSx API de Amazon que admiten el etiquetado en el momento de la 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.

Para controlar qué claves y valores de etiquetas se configuran en tus recursos existentes, puedes aplicar permisos a nivel de recursos a las acciones de la FSx API de Amazon y a las de TagResource UntagResource Amazon en tus políticas de IAM.

Para obtener más información sobre los permisos necesarios para etiquetar los FSx recursos de Amazon en el momento de la creación, consulte [Conceder permisos para etiquetar recursos durante la creación](#).

Para obtener más información sobre el uso de etiquetas para restringir el acceso a FSx los recursos de Amazon en las políticas de IAM, consulte [Uso de etiquetas para controlar el acceso a tus FSx recursos de Amazon](#).

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

Al crear o actualizar un volumen en la FSx API de Amazon AWS CLI, o bien, puede habilitar CopyTagsToBackups la copia automática de cualquier etiqueta de sus volúmenes a las copias de seguridad.

Note

Si especificas etiquetas al crear una copia de seguridad iniciada por el usuario (incluida la etiqueta de nombre cuando creas una copia de seguridad con la FSx consola de Amazon), las etiquetas no se copiarán del volumen aunque las hayas activado CopyTagsToBackups.

Para obtener más información sobre las copias de seguridad, consulte [Protección de datos con copias de seguridad de volúmenes](#). Para obtener más información sobre la activación CopyTagsToBackups, consulte [Cómo crear un volumen \(CLI\)](#) y [Cómo actualizar la configuración de un volumen \(CLI\)](#) en la Guía del usuario de Amazon FSx for NetApp ONTAP o [UpdateVolume](#) en la [CreateVolume](#) referencia de la API de Amazon FSx for 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 `aws :` prefijo está reservado para su AWS uso. 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`.

Al etiquetar recursos públicos o compartidos, las etiquetas que asigne están disponibles solo para usted Cuenta de AWS; ninguna otra persona Cuenta de AWS tiene acceso a esas etiquetas. Para el control de acceso a los recursos compartidos basado en etiquetas, cada uno Cuenta de AWS debe asignar su propio conjunto de etiquetas para controlar el acceso al recurso.

Permisos y etiqueta

Para obtener más información sobre los permisos necesarios para etiquetar los FSx recursos de Amazon en el momento de la creación, consulte [Conceder permisos para etiquetar recursos durante la creación](#).

Para obtener más información sobre el uso de etiquetas para restringir el acceso a FSx los recursos de Amazon en las políticas de IAM, consulte [Uso de etiquetas para controlar el acceso a tus FSx recursos de Amazon](#).

Protección de datos

Además de replicar automáticamente los datos de tu sistema de archivos para garantizar [una alta durabilidad](#), con Amazon también FSx dispones de las siguientes opciones que puedes utilizar para proteger aún más tus datos:

- Copias de seguridad por FSx volumen nativas de Amazon que respaldan sus necesidades de retención y conformidad de copias de seguridad dentro de Amazon FSx.
- Se utiliza AWS Backup para implementar una estrategia de respaldo y retención automatizada y administrada de forma centralizada en múltiples áreas Servicios de AWS.
- Instantáneas que permiten a los usuarios deshacer fácilmente los cambios no deseados en los archivos mediante la restauración de los archivos a versiones anteriores.
- Uso SnapLock para crear, escriba una vez, lea varios volúmenes de almacenamiento (WORM) para evitar que se modifiquen o eliminen los archivos una vez realizados, durante un período de retención específico.
- FlexCache Los volúmenes ofrecen una replicación de datos rentable, eficiente en términos de almacenamiento y de alto rendimiento para cargas de trabajo con un uso intensivo de lecturas, con datos que permanecen prácticamente inalterados.
- Uso SnapMirror para crear una replicación automática y programada del sistema de archivos en un segundo sistema de archivos para la protección de datos y la recuperación ante desastres.

Temas

- [Protección de datos con copias de seguridad de volúmenes](#)
- [Protección de los datos con instantáneas](#)
- [Proteja sus datos con la protección autónoma contra el ransomware](#)
- [Proteja sus datos con SnapLock](#)
- [Replicar sus datos con FlexCache](#)
- [Replicar sus datos mediante NetApp SnapMirror](#)

Protección de datos con copias de seguridad de volúmenes

Con FSx ONTAP, puede proteger sus datos realizando copias de seguridad automáticas diarias y copias de seguridad iniciadas por el usuario de los volúmenes de su sistema de archivos. Crear

copias de seguridad periódicas para los volúmenes es una práctica recomendada que le ayuda a satisfacer sus necesidades de cumplimiento y retención de datos. Puede restaurar las copias de seguridad FSx por volumen en cualquier sistema de archivos de ONTAP al que tenga acceso y que se encuentre en el mismo Región de AWS lugar donde está almacenada la copia de seguridad. Al trabajar con FSx copias de seguridad de Amazon, es fácil crear, ver, restaurar y eliminar copias de seguridad de sus volúmenes.

Amazon FSx admite copias de seguridad de ONTAP volúmenes con un formato `OntapVolumeType` de lectura-escritura (RW).

 Note

Amazon FSx no admite la creación de copias de seguridad de volúmenes de protección de datos (DP), volúmenes espejo de carga compartida (LSM) ni volúmenes de destino para FlexCache y SnapMirror.

Temas

- [Cómo funcionan las copias de seguridad](#)
- [Requisitos de almacenamiento](#)
- [Copias de seguridad diarias automáticas](#)
- [Copias de seguridad iniciadas por el usuario](#)
- [Copiar etiquetas en copias de seguridad](#)
- [Uso AWS Backup con Amazon FSx](#)
- [Restauración de copias de seguridad en un volumen nuevo](#)
- [Copia de seguridad y restauración del rendimiento](#)
- [Copia de seguridad de volúmenes SnapLock](#)
- [Crear copias de seguridad iniciadas por el usuario](#)
- [Restauración de una copia de seguridad en un volumen nuevo](#)
- [Restauración de un subconjunto de datos](#)
- [Supervisión del progreso al restaurar una copia de seguridad](#)
- [Eliminación de copias de seguridad](#)

Cómo funcionan las copias de seguridad

Todas las FSx copias de seguridad de Amazon (copias de seguridad diarias automáticas y copias de seguridad iniciadas por el usuario) son incrementales, lo que significa que solo almacenan los cambios en los datos desde que se completó la copia de seguridad anterior. Esto minimiza tanto el tiempo necesario para crear una copia de seguridad como la cantidad de almacenamiento usado por cada copia de seguridad. Las copias de seguridad incrementales optimizan los costos de almacenamiento al no almacenar datos duplicados. FSx en el caso de ONTAP, las copias de seguridad se realizan por volumen, y cada copia de seguridad contiene solo los datos de un volumen específico. Las FSx copias de seguridad de Amazon se almacenan de forma redundante en varias zonas de disponibilidad para lograr una alta durabilidad.

FSx Las copias de seguridad de Amazon utilizan instantáneas (point-in-time imágenes 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 consume espacio de almacenamiento en el volumen. FSx A continuación, Amazon 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 las copias de seguridad, ONTAP preserva la eficiencia de almacenamiento de un volumen y ahorra en las copias de seguridad.

Cuando se [elimina](#) una copia de seguridad, solo se borran los datos que son únicos de dicha copia de seguridad. Cada FSx copia de seguridad de Amazon 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.

El número de copias de seguridad que puede almacenar por volumen Cuenta de AWS y por volumen está limitado. Para obtener más información, consulte [Cuotas que puede aumentar](#) y [Cuotas de recursos para cada sistema de archivos](#).

Requisitos de almacenamiento

Tanto el volumen como el sistema de archivos deben tener suficiente capacidad de almacenamiento en SSD disponible para almacenar una instantánea de respaldo. Cuando se realice la instantánea de 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 en SSD. Si esto ocurre, la copia de seguridad fallará. Puede [aumentar en un volumen](#) o en un [sistema de archivos](#) el almacenamiento en SSD en cualquier momento para corroborar que las copias de seguridad no se interrumpan.

Copias de seguridad diarias automáticas

Al crear un sistema de archivos, las copias de seguridad diarias automáticas se habilitan de forma predeterminada para los volúmenes del sistema de archivos. Puede habilitar o deshabilitar las copias de seguridad diarias automáticas de los sistemas de archivos existentes en cualquier momento. Las copias de seguridad diarias automáticas de todos los volúmenes se realizan durante el periodo de copia de seguridad diaria del sistema de archivos, que se establece automáticamente al crear un sistema de archivos. Puede modificar el periodo de copia de seguridad diaria en cualquier momento. Para obtener un [rendimiento de copia de seguridad](#) óptimo, le recomendamos que elija un periodo de respaldo diario que esté fuera del horario normal de funcionamiento cuando los clientes y las aplicaciones accedan a los datos de los volúmenes.

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

Las copias de seguridad diarias automáticas, el periodo de copia de seguridad diaria y el periodo de retención de copias de seguridad son ajustes del sistema de archivos que se aplican a todos los volúmenes de dicho sistema. Puedes usar la FSx consola de Amazon AWS CLI, la o la API para cambiar esta configuración. Para obtener más información, consulte [Actualizar sistemas de archivos](#).

No puede crear una copia de seguridad de volumen (copias de seguridad diarias automáticas o copias de seguridad iniciadas por el usuario) si el volumen está desconectado. Para obtener más información, consulte [Visualización de 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 crees, incluidas las copias de seguridad creadas con ella AWS Backup, se conservan para siempre, a menos que tú o las AWS Backup elimines.

Puede [eliminar](#) manualmente una copia de seguridad diaria automática mediante la FSx consola, la CLI y la API de Amazon. Al eliminar un volumen, también elimina 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.

Copias de seguridad iniciadas por el usuario

Con Amazon FSx, puedes realizar copias de seguridad manuales de los volúmenes de tu 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 retienen para siempre, a menos que las elimine. Las copias de seguridad iniciadas por el usuario se retienen 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](#) mediante la FSx consola, la API o la CLI de Amazon. Amazon nunca los elimina automáticamente FSx.

Para obtener instrucciones sobre cómo crear una copia de seguridad iniciada por el usuario, consulte [Crear copias de seguridad iniciadas por el usuario](#).

Copiar etiquetas en copias de seguridad

Cuando crea o actualiza un volumen mediante la CLI o la API, puede habilitar CopyTagsToBackups para [copiar automáticamente etiquetas](#) de sus volúmenes a las copias de seguridad. Sin embargo, si añade etiquetas 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, Amazon FSx no copia las etiquetas del volumen, aunque CopyTagsToBackups esté habilitada.

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 volúmenes de Amazon FSx for 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. Gracias a AWS Backup, se facilita el desarrollo de una estrategia de copia de seguridad centralizada para el cumplimiento jurídico, normativo y profesional. También simplifica la protección de los volúmenes AWS de almacenamiento, las bases de datos y los sistemas de archivos, ya que proporciona un lugar central en el que puede hacer lo siguiente:

- Configurar y auditar 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 función 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 FSx iniciada por un usuario de Amazon que se tome de su volumen y ofrecen las mismas opciones de restauración que las copias de seguridad realizadas con la FSx consola de Amazon. El uso AWS Backup para gestionar estas copias de seguridad proporciona una funcionalidad adicional, incluida la posibilidad de crear copias de seguridad programadas con una frecuencia de hasta una hora. Puede agregar una capa de defensa adicional para proteger las copias de seguridad de eliminaciones inadvertidas o malintencionadas almacenándolas en una [bóveda de copias de seguridad](#).

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 AWS Backup mediante la FSx consola, la CLI y la API de Amazon. Sin embargo, no puedes eliminar las copias de seguridad creadas AWS Backup en la FSx consola, la CLI o la API de Amazon. Para obtener más información, consulta [Cómo empezar con 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.

Puede usar etiquetas para seleccionar cuáles de sus FSx recursos de ONTAP están protegidos en un plan de respaldo. Estas etiquetas se deben aplicar a nivel de volumen y no a nivel del sistema de archivos en su conjunto. Para obtener más información, consulte [Asignación de recursos a un plan de respaldo](#) en la Guía para AWS Backup desarrolladores.

Restauración de copias de seguridad en un volumen nuevo

Puede restaurar una copia de seguridad de un volumen en un volumen nuevo de un sistema de archivos que se encuentre en la misma Región de AWS donde está almacenada la copia de seguridad. No puede restaurar una copia de seguridad en un sistema de archivos que esté ubicado en un lugar Región de AWS diferente al de la copia de seguridad.

Al restaurar una copia de seguridad en FSx los sistemas de archivos de segunda generación de ONTAP, los clientes pueden montar y leer los datos de un volumen mientras se restaura. Los clientes pueden montar el volumen que está restaurando y leer los datos del archivo una vez que Amazon FSx haya cargado todos los metadatos en el nuevo volumen y este informe de un estado de ciclo de vida deCREATED. Puede encontrar el estado del ciclo de vida de un volumen en la página de [detalles de los volúmenes](#) de la FSx consola de Amazon y en la respuesta del comando CLI [describe-volumes](#).

Al leer datos de un volumen mientras se restaura a partir de una copia de seguridad, si los datos aún no se han descargado al volumen, se producirán latencias de lectura de hasta decenas de milisegundos en el primer acceso. Estas lecturas se almacenan en caché en el nivel de SSD, por lo que puede esperar latencias de lectura inferiores a un milisegundo en las siguientes lecturas.

El tiempo que Amazon FSx tarda en hacer que un volumen esté disponible para el acceso de solo lectura es proporcional a la cantidad de metadatos de archivos almacenados en la copia de seguridad. Los metadatos de los archivos suelen consumir entre el 1 % y el 7 % del total de los datos de copias de seguridad, en función del tamaño promedio de los archivos del conjunto de datos (los conjuntos de datos de archivos pequeños consumen más metadatos que los conjuntos de datos de archivos grandes).

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 añade volúmenes constitutivos adicionales para garantizar que los componentes se distribuyan uniformemente.

 Note

Amazon FSx no admite el acceso de lectura a los datos mientras se restaura un volumen a partir de una copia de seguridad para SnapLock los volúmenes o para los volúmenes de los sistemas de archivos de primera generación. Al restaurar estas copias de seguridad, el volumen queda disponible para montar y acceder a los datos una vez finalizado el proceso de restauración y todos los metadatos y datos se cargan en el nuevo volumen.

Al restaurar una copia de seguridad, todos los datos se escriben inicialmente en el nivel de almacenamiento en SSD. Mientras la restauración está en curso, los datos se agrupan en niveles en el almacenamiento del grupo de capacidad de acuerdo con la [política de estratificación](#) del volumen que se va a restaurar. Dado que los datos se escriben primero en el nivel SSD, Amazon FSx pausará el proceso de restauración si el sistema de archivos se queda sin espacio de almacenamiento SSD. La restauración se reanudará automáticamente en cuanto haya suficiente espacio en SSD disponible para continuar con el proceso. Si la política de estratificación por niveles del volumen restaurado es All, se lleva a cabo un proceso periódico en segundo plano para distribuir los datos por niveles en el grupo de capacidad. Si la política de estratificación del volumen restaurado es Snapshot Only o Auto, los datos se agrupan en niveles en el grupo 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 periodo de enfriamiento de la política de estratificación.

Si la carga de trabajo requiere latencias de lectura consistentes de menos de un milisegundo al restaurar una copia de seguridad en un volumen nuevo en sistemas de archivos de segunda generación, recomendamos que establezca la política de estratificación del volumen en None al iniciar la restauración. A continuación, espere hasta que todos los datos se hayan descargado completamente en el volumen antes de acceder a él. Todos los datos se cargarán en un almacenamiento en SSD antes de que intente acceder a ellos, lo que proporcionará un acceso uniforme y de baja latencia a los datos.

Para step-by-step obtener instrucciones sobre cómo restaurar una copia de seguridad en un volumen nuevo, consulte [Restauración de una copia de seguridad en un volumen nuevo](#).

En los sistemas de archivos de segunda generación, también puede restaurar solo un subconjunto de datos de una copia de seguridad sin tener que esperar a que se complete toda la operación de restauración. La restauración de solo un subconjunto de los datos de una copia de seguridad le permite reanudar las operaciones con mayor rapidez en caso de que los datos se eliminen,

modifiquen o dañen accidentalmente. Para obtener más información, consulte [Restauración de un subconjunto de datos](#).

Puede supervisar el progreso al restaurar una copia de seguridad en un sistema de archivos de segunda generación en la API AWS Management Console AWS CLI, y. Para obtener más información, consulte [Supervisión del progreso al restaurar una copia de seguridad](#).

 Note

- No puede crear una instantánea de un volumen ni realizar operaciones basadas en instantáneas, como la clonación, la SnapMirror replicación y la creación de copias de seguridad de un volumen mientras se está restaurando a partir de una copia de seguridad.
- Un volumen restaurado siempre tiene el mismo estilo de volumen que el volumen original. No puede cambiar el estilo del volumen al restaurarlo.

Copia de seguridad y restauración del rendimiento

Diversos factores pueden influir en el rendimiento de las operaciones de copias de seguridad y restauración. Las operaciones de copias de seguridad 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 lecturas y escrituras de metadatos y datos de NFS, CIFS e iSCSI. Todos los procesos en segundo plano usan solo la parte no utilizada de la capacidad de rendimiento 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 usada en el sistema de archivos.

Otros factores que afectan al rendimiento de las copias de seguridad y la restauración incluyen 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 los volúmenes cuando la mayoría de los datos estén en un almacenamiento en 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 el procesamiento de grandes cantidades de archivos pequeños consume más ciclos de CPU y sobrecarga de red que el procesamiento de menos archivos grandes.

En general, cabe esperar las siguientes velocidades de copia de seguridad al realizar copias de seguridad de datos almacenados en el nivel de almacenamiento de la 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.

En general, cabe esperar las siguientes velocidades 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 en su mayoría archivos pequeños.

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 se puede hacer una copia de seguridad de un volumen SnapLock FlexGroup.

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, consulte [Cómo SnapLock funciona](#).

Crear copias de seguridad iniciadas por el usuario

En el siguiente procedimiento, se describe cómo crear la copia de seguridad de un volumen iniciada por el usuario.

No puede crear una copia de seguridad de un volumen si este está desconectado. Para obtener más información, consulte [Visualización de volúmenes sin conexión](#).

Cómo crear una copia de seguridad iniciada por el usuario (consola)

1. Abre la FSx consola de Amazon en <https://console.aws.amazon.com/fsx/>.
2. Vaya a Sistemas de archivos y elija el sistema de archivos ONTAP 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. Puedes ver todas tus copias de seguridad en la FSx consola de Amazon seleccionando Backups en el menú 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.

Restauración de una copia de seguridad en un volumen nuevo

Los siguientes procedimientos describen cómo restaurar una copia de seguridad FSx de ONTAP en un volumen nuevo mediante el AWS Management Console comando and. AWS CLI Al restaurar un volumen en un sistema de archivos de segunda generación, puede [supervisar](#) el progreso mediante la API AWS Management Console AWS CLI, y.

Para restaurar la copia de seguridad de un volumen en un volumen nuevo (consola)

1. Abre la FSx consola de Amazon 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 FSx por volumen de ONTAP que desee restaurar.
3. En el menú superior derecho Acciones, seleccione Restaurar copia de seguridad. Aparecerá la página Crear volumen a partir de una copia de seguridad.

4. Seleccione en FSx los menús desplegables la máquina virtual del sistema de archivos y almacenamiento de ONTAP en la que desee restaurar la copia de seguridad.
5. En el menú superior derecho Acciones, seleccione Restaurar copia de seguridad. Aparecerá la página Crear volumen a partir de una copia de seguridad.
6. Seleccione en FSx los menús desplegables la máquina virtual del sistema de archivos y almacenamiento de ONTAP en la que desee restaurar la copia de seguridad.
7. En Detalles del volumen, hay varias selecciones. En primer lugar, introduzca el nombre del volumen. Puede usar hasta 203 caracteres alfanuméricos o de subrayado (_).
8. En Volume size, introduzca cualquier número entero en el rango de 20 a 314 572 800 para especificar el tamaño en mebibytes (MiB).
9. En Tipo de volumen, seleccione Lectura-escritura (RW) para crear un volumen con capacidad de lectura y escritura o Protección de datos (DP) para crear un volumen que sea de solo lectura y que pueda usarse como destino de una relación entre SnapMirror o SnapVault de NetApp. Para obtener más información, consulte [Tipos de volúmenes](#).
10. 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.
11. En Eficiencia del almacenamiento, seleccione Activado para activar las características de eficiencia del almacenamiento de ONTAP (desduplicación, compresión y compactación). Para obtener más información, consulte [Eficacia de almacenamiento](#).
12. 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 NTFS o UNIX ACLs para el acceso multiprotocolo. El modo MIXTO no es necesario para el acceso multiprotocolo y solo se recomienda para usuarios avanzados.
13. 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 o la API de REST de ONTAP. Para obtener más información, consulte [Crear una política de instantáneas](#) en la documentación del producto NetApp ONTAP.

14. 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.

15. En la sección Avanzada, en Configuración de SnapLock, puede dejar la configuración predeterminada Desactivada o elegir Activada para configurar un volumen de SnapLock. Para obtener más información sobre la configuración de un volumen de conformidad de SnapLock o un volumen de empresa de SnapLock, consulte [Descripción SnapLock Conformidad](#) y [Descripción SnapLock Enterprise](#). Para obtener más información acerca de SnapLock, consulte [Proteja sus datos con SnapLock](#).
16. Seleccione Confirm (Confirmar) para crear el volumen.
17. Si va a restaurar la copia de seguridad en un sistema de archivos de segunda generación, puede supervisar el progreso de la restauración de la copia de seguridad en la pestaña Actualizaciones de la página Volumen. Para obtener más información, consulte [Supervisión del progreso al restaurar una copia de seguridad](#).

Cómo restaurar una copia de seguridad en un volumen nuevo (CLI)

Utilice el comando [create-volume-from-backup](#) CLI o el comando [CreateVolumeFromBackup](#) API 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 a una solicitud de restauración correcta para restaurar una copia de seguridad en un sistema de archivos de segunda generación es la siguiente. La respuesta incluye el objeto "AdministrativeActions" que proporciona información sobre el estado y el progreso de la solicitud.

```
{
  "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",
  "AdministrativeActions": [
    {
      "AdministrativeActionType": "DOWNLOAD_DATA_FROM_BACKUP",
      "RequestTime": 1685729972.069,
      "Status": "PENDING"
    }
  ]
}

```

La respuesta del sistema a una solicitud correcta para restaurar una copia de seguridad en un sistema de archivos de primera generación es la siguiente.

```
{
  "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",
}
}
```

Al restaurar un volumen en un sistema de archivos de segunda generación, puede [supervisar el progreso](#) mediante la API AWS Management Console AWS CLI, y.

Restauración de un subconjunto de datos

Puede restaurar un subconjunto de datos de una copia de seguridad mientras se está restaurando en un nuevo volumen en los sistemas de archivos de segunda generación sin tener que esperar a que todo el conjunto de datos de la copia de seguridad se haya restaurado por completo.

En el siguiente procedimiento, se enumeran los pasos que se deben seguir cuando se necesita recuperar un subconjunto de datos al restaurar una copia de seguridad y no se puede esperar a que se complete toda la restauración:

Cómo restaurar un subconjunto de datos mientras se restaura una copia de seguridad

1. Abra la FSx consola de Amazon en <https://console.aws.amazon.com/fsx/>.
2. En la página Copias de seguridad, busque la copia de seguridad que contiene la versión de los datos que desea restaurar.
3. En el menú superior derecho Acciones, seleccione Restaurar copia de seguridad. Aparecerá la página Crear volumen a partir de una copia de seguridad.
4. Seleccione en FSx los menús desplegables la máquina virtual del sistema de archivos y almacenamiento de ONTAP en la que desee restaurar la copia de seguridad.
5. En Detalles del volumen, configure el volumen según sus necesidades.
6. Seleccione Confirm (Confirmar) para crear el volumen.
7. [Supervise el progreso](#) de la restauración de la copia de seguridad.
8. [Monte el volumen](#) que se va a restaurar cuando informe el estado del ciclo de vida CREATED.

9. Localice el subconjunto de datos en el volumen que necesita copiar.
10. Copie los datos en el volumen existente que usa la aplicación.
11. Una vez que los datos necesarios de la copia de seguridad se hayan copiado en la ubicación de destino, puede eliminar el volumen que se va a restaurar antes de que se complete para optimizar la utilización de los recursos del sistema de archivos.

Supervisión del progreso al restaurar una copia de seguridad

Puede supervisar el progreso al restaurar una copia de seguridad por volumen en un sistema de archivos de segunda generación en la API AWS Management Console AWS CLI, y. Como ocurre con todas las acciones FSx administrativas de Amazon, el estado de restauración de la copia de seguridad está disponible en la consola, la CLI y la API durante 30 días después de que se complete la operación.

Cómo supervisar el progreso al restaurar una copia de seguridad (consola)

Abre la FSx consola de Amazon en <https://console.aws.amazon.com/fsx/>.

1. En el menú de navegación izquierdo, seleccione Volúmenes.
2. Seleccione el volumen en el que se va a restaurar la copia de seguridad.
3. Seleccione la pestaña Actualizaciones.
4. El tipo de actualización de la restauración de la copia de seguridad proporciona la siguiente información:
 - PENDIENTE indica que los metadatos del archivo se están descargando al volumen. El estado del ciclo de vida del volumen es EN CREACIÓN.
 - EN_PROGRESO indica que el volumen está disponible y que los clientes pueden montarlo con acceso de solo lectura a los datos. El estado % de progreso muestra el porcentaje de datos que se han descargado en el volumen.
 - COMPLETADO indica que todos los datos se han descargado en el volumen y que se ha completado la restauración de la copia de seguridad. Los clientes ahora tienen acceso de lectura y escritura. En el caso de los volúmenes de RW, el tipo de volumen cambia de DP a RW en este punto.

Cómo supervisar el progreso al restaurar una copia de seguridad (CLI)

- Al restaurar una copia de seguridad en un volumen nuevo en un sistema de archivos de segunda generación FSx para ONTAP, puede supervisar el progreso de la restauración mediante el comando [describe-volumes](#) CLI.

Al restaurar una copia de seguridad en un sistema de archivos de segunda generación, la respuesta incluye el objeto `AdministrativeActions`, que proporciona información sobre el estado del proceso de descarga de datos. La

```
$ aws fsx describe-volumes
{
  "Volumes": [
    {
      "CreationTime": 1691686114.674,
      "FileSystemId": fs-029ff92192bd4d375,
      "Lifecycle": "CREATING",
      "Name": vol1,
      "OntapConfiguration": {
        "FlexCacheEndpointType": "NONE",
        "JunctionPath": "/vol1",
        "SizeInMegabytes": 100000,
        "StorageEfficiencyEnabled": true,
        "StorageVirtualMachineId": "svm-0ed1d714019426ca9",
        "StorageVirtualMachineRoot": false,
        "TieringPolicy": {
          "Name": "ALL"
        },
        "OntapVolumeType": "DP",
        "SnapshotPolicy": "default",
        "CopyTagsToBackups": false,
      },
      "ResourceARN": "arn:aws:fsx:us-east-1:630831496844:volume/fs-08ac75f715c6aec76/fsvol-094c015af930790fa",
      "VolumeId": "fsvol-094c015af930790fa",
      "VolumeType": "ONTAP",
      "AdministrativeActions": [
        {
          "AdministrativeActionType": "DOWNLOAD_DATA_FROM_BACKUP",
          "RequestTime": 1685729972.069,
          "Status": "PENDING"
        }
      ]
    }
  ]
}
```

```
}
```

Una vez que Amazon FSx carga todos los metadatos del archivo en el volumen restaurado, estos campos tienen los siguientes valores:

- "LifeCycle": "CREATED": indica que el volumen está listo para ser montado.
- "OntapVolumeType": "DP": indica que el volumen es de solo lectura mientras se descargan los datos del archivo.
- "ProgressPercent": muestra el porcentaje de datos del archivo que se carga en el volumen.
- "Status": "IN_PROGRESS": la descarga de datos del archivo en el volumen está en curso.

En esta fase del proceso de restauración, puede montar el volumen con acceso de solo lectura a todos los datos de la copia de seguridad que está restaurando.

Cuando Amazon FSx haya terminado de descargar todos los datos del archivo en el nuevo volumen, los clientes tendrán pleno acceso de lectura y escritura si se RW trata de un volumen. Los indicadores tienen los siguientes valores:

- "LifeCycle": "CREATED": sin cambios
- "OntapVolumeType": "RW": indica que los clientes tienen acceso total de lectura y escritura.
- "Status": "COMPLETED": indica que la restauración se ha completado.

Si se produce un error en el proceso de restauración, el `AdministrativeAction > Status` tendrá un valor de `FAILED`. Se proporciona un mensaje de error en el objeto `FailureDetails`. Para obtener más información, consulta [AdministrativeActionFailureDetails](#) la referencia de la FSx API de Amazon

Eliminación de copias de seguridad

Puede eliminar tanto las copias de seguridad diarias automáticas como las copias de seguridad iniciadas por el usuario de sus volúmenes mediante la FSx consola de Amazon, la FSx API de Amazon o AWS Command Line Interface (AWS CLI). Eliminar una copia de seguridad es una acción permanente e irre recuperable. También se eliminan todos los datos de una copia de seguridad eliminada. No elimine una copia de seguridad a menos que esté seguro de que no la necesitará

de nuevo en el futuro. No puede eliminar una copia de seguridad si el volumen de origen está [desconectado](#).

Puede eliminar un volumen mientras se está restaurando a partir de una copia de seguridad en todos los sistemas de archivos FSx de ONTAP. Al eliminar un volumen durante la restauración, se cancela de forma efectiva la operación de restauración en curso.

 Note

Amazon FSx no admite la eliminación de la AVAILABLE copia de seguridad más reciente de un ONTAP volumen a menos que se hayan eliminado todas las demás copias de seguridad del volumen.

Para eliminar las copias de seguridad creadas con AWS Backup ella, consulta [Eliminar copias de seguridad](#) en la Guía para AWS Backup desarrolladores.

Cómo eliminar una copia de seguridad (consola)

1. Abre la FSx consola de Amazon 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 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 irre recuperable.

Cómo eliminar una copia de seguridad (CLI)

- Utilice el comando CLI delete-backup o la acción de DeleteBackup API equivalente FSx para eliminar una copia de seguridad de un volumen 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 del ciclo de vida con un valor de DELETED, lo que indica que la solicitud se ha realizado correctamente.

```
{
  "BackupId": "backup-a0123456789abcdef",
  "Lifecycle": "DELETED"
}
```

Protección de los datos con 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 para deshacer los cambios, recuperar contenido eliminado y comparar versiones de archivos.

Una instantánea contiene los datos que han cambiado desde la última instantánea, que consume la capacidad de almacenamiento en SSD del sistema de archivos. Las instantáneas no se incluyen en ninguna [copias de seguridad](#) de volumen. Las instantáneas están habilitadas de forma predeterminada en los volúmenes mediante la política de instantáneas default. Las instantáneas se almacenan en el directorio .snapshot de la raíz de un volumen. Puede almacenar hasta un máximo de 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](#)
- [Restauración de archivos a partir de instantáneas](#)
- [Visualización de la instantánea común](#)
- [Actualización de la reserva de instantáneas del volumen](#)
- [Desactivación de las instantáneas automáticas](#)
- [Eliminación de instantáneas](#)

- [Eliminación de instantáneas](#)
- [Reserva de instantáneas](#)

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. ONTAP tiene tres políticas de instantáneas integradas: FSx

- `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). Puede configurar una zona horaria FSx para el sistema de archivos ONTAP mediante el comando `timezone -timezone time_zone` ONTAP CLI. Para obtener más información sobre el acceso a la ONTAP CLI, consulte [Uso de NetApp ONTAP CLI](#).

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 de instantáneas](#) en la documentación del producto NetApp ONTAP. Puede elegir una política de instantáneas al crear o actualizar un volumen en la FSx consola de Amazon AWS CLI, la o la FSx API de Amazon. Para obtener más información, consulte [Creación de volúmenes](#) y [Actualización de volúmenes](#).

Restauración de archivos a partir de instantáneas

Con las instantáneas de tu sistema de FSx archivos de Amazon, puedes restaurar rápidamente versiones anteriores de archivos o carpetas individuales.

Si usa clientes de Linux y macOS, puede ver las instantáneas en el directorio `.snapshot` de la raíz de un volumen. Si usa los clientes de Windows, puede ver las instantáneas en la pestaña `Previous Versions` del Explorador de Windows (al hacer clic derecho en un archivo o carpeta).

Cómo 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.

Cómo 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.

Visualización de la instantánea común

La instantánea común se usa para mantener la incrementalidad entre las copias de seguridad. En este procedimiento, se explica cómo identificar la instantánea común del volumen.

Cómo ver una instantánea común de un volumen

- Para determinar qué instantánea es la instantánea común de un volumen, use el comando `volume snapshot show` de la CLI de ONTAP.

```
volume snapshot show -volume volume-name
```

En el resultado, el nombre de la instantánea común tiene el formato debackup-*id*, donde *id* es una cadena alfanumérica de 17 dígitos, como se muestra en el siguiente ejemplo:

```
FsxIdabc12345::> volume snapshot show -volume test_vol
                               ---Blocks---
Vserver Volume      Snapshot                               Size      Total% Used%
-----
dest-svm test_vol
      snap1              144KB      0%      3%
      snap2              832KB      0%     16%
      ---> backup-abcdef0123456789a 4.87MB      0%     53% <---
      weekly.2024-05-26_0015 5.02MB      0%     54%
      weekly.2024-06-02_0015 2.22MB      0%     34%
      daily.2024-06-04_0010  284KB      0%      6%
      daily.2024-06-05_0010  4.29MB      0%    50%
      hourly.2024-06-05_0705  168KB      0%      4%

8 entries were displayed.
```

 Important

No elimine la instantánea común en el volumen porque se usa para mantener la incrementalidad entre las copias de seguridad. Al eliminar la instantánea común de un

volumen, la siguiente copia de seguridad abarcará todo el volumen y no una copia de seguridad incremental.

Actualización de la reserva de instantáneas del volumen

Puede cambiar la cantidad de reserva de instantáneas en un volumen mediante la CLI de o la API de NetApp ONTAP, tal como se describe en el siguiente procedimiento.

1. Para acceder a la ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando. 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 [Administrar sistemas de archivos con el ONTAP CLI](#).

2. Use el comando `volume modify` de la CLI de ONTAP para cambiar el porcentaje de espacio en disco usado para la reserva de copias de instantáneas. Sustituya los siguientes valores de muestra con los datos:
 - *svm_name*: use el nombre de la SVM.
 - *vol_name*: use el nombre del volumen.
 - *percent*: el porcentaje de espacio en disco que desea reservar para copias de instantáneas.

```
::> volume modify -vserver svm_name -volume vol_name -percent-snapshot-space percent
```

En el siguiente ejemplo, se cambia la reserva de instantáneas del volumen 1 % al 25 % de la capacidad de almacenamiento del volumen.

```
::> volume modify -vserver vs0 -volume vol1 -percent-snapshot-space 25
```

Desactivación de las instantáneas automáticas

La política de instantáneas predeterminada habilita las instantáneas automáticas para los volúmenes del sistema de archivos de ONTAP. FSx 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 (consola)AWS

1. Abra la FSx consola de Amazon 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 Política de instantáneas, seleccione Ninguno.
7. Seleccione Actualizar para actualizar el volumen.

Para deshabilitar las instantáneas automáticas (AWS CLI)

- Utilice el comando [AWS CLI update-volume](#) (o el comando [UpdateVolume](#)API 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
```

Cómo deshabilitar las instantáneas automáticas (CLI de ONTAP)

Configure la política de instantáneas del volumen para usar la política none predeterminada para desactivar las instantáneas automáticas.

1. Para mostrar la política none, use el comando [volume snapshot policy show](#) de la CLI de ONTAP.

```
::> snapshot policy show -policy none
```

```
Vserver: FsxIdabcdef01234567892
```

Policy Name	Number of Is Schedules	Enabled	Comment
none	0	false	Policy for no automatic snapshots.
Schedule	Count	Prefix	SnapMirror Label
-----	----	-----	-----
-	-	-	-

2. Use el comando [volume modify](#) de la CLI de ONTAP para configurar la política de instantáneas del volumen en none para deshabilitar las instantáneas automáticas. Sustituya los siguientes valores de muestra con los datos:

- **svm_name**: use el nombre de la SVM.
- **vol_name**: use el nombre del 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.
```

Eliminación de instantáneas

Las instantáneas ocupan capacidad de almacenamiento solo para los datos en un volumen que ha cambiado desde la última instantánea. Por este motivo, si la carga de trabajo escribe datos rápidamente, las instantáneas de datos antiguos pueden ocupar una cantidad importante de la capacidad de almacenamiento del volumen.

Por ejemplo, el resultado del comando [volume show-space](#) de la CLI de ONTAP da 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. Como las instantáneas son incrementales, no se recupera la cantidad de almacenamiento igual al tamaño de la instantánea cuando se elimina. Puede ver la cantidad de almacenamiento que puede recuperar al eliminar una instantánea mediante el comando [volume snapshot compute-reclaimable -vserver](#) ONTAP CLI, utilizando sus datos para reemplazar, y. *svm_name vol_name snapshot_name*

```
fsid8970abc52::> volume snapshot compute-reclaimable -vserver svm_name -volume vol_name  
-snapshot snapshot_name  
A total of 667648 bytes can be reclaimed.
```

Puede eliminar instantáneas mediante la creación de una política [snapshot auto-delete policy](#) o [eliminando las instantáneas manualmente](#). Al eliminar una instantánea, se eliminan los datos modificados almacenados en la instantánea.

Eliminación de instantáneas

Use el comando [volume snapshot delete](#) de la CLI de ONTAP para eliminar las instantáneas manualmente y reemplazar los siguientes valores de marcador de posición por sus datos:

- 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 FSx copias de seguridad de Amazon, Amazon FSx conserva una instantánea de la FSx copia de seguridad de Amazon 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. Para obtener más información, consulte [Visualización de la instantánea común](#).

```
FsxIdabcdef01234567892::> volume snapshot delete -vserver svm_name -volume vol_name -  
snapshot snapshot_name
```

Creación de 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. Use el comando [volume snapshot autodelete modify](#) de la CLI de ONTAP para establecer una política de eliminación automática para un volumen.

Cuando use este comando, use los datos para reemplazar los siguientes valores de marcador de posición:

- 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.

Reserva de instantáneas

La reserva de copias de instantáneas establece un porcentaje específico de la capacidad de almacenamiento de un volumen para almacenar copias de instantáneas, con un valor predeterminado del 5 %. La reserva de copias de instantáneas debe tener suficiente espacio asignado para las copias de instantáneas, incluidas las [copias de seguridad en volumen](#). Si las copias de instantáneas superan el espacio de reserva de instantáneas, debe eliminar las copias de instantáneas existentes del sistema de archivos activo para recuperar la capacidad de almacenamiento necesaria para su uso en el sistema de archivos. También puede modificar el porcentaje de espacio en disco que se asigna a las copias de 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, este corre el riesgo de llenarse. Si el sistema de archivos 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 de instantáneas.

Como no hay forma de evitar que las instantáneas consuman un 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 de 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 del nivel de SSD principal no se crea espacio libre, ya que la instantánea recién creada también hace referencia a todos esos datos. Debe [eliminar la instantánea](#) 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 CLI de NetApp ONTAP. Para obtener más información, consulte [Actualización de la reserva de instantáneas del volumen](#).

Proteja sus datos con la protección autónoma contra el ransomware

La protección autónoma contra el ransomware (ARP) es NetApp ONTAP Función impulsada por la IA que monitorea y protege sus datos contra los ataques de ransomware y malware en caso de que sus clientes de Windows o Linux se vean comprometidos. Gracias al aprendizaje automático, ARP se familiariza con los sistemas de archivos de ONTAP FSx para detectar de forma proactiva cualquier actividad anómala. El ARP está disponible para todos los sistemas de archivos nuevos y existentes FSx de ONTAP en todos los lugares donde Regiones de AWS Amazon FSx for NetApp ONTAP esté disponible.

¿Cómo funciona ARP

Puede habilitar el ARP por volumen o de forma predeterminada en todos los volúmenes nuevos de una SVM mediante el ONTAP CLI o API REST. Para obtener más información sobre cómo habilitar ARP, consulte [Habilitación de la protección autónoma contra el ransomware](#).

El ARP funciona en dos modos: activo y de aprendizaje. La primera vez que habilita el ARP FSx para su volumen de ONTAP, se ejecuta en modo de aprendizaje. En el modo de aprendizaje, ARP analiza los patrones de acceso a la carga de trabajo. ONTAP determina automáticamente el período de aprendizaje óptimo en función de la carga de trabajo del volumen, que puede tardar hasta 30 días. Cuando termina, el ARP pasa al modo activo. En el modo activo, el ARP monitorea los datos entrantes y la actividad del volumen para identificar posibles ataques de ransomware y malware. Para obtener más información, consulte [¿Qué busca ARP](#). Si el ARP detecta alguna actividad anormal, un ONTAP La instantánea se crea automáticamente para ayudarle a recuperar los datos lo más cerca posible del momento del posible ataque. La instantánea tendrá el prefijo deAnti_ransomware_backup, por lo que es fácil de identificar. Si se determina que la probabilidad de ataque es moderada, ONTAP generará un mensaje del Sistema de Gestión de Eventos (EMS) para que lo revise. Para obtener más información, consulte [¿Cómo responder a un presunto ataque con ARP](#) y [Descripción de las alertas de EMS para la protección autónoma contra el ransomware](#).

La sobrecarga de rendimiento del ARP es mínima para la mayoría de las cargas de trabajo. Si sus volúmenes tienen cargas de trabajo de lectura intensiva, NetApp recomienda proteger no más

de 150 volúmenes de este tipo por sistema de archivos. Si supera este número, las IOPS de esa carga de trabajo podrían reducirse hasta un 4%. Si sus volúmenes tienen cargas de trabajo de escritura intensiva, NetApp recomienda proteger no más de 60 volúmenes de este tipo por sistema de archivos. De lo contrario, las IOPS de esa carga de trabajo podrían reducirse hasta un 10%. Para obtener más información acerca del desempeño, consulte [Amazon FSx para el rendimiento de NetApp ONTAP](#).

La activación del ARP en el sistema de archivos de ONTAP no conlleva FSx ningún coste adicional.

¿Qué busca ARP

ARP busca señales de que sus clientes de Windows o Linux están en peligro. Una vez que ARP conoce el volumen FSx de ONTAP y pasa al modo activo, busca los siguientes tipos de actividad en el volumen:

- Cambios en la entropía, es decir, diferencias en la aleatoriedad de los datos de un archivo.
- Cambios en los tipos de extensión de archivo, lo que significa que la nueva extensión no es coherente con el tipo de extensión que se utiliza normalmente. El valor predeterminado es de 20 archivos con extensiones de archivo que no se habían observado anteriormente en el volumen.
- Cambios en las IOPS de los archivos, lo que se traduce en un aumento de la actividad anormal del volumen de datos cifrados.

Si es necesario, puede modificar los parámetros de detección de ransomware de su volumen. Por ejemplo, si su volumen aloja muchos tipos de extensiones de archivo. Para obtener más información, consulte [Administrar los parámetros de detección de ataques de ONTAP Autonomous Ransomware Protection](#) en el Centro de NetApp documentación.

Note

El ARP no impide que administradores deshonestos con credenciales accedan al sistema de archivos de FSx ONTAP. AWS recomienda un enfoque de seguridad por capas que incluya, AWS BackupONTAP instantáneas y SnapLock.

¿Cómo responder a un presunto ataque con ARP

Si el ARP detecta un ataque, generará una instantánea que se puede utilizar como punto de recuperación. La instantánea está bloqueada y no se puede eliminar de forma normal. Dependiendo

de la gravedad del ataque, también generará una alerta EMS que muestra el volumen afectado, la probabilidad de ataque y la cronología del ataque. Si desea recibir alertas sobre la creación de una nueva instantánea o la observación de una nueva extensión de archivo en su volumen, puede configurar ARP para que envíe estas alertas. Para obtener más información, consulte [Configurar las alertas de ARP](#) en el Centro de NetApp documentación.

Puede generar un informe para ver información detallada sobre un presunto ataque. Tras revisar el informe, podrá darse cuenta ONTAP si la alerta se generó a partir de un falso positivo o de un presunto ataque. Si etiqueta la alerta como un presunto ataque, debe determinar el alcance del ataque y, a continuación, recuperar los datos de la instantánea creada por el ARP. Si etiqueta el ataque como un falso positivo, la instantánea creada por el ARP se elimina automáticamente. Para obtener más información, consulte [Responder a las alertas de protección autónoma contra el ransomware](#).

Le recomendamos que supervise los mensajes EMS del sistema de archivos y el estado de los volúmenes en el ONTAP CLI y API REST. Para obtener más información sobre los mensajes EMS para ARP, consulte [Descripción de las alertas de EMS para la protección autónoma contra el ransomware](#).

Temas

- [Habilitación de la protección autónoma contra el ransomware](#)
- [Responder a las alertas de protección autónoma contra el ransomware](#)
- [Descripción de las alertas de EMS para la protección autónoma contra el ransomware](#)

Habilitación de la protección autónoma contra el ransomware

En los siguientes procedimientos se explica cómo utilizar el ONTAP CLI para habilitar la protección autónoma contra el ransomware (ARP) en los modos de aprendizaje y activo, así como para verificar que la ARP esté habilitada. Para obtener más información sobre ARP, consulte. [¿Cómo funciona ARP](#)

Habilitar el ARP en el modo de aprendizaje

Para habilitar el ARP en el modo de aprendizaje en un volumen existente mediante el ONTAP CLI

- Ejecute el siguiente comando. Sustituya *vol_name* y *svm_name* con su propia información.

```
security anti-ransomware volume dry-run -volume vol_name -vserver svm_name
```

Para obtener más información sobre este comando, consulte [security anti-ransomware volume dry-run](#) en la NetApp centro de documentación.

 Note

El modo de aprendizaje solo se aplica a los datos recién escritos. Los datos existentes no se escanean ni analizan. Los comportamientos normales del tráfico de datos se determinan en función de los nuevos datos que se escriben después de activar el ARP en el volumen.

Para habilitar el ARP en el modo de aprendizaje en un volumen nuevo mediante el ONTAP CLI

- Ejecute el siguiente comando. Sustituya *vol_name*, *svm_name*, *size*, y */path_name* por su información.

```
volume create -volume vol_name -vserver svm_name -aggregate aggr_name -size size -  
anti-ransomware-state dry-run -junction-path /path_name
```

Para obtener más información acerca de este comando, consulte [volume create](#) en la NetApp centro de documentación.

Habilitar ARP en modo activo

Para habilitar el ARP en modo activo en un volumen existente mediante el ONTAP CLI

- Ejecute el siguiente comando. Sustituya *vol_name* y *svm_name* con su propia información.

```
security anti-ransomware volume enable -volume vol_name -vserver svm_name
```

Para obtener más información sobre este comando, consulte [security anti-ransomware volume enable](#) en la NetApp centro de documentación.

 Note

Recomendamos mantener un volumen en modo de aprendizaje durante un mínimo de 30 días antes de convertirlo al modo activo. El ARP determina automáticamente el

período de aprendizaje óptimo y cambia del modo de aprendizaje cuando está listo. Este proceso puede producirse en menos de 30 días.

Habilitar ARP de forma predeterminada en el nivel de SVM

Para habilitar el ARP de forma predeterminada en un SVM existente mediante el ONTAP CLI

- Ejecute el siguiente comando. *svm_name* Sustitúyalo por su propia información.

```
vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run
```

Para obtener más información sobre este comando, consulte [vserver modify](#) en la NetApp centro de documentación.

Verificación del estado del ARP

Para verificar el estado del ARP mediante el ONTAP CLI

- Ejecute el siguiente comando.

```
security anti-ransomware volume show
```

Para obtener más información acerca de este comando, consulte [security anti-ransomware volume show](#) en la NetApp centro de documentación.

Puede suspender temporalmente (y luego reanudar) el ARP si anticipa eventos de gran carga de trabajo. Para obtener más información, consulte [Pausar la protección autónoma contra el ransomware de ONTAP para excluir del análisis los eventos de carga de](#) trabajo en el NetApp Centro de documentación.

Responder a las alertas de protección autónoma contra el ransomware

Los siguientes procedimientos explican cómo utilizar la ONTAP CLI para ver las alertas de protección autónoma contra el ransomware (ARP), generar informes de ataques y tomar medidas en función de los informes. Para obtener más información sobre cómo ARP detecta y responde a los ataques, consulte [¿Qué busca ARP](#) y [¿Cómo responder a un presunto ataque con ARP](#)

Visualización de las alertas ARP

Para ver una alerta ARP en un volumen mediante el ONTAP CLI

- Ejecute el siguiente comando. Sustituya *svm_name* y *vol_name* con su propia información.

```
security anti-ransomware volume show -vserver svm_name -volume vol_name
```

Tras ejecutar el comando, verá un resultado similar al siguiente ejemplo:

```
Vserver Name: fsx
Volume Name: vol1
State: enabled
Attack Probability: moderate
Attack Timeline: 9/14/2021 01:03:23
Number of Attacks: 1
```

Para obtener más información sobre este comando, consulte [security anti-ransomware volume show](#) en la NetApp centro de documentación.

Generación de informes ARP

Para generar informes ARP mediante ONTAP CLI

- Ejecute el siguiente comando. Sustituya *vol_name* y */file_location/* con su propia información. Tras generar el informe, podrá verlo en un sistema cliente.

```
security anti-ransomware volume attack generate-report -volume vol_name -dest-path /file_location/
```

Para obtener más información sobre este comando, consulte [security anti-ransomware volume attack generate-report](#) en la NetApp centro de documentación.

Tomar medidas en relación con los informes del ARP

Para tomar medidas en caso de un ataque de falso positivo derivado de un informe de ARP utilizando el ONTAP CLI

- Ejecute el siguiente comando. Sustituya *svm_name**vol_name*, y *[extension identifiers]* por su propia información.

```
security anti-ransomware volume attack clear-suspect -vserver svm_name -  
volume vol_name [extension identifiers] -false-positive true
```

Para obtener más información acerca de este comando, consulte [security anti-ransomware volume attack clear-suspect](#) en la NetApp centro de documentación.

Note

Cuando marcas una alerta como un falso positivo, se actualiza el perfil del ransomware. Después de hacerlo, no volverá a recibir una alerta sobre ese escenario en particular.

Para tomar medidas ante un posible ataque a partir de un informe de ARP, utilice el ONTAP CLI

- Ejecute el siguiente comando. Sustituya *svm_name**vol_name*, y *[extension identifiers]* por su propia información.

```
security anti-ransomware volume attack clear-suspect -vserver svm_name -  
volume vol_name [extension identifiers] -false-positive false
```

Para obtener más información acerca de este comando, consulte [security anti-ransomware volume attack clear-suspect](#) en la NetApp centro de documentación.

Descripción de las alertas de EMS para la protección autónoma contra el ransomware

Puede usar... NetApp ONTAP's Sistema de gestión de eventos (EMS) para monitorear los eventos relacionados con el ARP, incluidos los posibles ataques. Para obtener más información sobre el ARP y cómo detecta los ataques, consulte [¿Cómo funciona ARP](#) y [¿Qué busca ARP](#)

La siguiente tabla contiene todas las alertas relacionadas con el ARP. Para obtener más información sobre EMS, consulte [Supervisión FSx de eventos EMS de ONTAP](#).

Nombre del mensaje EMS	Descripción del mensaje EMS
<code>arw.analytics.ext.report</code>	Este mensaje aparece cuando los análisis antiransomware generan o actualizan el informe de extensiones de archivo sospechosas de un volumen.
<code>arw.analytics.high.entropy</code>	Este mensaje aparece cuando el número de mensajes de registro de datos de alta entropía (relacionados con la detección y el análisis del ransomware) supera el umbral predefinido para un volumen.
<code>arw.analytics.probability</code>	Este mensaje aparece cuando la probabilidad de un ataque contra el ransomware ha cambiado de un low volumen a high otro.
<code>arw.analytics.report</code>	Este mensaje aparece cuando se genera o actualiza un informe de análisis antiransomware para un volumen.
<code>arw.analytics.suspects</code>	Este mensaje aparece cuando la lista de sospechosos generada por los análisis de la lucha contra el ransomware aumenta hasta el punto de que es necesario investigar más a fondo.
<code>arw.auto.switch.enabled</code>	Este mensaje aparece cuando la protección contra el ransomware pasa automáticamente del modo de aprendizaje a la activación, una vez cumplidas varias condiciones, como el período de aprendizaje, la creación de archivos, la escritura de archivos y las actividades de descubrimiento de extensiones de archivos.

Nombre del mensaje EMS	Descripción del mensaje EMS
<code>arw.new.file.extn.seen</code>	Este mensaje aparece cuando se observa una nueva extensión de archivo en un volumen habilitado para la protección contra el ransomware. Su objetivo es notificar rápidamente al usuario acerca de la extensión observada, lo que permite una investigación oportuna.
<code>arw.snapshot.created</code>	Este mensaje aparece cuando se crea una nueva instantánea de ARP en un volumen compatible con la protección contra el ransomware. Además, proporciona información sobre el motivo por el que se creó la instantánea.
<code>arw.volume.state</code>	Este mensaje aparece cuando se cambia el estado antiransomware de un volumen.
<code>arw.vserver.state</code>	Este mensaje aparece cuando se cambia el estado antiransomware de un SVM.

Proteja sus datos con SnapLock

SnapLock es una función que le permite proteger sus archivos mediante la transición a un estado de escritura una vez, lectura múltiple (WORM), lo que impide su modificación o eliminación durante un período de retención específico. Puede usar... SnapLock para cumplir con la normativa, 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 for NetApp ONTAP admite los modos de retención empresarial y de conformidad con SnapLock. Para obtener más información, consulte [Descripción SnapLock Conformidad](#) y [Descripción SnapLock Enterprise](#).

Puede crear SnapLock volúmenes activados FSx para los sistemas de archivos ONTAP creados a partir del 13 de julio de 2023. Los sistemas de archivos existentes obtendrán SnapLock soporte durante una próxima ventana de mantenimiento semanal.

Temas

- [Cómo SnapLock funciona](#)
- [Descripción SnapLock Conformidad](#)
- [Descripción SnapLock Enterprise](#)
- [Entender el SnapLock periodo de retención](#)
- [Pasar archivos a estado WORM](#)

Cómo SnapLock funciona

SnapLock puede ayudarlo a cumplir con los fines regulatorios y de gobierno al evitar que sus archivos se eliminen, cambien o cambien de nombre. Al crear un SnapLock volumen, usted compromete sus archivos para que se escriban una vez, lean muchos (WORM) y establezcan períodos 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 SnapLock configuración en el momento de la creación. Un no-SnapLock el volumen no se puede convertir en un SnapLock volumen después de la creación.

Modos de retención

SnapLock tiene dos modos de retención: Compliance y Enterprise. Amazon FSx for 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.

SnapLock feature	Descripción SnapLock Conformidad	Descripción SnapLock Enterprise
Descripción	Los archivos que se hayan transferido a WORM en un volumen de Conformidad	Los usuarios autorizados pueden eliminar los archivos que hayan pasado a WORM

SnapLock feature	Descripción SnapLock Conformidad	Descripción SnapLock Enterprise
	no se pueden eliminar hasta que venzan sus períodos de retención.	en un volumen empresari al antes de que venzan 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. • Cómo 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 usarla SnapLock Conformidad.
Confirmación automática	Sí	Sí
Retención basada en eventos (EBR)¹	Sí	Sí
Retención legal¹	Sí	No
Uso de la eliminación privilegiada	No	Sí
Modo añadir volumen	Sí	Sí
SnapLock auditar volúmenes de registro	Sí	Sí

 Note

¹. Las operaciones EBR y Legal Hold están respaldadas por el ONTAP CLI y API REST.

 Note

FSx para ONTAP, admite la organización en niveles de los datos en el conjunto de capacidades en todos SnapLock volúmenes, independientemente de SnapLock . Para obtener más información, consulte [Organización de datos de volumen en niveles](#).

SnapLock administrator

Debe tener... SnapLock privilegios de administrador para realizar determinadas acciones en SnapLock volúmenes. SnapLock los privilegios de administrador se definen en el `vsadmin-snaplock` rol del ONTAP CLI. Debe ser administrador de clústeres para crear una cuenta de administrador de máquinas virtuales de almacenamiento (SVM) con SnapLock rol de administrador.

Puede realizar las siguientes acciones con el `vsadmin-snaplock` rol en ONTAP CLI:

- 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
- Realización SnapLock acciones, incluida 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 SnapLock administrador en el ONTAP CLI. 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 ONTAP CLI

- Ejecute el siguiente comando. Sustituya *SVM_name* y *SnapLockAdmin* con su propia información.

```
cluster1::> security login create -vserver SVM_name -user-or-group-name SnapLockAdmin -application ssh -authentication-method password -role vsadmin-snaplock
```

Para obtener más información, consulte [Usuarios y roles de ONTAP](#).

SnapLock auditar volúmenes de registro

A SnapLock el volumen del registro de auditoría contiene SnapLock registros de auditoría, que contienen marcas de tiempo de eventos, como cuando un SnapLock se creó un administrador cuando se ejecutaron operaciones de eliminación con privilegios o cuando se impuso una retención legal a los archivos. La SnapLock El volumen del registro de auditoría es un registro de eventos que no se puede borrar.

Debe crear un SnapLock volumen de registro de auditoría en el mismo SVM que el SnapLock volumen para las siguientes acciones:

- Para activar o desactivar la eliminación privilegiada en un SnapLock Volumen empresarial.
- Para aplicar una retención legal a un archivo de un SnapLock Volumen de cumplimiento.

Warning

- El período mínimo de retención de un SnapLock el volumen del registro de auditoría es de seis meses. Hasta que venza este período de retención, el SnapLock El volumen del registro de auditoría y el SVM y el sistema de archivos asociados a él no se pueden eliminar aunque el volumen se haya creado en SnapLock Modo empresarial.
- 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.

Solo puedes tener uno activo SnapLock el volumen del registro de auditoría en una SVM, pero puede ser compartido por varios SnapLock volúmenes en el SVM. Para montar un SnapLock audite correctamente el volumen del registro, 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.

Puedes encontrar SnapLock los registros de auditoría se encuentran en el `/snaplock_log` directorio situado 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 SnapLock volumen de registro de auditoría con la FSx consola de Amazon AWS CLI, la FSx API de Amazon y la ONTAP CLI y API REST.

Note

Un volumen de protección de datos (DP) no se puede utilizar como SnapLock volumen de registro de auditoría.

Para activar el SnapLock volumen de registro de auditoría con la FSx API de Amazon, utilizado `AuditLogVolume` en [CreateSnaplockConfiguration](#). En la FSx consola de Amazon, en Audit log volume, selecciona Enabled. Asegúrese de que la Ruta de unión está configurada como `/snaplock_audit_log`.

Acceder a sus datos en un SnapLock volume

Puede utilizar protocolos de archivos abiertos, como NFS y SMB, para acceder a sus datos en un SnapLock volumen. Escribir datos en un SnapLock volumen o por leer datos protegidos por WORM.

Puede copiar archivos de un lado a otro SnapLock volúmenes con NFS y SMB, pero no conservarán sus propiedades WORM en el destino SnapLock volumen. Debe volver a enviar los archivos copiados a WORM para evitar que se modifiquen o eliminen. Para obtener más información, consulte [Pasas archivos a estado WORM](#).

También puedes replicar SnapLock datos con SnapMirror, pero los volúmenes de origen y destino deben ser SnapLock volúmenes con el mismo modo de retención (por ejemplo, ambos deben ser de cumplimiento o empresarial).

Descripción SnapLock Conformidad

En esta sección se describen los casos de uso y las consideraciones para SnapLock Modo de retención de conformidad.

Puede elegir el modo de retención de Conformidad para los siguientes casos de uso.

- Puede usar... SnapLock Cumplimiento para cumplir con los mandatos gubernamentales o específicos de la industria, como la Regla 17a-4 (f) de la SEC, la Regla 4511 de la FINRA y el Reglamento 1.31 de la CFTC. SnapLock La conformidad de NetApp ONTAP en Amazon FSx con respecto a estos mandatos y reglamentos fue evaluada por Cohasset Associates. Para obtener más información, consulte el [Informe de evaluación de conformidad de Amazon FSx para NetApp ONTAP](#).
- Puede usar... SnapLock Cumplimiento para complementar o mejorar una estrategia integral de protección de datos para combatir los ataques de ransomware.

Estos son algunos aspectos importantes que se deben tener en cuenta sobre la SnapLock Modo de retención de conformidad.

- Después de que un archivo pase al estado de escritura una vez, lea muchos (WORM) en un SnapLock Volumen de conformidad, ningún usuario puede eliminarlo antes de que venza su período de retención.
- A SnapLock El volumen de conformidad solo 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 puede cambiar el nombre de un SnapLock Volumen de conformidad tras 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).
- A SnapLock El volumen de conformidad no se puede convertir en un SnapLock Volumen empresarial y viceversa.

Descripción SnapLock Enterprise

En esta sección se describen los casos de uso y las consideraciones para SnapLock Modo de retención empresarial.

Puede elegir el SnapLock Modo de retención empresarial para los siguientes casos de uso.

- Puede usar... SnapLock Enterprise autorizará solo a usuarios específicos a eliminar archivos.
- Puede usar... SnapLock Enterprise para mejorar la integridad de los datos y el cumplimiento interno de su organización.

- Puede usar... SnapLock Enterprise probará la configuración de retención antes de usarla SnapLock Cumplimiento.

Estos son algunos aspectos importantes que se deben tener en cuenta acerca del SnapLock Modo de retención empresarial.

- Puede usar... 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 empresariales).
- A SnapLock el volumen no se puede convertir de Enterprise a Compliance ni de Compliance a Enterprise.
- SnapLock Enterprise no admite Legal Hold.

Uso de la eliminación privilegiada

Una de las principales diferencias entre SnapLock Enterprise y SnapLock El cumplimiento es eso SnapLock el administrador puede activar la eliminación privilegiada en un SnapLock Volumen empresarial para permitir eliminar un archivo antes de que venza el período de retención del archivo. La SnapLock el administrador es el único usuario que puede eliminar archivos de un SnapLock Volumen empresarial que incluye políticas de retención activas. Para obtener más información, consulte [SnapLock administrator](#).

Puedes activar o desactivar la eliminación con privilegios con la FSx consola de Amazon AWS CLI, la FSx API de Amazon y la ONTAP CLI y API REST. Para activar la eliminación con privilegios, primero debe crear un SnapLock volumen de registro de auditoría en el mismo SVM que el SnapLock volumen. Para obtener más información, consulte [SnapLock auditar volúmenes de registro](#).

Para activar la eliminación con privilegios con la FSx API de Amazon, `PrivilegedDelete` utilízala en [CreateSnaplockConfiguration](#). En la FSx consola de Amazon, en Privileged Delete, selecciona Enabled.

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 privilegiada está desactivada permanentemente, no necesitas tener una SnapLock volumen del registro de auditoría asociado al SnapLock Volumen empresarial.

Para desactivar permanentemente la eliminación con privilegios con la FSx API de Amazon, PrivilegedDelete utilízala en [CreateSnaplockConfiguration](#). En la FSx consola de Amazon, en Eliminación privilegiada, selecciona Desactivado permanentemente.

Pasando por alto SnapLock Modo empresarial

Si utilizas la FSx consola de Amazon o la FSx API de Amazon, debes tener el `fsx:BypassSnapLockEnterpriseRetention` permiso de IAM para eliminar un SnapLock Volumen empresarial que contiene archivos WORM con políticas de retención activas.

Para obtener más información, consulte [Eliminación SnapLock volumes](#).

Entender el SnapLock periodo de retención

Al crear un SnapLock volumen, puede establecer un período de retención predeterminado para el volumen o puede establecer el período de retención para los archivos que se escriben una vez y se leen varios (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 a 65 535	
Minutos	0 a 65 535	
Horas	0 a 24	
Días	0 a 365	
Meses	0 a 12	
Años	0 a 100	
Infinito	-	Conserva los archivos para siempre. Disponible para la Retención predeterminada, la Retención máxima y la Retención mínima.
Sin especificar (1)	-	Conserva los archivos hasta que establezca un período de retención. Disponible sólo para la Retención predeterminada.

 Note

¹ Cuando se transfieren archivos a WORM con un período de retención no especificado, se les asigna el período de retención mínimo configurado para SnapLock volumen. 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 vence el período de retención, no puede modificar un archivo WORM.

Establecer el período de retención de un SnapLock volume

Puede establecer el período de retención de un SnapLock volumen con la FSx consola de Amazon AWS CLI, la FSx API de Amazon y la ONTAP CLI y API REST.

Para establecer el período de retención con la FSx API de Amazon, usa la [SnaplockRetentionPeriod](#) configuración. En la FSx consola de Amazon, para el período de retención, introduce los valores de Retención predeterminada, Retención mínima y Retención máxima. A continuación, elija la Unidad correspondiente para cada uno.

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. Puedes activar la confirmación automática con la FSx consola de Amazon AWS CLI, la FSx API de Amazon y la ONTAP CLI y API 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 a 65 535
Horas	1 a 65 535
Días	1 a 3650
Meses	1 a 120
Años	1 a 10

Para activar la confirmación automática con la FSx API de Amazon, utilízala `AutocommitPeriod` en. [CreateSnaplockConfiguration](#) En la FSx consola de Amazon, para `Autocommit`, selecciona `Enabled`. En `Periodo de confirmación automática`, ingrese un valor y seleccione la Unidad de confirmación automática correspondiente.

Puede especificar un valor entre 5 minutos y 10 años.

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. Puedes activar o desactivar el modo de adición de volumen con la FSx consola de Amazon, AWS CLI la FSx API de Amazon y la ONTAP CLI y API REST.

Requisitos para actualizar el modo añadir volúmenes

- La SnapLock el volumen debe estar desmontado.
- La SnapLock el volumen debe estar vacío de copias instantáneas y datos de usuario.

Para activar el modo de adición de volumen con la FSx API de Amazon, `VolumeAppendModeEnabled` utilízalo en. [CreateSnaplockConfiguration](#) En la FSx consola de Amazon, en el modo de adición de volúmenes, selecciona `Enabled`.

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.

El EBR es compatible con el ONTAP CLI y API REST.

Note

ONTAP no admite EBR con FlexGroup volúmenes.

En los siguientes procedimientos se explica cómo crear, aplicar, modificar y eliminar una política de EBR. Debes ser un SnapLock administrador (tener la `vsadmin-snaplock` función) para completar estas tareas en el ONTAP CLI. Para obtener más información, consulte [SnapLock administrator](#).

Crear una política de EBR en la ONTAP CLI

Para crear una política de EBR en el ONTAP CLI

- Ejecute el siguiente comando. Sustituya *p1* y *"10 years"* con su propia información.

```
vs1::> snaplock event-retention policy create -name p1 -retention-period "10 years"
```

Aplicar una política de EBR en el ONTAP CLI

Para aplicar una política de EBR en el ONTAP CLI

- Ejecute el siguiente comando. Sustituya *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 /
```

Modificar una política de EBR en el ONTAP CLI

Para modificar una política de EBR en el ONTAP CLI

- Ejecute el siguiente comando. Sustituya *p1* y *"5 years"* con su propia información.

```
vs1::> snaplock event-retention policy modify -name p1 -retention-period "5 years"
```

Eliminar una política de EBR en el ONTAP CLI

Para eliminar una política de EBR en el ONTAP CLI

- Ejecute el siguiente comando. *p1* Sustitúyala por tu propia información.

```
vs1::> snaplock event-retention policy delete -name p1
```

Comandos relacionados en el NetApp Centro de documentación:

- [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.

Legal Hold cuenta con el apoyo de ONTAP CLI y API REST.

Note

ONTAP no admite la retención legal con FlexGroup volúmenes.

En los siguientes procedimientos se explica cómo iniciar y finalizar una Retención legal. Debes ser un SnapLock administrador (tener la `vsadmin-snaplock` función) para completar estas tareas en el ONTAP CLI. Para obtener más información, consulte [SnapLock administrator](#).

Iniciar una retención legal sobre un archivo en un SnapLock Volumen de conformidad con la ONTAP CLI

Para iniciar una retención legal sobre un archivo de un SnapLock Volumen de conformidad con la ONTAP CLI

- Ejecute el siguiente comando. Sustituya *litigation1slc_vol1*, y *file1* por su propia información.

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -  
path /file1
```

Iniciar una retención legal de todos los archivos de un SnapLock Volumen de conformidad con la ONTAP CLI

Para iniciar una retención legal de todos los archivos de un SnapLock Volumen de conformidad con la ONTAP CLI

- Ejecute el siguiente comando. Sustituya *litigation1* y *slc_vol1* con su propia información.

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -  
path /
```

Poner fin a una retención legal de un archivo en un SnapLock Volumen de conformidad con la ONTAP CLI

Para poner fin a una retención legal sobre un archivo en un SnapLock Volumen de conformidad con la ONTAP CLI

- Ejecute el siguiente comando. Sustituya *litigation1slc_vol1*, y *file1* por su propia información.

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -  
path /file1
```

 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.

Poner fin a la retención legal de todos los archivos de un SnapLock Volumen de conformidad con la ONTAP CLI

Para poner fin a una retención legal de todos los archivos de un SnapLock Volumen de conformidad con la ONTAP CLI

- Ejecute el siguiente comando. Sustituya *litigation1* y *slc_voll* con su propia información.

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_voll -  
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 NetApp Centro de documentación:

- [snaplock legal-hold abort](#)
- [snaplock legal-hold dump-files](#)
- [snaplock legal-hold dump-litigations](#)
- [snaplock legal-hold show](#)

Replicar sus datos con FlexCache

FlexCache es una capacidad de almacenamiento NetApp ONTAP's remoto en caché que acerca los conjuntos de datos a los clientes, lo que mejora el rendimiento del acceso y reduce los costes. Simplifica la distribución de archivos y reduce los costes de la WAN. Al crear un FlexCache volumen, inicialmente solo copia los metadatos del sistema de archivos de origen. Este enfoque es más rápido

y ahorra más espacio que una copia completa de los datos, ya que solo consume una fracción de la capacidad de almacenamiento.

Cómo funciona FlexCache

Un FlexCache volumen es una memoria caché poco poblada que proporciona acceso a los datos almacenados en un volumen de origen. La memoria caché se puede ubicar en un sistema de archivos diferente, opcionalmente remoto. En lugar de copiar todos los datos del volumen de origen, FlexCache copia los datos solo cuando es necesario. FlexCachelos volúmenes son más adecuados para flujos de trabajo de lectura intensiva con cambios de datos poco frecuentes, ya que cualquier cambio en los datos de origen requiere que se actualice la caché.

Se puede utilizar FlexCache con ONTAP en FSx las siguientes configuraciones:

Volumen de origen	FlexCache volume
En las instalaciones NetApp ONTAP	FSx para ONTAP
FSx para ONTAP	En las instalaciones NetApp ONTAP
FSx para ONTAP	FSx para ONTAP

FlexCachemodos de escritura

FlexCachelos volúmenes admiten dos modos de operación para las operaciones de escritura: modo de reescritura y modo de reescritura.

En el modo de anulación, que es el modo predeterminado, las escrituras se reenvían desde la memoria caché al volumen de origen. El cliente no reconoce la operación de escritura hasta que los datos se hayan guardado en el volumen de origen y el origen confirme que se ha vuelto a escribir en la caché. Como cada escritura debe atravesar la red entre la caché y el origen, este modo tiene una latencia mayor que el modo de reescritura.

En el modo de reescritura, introducido en la versión ONTAP 9.15.1, las escrituras se guardan en la ubicación de la caché y el cliente las recibe inmediatamente. A continuación, los datos se escriben de forma asíncrona en el volumen de origen. Este modo permite que las escrituras se realicen a velocidades casi locales, lo que puede mejorar considerablemente el rendimiento de las cargas de trabajo distribuidas.

Utilice el modo de reescritura para cargas de trabajo de escritura intensiva que requieren escrituras en caché de baja latencia. Utilice el modo de escritura alternativa para cargas de trabajo de lectura intensiva que no sean sensibles a la latencia, o cuando el sistema de archivos de origen tenga más de 10 volúmenes de origen. FlexCache

FlexCache descripción general de la creación de volúmenes

La creación de un FlexCache volumen consta de los siguientes pasos:

- Recopile las interfaces lógicas de origen y destino (LIFs)
- Establezca el emparejamiento de clústeres entre los sistemas de archivos de origen y caché
- Cree una relación de interconexión entre máquinas virtuales de almacenamiento SVM
- Cree el FlexCache volumen y seleccione un modo de escritura
- Monta el FlexCache volumen en tus clientes

Para obtener instrucciones detalladas, consulta [Creación de un FlexCache](#).

Creación de un FlexCache

Mediante los siguientes procedimientos, creará un FlexCache volumen en un sistema de archivos de Amazon FSx for NetApp ONTAP, respaldado por un volumen de origen ubicado en un clúster localNetApp ONTAP.

Uso de la ONTAP CLI

Utilizará la ONTAP CLI para crear y gestionar una FlexCache configuración en el sistema de archivos FSx de ONTAP.

Los comandos de estos procedimientos utilizan los siguientes alias para el clúster, la SVM y el volumen:

- `Cache_ID`— el ID del clúster de caché (con el formato FSx IDABCDEF1234567890A)
- `Origin_ID`— el ID del clúster de origen
- `CacheSVM`— el nombre del SVM de la caché
- `OriginSVM`— el nombre SVM de origen
- `OriginVol`— el nombre del volumen de origen

- CacheVol— el nombre FlexCache del volumen

Los procedimientos de esta sección utilizan los siguientes comandos NetApp ONTAP CLI.

- [network interfaces show](#)
- Comandos de la [cluster peer](#)
- [volume flexcache create](#)

Requisitos previos

Antes de empezar a utilizar los procedimientos de las siguientes secciones, asegúrese de cumplir los siguientes requisitos previos:

- Los sistemas de archivos de origen y destino están conectados en la misma VPC o se encuentran en redes interconectadas mediante Amazon VPC, o. AWS Transit Gateway AWS Direct Connect AWS VPN Para obtener más información, consulte [Acceder a los datos desde el Nube de AWS ¿Qué es la interconexión de VPC?](#) en la Guía de peering de Amazon VPC.
- El grupo de seguridad de VPC FSx para el sistema de archivos de ONTAP tiene reglas de entrada y salida que permiten el ICMP y el TCP en los puertos 11104 y 11105 para los puntos de conexión entre clústeres (). LIFs
- Ha creado un destino FSx para el sistema de archivos de ONTAP con una SVM, pero no ha creado el volumen que se utilizará como. FlexCache Para obtener más información, consulte [Creación de sistemas de archivos](#).

Registre el origen y el destino entre clústeres LIFs

1. FSx Para el sistema de archivos de ONTAP que es el clúster de destino:
 - a. Abre la FSx consola de Amazon en <https://console.aws.amazon.com/fsx/>.
 - b. Seleccione Sistemas de archivos y, a continuación, elija el FSx sistema de archivos de ONTAP que sea el clúster de destino para abrir la página de detalles del sistema de archivos.
 - c. En Administración, busque el punto final entre clústeres (direcciones IP) y registre el valor.

Note

En el caso de los sistemas de archivos escalables, hay dos direcciones IP de punto final entre clústeres para cada par de alta disponibilidad (HA).

2. Para el clúster de origen local, recupere las direcciones IP LIF entre clústeres mediante el siguiente comando de CLIONTAP:

```
Origin:> network interface show -role intercluster
```

Logical			Network
Vserver	Interface	Status	Address/Mask
-----	-----	-----	-----
OriginSVM			
	inter_1	up/up	10.0.0.36/24
	inter_2	up/up	10.0.1.69/24

3. Guarde las direcciones y `inter_1`. `inter_2` IP Se hace referencia a ellas en el `OriginSVM` alias como `origin_inter_1` `origin_inter_2` y en el `CacheSVM` alias como `cache_inter_1` y `cache_inter_2`.

Establezca la interconexión de clústeres entre el origen y la caché

Establezca una relación de pares del clúster en el Source clúster Cache y mediante el comando [cluster peer create](#) ONTAPCLI. Proporcionará las direcciones IP entre clústeres que guardó anteriormente en el [Registre el origen y el destino entre clústeres LIFs](#) procedimiento. Cuando se le pida, se le pedirá que cree una *cluster-peer-passphrase* que tendrá que introducir cuando establezca la interconexión de clústeres en el Origin clúster.

1. Configure el emparejamiento de clústeres en el Cache clúster (el sistema de archivos FSx de ONTAP).
 - a. Para acceder a la ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando. 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 [Administrar sistemas de archivos con el ONTAP CLI](#).

- b. Utilice el siguiente comando y registre la contraseña que ha creado. Para sistemas de archivos escalables, proporcione las direcciones `inter_2` IP `inter_1` y de cada par de alta disponibilidad.

```
FSx-Cache::> cluster peer create -address-family ipv4 -peer-  
addrs origin_inter_1,origin_inter_2
```

Enter the passphrase: **cluster-peer-passphrase**

Confirm the passphrase: **cluster-peer-passphrase**

Notice: Now use the same passphrase in the "cluster peer create" command in the other cluster.

2. Use el siguiente comando para configurar el emparejamiento de clústeres en el clúster source (local). Deberás introducir la contraseña que creaste en el paso anterior para autenticarte. Para los sistemas de archivos escalables, tendrá que proporcionar la dirección IP entre clústeres para cada par de HA.

```
Origin::> cluster peer create -address-family ipv4 -peer-  
addrs cache_inter_1,cache_inter_2
```

Enter the passphrase: **cluster-peer-passphrase**

Confirm the passphrase: **cluster-peer-passphrase**

3. En el source clúster, compruebe que el emparejamiento de clústeres se haya configurado correctamente mediante el siguiente comando. En la salida, Availability debe configurarse en Available.

```
Origin::> cluster peer show
```

Peer Cluster Name	Availability	Authentication
-----	-----	-----
Cache_ID	Available	ok

Si el resultado no aparece `Available`, repita los pasos anteriores en los cache clústeres source y.

Configure el emparejamiento de máquinas virtuales de almacenamiento (SVM)

Una vez que haya establecido correctamente el emparejamiento de clústeres, el siguiente paso consiste en crear una relación de emparejamiento de SVM en el clúster de caché (caché) mediante el comando `vserver peer`. Los alias adicionales que se utilizan en el siguiente procedimiento son los siguientes:

- **CacheLocalName**— el nombre utilizado para identificar la cache SVM al configurar el emparejamiento de la SVM en la SVM. origin
- **OriginLocalName**— el nombre utilizado para identificar el origin SVM al configurar el emparejamiento del SVM en el SVM. cache

1. En el cache SVM, utilice el siguiente comando para crear una relación de emparejamiento del SVM.

```
FSx-Cache::> vserver peer create -vserver CacheSVM -peer-vserver OriginSVM -peer-cluster Origin_ID -local-name OriginLocalName -application flexcache
```

2. En el clúster de origen, utilice el siguiente comando para aceptar la relación de emparejamiento de SVM.

```
Origin::> vserver peer accept -vserver OriginSVM -peer-vserver CacheSVM -local-name CacheLocalName
```

3. En el clúster de origen, acepte la relación de emparejamiento.

```
Origin::> vserver peer accept -vserver OriginSVM -peer-vserver CacheSVM -local-name CacheLocalName
```

4. Compruebe que el emparejamiento del SVM se haya realizado correctamente mediante el siguiente comando; Peer State debe configurarse `peered` en la respuesta.

```
Origin::> vserver peer show
```

Vserver	Peer Vserver	Peer State	Peering Cluster	Remote Applications
-----	-----	-----	-----	
OriginSVM	CacheSVM	peered	FSx-Cache	flexcache

Cree el volumen FlexCache

Tras crear correctamente la relación de emparejamiento del SVM, el siguiente paso es crear el FlexCache volumen en el SVM de la caché. El FlexCache volumen debe ser un FlexGroup. También elegirá un modo de operación para su FlexCache volumen. Para obtener más información, consulte [FlexCache modos de escritura](#).

1. En el clúster de caché, utilice el siguiente comando CLI de ONTAP para crear el FlexCache volumen. En el ejemplo se crea un FlexCache volumen de 2 TB denominado *CacheVol*.

- Para crear un FlexCache volumen rotativo, utilice el siguiente comando.

```
FSx-Cache::> volume flexcache create -vserver CacheSVM -size 2t -volume CacheVol
               -origin-volume OriginVol -origin-vserver OriginSVM -junction-path /flexcache -
               aggr-list aggr1
```

- Para crear un FlexCache volumen de reescritura, utilice el siguiente comando.

```
FSx-Cache::> volume flexcache create -vserver CacheSVM -size 2t -volume CacheVol
               -origin-volume OriginVol -origin-vserver OriginSVM -junction-path /flexcache -
               aggr-list aggr1 -is-writeback-enabled true
```

Note

Puede utilizar el `volume flexcache config modify -is-writeback-enabled {true|false}` comando para modificar el modo de escritura. Antes de utilizar este comando, asegúrese de entrar en el modo avanzado de ONTAP CLI mediante el `set - privilege advanced` comando.

2. Compruebe la FlexCache relación entre el FlexCache volumen y el volumen de origen.

- En el caso de un volumen FlexCache de escritura circular, la salida tendrá un aspecto similar al del siguiente ejemplo.

```
FSx-Cache::> volume flexcache show
```

Vserver	Volume	Size	Origin-Vserver	Origin-Volume	Origin-Cluster
-----	-----	-----	-----	-----	-----
CacheSVM	CacheVol	2TB	OriginSVM	OriginVol	Origin

- En el caso de un FlexCache volumen regrabable, la salida tendrá un aspecto similar al del siguiente ejemplo.

```
FSx-Cache::~> volume flexcache show
```

Vserver	Volume	Size	Origin-Vserver	Origin-Volume	Origin-Cluster
Writeback					
-----	-----	-----	-----	-----	-----
CacheSVM	CacheVol	2TB	OriginSVM	OriginVol	Origin
true					

Monta el volumen FlexCache

Una vez que el FlexCache volumen esté DISPONIBLE NFSv3 NFSv4, los clientes de pequeñas y medianas empresas podrán montarlo. Una vez FlexCache montado, los clientes tienen acceso a todo el conjunto de datos del volumen de origen local.

- Para crear un punto de montaje y montarlo FlexCache, ejecute los siguientes comandos en el cliente:

```
$ sudo mkdir -p /fsx/CacheVol
$ sudo mount -t nfs management.fs-01d2f606463087f6d.fsx.us-east-1.amazonaws.com:/
CacheVol /fsx/CacheVol
```

Replicar sus datos mediante NetApp SnapMirror

Puede usar... NetApp SnapMirror para programar la replicación periódica del sistema de archivos de ONTAP hacia o desde un segundo sistema de archivos. FSx 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 los datos y una rápida replicación de los datos en todas partes ONTAP sistemas, ya sea que esté replicando entre dos sistemas de FSx archivos de Amazon o desde un entorno local. AWS AWS La replicación se puede programar con una frecuencia de hasta 5 minutos, aunque los intervalos se deben elegir cuidadosamente en función de RPOs (los objetivos del punto de recuperación), RTOs los objetivos de tiempo de recuperación y las consideraciones de rendimiento.

Al replicar datos a NetApp los sistemas de almacenamiento y la actualización continua de los datos secundarios, sus datos se mantienen actualizados y permanecen disponibles siempre que los necesite. No se requieren servidores de replicación externos. Para obtener más información sobre el uso NetApp SnapMirror para replicar sus datos, consulte [Más información sobre el servicio de replicación](#) en NetApp BlueXP documentación.

Puede crear un volumen de destino de protección de datos (DP) para NetApp SnapMirror mediante la FSx consola de Amazon AWS CLI, la API de Amazon y la FSx API de Amazon, además de NetApp ONTAP CLI y API REST. Para obtener información sobre la creación de un volumen de destino mediante la FSx consola de Amazon y AWS CLI, consulte [Creación de volúmenes](#).

Puede usar... NetApp BlueXP o el ONTAP CLI para programar la replicación de su sistema de archivos.

Note

Existen dos tipos de SnapMirror replicación: a nivel de volumen SnapMirror y SVM Disaster Recovery (SVMDR). Solo a nivel de volumen SnapMirror ONTAP admite la FSx replicación. Synchronous SnapMirror, incluyendo StrictSync, no es compatible.

Utilización NetApp BlueXP para programar la replicación

Puede usar NetApp BlueXP para configurar la replicación SnapMirror en su sistema de archivos FSx de ONTAP. Para obtener más información, consulte [Replicación de datos entre sistemas](#) en la documentación de BlueXP. NetApp

Uso de ONTAP CLI para programar la replicación

Puede utilizar el ONTAP CLI para configurar la replicación de volúmenes programada. Para obtener más información, consulte [Administrar la replicación de SnapMirror volúmenes](#) en NetApp ONTAP Centro de documentación.

AWS informes de facturación y uso FSx para ONTAP

AWS proporciona dos informes de uso FSx para ONTAP:

- El informe AWS de facturación es una vista general de toda la actividad Servicios de AWS que utilizas, incluida FSx ONTAP.
- El informe de AWS uso es un resumen de la actividad de un servicio específico, agregado por hora, día o mes. También incluye gráficos de uso que proporcionan una representación gráfica de su uso FSx de ONTAP.

Note

Al igual que otros Servicios de AWS, FSx for ONTAP solo te cobra por lo que utilizas. Para obtener más información, consulta los [precios de Amazon FSx for NetApp ONTAP](#).

Consulta el informe AWS de facturación de FSx ONTAP

Puedes ver un resumen del AWS uso y los cargos, ordenados por servicio, en la página de facturas de la Administración de facturación y costos de AWS consola.

Para ver el informe AWS de facturación

1. Inicie sesión en AWS Management Console y abra la Administración de facturación y costos de AWS consola en <https://console.aws.amazon.com/costmanagement/>.
2. En el panel de navegación, seleccione Facturas.
3. Elige un período de facturación (por ejemplo, agosto de 2024).
4. Para ver FSx los cargos de Amazon, en la pestaña Cargos por servicio, ingresa FSx al campo de texto filtrar por servicio y luego expande FSx para ver los cargos por Región de AWS.

Los cargos de FSx los sistemas de archivos ONTAP aparecen en las FSx CreateFileSystem entradas de Amazon:ONTAP del informe.

5. Para descargar el informe de facturación detallado en formato CSV, selecciona Descargar todo a CSV en la parte superior de la página de facturas.

Para obtener más información sobre tu AWS factura, consulta Cómo [ver tu factura](#) en la Guía del AWS Billing usuario.

El informe de facturación incluye los siguientes tipos de uso aplicables a los sistemas FSx de archivos de ONTAP:

First generation FSx for ONTAP file systems

Tipo de cargo	Unidades	Descripción	
Almacenamiento SSD ONTAP Single-AZ	GB-mes	La cantidad de almacenamiento SSD aprovisionada en un sistema de archivos ONTAP Single-AZ de primera generación	
Almacenamiento SSD Multi-AZ de ONTAP	GB-mes	La cantidad de almacenamiento SSD aprovisionada en un FSx Multi-AZ de primera generación para el sistema de archivos ONTAP	
Capacidad de rendimiento Single-AZ de ONTAP	MBps-Mes	La cantidad de capacidad de rendimiento aprovisionada en un sistema de archivos FSx Single-AZ de primera generación para ONTAP	
Capacidad de rendimiento Multi-AZ de ONTAP	MBps-Mes	La cantidad de capacidad de rendimiento aprovisionada en un sistema de archivos FSx Multi-AZ de primera generación para ONTAP	
IOPS de SSD ONTAP Single-AZ aprovisionadas	IOPS por mes	La cantidad de IOPS de SSD aprovisionadas en un sistema de archivos Single-	

Tipo de cargo	Unidades	Descripción	
		AZ de primera generación para ONTAP FSx	
IOPS de SSD Multi-AZ de ONTAP aprovisionadas	IOPS por mes	La cantidad de IOPS de SSD aprovisionadas en un sistema de archivos Multi-AZ de primera generación para ONTAP FSx	

Second generation FSx for ONTAP file systems

Tipo de cargo	Unidades	Descripción	
Almacenamiento SSD ONTAP Single-AZ-2	GB-mes	La cantidad de almacenamiento SSD aprovisionada en un sistema de archivos Single-AZ de segunda generación para ONTAP FSx	
Almacenamiento SSD Multi-AZ-2 de ONTAP	GB-mes	La cantidad de almacenamiento SSD aprovisionada en un sistema de archivos Multi-AZ de segunda generación para ONTAP FSx	
Capacidad de rendimiento de ONTAP Single-AZ-2	MBps-Mes	La cantidad de capacidad de rendimiento aprovisionada en un sistema de archivos FSx Single-AZ de segunda generación para ONTAP	
Capacidad de rendimiento Multi-AZ-2 de ONTAP	MBps-Mes	La cantidad de capacidad de rendimiento aprovisionada en un sistema de archivos	

Tipo de cargo	Unidades	Descripción	
		FSx Multi-AZ de segunda generación para ONTAP	
IOPS de SSD ONTAP Single-AZ-2 aprovisionadas	IOPS por mes	La cantidad de IOPS de SSD aprovisionadas en un sistema de archivos Single-AZ de segunda generación para ONTAP FSx	
IOPS de SSD ONTAP Multi-AZ-2 aprovisionadas	IOPS por mes	La cantidad de IOPS de SSD aprovisionadas en un sistema de archivos Multi-AZ de segunda generación para ONTAP FSx	

All FSx for ONTAP filesystems

Tipo de cargo	Unidades	Descripción	
Almacenamiento agrupado de capacidad estándar de ONTAP	GB-mes	La cantidad de almacenamiento agrupado de capacidad utilizada FSx por el sistema de archivos ONTAP.	
Almacenamiento de copias de seguridad de ONTAP	GB-mes	La cantidad de capacidad de almacenamiento utilizada para las copias de seguridad	
SnapLock uso	GB-mes	La cantidad de capacidad de almacenamiento utilizada por SnapLock volumes	
Lea las solicitudes de almacenamiento agrupadas	Operaciones	Número de solicitudes de lectura realizadas al almacenamiento agrupado	

Tipo de cargo	Unidades	Descripción	
de capacidad estándar de ONTAP		de capacidad estándar de un sistema FSx de archivos ONTAP	
Escriba las solicitudes al almacenamiento agrupado de capacidad estándar de ONTAP	Operaciones	Número de solicitudes de escritura realizadas en el almacenamiento agrupado de capacidad estándar de un sistema FSx de archivos ONTAP	

Consulte el informe AWS de uso de FSx ONTAP

AWS proporciona un informe FSx de uso más detallado que el informe de facturación. El informe de uso proporciona datos de uso agregados por hora, día o mes, y enumera las operaciones por región y tipo de uso.

Para ver el informe AWS de uso

1. Inicie sesión en AWS Management Console y abra la Administración de facturación y costos de AWS consola en <https://console.aws.amazon.com/costmanagement/>.
2. En el panel de navegación, seleccione Explorador de costos.
3. En la sección Parámetros del informe, elija el rango de fechas y la granularidad del informe.
4. Deje la opción Agrupar por > dimensión configurada en Servicio.
5. En Filtros > Servicio, elija FSx
6. Elija el Tipo de uso. Consulte la tabla que sigue este procedimiento para ver una lista de los tipos de FSx uso de ONTAP.
7. Seleccione los filtros adicionales que desee para su informe.
8. Para descargar los detalles del informe a un archivo, selecciona Descargar como CSV.

En la siguiente tabla se enumeran los tipos de uso de ONTAP que puede utilizar FSx para filtrar el informe y ver los datos de uso de los sistemas de archivos de ONTAP. Para obtener más información

sobre el uso del Cost Explorer, [consulte Análisis de los costos y el uso AWS Cost Explorer](#) en la Guía del AWS Cost Management usuario.

First generation FSx for ONTAP file systems

Tipo de uso	Unidades	Descripción
<i>region</i> - Almacenamiento. SAZ_2N: SSD	GB-mes	La cantidad de almacenamiento SSD aprovisionada en un sistema de archivos Single-AZ de primera generación para ONTAP. FSx
<i>region</i> - Almacenamiento.MAZ: SSD	GB-mes	La cantidad de almacenamiento SSD aprovisionada en un sistema de archivos Multi-AZ de primera generación para ONTAP. FSx
<i>region</i> ThroughputCapacity - .SAZ_2N	MiBps-No	La cantidad de capacidad de rendimiento aprovisionada en un sistema de archivos Single-AZ FSx de primera generación para ONTAP.
<i>region</i> - .MAZ ThroughputCapacity	MiBps-No	La cantidad de capacidad de rendimiento aprovisionada en un sistema de archivos Multi-AZ FSx de primera generación para ONTAP.
<i>region</i> - SSDIOPS.SAZ_2N aprovisionados	iOPS-mo	La cantidad de IOPS de SSD aprovisionadas por encima de 3 IOPS por GiB de almacenamiento SSD en un sistema de archivos Single-AZ de primera generación para ONTAP. FSx
<i>region</i> - SSDIOPS.maz aprovisio nados	iOPS-MO	La cantidad de IOPS de SSD aprovisionadas por encima de 3

Tipo de uso	Unidades	Descripción
		IOPS por GiB de almacenamiento SSD en un sistema de archivos Multi-AZ de primera generación para ONTAP. FSx

Second generation FSx for ONTAP file systems

Tipo de uso	Unidades	Descripción
<i>region</i> - Storage.SAZ_2N2: SSD	GB-mes	La cantidad de almacenamiento SSD aprovisionada en un sistema de archivos Single-AZ de segunda generación para ONTAP. FSx
<i>region</i> -Almacenamiento. MAZ2-Almacenamiento. ----SEP----:SSD	GB-mes	La cantidad de almacenamiento SSD aprovisionada en un sistema de archivos Multi-AZ de segunda generación FSx para ONTAP.
<i>region</i> ThroughputCapacity - .SAZ_2N2	MiBps-No	La cantidad de capacidad de rendimiento aprovisionada en un sistema de archivos Single-AZ FSx de segunda generación para ONTAP.
<i>region</i> -ThroughputCapacity.MAZ2	MiBps-No	La cantidad de capacidad de rendimiento aprovisionada en un sistema de archivos Multi-AZ FSx de segunda generación para ONTAP.
<i>region</i> - SSDIOPS.SAZ_2N2 aprovisionados	iOPS-MO	La cantidad de IOPS de SSD aprovisionadas por encima de 3 IOPS por GiB de almacenamiento SSD en un sistema de archivos

Tipo de uso	Unidades	Descripción
		Single-AZ de segunda generación para ONTAP. FSx
<i>region</i> - SSD IOPS aprovisionadas. MAZ2	iOPS-MO	La cantidad de IOPS de SSD aprovisionadas por encima de 3 IOPS por GiB de almacenamiento SSD en un sistema de archivos Multi-AZ de segunda generación para ONTAP. FSx

All FSx for ONTAP file systems

Tipo de uso	Unidades	Descripción
<i>region</i> CPool-Storage.SAZ_2n: Estándar	GB-MO	La cantidad de almacenamiento agrupado de capacidad estándar utilizada en un sistema de archivos Single-AZ de primera o segunda generación FSx para ONTAP.
<i>region</i> -Storage.maz: Estándar CPool	GB-MO	La cantidad de almacenamiento agrupado de capacidad estándar utilizada en un sistema de archivos Multi-AZ de primera o segunda generación FSx para ONTAP.
<i>region</i> -BackupUsage	GB-mes	La cantidad de capacidad de almacenamiento utilizada para las copias de seguridad.
<i>region</i> -SnaplockUsage	GB-mes	La cantidad de capacidad de almacenamiento utilizada por SnapLock volúmenes.
	Operaciones	El número de solicitudes de lectura realizadas al almacenamiento

Tipo de uso	Unidades	Descripción
<i>region</i> -Solicitudes.saz_2n: CPool StdRd		agrupado de capacidad estándar en un sistema de archivos Single-AZ para ONTAP. FSx
<i>region</i> -Solicitudes.SAZ_2N: CPool StdWr	Operaciones	El número de solicitudes de escritura realizadas al almacenamiento agrupado de capacidad estándar en un sistema de archivos Single-AZ para ONTAP. FSx
<i>region</i> -Solicitudes.MAZ: CPool StdRd	Operaciones	El número de solicitudes de lectura realizadas al almacenamiento agrupado de capacidad estándar en un sistema de archivos FSx Multi-AZ para ONTAP.
<i>region</i> -Solicitudes.MAZ: CPool StdWr	Operaciones	El número de solicitudes de escritura realizadas al almacenamiento agrupado de capacidad estándar en un sistema de archivos FSx Multi-AZ para ONTAP.

Supervisión de Amazon FSx para NetApp ONTAP

Puedes usar los siguientes servicios y herramientas para monitorizar el uso y la actividad de NetApp ONTAP en Amazon FSx :

- **Amazon CloudWatch:** puede supervisar los sistemas de archivos con Amazon CloudWatch, que recopila y procesa automáticamente los datos sin procesar de ONTAP FSx 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 sistema de archivos FSx para ONTAP utilizando los 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 Información sobre la infraestructura de datos:** puede supervisar las métricas de configuración, capacidad y rendimiento de sus FSx sistemas de archivos de ONTAP mediante el servicio NetApp Data Infrastructure Insights. También puede crear alertas en función de las condiciones métricas.
- **NetApp Harvest y NetApp Grafana:** puede monitorear su FSx sistema de archivos ONTAP mediante Harvest NetApp y Grafana. NetApp NetApp Harvest supervisa los sistemas de archivos de ONTAP recopilando métricas de rendimiento, capacidad y hardware de los sistemas de archivos de FSx 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, un rol o un AWS servicio en Amazon FSx.

Temas

- [Monitorización con Amazon CloudWatch](#)
- [Supervisión FSx de eventos EMS de ONTAP](#)
- [Supervisión con Data Infrastructure Insights](#)
- [Supervisión de FSx los sistemas de archivos ONTAP mediante Harvest y Grafana](#)

- [Supervisión de FSx las llamadas a la API de 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 período de 15 meses para que pueda acceder a la información histórica y determinar el rendimiento de su sistema de archivos. FSx en el caso de ONTAP, los datos métricos se envían automáticamente CloudWatch en períodos de 1 minuto de forma predeterminada. Para obtener más información CloudWatch, consulta [¿Qué es Amazon CloudWatch?](#) en la Guía del CloudWatch usuario de Amazon.

Note

De forma predeterminada, FSx 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 FSx de ONTAP se organizan en cuatro categorías, definidas por 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 File-system-level rendimiento y capacidad de almacenamiento.
- Métricas del servidor de archivos: File-server-level métricas.
- Métricas detalladas de agregados del sistema de archivos:: métricas detalladas del sistema de archivos por agregado.
- Métricas detalladas del sistema de archivos: File-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 FSx de ONTAP se publican en el espacio de AWS/FSx nombres de. CloudWatch

Temas

- [Acceder a las CloudWatch métricas](#)
- [Monitorización en la FSx consola de Amazon](#)
- [Métricas del sistema de archivos](#)
- [Métricas del sistema de archivos de segunda generación](#)
- [Métricas de volumen](#)

Acceder a las CloudWatch métricas

Puedes ver CloudWatch las estadísticas de Amazon FSx de las siguientes maneras:

- La FSx consola Amazon
- 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 FSx consola de Amazon.

Para ver CloudWatch las métricas de tu sistema de archivos mediante la FSx consola de Amazon

1. Abre la FSx consola de Amazon en <https://console.aws.amazon.com/fsx/>.
2. En el panel de navegación izquierdo, elija Sistemas de archivos 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).

- Selecciona Resumen (la pestaña predeterminada) para ver 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 tu volumen con la FSx consola de Amazon.

Para ver CloudWatch las métricas de tu volumen mediante la FSx consola de Amazon

1. Abre la FSx consola de Amazon 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 desees 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 métricas del sistema FSx de archivos ONTAP a un panel de control de la CloudWatch consola de Amazon.

Para añadir métricas a una CloudWatch consola de Amazon

1. Elige el conjunto de métricas (resumen, almacenamiento o rendimiento) en el panel Supervisión y rendimiento de la FSx consola de Amazon.

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 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](#).

Monitorización en la FSx consola de Amazon

Las CloudWatch métricas publicadas por Amazon FSx proporcionan información valiosa sobre sus volúmenes y sistemas FSx de archivos de ONTAP.

Temas

- [Supervisión de las métricas del sistema de archivos en la FSx consola de Amazon](#)
- [Supervisión de las métricas de volumen en la FSx consola de Amazon](#)
- [Advertencias y recomendaciones de rendimiento](#)
- [Creación de CloudWatch alarmas de Amazon para monitorear Amazon FSx](#)

Supervisión de las métricas del sistema de archivos en la FSx consola de Amazon

Puedes usar el panel Supervisión y rendimiento del panel de control de tu sistema de archivos en la FSx consola de Amazon 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 disponible (bytes)	StorageCapacity {SSD} - StorageUsed {SSD}
	... determinar el rendimiento total de los clientes de mi sistema de archivos?	Rendimiento total del cliente (bytes/seg)	SUMA (DataReadBytes + DataWriteBytes) / PERÍODO (en segundos)
	... determinar el total de IOPS de los clientes de mi sistema de archivos?	IOPS totales del cliente (operaciones/segundo)	SUMA (DataReadOperations + DataWriteOperations + MetadataOperations) / PERÍODO (en segundos)
	... determinar la latencia media de las operaciones de lectura, escritura y metadatos de mi sistema de archivos?	Latencia promedio (ms/seg)	Latencia de lectura promedio: DataReadOperationTime

Monitoreo y rendimiento	¿Cómo...	Gráfico	Métricas relevantes
		operación)	$\ast 1000/\text{DataReadOperations}$ Latencia media de escritura: $\text{DataWriteOperationTime} \ast 1000/\text{DataWriteOperations}$ Latencia media de metadatos: $\text{MetadataOperationTime} \ast 1000/\text{MetadataOperations}$
	... determinar la distribución de la capacidad de almacenamiento utilizada y libre en mi sistema de archivos?	Distribución de almacenamiento	Nivel principal disponible: $\text{StorageCapacity} \{\text{SSD}\} - \text{StorageUsed} \{\text{SSD}\}$ Nivel principal utilizado: $\text{StorageUsed} \{\text{SSD}\}$ Pool de capacidad utilizado: $\text{StorageUsed} \{\text{StandardCapacityPool}\}$
	... determinar los ahorros derivados de la eficiencia del almacenamiento (compresión, deduplicación y compactación)?	Ahorros en eficiencia de almacenamiento	$\text{StorageEfficiencySavings}$

Monitoreo y rendimiento	¿Cómo...	Gráfico	Métricas relevantes
Almacenamiento	... determinar cuánto almacenamiento principal está disponible?	Capacidad de almacenamiento principal disponible (bytes)	StorageCapacity {SSD} - StorageUsed {SSD}
	... determinar el porcentaje de almacenamiento principal utilizado para mi sistema de archivos?	Utilización de la capacidad de almacenamiento principal (porcentaje)	StorageUsed {SSD} * 100/StorageCapacity {SSD}
Rendimiento del servidor de archivos	... determinar si mi sistema de archivos se acerca al límite de rendimiento de la red?	Rendimiento de la red: utilización (porcentaje)	NetworkThroughputUtilization
	... determinar si mi sistema de archivos se acerca al límite de rendimiento del disco?	Rendimiento del disco: utilización (porcentaje)	FileServerDiskThroughputUtilization

Monitoreo y rendimiento	¿Cómo...	Gráfico	Métricas relevantes
	... determinar si mi sistema de archivos ha agotado los créditos de ráfaga permitidos para el rendimiento del disco?	Rendimiento del disco: balance de ráfagas (porcentaje)	FileServerDiskThroughputBalance
	... determinar si mi sistema de archivos se acerca al límite de IOPS de SSD de sus servidores de archivos?	IOPS de disco: utilización (porcentaje)	FileServerDiskIopsUtilization
	... determinar si mi sistema de archivos ha agotado los créditos de ráfaga permitidos por sus servidores de archivos para las IOPS de las unidades SSD de disco?	IOPS de disco: balance de ráfaga (porcentaje)	FileServerDiskIopsBalance
	... determinar la utilización media de la CPU del sistema de archivos?	Utilización de la CPU (porcentaje)	CPUUtilization
	... determinar si mi carga de trabajo está haciendo un uso eficiente de la RAM y las cachés de NVMe lectura de mi sistema de archivos?	Porcentaje de aciertos de caché	FileServerCacheHitRatio

Monitoreo y rendimiento	¿Cómo...	Gráfico	Métricas relevantes
Desempeño de disco	... determinar si mi sistema de archivos se acerca a la capacidad de IOPS de SSD aprovisionada actualmente?	IOPS de disco: utilización (SSD) (porcentaje)	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).

Supervisión de las métricas de volumen en la FSx consola de Amazon

Puedes ver el panel de monitorización en el panel de control de tu volumen en la FSx consola de Amazon para ver métricas de rendimiento adicionales. Para obtener más información, consulte [Acceder a las CloudWatch métricas](#).

Monitoreo	¿Cómo...?	Gráfico	Métricas relevantes
	... determinar la capacidad de almacenamiento disponible de mi volumen?	Capacidad de almacenamiento	StorageCapacity

Monitoreo	¿Cómo...?	Gráfico	Métricas relevantes
		disponible	
	... 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 (operaciones/segundo)	SUMA (DataReadOperations + DataWriteOperations + MetadataOperations) / 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

Monitoreo	¿Cómo...?	Gráfico	Métricas relevantes
	... determinar la latencia media de las operaciones de lectura, escritura y metadatos de mi volumen?	Latencia promedio (ms/operación)	Latencia de lectura promedio: $\text{DataRead0OperationTime} * 1000 / \text{DataRead0Operations}$ Latencia media de escritura: $\text{DataWrite0OperationTime} * 1000 / \text{DataWriteOperations}$ Latencia media de metadatos: $\text{Metadata0OperationTime} * 1000 / \text{Metadata0Operations}$
	... determinar la cantidad de archivos o inodos que están disponibles en mi volumen?	Archivos disponibles (inodos)	$\text{FilesCapacity} - \text{FilesUsed}$
	... determinar la distribución de la capacidad de almacenamiento usada y libre en mi volumen?	Distribución de almacenamiento	$\text{StorageCapacity} - \text{StorageUsed}$

Advertencias y recomendaciones de rendimiento

FSx en el caso de ONTAP, muestra una advertencia sobre 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 FSx rendimiento de Amazon activas o

recientes y cualquier CloudWatch alarma configurada para el sistema de archivos que esté 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.

Puedes crear CloudWatch alarmas para cualquiera de las FSx métricas de Amazon. Para obtener más información, consulte [Creación de CloudWatch alarmas de Amazon para monitorear 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 del 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 del sistema de archivos si este aún no tiene la capacidad máxima de almacenamiento en SSD. Para obtener más información, consulte Actualización de la capacidad de almacenamiento y las IOPS aprovisionadas. Si el sistema de archivos tiene varios pares de HA y la utilización de la capacidad de almacenamiento principal solo es mayor para un subconjunto de 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 utilización de la capacidad de almacenamiento principal se distribuya de manera más uniforme en todo el sistema de archivos. Para obtener más información sobre reequilibrar cargas de trabajo,

Sección del panel	Si hay una advertencia para esta métrica	Haga lo siguiente
		consulte Equilibrar las cargas de trabajo entre pares de alta disponibilidad .
Rendimiento del servidor de archivos	Network throughput	Aumente la capacidad de rendimiento del sistema de archivos si este aún no tiene la capacidad máxima de rendimiento. Para obtener más información sobre la actualización de la capacidad de rendimiento, consulte Actualización de la capacidad de rendimiento .
	Rendimiento del disco	
	IOPS de disco	
	Utilización de la CPU	Si el sistema de archivos tiene varios pares de HA y la utilización es alta solo para un subconjunto de servidores de archivos, también puede reequilibrar la carga de trabajo para que sea más uniforme usando las capacidades de rendimiento de cada uno de los pares de HA del sistema de archivos. Para obtener más información sobre reequilibrar cargas de trabajo, consulte Equilibrar las cargas de trabajo entre pares de alta disponibilidad .

Sección del panel	Si hay una advertencia para esta métrica	Haga lo siguiente
Desempeño de disco	IOPS de disco	Aumente las IOPS de SSD si el sistema de archivos aún no tiene las IOPS de SSD máximas de la capacidad de rendimiento actual del sistema de archivos. Para obtener más información sobre la actualización de las IOPS aprovisionadas del sistema de archivos, consulte Actualización de la capacidad de almacenamiento y las IOPS aprovisionadas. Si el sistema de archivos tiene varios pares de HA y la utilización IOPS del disco es superior al subconjunto de 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 utilización de IOPS del disco se distribuya de manera más uniforme en todo el sistema de archivos. Para obtener más información sobre reequilibrar cargas de trabajo, consulte Equilibrar las cargas de trabajo entre pares de alta disponibilidad.

Para obtener más información sobre el rendimiento del sistema de archivos, consulte [Amazon FSx para el rendimiento de NetApp ONTAP](#).

Creación de CloudWatch alarmas de Amazon para monitorear 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 periodos 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 periodos. Puedes crear una alarma desde la FSx consola de Amazon o desde la CloudWatch consola de Amazon.

Los siguientes procedimientos describen cómo crear alarmas mediante la FSx consola, AWS Command Line Interface (AWS CLI) y la API de Amazon.

Para configurar alarmas con la FSx consola de Amazon

1. Abre la FSx consola de Amazon en <https://console.aws.amazon.com/fsx/>.
2. En el panel de navegación izquierdo, elija Sistemas de archivos 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. Selecciona 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 Métricas, selecciona 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. Elija Crear alarma para iniciar el Asistente de creación de alarmas.
3. Sigue el procedimiento descrito en Para configurar alarmas con la FSx consola de Amazon, empezando por el paso 6.

Para configurar una alarma mediante el AWS CLI

- Llame al comando [put-metric-alarm](#) CLI. 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](#).

Métricas del sistema de archivos

Las métricas del sistema de archivos de Amazon FSx for 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`.

Ten en cuenta lo siguiente sobre cuándo Amazon FSx publica puntos de datos para estas métricas CloudWatch:

- Para las métricas de utilización (cualquier métrica cuyo nombre termine en `Utilización`, por ejemplo `NetworkThroughputUtilization`), se emite un punto de datos en cada periodo 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 agregado de `FileServerDiskIopsUtilization` `DiskIopsUtilization`.
- Para todas las demás métricas, se emite un único punto de datos en cada periodo, que corresponde al valor total de la métrica en todos los servidores de archivos activos (como `DataReadBytes`, en el caso de las métricas de servidores de archivos) o en todos los agregados (como `DiskReadBytes`, en el caso de las métricas de almacenamiento).

Temas

- [Métricas de E/S de red](#)
- [Métricas del servidor de archivos](#)
- [Métricas de E/S de disco](#)
- [Métricas de capacidad de almacenamiento](#)
- [Métricas detalladas del sistema de archivos](#)

Métricas de E/S de red

Todas estas métricas tienen una dimensión, `FileSystemId`.

Métrica	Descripción
<code>NetworkThroughputUtilization</code>	Porcentaje de utilización del rendimiento de la red del sistema de archivos. La estadística <code>Average</code> es la utilización media del rendimiento de red del sistema de archivos durante un período específico. La estadística <code>Minimum</code> es la utilización más baja del rendimiento de red del sistema de archivos durante un período específico. La estadística <code>Maximum</code> es la utilización máxima del rendimiento de red del sistema de archivos durante un período específico. Unidad: porcentaje Estadísticas válidas: <code>Average</code>, <code>Minimum</code> y <code>Maximum</code>.
<code>NetworkSentBytes</code>	El número de bytes (E/S de red) enviados por el sistema de archivos. La estadística <code>Sum</code> 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: <code>Sum</code>

Métrica	Descripción
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
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

Métrica	Descripción
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
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

Métrica	Descripción
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
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

Métrica	Descripción
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
DataWriteOperationTime	La suma del tiempo total empleado en el sistema de archivos para realizar las operaciones 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

Métrica	Descripción
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 específico. 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 solicitudes 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 <code>Minimum</code> es la utilización más baja de la CPU del sistema de archivos durante un período específico. La estadística <code>Maximum</code> es la utilización máxima de la CPU del sistema de archivos durante un período específico. Unidad: porcentaje Estadísticas válidas: <code>Average</code>, <code>Minimum</code> y <code>Maximum</code>.
<code>FileServerDiskThroughputUtilization</code>	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 <code>Average</code> es el porcentaje medio de utilización del rendimiento del disco de los servidores de archivos durante un período específico. La estadística <code>Minimum</code> es el porcentaje más bajo de utilización del rendimiento del disco de los servidores de archivos durante un período específico. La estadística <code>Maximum</code> es la utilización máxima del rendimiento del disco de los servidores de archivos durante un período específico. Unidad: porcentaje Estadísticas válidas: <code>Average</code>, <code>Minimum</code> y <code>Maximum</code>.

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 aprovisionan con una capacidad de rendimiento inferior a 512. MBps La estadística <code>Average</code> es el balance medio de ráfagas disponible durante un período específico. La estadística <code>Minimum</code> es el saldo de ráfagas mínimo disponible durante un período específico. La estadística <code>Maximum</code> es el saldo máximo de ráfagas disponible durante un período específico. Unidad: porcentaje Estadísticas válidas: <code>Average</code>, <code>Minimum</code> y <code>Maximum</code>.

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 inferior a 512 MBps. 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. Unidad: 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. Unidad: porcentaje Estadísticas válidas: Average, Minimum y Maximum.

Métrica	Descripción
FileServerCacheHitRatio	El porcentaje de todas las solicitudes de lectura que se atienden mediante datos de la RAM y NVMe las cachés del sistema de archivos. Un porcentaje más alto significa que las cachés de lectura del sistema de archivos atienden más lecturas. Unidad: 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 <code>Average</code> es la utilización media de las IOPS de disco del sistema de archivos durante un período específico. La estadística <code>Minimum</code> es la utilización mínima de IOPS de disco del sistema de archivos durante un período específico. La estadística <code>Maximum</code> es la utilización máxima de IOPS de disco del sistema de archivos durante un período específico. Unidad: porcentaje Estadísticas válidas: <code>Average</code>, <code>Minimum</code> y <code>Maximum</code>.
DiskReadOperations	El número de operaciones de lectura (E/S de disco) desde el nivel principal del sistema de archivos. La estadística <code>Sum</code> es el número total de operaciones de lectura del nivel principal durante un período específico. Unidades: recuento Estadísticas válidas: <code>Sum</code>

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 <code>StorageEfficiencySavings</code> entre la suma de <code>StorageEfficiencySavings</code> y la métrica del sistema de archivos <code>StorageUsed</code>, utilizando la estadística de Sum para <code>StorageUsed</code>.

Métrica	Descripción
	La estadística <code>Minimum</code> es el ahorro mínimo en eficiencia de almacenamiento durante un período específico. La estadística <code>Maximum</code> es el ahorro máximo en eficiencia de almacenamiento durante un período específico. Unidades: bytes Estadísticas válidas: <code>Average</code>, <code>Minimum</code> y <code>Maximum</code>
<code>StorageUsed</code>	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: <code>Average</code>, <code>Minimum</code> y <code>Maximum</code>

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 eficiencia de almacenamiento logrados mediante la compresión, la compactación y la deduplicación. 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
<code>StorageCapacityUtilization</code>	La utilización 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 estadística <code>Average</code> es la cantidad promedio de utilización de la capacidad de almacenamiento del nivel de rendimiento del sistema de archivos en cuestión durante un periodo específico. La estadística <code>Minimum</code> es la cantidad más baja de utilización de la capacidad de almacenamiento del nivel de rendimiento del sistema de archivos en cuestión durante un periodo específico. La estadística <code>Maximum</code> es la cantidad más alta de utilización de la capacidad de almacenamiento del nivel de rendimiento del sistema de archivos en cuestión durante un periodo específico.

Métrica	Descripción
	Unidad: porcentaje 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 eficiencia del almacenamiento, como la compresión y la deduplicación de datos. Los valores de dimensión válidos para <code>StorageTier</code> son <code>SSD</code> y <code>StandardCapacityPool</code>, correspondientes al nivel de almacenamiento que mide esta métrica. Esta métrica también requiere la dimensión <code>DataType</code> con el valor <code>All</code>. Las estadísticas <code>Average</code>, <code>Minimum</code> y <code>Maximum</code> 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 almacenamiento principal (<code>SSD</code>), divida cualquiera de estas estadísticas entre <code>Maximum StorageCapacity</code> al mismo período, con la dimensión <code>StorageTier</code> igual a <code>SSD</code>. Para calcular la capacidad de almacenamiento libre de su nivel de almacenamiento principal (<code>SSD</code>) en bytes, reste cualquiera de estas estadísticas del <code>Maximum StorageCapacity</code> durante el mismo período y obtenga la dimensión <code>StorageTier</code> igual a <code>SSD</code>. Unidades: bytes Estadísticas válidas: <code>Average</code>, <code>Minimum</code> y <code>Maximum</code>

Métricas del sistema de archivos de segunda generación

Se proporcionan las siguientes métricas FSx para los sistemas de archivos de segunda generación de ONTAP. Para las métricas, se emite un punto de datos para cada par de HA y para cada agregado (para las métricas de utilización del almacenamiento).

Note

Si tiene un sistema de archivos con varios pares de HA, también puede usar las [métricas del sistema de archivos de un solo par de HA](#) y las [métricas de volumen](#).

Temas

- [Métricas de E/S de red](#)
- [Métricas del servidor de archivos](#)
- [Métricas de E/S de disco](#)
- [Métricas detalladas del sistema de archivos](#)

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 preferidos (es decir, prestan servicio al tráfico a menos que el sistema de archivos se haya transferido al servidor de archivos secundario), mientras que los servidores de archivos con números pares son secundarios (es decir, solo prestan servicio al tráfico cuando el socio no está disponible). Por este motivo, los servidores de archivos secundarios tienen menos utilización que los servidores de archivos preferidos.

Métrica	Descripción
<code>NetworkThroughputUtilization</code>	Utilización del rendimiento de la red como porcentaje del rendimiento de la red disponible para el sistema de archivos. Esta métrica

Métrica	Descripción
	equivale al máximo de <code>NetworkSentBytes</code> y <code>NetworkReceivedBytes</code> como porcentaje de la capacidad de rendimiento de la red de un par de HA del sistema de archivos. En esta métrica se tiene en cuenta todo el tráfico, incluidas las tareas en segundo plano (como <code>SnapMirror</code> la organización por 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 estadística <code>Average</code> es la utilización promedio del rendimiento de la red para el servidor de archivos determinado durante un periodo específico. La estadística <code>Minimum</code> es la utilización más baja del rendimiento de la red para el servidor de archivos determinado por un minuto, durante un periodo específico. La estadística <code>Maximum</code> es la utilización más alta del rendimiento de la red para el servidor de archivos determinado por un minuto, durante un periodo específico. Unidad: porcentaje Estadísticas válidas: <code>Average</code>, <code>Minimum</code> y <code>Maximum</code>.

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

Métrica	Descripción
	Estadísticas válidas: Sum, Average, Minimum y Maximum

Métrica	Descripción
NetworkReceivedBytes	La cantidad de bytes (E/S de red) recibidos por el sistema de archivos. En esta métrica se tiene en cuenta todo el tráfico, incluidas las tareas en segundo plano (como SnapMirror la organización por 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 estadística Sum es la cantidad total de bytes recibidos a través de la red por el servidor de archivos en cuestión durante un periodo específico. La estadística Average es la cantidad promedio de bytes recibidos a través de la red por el servidor de archivos en cuestión por minuto durante un periodo específico. La estadística Minimum es la cantidad más baja de bytes recibidos a través de la red por el servidor de archivos en cuestión por minuto durante un periodo específico. La estadística Maximum es la cantidad más alta de bytes recibidos a través de la red por el servidor de archivos en cuestión por minuto durante un periodo específico. Para calcular el rendimiento recibido (bytes por segundo) de cualquier estadística, divídala por los segundos del periodo. Unidades: bytes

Métrica	Descripción
	Estadísticas válidas: Sum, Average, Minimum y Maximum

Métricas del servidor de archivos

Todas estas métricas tienen dos dimensiones, `FileSystemId` y `FileServer`.

Métrica	Descripción
<code>CPUUtilization</code>	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 del sistema de archivos. La estadística <code>Average</code> es el uso medio de la CPU del sistema de archivos durante un período específico. La estadística <code>Minimum</code> es la utilización más baja de la CPU del servidor de archivos en cuestión durante un periodo específico. La estadística <code>Maximum</code> es la utilización más alta de la CPU del servidor de archivos en cuestión durante un periodo específico. Unidad: porcentaje Estadísticas válidas: <code>Average</code>, <code>Minimum</code> y <code>Maximum</code>.
<code>FileServerDiskThroughputUtilization</code>	El rendimiento del disco entre el servidor de archivos y el agregado, expresado en el porcentaje del límite aprovisionado que lo determina la capacidad de rendimiento. En esta métrica se tiene en cuenta todo el tráfico,

Métrica	Descripción
	incluidas las tareas en segundo plano (como SnapMirror la organización por niveles y las copias de seguridad). Esta métrica equivale a la suma de <code>DiskReadBytes</code> y <code>DiskWrite Bytes</code> como porcentaje de la capacidad de rendimiento del disco del servidor de archivos de un par de HA del sistema de archivos. Se emite una métrica por minuto para cada uno de los servidores de archivos del sistema de archivos. La estadística <code>Average</code> es la utilización promedio del rendimiento del disco para el servidor de archivos determinado durante un periodo específico. La estadística <code>Minimum</code> es la utilización más baja del rendimiento del disco para el servidor de archivos determinado durante un periodo específico. La estadística <code>Maximum</code> es la utilización más alta del rendimiento del disco para el servidor de archivos determinado durante un periodo específico. Unidad: porcentaje Estadísticas válidas: <code>Average</code>, <code>Minimum</code> y <code>Maximum</code>.

Métrica	Descripción
FileServerDiskIopsUtilization	La utilización de IOPS de la capacidad disponible de IOPS del disco para el servidor de archivos, expresada como porcentaje del límite de IOPS del disco. La diferencia con <code>DiskIopsUtilization</code> radica en que las IOPS del disco se usan por encima del máximo que puede gestionar el servidor de archivos, a diferencia de las IOPS de disco aprovisionadas. En esta métrica se tiene en cuenta todo el tráfico, incluidas las tareas en segundo plano (como SnapMirror la organización por 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 estadística <code>Average</code> es la utilización promedio de IOPS del disco para el servidor de archivos en cuestión durante un periodo específico. La estadística <code>Minimum</code> es la utilización más baja de IOPS del disco para el servidor de archivos en cuestión durante un periodo específico. La estadística <code>Maximum</code> es la utilización más alta de IOPS del disco para el servidor de archivos en cuestión durante un periodo específico. Unidad: porcentaje Estadísticas válidas: <code>Average</code>, <code>Minimum</code> y <code>Maximum</code>.

Métrica	Descripción
FileServerCacheHitRatio	El porcentaje de todas las solicitudes de lectura atendidas por datos que residen en la RAM o las NVMe cachés 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 disponibilidad). 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 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. Unidad: porcentaje La estadística <i>Average</i> es la proporción promedio de aciertos de caché de uno de los pares de HA del sistema de archivos durante el periodo especificado. La estadística <i>Minimum</i> es la proporción más baja de aciertos de caché de uno de los pares de HA del sistema de archivos durante el periodo especificado. La estadística <i>Maximum</i> es la proporción más alta de aciertos de caché de uno de los pares de HA del sistema de archivos durante el periodo especificado. Estadísticas válidas: <i>Average</i>, <i>Minimum</i> y <i>Maximum</i>

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 del sistema de archivos se compone de varios grupos de almacenamiento denominados agregados. Hay un agregado para cada par de HA. Por ejemplo, el agregado `aggr1` se asigna al servidor de archivos `FsxD01234567890abcdef-01` (el servidor de archivos activo) y al servidor de archivos `FsxD01234567890abcdef-02` (el servidor de archivos secundario) en un par de HA.

Métrica	Descripción
<code>DiskReadBytes</code>	La cantidad de bytes (E/S del disco) de cualquier disco que se lee en este agregado. En esta métrica se tiene en cuenta todo el tráfico, incluidas las tareas en segundo plano (como SnapMirror la organización por niveles y las copias de seguridad). Se emite una métrica por minuto para cada uno de los agregados del sistema de archivos. La estadística <code>Sum</code> es la cantidad total de bytes leídos en un minuto desde el agregado en cuestión durante un periodo específico. La estadística <code>Average</code> es la cantidad promedio de bytes leídos en un minuto desde el agregado en cuestión durante un periodo específico. La estadística <code>Minimum</code> es la cantidad más baja de bytes leídos en un minuto desde el agregado en cuestión durante un periodo específico. La estadística <code>Maximum</code> es la cantidad más alta de bytes leídos en un minuto desde el

Métrica	Descripción
	agregado en cuestión durante un periodo específico. Para calcular el rendimiento de lectura en disco (bytes por segundo) de cualquier estadística, divídala por los segundos del periodo. Unidades: bytes Estadísticas válidas: Sum, Average, Minimum y Maximum

Métrica	Descripción
DiskWriteBytes	La cantidad de bytes (E/S del disco) de cualquier disco que se escribe en este agregado. En esta métrica se tiene en cuenta todo el tráfico, incluidas las tareas en segundo plano (como SnapMirror la organización por niveles y las copias de seguridad). Se emite una métrica por minuto para cada uno de los agregados del sistema de archivos. La estadística Sum es la cantidad total de bytes escritos en el agregado en cuestión durante un periodo específico. La estadística Average es la cantidad promedio de bytes escritos en el agregado en cuestión durante un periodo específico. La estadística Minimum es la cantidad más baja de bytes escritos en el agregado en cuestión durante un periodo específico. La estadística Maximum es la cantidad más alta de bytes escritos en el agregado en cuestión durante un periodo específico. 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	La utilización de IOPS del disco de un agregado, expresado como porcentaje del límite de IOPS del disco del agregado (es decir, el total de IOPS del sistema de archivos dividido por el número de pares de HA del sistema de archivos). Esto se diferencia de <code>FileServerDiskIopsUtilization</code> en que se trata de la utilización de las IOPS del disco aprovisionadas en relación con el límite de IOPS aprovisionadas, a diferencia de las IOPS del 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 por niveles y las copias de seguridad). Se emite una métrica por minuto para cada uno de los agregados del sistema de archivos. La estadística <code>Average</code> es la utilización promedio de IOPS del disco del agregado en cuestión durante un periodo específico. La estadística <code>Minimum</code> es la utilización más baja de IOPS del disco del agregado en cuestión durante un periodo específico. La estadística <code>Maximum</code> es la utilización más alta de IOPS del disco del agregado en cuestión durante un periodo específico. Unidad: porcentaje Estadísticas válidas: <code>Average</code>, <code>Minimum</code> y <code>Maximum</code>.

Métrica	Descripción
DiskReadOperations	La cantidad de operaciones de lectura (E/S del disco) de este agregado. En esta métrica se tiene en cuenta todo el tráfico, incluidas las tareas en segundo plano (como SnapMirror y la organización por niveles y las copias de seguridad). Se emite una métrica por minuto para cada uno de los agregados del sistema de archivos. La estadística Sum es la cantidad total de operaciones de lectura realizadas por el agregado en cuestión durante un periodo específico. La estadística Average es la cantidad promedio de operaciones de lectura realizadas por minuto por el agregado en cuestión durante un periodo específico. La estadística Minimum es la cantidad más baja de operaciones de lectura realizadas por minuto por el agregado en cuestión durante un periodo específico. La estadística Maximum es la cantidad más alta de operaciones de lectura realizadas por minuto por el agregado en cuestión durante un periodo específico. Para calcular las IOPS promedio del disco durante el periodo, use la estadística Average y divida el resultado por 60 (segundos). Unidades: recuento

Métrica	Descripción
	Estadísticas válidas: Sum, Average, Minimum y Maximum
DiskWriteOperations	La cantidad de operaciones de lectura (E/S del disco) de este agregado. En esta métrica se tiene en cuenta todo el tráfico, incluidas las tareas en segundo plano (como SnapMirror y la organización por niveles y las copias de seguridad). Se emite una métrica por minuto para cada uno de los agregados del sistema de archivos. La estadística Sum es la cantidad total de operaciones de escritura realizadas por el agregado en cuestión durante un periodo específico. La estadística Average es la cantidad promedio de operaciones de escritura realizadas por minuto por el agregado en cuestión durante un periodo específico. Para calcular las IOPS promedio del disco durante el periodo, use la estadística Average y divida el resultado por 60 (segundos). Unidades: recuento Estadísticas válidas: Sum y 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 las dimensiones FileSystemId, StorageTier y DataType o las dimensiones FileSystemId, StorageTier, DataType y Aggregate.

- Si no se proporciona la dimensión Aggregate, las métricas son para todo el sistema de archivos. Las métricas `StorageUsed` y `StorageCapacity` 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 de SSD). Mientras tanto, la métrica `StorageCapacityUtilization` emite una métrica por minuto para cada agregado.
- Cuando se proporciona la dimensión Aggregate, 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 del sistema de archivos se compone de varios grupos de almacenamiento denominados agregados. Hay un agregado para cada par de HA. Por ejemplo, el agregado `aggr1` se asigna al servidor de archivos `FsxD01234567890abcdef-01` (el servidor de archivos activo) y al servidor de archivos `FsxD01234567890abcdef-02` (el servidor de archivos secundario) en un par de HA.
- `StorageTier`: indica el nivel de almacenamiento que mide la métrica, con posibles valores de `SSD` y `StandardCapacityPool`.
- `DataType`: indica el tipo de datos que mide la métrica, con el posible valor `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
<code>StorageCapacityUtilization</code>	La utilización de la capacidad de almacenamiento del agregado de un sistema de archivos determinado. Se emite una métrica por minuto para cada uno de los agregados del sistema de archivos. La estadística <code>Average</code> es la cantidad promedio de utilización de la capacidad de almacenamiento del agregado en cuestión durante el periodo específico.

Métrica	Descripción
	La estadística <code>Minimum</code> es la cantidad mínima de utilización de la capacidad de almacenamiento del agregado en cuestión durante el periodo específico. La estadística <code>Maximum</code> es la cantidad máxima de utilización de la capacidad de almacenamiento del agregado en cuestión durante el periodo específico. Unidad: porcentaje Estadísticas válidas: <code>Average</code>, <code>Minimum</code> y <code>Maximum</code>.

Métrica	Descripción
StorageCapacity	La capacidad de almacenamiento del agregado de un sistema de archivos determinado. Se emite una métrica por minuto para cada uno de los agregados del sistema de archivos. La estadística <code>Average</code> es la cantidad promedio de la capacidad de almacenamiento del agregado en cuestión durante el periodo específico. La estadística <code>Minimum</code> es la cantidad mínima de la capacidad de almacenamiento del agregado en cuestión durante el periodo específico. La estadística <code>Maximum</code> es la cantidad máxima de la capacidad de almacenamiento del agregado en cuestión durante el periodo específico. Unidades: bytes Estadísticas válidas: <code>Average</code>, <code>Minimum</code> y <code>Maximum</code>

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 eficiencia del almacenamiento, como la compresión y la deduplicación de datos. Los valores de dimensión válidos para <code>StorageTier</code> son <code>SSD</code> y <code>StandardCapacityPool</code>, correspondientes 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 estadística <code>Average</code> es la cantidad promedio de la capacidad de almacenamiento física consumida en el nivel de almacenamiento por el agregado en cuestión durante el periodo específico. La estadística <code>Minimum</code> es la cantidad mínima de la capacidad de almacenamiento física consumida en el nivel de almacenamiento por el agregado en cuestión durante el periodo específico. La estadística <code>Maximum</code> es la cantidad máxima de la capacidad de almacenamiento física consumida en el nivel de almacenamiento por el agregado en cuestión durante el periodo específico. Unidades: bytes Estadísticas válidas: <code>Average</code>, <code>Minimum</code> y <code>Maximum</code>

Métricas de volumen

Su sistema de archivos Amazon FSx for NetApp ONTAP puede tener uno o más volúmenes que almacenen sus datos. Cada uno de estos volúmenes tiene un conjunto de CloudWatch métricas, clasificadas 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](#)
- [Métricas de capacidad de almacenamiento](#)
- [Métricas de volumen detalladas](#)

Métricas de E/S de red

Todas estas métricas tienen dos dimensiones, `FileSystemId` y `VolumeId`.

Métrica	Descripción
<code>DataReadBytes</code>	El número de bytes (E/S de red) leídos del volumen por los clientes. La estadística <code>Sum</code> 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 <code>Sum</code> 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
StorageCapacityUtilization	Unidades: bytes
	Estadísticas válidas: Average
	La utilización de la capacidad de almacenamiento del volumen.
	Unidad: porcentaje
FilesUsed	Estadísticas válidas: Average
	Los archivos utilizados (número de archivos o inodos) en el volumen.
	Unidades: recuento
	Estadísticas válidas: Average
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
<code>StorageUsed</code>	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 <code>StorageTier</code> en <code>SSD</code> o <code>StandardCapacityPool</code> y se establece <code>DataType</code> en <code>All</code>, esta métrica mide el uso del espacio lógico de este volumen para los niveles de <code>SSD</code> y de pool de capacidad, respectivamente. Cuando se establece la dimensión <code>DataType</code> en <code>User</code>, <code>Snapshot</code> o <code>Other</code> y se establece <code>StorageTier</code> en <code>All</code>, esta métrica mide el uso del espacio lógico para cada tipo de datos respectivo. El consumo de datos <code>Snapshot</code> incluye la reserva de instantáneas, que es el 5% del tamaño del volumen de forma predeterminada. Unidades: bytes Estadísticas válidas: <code>Average</code>, <code>Minimum</code> y <code>Maximum</code>
<code>StorageCapacityUtilization</code>	El porcentaje del espacio en disco físico utilizado por el volumen. Unidad: porcentaje Estadísticas válidas: <code>Maximum</code>

Supervisión FSx de eventos EMS de ONTAP

Puede supervisar los eventos del sistema FSx de archivos de ONTAP mediante el sistema de gestión de eventos (EMS) nativo de ONTAP de NetApp. 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 del EMS a un servidor Syslog](#)

Información general sobre los eventos del EMS

Los eventos de EMS son notificaciones generadas automáticamente que le avisan cuando se produce una condición predefinida en el sistema de archivos FSx de 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 FlexGroup se aproxime a su capacidad máxima, la conexión o desconexión manual de un número de unidad lógica (LUN) o el cambio de tamaño 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 FSx para los sistemas de archivos de ONTAP. Para ver una lista de los mensajes EMS de ONTAP disponibles, utilice el comando [show del catálogo de eventos](#) de NetApp ONTAP CLI.

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 [waf1.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 comando NetApp ONTAP CLI [event log show](#) 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
<code>-detail</code>	Muestra información adicional sobre el evento.
<code>-detailtime</code>	Muestra la información detallada de eventos en orden cronológico inverso.
<code>-instance</code>	Muestra información detallada sobre todos los campos.

Opciones de eventos	Descripción
<code>-node <i>nodename</i> local</code>	Muestra una lista de eventos del nodo que especifique. Utilice esta opción con <code>-seqnum</code> para mostrar información detallada.
<code>-seqnum <i>sequence_number</i></code>	Selecciona los eventos de la secuencia que coinciden con este número. Utilice esta opción con <code>-node</code> para mostrar información detallada.

Opciones de eventos	Descripción
<code>-time</code> <i>MM/DD/YYYY HH:MM:SS</i>	Selecciona los eventos que ocurrieron en este momento específico. Utilice el formato: MM/DD/YYYY HH:MM:SS [+HH:MM]. Puede especificar un intervalo de tiempo mediante el operador <code>..</code> entre dos marcas de tiempo. <pre>event log show - time "04/17/2023 05:55:00".. "04/17/ 2023 06:10:00"</pre> 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: <pre>event log show -time >1m</pre> Los campos de mes y fecha de esta opción no están rellenos con ceros. Estos campos pueden ser de un solo dígito; por ejemplo, 4/1/2023 06:45:00.

Opciones de eventos	Descripción
<code>-severity <i>sev_level</i></code>	Selecciona los eventos que coinciden con el <i>sev_level</i> valor, 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: <pre>event log show -severity <=DEBUG</pre>

Opciones de eventos	Descripción
<code>-ems-severity</code> <i>ems_sev_level</i>	Selecciona los eventos que coinciden con el <i>ems_sev_level</i> valor, que debe ser uno de los siguientes: • <code>NODE_FAULT</code> : se detecta un daño en los datos o el nodo no puede proporcionar el servicio de atención al cliente. • <code>SVC_FAULT</code> : se detecta una pérdida temporal de servicio (normalmente un error de software transitorio). • <code>NODE_ERROR</code> : se detecta un error de hardware que no es inmediatamente fatal. • <code>SVC_ERROR</code> : se detecta un error de software que no es inmediatamente fatal. • <code>WARNING</code>: un mensaje de alta prioridad que no indica ningún error. • <code>NOTICE</code>: un mensaje de prioridad normal que no indica ningún error. • <code>INFO</code>: un mensaje de baja prioridad que no indica ningún error. • <code>DEBUG</code>: 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: <pre>event log show -ems-severity <=DEBUG</pre>
<code>-source <i>text</i></code>	Selecciona los eventos que coinciden con el <i>text</i> valor. La fuente suele ser un módulo de software.
<code>-message-name <i>message_name</i></code>	Selecciona los eventos que coinciden con el <i>message_name</i> valor. Los nombres de los mensajes son descriptivos, por lo que filtrar la salida por nombre de mensaje muestra mensajes de un tipo específico.
<code>-event <i>text</i></code>	Selecciona los eventos que coinciden con el <i>text</i> valor. El campo event contiene el texto completo del evento, incluidos los parámetros.

Opciones de eventos	Descripción
<code>-kernel-generation-num</code> <i>integer</i>	Selecciona los eventos que coinciden con el <i>integer</i> valor. Solo los eventos que provienen del núcleo tienen números de generación del núcleo.
<code>-kernel-sequence-num</code> <i>integer</i>	Selecciona los eventos que coinciden con el <i>integer</i> valor. Solo los eventos que provienen del núcleo tienen números de generación del núcleo.
<code>-action</code> <i>text</i>	Selecciona los eventos que coinciden con el <i>text</i> valor. El campo <code>action</code> describe qué medidas correctivas, si las hay, debe tomar para corregir la situación.
<code>-description</code> <i>text</i>	Selecciona los eventos que coinciden con el <i>text</i> valor. El campo <code>description</code> describe por qué ocurrió el evento y qué significa.
<code>-filter-name</code> <i>filter_name</i>	Selecciona los eventos que coinciden con el <i>filter_name</i> valor. Solo se muestran los eventos incluidos en los filtros existentes que coinciden con este valor.

Opciones de eventos	Descripción
<code>-fields <i>fieldname</i> ,...</code>	Indica que el resultado del comando también incluye el campo o los campos especificados. Puede utilizar <code>-fields ?</code> para elegir los campos que desee especificar.

Cómo 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 NetApp ONTAP CLI](#) sección de la Guía del usuario de Amazon FSx for 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 NetApp centro de documentación de ONTAP.

Reenvío de eventos del EMS a un servidor Syslog

Puede configurar los eventos del EMS para reenviar notificaciones a un servidor Syslog. El reenvío de eventos del 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 no contiene aún un servidor Syslog para notificaciones de eventos, primero debe crear uno. El DNS debe estar configurado en el sistema de archivos para resolver el nombre del servidor Syslog.

Note

El destino de Syslog debe ubicarse en la subred principal que usa el sistema de archivos.

Cómo configurar eventos del EMS para reenviar notificaciones a un servidor de 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 NetApp ONTAP CLI](#) sección de la Guía del usuario de Amazon FSx for NetApp ONTAP.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. Use el comando [event notification destination create](#) para crear un destino de notificación de eventos de tipo syslog y especifique 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 una longitud de 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 de Syslog o la dirección IP a la que se envían los mensajes de Syslog.
 - **transport_protocol**: el protocolo que se usa para enviar los eventos.
 - udp-unencrypted: protocolo de datagramas de usuario sin seguridad. Es el protocolo TCP predeterminado.
 - tcp-unencrypted: protocolo de control de transmisión sin seguridad.
 - tcp-encrypted: protocolo de control de transmisión con seguridad de la capa de transporte (TLS). Si se especifica esta opción, FSx ya que ONTAP verifica la identidad del host de destino validando su certificado.
 - **port_number**: el puerto del servidor de Syslog al que se envían los mensajes de Syslog. El parámetro syslog-port de valor predeterminado depende de la configuración del parámetro syslog-transport. Si syslog-transport se establece en tcp-encrypted, el valor predeterminado syslog-port es 6514. Si syslog-transport se establece en tcp-unencrypted, syslog-port tiene el valor predeterminado 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. Use el comando [event notification create](#) para crear una nueva notificación de un conjunto de eventos definido por un filtro de eventos para el destino de la notificación creada en el paso anterior. Especifique 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 parámetro `-destinations`.
 - *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. Si seleccionó TCP como *transport_protocol*, puede usar el comando `event notification destination check` 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, `FsxD07353f551e6b557b4-01`).
 - *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
```

Supervisión con Data Infrastructure Insights

NetApp Data Infrastructure Insights (anteriormente Cloud Insights) es un NetApp servicio que puedes usar para monitorizar tus sistemas de archivos Amazon FSx for NetApp ONTAP junto con tus otras soluciones NetApp de almacenamiento. Con Data Infrastructure Insights, puede monitorear las métricas de configuración, capacidad y rendimiento a lo largo del tiempo para comprender las tendencias de su 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

Data Infrastructure Insights no es compatible con los sistemas de archivos de segunda generación con más de un par de alta disponibilidad.

Data Infrastructure 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 más eficiente FSx para ONTAP. También puede utilizar esta información para planificar cuándo necesitará más rendimiento o capacidad FSx para su implementación de ONTAP.

Para obtener más información, consulte la [documentación sobre información sobre la infraestructura de datos en la documentación](#) del producto de NetApp ONTAP.

Supervisión de FSx los sistemas de archivos 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 ONTAP. Puede usar Harvest con Grafana como una solución de supervisión de código abierto.

Introducción a Harvest y Grafana

La siguiente sección detalla cómo puede configurar Harvest y Grafana FSx para medir el rendimiento y la utilización de la capacidad de almacenamiento del sistema de archivos ONTAP.

Puede monitorizar su sistema de archivos Amazon FSx for NetApp ONTAP mediante Harvest y Grafana. NetApp Harvest monitorea ONTAP centros de datos mediante la recopilación de métricas de rendimiento, capacidad y hardware de los sistemas FSx de archivos ONTAP. Grafana proporciona un panel de control donde se recopilan Harvest se pueden mostrar las métricas.

Paneles de Harvest compatibles

Amazon FSx for NetApp ONTAP expone un conjunto de métricas diferente al de las instalaciones locales NetApp ONTAP. Por lo tanto, solo lo siguiente out-of-the-box Harvest Actualmente, ONTAP fsx admite el uso de los paneles etiquetados con FSx . Es posible que a algunos de los paneles de estos paneles les falte información que no es compatible.

- Cosecha: metadatos
- ONTAP: cDOT
- ONTAP: Clúster
- ONTAP: Conformidad
- ONTAP: centro de datos
- ONTAP: Instantáneas de protección de datos
- ONTAP: LUN
- ONTAP: Nodo
- ONTAP: Qtree
- ONTAP: Seguridad
- ONTAP: SnapMirror
- ONTAP: SVM
- ONTAP: Volumen

Los siguientes ejemplos de Harvest ONTAP admite los FSx paneles, pero no están habilitados de forma predeterminada en Harvest.

- ONTAP: FlexCache
- ONTAP: FlexGroup
- ONTAP: Clientes NFS
- ONTAP: Monitores Storepool NFSv4
- ONTAP: Solución de problemas de NFS

- ONTAP: SMB
- ONTAP: Carga de trabajo

No se admite Harvest paneles

Los siguientes ejemplos de Harvest ONTAP no admite paneles. FSx

- ONTAP: agregado
- ONTAP: Disco
- ONTAP: Operación de servicio externo
- ONTAP: Análisis de sistemas de archivos (FSA)
- ONTAP: Health
- ONTAP: MetroCluster
- ONTAP: Alimentación
- ONTAP: Estantería
- ONTAP: Almacenes de objetos S3

AWS CloudFormation plantilla

Para empezar, puedes implementar una AWS CloudFormation plantilla que lance automáticamente una EC2 instancia de Amazon que ejecute Harvest y Grafana. Como entrada a la AWS CloudFormation plantilla, especificas el `fsxadmin` usuario y el terminal de FSx administración de Amazon 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 el despliegue de las soluciones Harvest y Grafana. La plantilla crea una instancia de Amazon EC2 Linux e instala el software Harvest y Grafana. Para usar esta solución, descargue la plantilla [fsx-ontap-harvest-grafana.template](#). AWS CloudFormation

Note

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

Tipos de EC2 instancias de Amazon

Al configurar la plantilla, debes proporcionar el tipo de EC2 instancia de Amazon. NetAppLa recomendación para el tamaño de la instancia depende del número de sistemas de archivos que monitorices y del número de métricas que decidas 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
40+	8 núcleos	2000 MB	t3.2xlarge

Para obtener más información sobre los tipos de EC2 instancias de Amazon, consulta [las instancias de uso general](#) en la Guía del EC2 usuario de Amazon.

Reglas de puertos de instancias

Al configurar la EC2 instancia de Amazon, 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 de Amazon EC2 Harvest y Grafana. Como la instancia que se inicializa se conecta a un punto de conexión a través de HTTPS, debe resolver el punto de conexión, que necesita el puerto 53 TCP/UDP para el DNS. Además, para llegar al punto de conexión, necesita el puerto 443 TCP para HTTPS y el acceso a Internet.

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 FSx para ONTAP que se ejecute en una Amazon Virtual Private Cloud (Amazon VPC) en AWS su cuenta 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 sistemas de archivos](#).

Cómo iniciar la pila de soluciones Harvest/Grafana

1. Descargue la plantilla [fsx-ontap-harvest-grafana.template](#). AWS CloudFormation Para obtener más información sobre la creación de una AWS CloudFormation pila, consulte [Creación de una pila en la AWS CloudFormation consola](#) en la Guía del AWS CloudFormation usuario.

Note

De forma predeterminada, esta plantilla se lanza en la AWS región EE.UU. Este (Norte de Virginia). Debe lanzar esta solución en un Región de AWS lugar donde Amazon FSx esté disponible. Para obtener más información, consulta los [FSx puntos de conexión y las cuotas de Amazon](#) en Referencia general de AWS

2. En Parámetros, revise los parámetros de la plantilla y modifíquelos para adaptarlos a las necesidades del sistema de archivos. Esta solución utiliza los siguientes valores predeterminados.

Parámetro	Predeterminado/a	Descripción
InstanceType	t3.micro	El tipo de EC2 instancia de Amazon. A continuación se muestran los tipos de instancias t3. • t3.micro • t3.small • t3.medium • t3.large • t3.xlarge • t3.2xlarge

Parámetro	Predeterminado/a	Descripción
		Para ver la lista completa de los valores de tipo de EC2 instancia de Amazon permitidos para este parámetro, consulta fsx-ontap-harvest-grafana .template.
KeyPair	Sin valor predeterminado	El par de claves que se utiliza para acceder a la EC2 instancia de Amazon.
SecurityGroup	Sin valor predeterminado	El ID del grupo de seguridad de la instancia de Harvest/ Grafana. Corrobore que los puertos de entrada 3000 y 9090, además de los puertos 53 y 443, estén abiertos desde los clientes que desea usar para acceder al 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 conectarse a Internet. Para obtener más información, consulte Tipos de subred en la Guía del usuario de Amazon VPC.

Parámetro	Predeterminado/a	Descripción
Subred	Sin valor predeterminado	Especifique la misma subred que la subred preferida de su sistema de archivos Amazon FSx for NetApp ONTAP. Puedes encontrar el ID de subred preferido del sistema de archivos en la FSx consola de Amazon, en la pestaña Red y seguridad de la página de detalles del sistema FSx de archivos de ONTAP.
LatestLinuxAmild	<code>/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2</code>	Es la última versión de la AMI de Amazon Linux 2 en un Región de AWS dado.
FSxEndPoint	Sin valor predeterminado	La dirección IP del punto de conexión de administración del sistema de archivos. Puedes encontrar la dirección IP del punto final de administración del sistema de archivos en la FSx consola de Amazon, en la pestaña Administración de la página de detalles del FSx sistema de archivos de ONTAP.

Parámetro	Predeterminado/a	Descripción
SecretName	Sin valor predeterminado	AWS Secrets Manager nombre secreto que contiene la contraseña del fsxadmin usuario del sistema de archivos. Es la contraseña que proporcionó al crear el sistema de archivos.

3. Elija Next (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 AWS CloudFormation consola en la columna Estado. Debería ver el estado CREATE_COMPLETE en aproximadamente cinco (5) minutos.

Iniciar sesión en Grafana

Una vez finalizada la implementación, usa tu 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, consulta la página de [NetApp Harvest](#) en GitHub.

Solución de problemas de Harvest y Grafana

Si te falta algún dato mencionado en los paneles de Harvest y Grafana o tienes problemas para configurar Harvest y Grafana FSx con ONTAP, consulta los siguientes temas para encontrar una posible solución.

Temas

- [Los paneles de SVM y de volumen están en blanco](#)
- [CloudFormation la pila se revierte tras agotarse el tiempo de espera](#)

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. Necesitarás acceso SSH a la EC2 instancia de Amazon en la que están desplegados Harvest y Grafana.

1. Utiliza SSH en la EC2 instancia de Amazon en la que se ejecutan tus clientes de Harvest y Grafana.

```
[~]$ ssh ec2-user@ec2_ip_address
```

2. Use el siguiente comando para abrir el archivo `harvest.yml` y haga lo siguiente
 - Compruebe que se haya creado una entrada FSx para su instancia de ONTAP como. `Cluster-2`
 - Compruebe que las entradas de nombre de usuario y contraseña coincidan con las credenciales de `fsxadmin`.

```
[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 contraseña de `fsxadmin`, de la siguiente manera:

```
[ec2-user@ip-ec2_ip_address ~]$ sudo vi /home/ec2-user/harvest_install/harvest/harvest.yml
```

4. Corrobore que las credenciales de usuario `fsxadmin` se almacenen en Secrets Manager con el siguiente formato para futuras implementaciones y sustituya `fsxadmin_password` por su contraseña.

```
{"username" : "fsxadmin", "password" : "fsxadmin_password"}
```

CloudFormation la pila se revierte tras 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. Necesitarás acceso SSH a la EC2 instancia implementada por la CloudFormation pila.

1. Vuelva a implementar la CloudFormation pila y asegúrese de que la reversión automática esté deshabilitada.
2. Utiliza SSH en la EC2 instancia de Amazon en la que se ejecutan tus clientes de Harvest y Grafana.

```
[~]$ ssh ec2-user@ec2_ip_address
```

3. Compruebe que los contenedores de Docker se hayan iniciado correctamente mediante el siguiente comando.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo docker ps
```

En la respuesta, debería 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	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 de Docker no se están ejecutando, compruebe si hay errores en el archivo `/var/log/cloud-init-output.log` 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 de 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 ejecutando `sudo docker ps` y conectándose a la URL de Harvest y Grafana.

Supervisión de FSx las llamadas a la API de ONTAP con AWS CloudTrail

Amazon FSx está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Amazon FSx. CloudTrail captura todas las llamadas a la FSx API de Amazon FSx para NetApp ONTAP como eventos. Las llamadas capturadas incluyen llamadas desde la FSx consola de Amazon y desde llamadas de código a operaciones de la FSx API de Amazon.

Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Amazon FSx. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puedes 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 CloudTrail, consulta la [Guía AWS CloudTrail del usuario](#).

FSx Información de Amazon en CloudTrail

CloudTrail está habilitada en su AWS cuenta al crear la cuenta. Cuando se produce una actividad de API en Amazon FSx, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puedes ver, buscar y descargar los eventos recientes en tu AWS cuenta. Para obtener más información, consulta Cómo [ver eventos con el historial de CloudTrail eventos](#).

Para tener un registro continuo de los eventos de tu AWS cuenta, incluidos los eventos de Amazon FSx, crea una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando crea una ruta en la consola, la ruta se aplica a todas AWS las regiones. La ruta registra los eventos de todas AWS las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para obtener más información, consulte los siguientes temas en la Guía del usuario de AWS CloudTrail :

- [Creando una ruta para tu Cuenta de AWS](#)
- [AWS integraciones de servicios con Logs CloudTrail](#)
- [Configuración de las notificaciones de Amazon SNS para CloudTrail](#)

- [Recibir archivos de CloudTrail registro de varias regiones](#) y [recibir archivos de CloudTrail registro de varias cuentas](#)

Todas las [llamadas a la FSx API](#) de Amazon las registra CloudTrail. Por ejemplo, las llamadas a las TagResource operaciones CreateFileSystem y generan entradas en los archivos de CloudTrail registro.

Cada entrada de registro o evento contiene información sobre 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 root o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el elemento [CloudTrail UserIdentity en la Guía del usuario](#).AWS CloudTrail

Descripción de las entradas de los archivos de FSx registro de Amazon

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra el TagResource funcionamiento 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 CloudTrail registro que muestra la `UntagResource` acción que se produce cuando se elimina de la consola una etiqueta de un sistema de archivos.

```

{
  "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"  
}
```

Cómo trabajar con Microsoft Active Directory en FSx ONTAP

Amazon FSx trabaja 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 FSx máquinas virtuales de almacenamiento de ONTAP (SVMs) a su dominio de Active Directory para autenticar a los usuarios y controlar el acceso a nivel de archivos y carpetas. A continuación, los clientes del bloque de mensajes de servidor (SMB) pueden usar las identidades de usuario existentes en Active Directory para autenticarse y acceder a los volúmenes de las 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 listas de control de acceso de seguridad (ACL) a Amazon FSx sin ninguna modificación.

Si la infraestructura de dominio de Microsoft Active Directory no está disponible, puede configurar un servidor de bloque de mensajes de servidor (SMB) en un grupo de trabajo de una SVM como alternativa a unir una SVM a una Microsoft Active Directory. Para obtener más información, consulte [Configuración de un servidor SMB en un grupo de trabajo](#).

Cuando une Amazon FSx for NetApp ONTAP a un Active Directory, une los sistemas de archivos SVMs al Active Directory de forma independiente. Esto significa que puede tener un sistema de archivos con algunos SVMs que estén unidos a un Active Directory y otros SVMs que no lo estén.

Después de unir una SVM a un Active Directory, puede actualizar las siguientes propiedades de configuración del Active Directory:

- Dirección IP del servidor DNS
- Nombre de usuario y contraseña de la cuenta de servicio autoadministrada de Active Directory

Temas

- [Requisitos previos para unir una SVM a un Microsoft AD autogestionado](#)
- [Prácticas recomendadas para trabajar con Oracle](#)
- [Cómo funciona SVMs la unión a Microsoft Active Directory](#)
- [Administración de las configuraciones del Active Directory de la SVM](#)

Requisitos previos para unir una SVM a un Microsoft AD autogestionado

Antes de unir una SVM 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](#)
- [Requisitos de configuración de la red](#)
- [Requisitos de la cuenta de servicio de Active Directory](#)

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 controlador de dominio de Active Directory tiene un nivel funcional de dominio de Windows Server 2000 o superior.
- El Active Directory usa un nombre de dominio que no tiene 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 FSx VPC asociadas al sistema de archivos de 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 los utiliza AWS Directory Service, ya que ONTAP no admite FSx la unión a la versión simple de Active Directory. SVMs

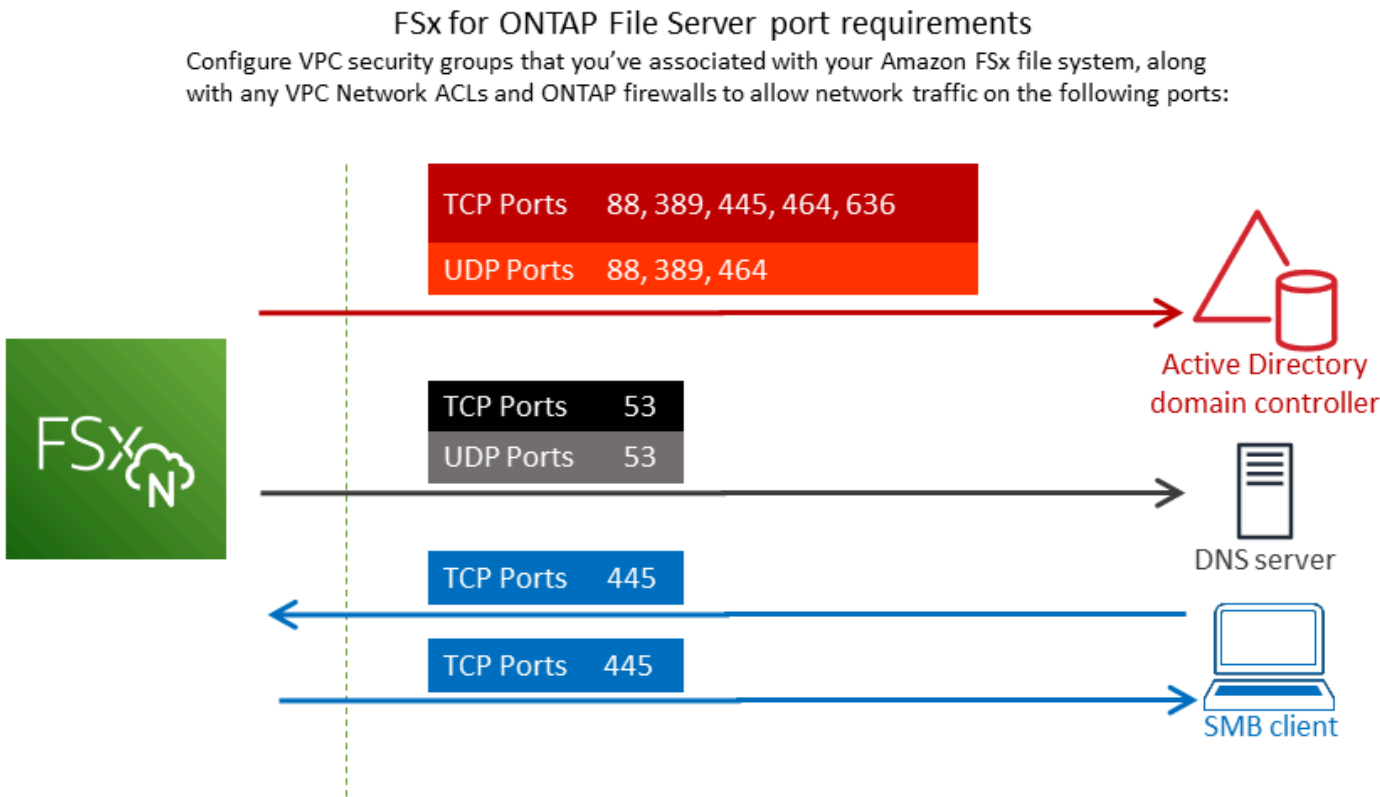
Requisitos de configuración de la red

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 iscsi_1 e iscsi_2 ()) en la SVM. LIFs

- 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 la red ACLs de VPC de las subredes en las que va a crear 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 directorios (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 deberían reflejarse en los firewalls que se aplican a cada uno de los controladores de dominio, servidores DNS, clientes y administradores de Active Directory. FSx FSx

Important

Si bien los grupos de seguridad de Amazon VPC requieren que los puertos se abran solo en la dirección en que se inicia el tráfico de red, la mayoría de los firewalls de Windows y las redes de VPC ACLs 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 del Active Directory autoadministrado a la que se le delegó permiso para realizar 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
- Capacidad de establecer la propiedad msDS-SupportedEncryptionTypes en objetos de equipo
- 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 [Delegar permisos a tu cuenta de FSx servicio de Amazon](#).

 Important

Amazon FSx requiere una cuenta de servicio válida durante toda la vida útil del sistema de FSx archivos de Amazon. Amazon FSx debe poder administrar completamente el sistema de archivos y realizar tareas que requieran separar y volver 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 NetApp al software de ONTAP. Mantén tu información de configuración de Active Directory actualizada con Amazon FSx, incluidas las credenciales de la cuenta de servicio. Para obtener más información, consulte [Mantener la configuración de Active Directory actualizada con Amazon FSx](#).

Si es la primera vez que utiliza AWS y 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 FSx para ONTAP](#).

⚠ Important

No muevas los objetos de ordenador que Amazon FSx crea en la unidad organizativa después de crearlos, ni elimines Active Directory mientras el SVM esté unido a él. Si lo hace, se configurará mal.

Prácticas recomendadas para trabajar con Oracle

Estas son algunas sugerencias y pautas que debe tener en cuenta al incorporar Amazon FSx for NetApp ONTAP SVMs a su Microsoft Active Directory autogestionado. Tenga en cuenta que se recomiendan como prácticas recomendadas, pero no son obligatorias.

Delegar permisos a tu cuenta de FSx servicio de Amazon

Asegúrese de configurar la cuenta de servicio que proporciona a Amazon FSx con los permisos mínimos necesarios. Además, separe la unidad organizativa (OU) de otras cuestiones relacionadas con el controlador de dominio.

Para unir Amazon FSx SVMs a tu dominio, asegúrate 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 únicamente los permisos necesarios FSx para unir ONTAP SVMs 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.

Cómo crear una cuenta de servicio para el dominio de Microsoft Active Directory

1. Procure haber iniciado sesión como administrador de dominio del dominio del 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 Delegate Control (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 Only the following objects in the folder (Sólo los siguientes objetos en la carpeta) y, a continuación, seleccione Computer objects (Objetos de equipo).
9. Elija Create selected objects in this folder (Crear los objetos seleccionados en esta carpeta) y Delete selected objects in this folder (Eliminar los objetos seleccionados en esta carpeta). A continuación, elija Siguiente.
10. En Mostrar estos permisos, procure 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 muevas los objetos de ordenador que Amazon FSx cree en la unidad organizativa una vez creados SVMs los tuyos. Si lo hace, se configurará mal. SVMs

Mantener la configuración de Active Directory actualizada con Amazon FSx

Para una disponibilidad ininterrumpida de su Amazon FSx SVMs, 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, asegúrate de actualizar la contraseña de la cuenta de servicio con Amazon FSx. Para ello, utilice la FSx consola de Amazon, la FSx API de Amazon o AWS CLI. Del mismo modo, si las direcciones IP del servidor DNS

cambian para su dominio de Active Directory, tan pronto como 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 las configuraciones de SVM Active Directory existentes mediante la AWS Management Console API AWS CLI, y](#) 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 a la interfaz de red elástica de su sistema de FSx archivos de Amazon. Para obtener más información, consulte [Control de acceso al sistema de archivos con Amazon VPC](#).

Cómo funciona SVMs la unión a Microsoft Active Directory

Su organización puede gestionar las identidades y los dispositivos mediante un Active Directory, ya sea en las instalaciones o en la nube. Con FSx ONTAP, puede unirlos SVMs directamente a su dominio de Active Directory existente de las siguientes maneras:

- Unir un elemento nuevo SVMs a un Active Directory en el momento de la creación:
 - Con la opción de creación estándar de la FSx consola de Amazon 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 [Cómo crear un sistema de archivos \(consola\)](#).

- Uso de la FSx consola de Amazon o de la FSx API de Amazon para crear una nueva SVM en un sistema de archivos existente FSx para ONTAP. AWS CLI Para obtener más información, consulte [Creación de máquinas virtuales de almacenamiento \(SVM\)](#).
- Unir lo existente SVMs 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 SVMs que ya estén unidas a un Active Directory. Para obtener más información, consulte [Administración de las configuraciones del Active Directory de la SVM](#).
 - 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 [Actualización de las configuraciones de SVM Active Directory mediante la CLI NetApp](#).

Important

- Amazon FSx solo registra los registros de DNS de una SVM si utilizas el DNS de Microsoft como servicio de DNS predeterminado. Si utilizas un DNS de terceros, debes configurar manualmente las entradas de DNS para tu Amazon FSx SVMs después de crearlas.
- Si lo usa AWS Managed Microsoft AD, debe especificar un grupo como FSx administradores AWS delegados, administradores AWS delegados o un grupo personalizado con permisos delegados para la OU.

Al unir un SVM FSx para 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 el Active Directory al unir una 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. Este es el nombre de la SVM en Active Directory, que debe ser único en el 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 ver una lista de direcciones AWS IP por región, consulta los [rangos 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 FSx que Amazon 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 el 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 especificas este grupo, Amazon FSx delega esta autoridad en el grupo de administradores de dominio de tu dominio de Active Directory de forma predeterminada.

Administración de las configuraciones del Active Directory de la SVM

En esta sección se describe cómo utilizar la AWS Management Console AWS CLI, la FSx API y la CLI de ONTAP para hacer lo siguiente:

- Unión de una SVM existente a un Active Directory
- Modificación de la configuración de un Active Directory de una SVM existente
- Eliminar SVMs de un Active Directory

Para eliminar un SVM de un Active Directory, debe usar la NetApp CLI de ONTAP.

Temas

- [Conexión SVMs a Active Directory mediante la API AWS Management Console y AWS CLI](#)
- [Actualización de las configuraciones de SVM Active Directory existentes mediante la AWS Management Console API AWS CLI, y](#)
- [Actualización de las configuraciones de SVM Active Directory mediante la CLI NetApp](#)

Conexión SVMs a Active Directory mediante la API AWS Management Console y AWS CLI

Use el siguiente procedimiento para unir una SVM existente a un Active Directory. En este procedimiento, la SVM aún no está unida a un Active Directory.

Para unir una SVM a un Active Directory (AWS Management Console)

1. Abre la FSx consola de Amazon en <https://console.aws.amazon.com/fsx/>.
2. Elija la SVM que desea 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 máquinas virtuales disponibles SVMs, en el panel de navegación izquierdo, expanda ONTAP y seleccione Almacenamiento de máquinas virtuales. Aparece una lista de todas las que Región de AWS hay SVMs en su cuenta en.

Seleccione la SVM que desea unir a un Active Directory 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 Join SVM to an Active Directory.
4. Introduzca la siguiente información para el Active Directory al que va a unir la SVM:
 - El nombre NetBIOS del objeto de equipo de Active Directory que se creará para la SVM. Este es el nombre de la SVM en Active Directory, que debe ser único en el 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.
 - Direcciones IP del servidor DNS: las IPv4 direcciones de los servidores DNS de tu 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 FSx administradores AWS delegados, administradores AWS delegados o un grupo personalizado con permisos delegados para la OU.

Si se va a unir a un Active Directory autoadministrado, use el nombre del grupo en el Active Directory. El grupo predeterminado es Domain Admins.

5. Elija Unir Active Directory para unir la SVM al Active Directory mediante la configuración que proporcionó.

Para unir un SVM a un Active Directory (AWS CLI)

- FSx Para unir un SVM de ONTAP a un Active Directory, utilice el comando [update-storage-virtual-machine](#)CLI (o la operación [UpdateStorageVirtualMachine](#)API 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
```

Tras 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",
    "IpAddresses": ["198.19.0.4"]
  },
  "Nfs": {
    "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com",
    "IpAddresses": ["198.19.0.4"]
  },
  "Smb": {
    "DnsName": "amznfsx12345",
    "IpAddresses": ["198.19.0.4"]
  },
  "SmbWindowsInterVpc": {
    "IpAddresses": ["198.19.0.5", "198.19.0.6"]
  },
  "Iscsi": {
    "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com",
    "IpAddresses": ["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 las configuraciones de SVM Active Directory existentes mediante la AWS Management Console API AWS CLI, y

Use el siguiente procedimiento para actualizar la configuración de Active Directory de una SVM que ya esté unida a un Active Directory.

Cómo actualizar la configuración de una SVM del Active Directory (AWS Management Console)

1. Abra la FSx consola de Amazon 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 máquinas virtuales SVMs disponibles, en el panel de navegación izquierdo, expanda ONTAP y seleccione Almacenamiento de máquinas virtuales.

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.
 - Direcciones IP de los servidores DNS: las IPv4 direcciones 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.

Use el siguiente procedimiento para actualizar la configuración de Active Directory de una SVM que ya esté unida a un Active Directory.

Cómo actualizar la configuración de una SVM del 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-machine](#)CLI (o la operación de [UpdateStorageVirtualMachine](#)API 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"]}'
```

Actualización de las configuraciones 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.

Unión de una SVM a un Active Directory mediante la CLI de ONTAP

Puede unir los existentes SVMs a un Active Directory mediante la CLI de ONTAP, tal y como se describe en el siguiente procedimiento. Puede hacerlo incluso si la SVM ya está unida a un Active Directory.

1. Para acceder al ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando. 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 [Administrar sistemas de archivos con el 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.
svm_name Sustitúyala por tu propia información.

```
FsxId0ae30e5b7f1a50b6a::>vserver services name-service dns check -vserver svm_name
```

Vserver	Name Server	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.

- 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` ello, introduzca el nombre al OUs que desee que se una el 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 del 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.

- 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 la configuración de un Active Directory existente.

1. Para acceder a ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando. 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 [Administrar sistemas de archivos con el 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 del DNS del 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 a los servidores DNS del Active Directory mediante el comando `vserver services name-service dns check -vserver svm_name`.

```
::>vserver services name-service dns check -vserver svm_name
```

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 propia configuración del Active Directory, puede cambiar los campos existentes mediante el siguiente comando y reemplazando lo siguiente:

- *computer_name*, si desea modificar el nombre 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 usó para unir este dispositivo al Active Directory.

```
::>vserver cifs modify -vserver svm_name -cifs-server computer_name -  
domain domain_name -OU organizational_unit
```

Puede verificar el estado de la conexión del Active Directory mediante el comando `vserver cifs check -vserver svm_name`.

5. Al terminar de modificar la configuración del Active Directory y el DNS, vuelva a poner en marcha 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 ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando. 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 [Administrar sistemas de archivos con el ONTAP CLI](#).

2. Elimine el servidor de CIFS que desunió el dispositivo del Active Directory ejecutando el siguiente comando. Para que ONTAP elimine la cuenta de máquina de la SVM, proporcione al Active Directory las credenciales que usó originalmente para unir la SVM.

```
FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
```

3. Si necesita modificar las entradas del DNS del 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.AEXAMPLE.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. Eliminar los servidores del DNS del 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 el dns debe eliminarse como ns-switch, y no tiene previsto volver a conectar 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
```

Migración a Amazon FSx para ONTAP NetApp

En las siguientes secciones se proporciona información sobre cómo migrar sus sistemas de archivos NetApp ONTAP existentes a Amazon FSx for NetApp ONTAP.

Note

Si planea usar la política de organización por niveles A11 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 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 conjunto de capacidad.

Temas

- [Migración a ONTAP mediante FSx NetApp SnapMirror](#)
- [Migración a FSx ONTAP mediante AWS DataSync](#)

Migración a ONTAP mediante FSx NetApp SnapMirror

Puede migrar sus sistemas de archivos NetApp ONTAP a Amazon FSx para usar NetApp ONTAP. NetApp SnapMirror

NetApp SnapMirror emplea la replicación a nivel de bloques entre dos sistemas de archivos ONTAP, replicando datos de un volumen de origen específico a un volumen de destino. Recomendamos usarlo SnapMirror para migrar los sistemas de archivos ONTAP locales a NetApp ONTAP. FSx

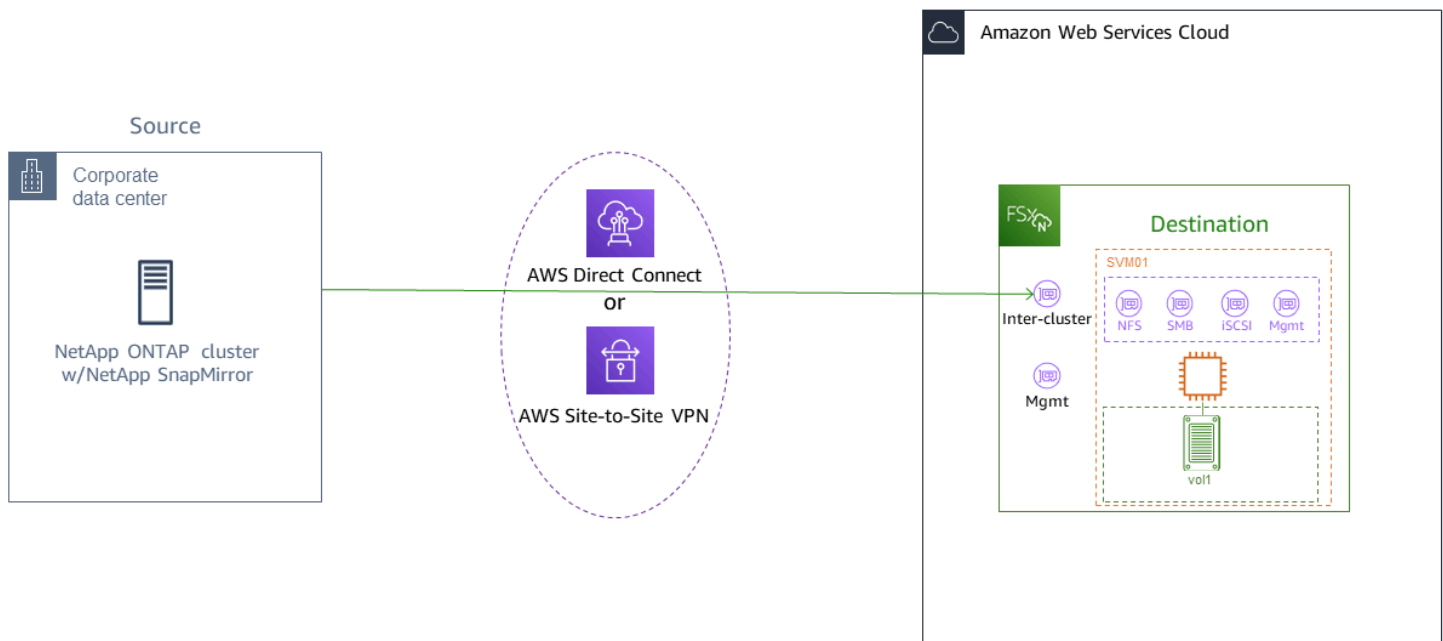
NetApp SnapMirrorLa replicación a nivel de bloque es rápida y eficaz incluso para sistemas de archivos con:

- Estructuras de directorio complejas
- Más de 50 millones de archivos
- Tamaños de archivo muy pequeños (del orden de kilobytes)

Cuando se migra SnapMirror a ONTAP, FSx 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 los sistemas de archivos ONTAP locales a NetApp ONTAP implica las siguientes FSx tareas de alto nivel:

1. Crea el volumen de destino en Amazon FSx.
2. Recopile las interfaces lógicas de origen y destino (LIFs).
3. Establezca un emparejamiento de clústeres entre sistemas de archivos de origen y de destino.
4. Cree una relación de emparejamiento de SVM.
5. Cree la SnapMirror relación.
6. Mantenga un clúster de destino actualizado.
7. Cambie a su sistema FSx de archivos 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 el origen y el destino entre clústeres LIFs](#)
- [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 FSx para ONTAP](#)
- [Pasando 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 por encima de las tareas en segundo plano, como la organización de los datos por 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 CloudWatch las métricas del sistema de archivos.](#) 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 o. AWS Direct Connect AWS VPN Para obtener más información, consulte [Acceder a los datos desde el Nube de AWS](#) y [¿Qué es el peering de VPC?](#) en la Guía de Amazon VPC Peering.
- El grupo de seguridad de VPC FSx para el sistema de archivos de 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 finales entre clústeres (). LIFs
- Compruebe que los volúmenes de origen y destino ejecutan versiones de ONTAP compatibles NetApp antes de crear una relación de protección de datos. SnapMirror 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 destino FSx para el sistema de archivos ONTAP con un SVM, pero no ha creado un volumen de destino. Para obtener más información, consulte [Creación de sistemas de archivos.](#)

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 FSx IDABCDEF1234567890A).
- ***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 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 el sistema de archivos FSx de ONTAP. Para obtener más información, consulte [Uso de NetApp ONTAP CLI](#).

Crear el volumen de destino

Puede crear un volumen de destino de protección de datos (DP) mediante la FSx consola de Amazon AWS CLI, la y la FSx API de Amazon, además de la CLI de NetApp ONTAP y la API REST. Para obtener información sobre la creación de un volumen de destino mediante la FSx consola de Amazon y AWS CLI, consulte [Creación de volúmenes](#).

Note

ONTAP no preserva los ahorros de compresión posteriores al proceso logrados en el origen en el volumen DP de destino cuando sí lo es la política de estratificación del volumen de destino. A11 Para conservar los ahorros en la compresión posterior al proceso, debe configurar la política de estratificación del volumen de destino Auto y habilitar inactive-data-compression en el sistema de archivos de destino la posibilidad de volver a aplicar los ahorros en la compresión posterior al proceso en el lugar de destino.

En el siguiente procedimiento, utilizará la CLI de NetApp ONTAP para crear un volumen de destino en el sistema de archivos FSx de 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 el origen y el destino entre clústeres LIFs

SnapMirror utiliza interfaces lógicas entre clústeres (LIFs), cada una con una dirección IP única, para facilitar la transferencia de datos entre los clústeres de origen y destino.

1. Para el destino FSx de los sistemas de archivos ONTAP, puede recuperar las direcciones IP de punto final entre clústeres desde la FSx consola de Amazon navegando a la pestaña Administración de la página de detalles de su sistema de archivos.
2. Para el clúster NetApp ONTAP de origen, recupere las direcciones IP LIF entre clústeres mediante la CLI de ONTAP. Ejecuta 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 Single-AZ de segunda generación, hay dos direcciones IP entre clústeres para cada par de alta disponibilidad (HA). Guarde estos valores para usarlos después.

Guarde las direcciones IP `inter_1` y `inter_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` y `source_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 el emparejamiento en el clúster de destino mediante el siguiente comando. En el caso de los sistemas de archivos Single-AZ de segunda generación, deberá 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 Single-AZ de segunda generación, deberá 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 establecida la interconexión de clústeres, el siguiente paso es la interconexión del. SVMs 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 el origen y el destino. SVMs

```
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 sincronizado el origen y el destino SVMs, 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 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 por hora o por día antes de completar la migración y trasladar sus clientes a FSx ONTAP. Puede establecer un programa de SnapMirror actualizaciones mediante el [snapmirror modify](#) comando.

```
FSx-Dest::> snapmirror modify -destination-path DestSVM:vol1 -schedule hourly
```

Pasando a Amazon FSx

Para preparar la transferencia a su sistema FSx de archivos 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 FSx de archivos de ONTAP.

1. Para garantizar que todos los datos del clúster de origen se transfieran al sistema FSx de archivos ONTAP, realice una transferencia final con 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 Path	Destination Path	Mirror State	Relationship Status	Last Transfer End 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 Path	Destination Path	Mirror State	Relationship Status
-----	-----	-----	-----
sourcesvm1:vol1	svm01:DestVol	Snapmirrored	Quiesced

6. Durante la migración, el volumen de destino es sólo de lectura. Para habilitar la lectura/escritura, tiene que romper la SnapMirror relación y pasarse al sistema de archivos FSx de 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 [Acceder a sus FSx datos de ONTAP](#).

Migración a FSx ONTAP mediante AWS DataSync

Recomendamos su uso AWS DataSync FSx para transferir datos entre sistemas de archivos de ONTAP y sistemas de archivos que no son de ONTAP, incluidos FSx Lustre, FSx OpenZFS, FSx Windows File Server, Amazon EFS, Amazon S3 y archivadores locales. Si va a transferir archivos entre ONTAP y ONTAP, le recomendamos que FSx utilice. NetApp [NetApp SnapMirror](#) AWS DataSync es 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 AWS o. 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 sistemas de archivos de ONTAP y también FSx para mover datos a un sistema de archivos de una cuenta o sistema de archivos diferente Región de AWS . AWS También se puede utilizar DataSync con los sistemas FSx 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 el punto final de un sistema de archivos FSx de ONTAP. Para obtener información sobre escenarios de transferencia específicos, consulte [Trabajar con ubicaciones](#) en la AWS DataSync Guía 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 monitorear 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 procesamiento de al menos 512 MBps, una regulación de 200 grados MBps normalmente equilibrará las velocidades de transferencia y organización de datos por niveles.

Requisitos previos

Para migrar los datos a su FSx configuración de ONTAP, necesita un servidor y una red que cumplan con los requisitos. DataSync Para obtener más información, consulte [los requisitos de DataSync](#) la Guía del AWS DataSync usuario.

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 uno y Servicios de AWS otro).
- Cree una ubicación de origen y de destino.

- Cree una tarea de .
- Ejecute la tarea para transferir archivos desde el origen al destino.

Para obtener más información, consulte los siguientes temas en la Guía del usuario de AWS DataSync :

- [Transferencia de datos entre el almacenamiento autogestionado y AWS](#)
- [Creación de una ubicación para Amazon FSx para NetApp ONTAP](#)

Seguridad en Amazon FSx para NetApp ONTAP

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 más información sobre los programas de conformidad que se aplican a Amazon FSx para NetApp ONTAP, consulte [AWS Servicios incluidos en el ámbito del programa de conformidad AWS Servicios incluidos](#) .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También eres responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación te ayuda a entender cómo aplicar el modelo de responsabilidad compartida cuando utilizas Amazon FSx. En los temas siguientes, se muestra cómo configurar Amazon FSx para que cumpla con sus objetivos de seguridad y conformidad. También aprenderás a utilizar otros AWS servicios que te ayudan a supervisar y proteger tus FSx recursos de Amazon.

Temas

- [Protección de datos en Amazon FSx para NetApp ONTAP](#)
- [Gestión de identidad y acceso para Amazon FSx for NetApp ONTAP](#)
- [AWS políticas gestionadas de Amazon FSx para OpenZFS](#)
- [Control de acceso al sistema de archivos con Amazon VPC](#)
- [Validación de conformidad de Amazon FSx para NetApp ONTAP](#)
- [Amazon FSx para NetApp ONTAP y puntos finales de VPC de interfaz \(\)AWS PrivateLink](#)
- [Resiliencia en Amazon FSx para NetApp ONTAP](#)
- [Seguridad de infraestructuras en Amazon FSx para NetApp ONTAP](#)
- [Utilice NetApp ONTAP Vscan con FSx ONTAP](#)

- [Usuarios y roles de ONTAP](#)

Protección de datos en Amazon FSx para NetApp ONTAP

El modelo de [responsabilidad AWS compartida modelo](#) se aplica a la 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. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulta las [Preguntas frecuentes sobre la privacidad de datos](#). Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el [Modelo de responsabilidad compartida de AWS y GDPR](#) en el Blog de seguridad de AWS .

Con fines de protección de datos, 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:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. 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. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte [Cómo trabajar con CloudTrail senderos](#) en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 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, consulta [Estándar de procesamiento de la información federal \(FIPS\) 140-3](#).

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabajas con Amazon FSx u otros Servicios de AWS empresa mediante la consola, la API o AWS SDKs. AWS CLI Cualquier dato que ingrese en etiquetas o campos de texto de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

El cifrado de datos es FSx para ONTAP

Amazon FSx for 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 automáticamente al crear un sistema de FSx archivos de Amazon. Amazon FSx for 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 [Cifrado de datos en reposo](#) y [Cifrado de datos en tránsito](#).

Cifrado de datos en reposo

Todos los sistemas de archivos y copias de seguridad de Amazon FSx for NetApp ONTAP están cifrados en reposo con claves gestionadas 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. Todas las copias de seguridad se cifran automáticamente al crearlas y se descifran automáticamente cuando se restaura en un volumen nuevo. Amazon gestiona estos procesos de forma transparente FSx, por lo que no tienes que modificar tus aplicaciones.

Amazon FSx utiliza un algoritmo de cifrado AES-256 estándar del sector para cifrar los FSx datos y metadatos de Amazon en reposo. 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 FSx usa Amazon AWS KMS

Amazon FSx se integra AWS KMS para la gestión de claves. Amazon FSx utiliza claves de KMS para cifrar el sistema de archivos y cualquier copia de seguridad de volumen. Usted elige la clave KMS utilizada para cifrar y descifrar los sistemas de archivos y las copias de seguridad en volumen (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 KMS, consulte [Creación de claves](#) en la Guía AWS Key Management Service para desarrolladores.

 Important

Amazon solo FSx acepta claves KMS de cifrado simétrico. No puedes usar 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 FSx clave de Amazon 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 Amazon admite FSx para copias de seguridad y 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 FSx sistema de archivos de ONTAP y los clientes conectados. También se proporciona orientación para ayudarlo a elegir el método de cifrado que mejor se adapte al 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 AWS instalaciones 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 for NetApp ONTAP admite los siguientes métodos para cifrar los datos en tránsito entre los sistemas de archivos FSx de 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 [Linux](#) y [Windows](#) compatibles.
- Cifrado basado en Kerberos mediante protocolos NFS y SMB.
- IPseccifrado basado en 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](#)
- [Cifrar los datos en tránsito con AWS Nitro System](#)
- [Cifrado de los datos en tránsito con un cifrado basado en Kerberos](#)
- [Cifrar los datos en tránsito con cifrado IPsec](#)
- [Habilitar el cifrado SMB de datos en tránsito](#)
- [Configuración IPsec mediante la autenticación PSK](#)
- [Configuración IPsec mediante autenticación mediante certificado](#)

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 ONTAP y FSx los clientes conectados. Estos factores incluyen:

- El sistema de archivos en el Región de AWS que se FSx ejecuta tu sistema de archivos para 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 usa 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. Para obtener más información, consulte [Cifrar los datos en tránsito con AWS Nitro System](#).

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 compatibles de Amazon EC2 Mac, [Linux](#) o [Windows](#), 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 usar Kerberos o el cifrado. 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 están ubicados en dispositivos interconectados VPCs, siempre y cuando el tráfico no pase por un dispositivo o

servicio de red virtual, como una puerta de enlace de tránsito. 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 EC2 instancias de Amazon compatibles utilizan las capacidades de descarga del hardware subyacente del sistema Nitro para cifrar automáticamente el tráfico en tránsito entre instancias.

El uso de Kerberos o el IPsec cifrado tiene un 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.

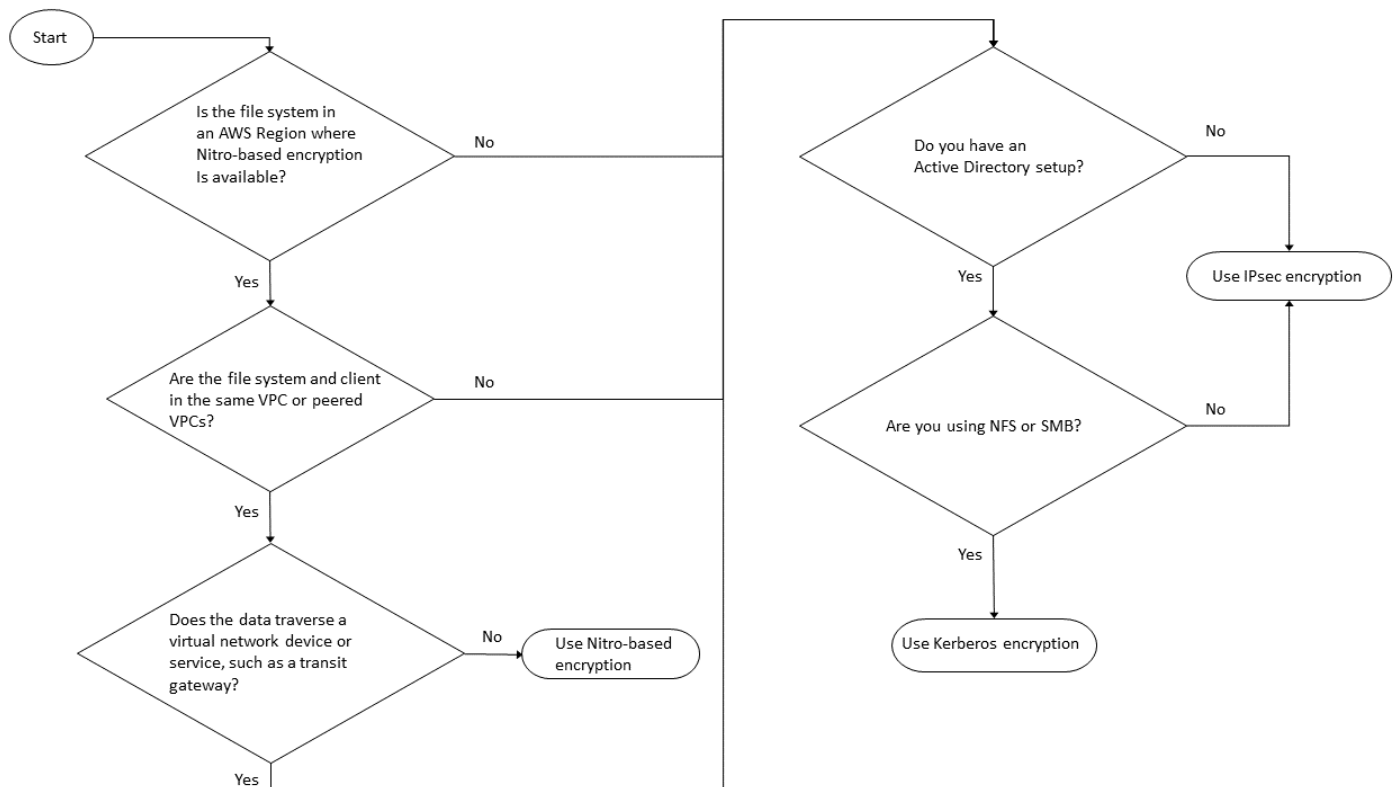
Protocolo de datos

Puede utilizar el cifrado basado en Amazon Nitro y el IPsec cifrado 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.



IPsec el cifrado es la única opción disponible cuando se cumplen todas las condiciones siguientes a su 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.

Cifrar los datos en tránsito con AWS Nitro System

Con el cifrado basado en Nitro, los datos en tránsito se cifran automáticamente cuando los clientes que acceden a sus sistemas de archivos se ejecutan en los tipos de instancias de Amazon EC2 [Linux](#) o [Windows](#) compatibles en los Regiones de AWS casos en que están disponibles FSx para ONTAP.

El uso del cifrado basado en Amazon Nitro no tiene impacto en el rendimiento de la red. Esto se debe a que las EC2 instancias de Amazon compatibles utilizan las capacidades de descarga del hardware subyacente del sistema Nitro para cifrar automáticamente 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, consulta la sección Cifrado en tránsito de la Guía del EC2 usuario de Amazon para tipos de instancias de [Linux](#) o [Windows](#).

En la siguiente tabla se detalla en qué Regiones de AWS se encuentra disponible el cifrado basado en Nitro.

Compatibilidad con el cifrado basado en Nitro

Generación	Tipos de implementación	Región de AWS
Sistemas de archivos de primera generación ¹	Single-AZ 1 Multi-AZ 1	Este de EE. UU. (Norte de Virginia), Este de EE. UU. (Ohio), Oeste de EE. UU. (Oregón), Europa (Irlanda)
Sistema de archivos de segunda generación	Single-AZ 2 Multi-AZ 2	Este de EE. UU. (Norte de Virginia), Este de EE. UU. (Ohio), Oeste de EE. UU. (Norte de California), Oeste de EE. UU. (Oregón), Europa (Fráncfort), Europa (Irlanda), Asia-Pacífico (Sídney)

¹ Los sistemas de archivos de primera generación creados el 28 de noviembre de 2022 o después admiten el cifrado en tránsito basado en Nitro que se indica en las Regiones de AWS enumeradas.

Para obtener más información sobre Regiones de AWS dónde FSx está disponible ONTAP, consulta los precios de [Amazon FSx for NetApp ONTAP](#).

Para obtener más información sobre las especificaciones de rendimiento de los sistemas de FSx archivos ONTAP, consulte. [Impacto de la capacidad de rendimiento en el rendimiento](#)

Cifrado de los datos en tránsito con un cifrado basado en Kerberos

Si utiliza Microsoft Active Directory, puede utilizar el cifrado basado en Kerberos a través de los protocolos NFS y SMB para cifrar los datos en tránsito de los volúmenes secundarios que [SVMs estén unidos](#) a un Microsoft Active Directory.

Cifrar los datos en tránsito a través de NFS mediante Kerberos

Se admite el cifrado de los datos en tránsito mediante Kerberos y sus protocolos. NFSv3 NFSv4 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 las versiones de Microsoft Windows desde Microsoft Windows Server 2012 y versiones posteriores, así como y Microsoft Windows 8 y versiones posteriores. Cuando está activado, FSx ONTAP cifra automáticamente los datos en tránsito mediante el cifrado SMB al acceder al sistema de archivos sin necesidad de modificar las aplicaciones.

FSx para ONTAP, SMB admite el cifrado de 128 y 256 bits, que viene determinado por 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 SMB FSx para ONTAP acepta todas las solicitudes estándar de los clientes de Windows y los controles detallados los gestiona la política de grupo o la configuración del registro de Microsoft.

La ONTAP CLI se utiliza para gestionar la configuración de cifrado en tránsito de ONTAP SVMs y de los volúmenes. FSx 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 [Administrar SVMs con el ONTAP CLI](#).

Para obtener instrucciones acerca de cómo habilitar el cifrado de SMB en una SVM o un volumen, consulte [Habilitar el cifrado SMB de datos en tránsito](#).

Cifrar los datos en tránsito con cifrado IPsec

FSx para ONTAP, es compatible con el uso del IPsec protocolo en modo 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 IPsec cifrado, se establece un IPsec túnel entre un FSx SVM de ONTAP configurado con IPsec activado y un cliente que se ejecuta en el IPsec cliente conectado y accede a los datos.

Le recomendamos que lo utilice IPsec para cifrar los datos en tránsito a través de los protocolos NFS, SMB e iSCSI cuando acceda a sus datos desde clientes que no admiten el [cifrado basado en Nitro](#), y si su cliente y yo no SVMs estamos unidos a un Active Directory, que es necesario para el cifrado basado en Kerberos. IPsec el cifrado 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 IPsec autenticación, puede usar claves previamente compartidas () o certificados. PSKs Si utiliza un PSK, el IPsec cliente que utilice debe ser compatible con la versión 2 (IKEv2) de Internet Key Exchange con un PSK. Los pasos básicos para configurar el IPsec cifrado tanto FSx en ONTAP como en el cliente son los siguientes:

1. Actívelo y IPsec configúrelo en su sistema de archivos.
2. Instálelo y IPsec configúrelo en su cliente
3. Configure IPsec para el acceso de varios clientes

Para obtener más información sobre cómo configurar IPsec mediante PSK, consulte [Configurar la seguridad IP \(IPsec\) mediante cifrado por cable](#) en el centro de NetApp ONTAP documentación.

Para obtener más información sobre cómo configurar el IPsec uso de certificados, consulte [Configuración IPsec mediante autenticación mediante certificado](#).

Habilitar el cifrado SMB de 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.

Cómo 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. Use el comando de la CLI de NetApp ONTAP [vserver cifs security modify](#) 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 configuración actual de is-smb-encryption-required en una SVM, use el comando de la CLI de NetApp ONTAP [vserver cifs security show](#):

```
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.

Cómo 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 [Administrar SVMs con el ONTAP CLI](#).
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 IPsec mediante la autenticación PSK

Si utiliza PSK para la autenticación, los pasos para configurar el IPsec cifrado tanto FSx en ONTAP como en el cliente son los siguientes:

1. Actívelo y configúrelo IPsec en su sistema de archivos.
2. Instálelo y IPsec configúrelo en su cliente
3. Configure IPsec para el acceso de varios clientes

Para obtener más información sobre la configuración IPsec mediante PSK, consulte [Configurar la seguridad IP \(IPsec\) mediante cifrado por cable](#) en el centro de NetApp ONTAP documentación.

Configuración IPsec mediante autenticación mediante certificado

En los temas siguientes se proporcionan instrucciones para configurar el IPsec cifrado mediante la autenticación mediante certificados en un sistema de archivos FSx compatible con ONTAP y en un cliente que ejecute IPsec Libreswan. Esta solución utiliza AWS Certificate Manager y AWS Private Certificate Authority crea una entidad de certificación privada y genera los certificados.

Los pasos generales para configurar el IPsec cifrado mediante la autenticación mediante certificados FSx para los sistemas de archivos de ONTAP y los clientes conectados son los siguientes:

1. Disponga de una autoridad de certificación para emitir certificados.
2. Genere y exporte certificados de CA para el sistema de archivos y el cliente.
3. Instale el certificado y configúrelo IPsec en la instancia del cliente.
4. Instale el certificado y IPsec configúrelo en su sistema de archivos.
5. Defina la base de datos de políticas de seguridad (SPD).
6. IPsec Configúrelo 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 el sistema de archivos de ONTAP y de los clientes que accederán a los datos de su sistema de archivos. FSx En el siguiente ejemplo, AWS Private Certificate Authority se configura una entidad de certificación privada y se generan los certificados que se van a instalar en el sistema de archivos y en el cliente. Con AWS Private Certificate Authority, puede crear una jerarquía completamente AWS alojada de autoridades de certificación raíz y subordinadas (CAs) 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.

Cómo 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 "R00T" \
  --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"
}
```

Cómo 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-----
MIICiTCcAFICCCQD6m7oRw0uX0jANBgkqhkiG9w0BAQUFADCBiDELMakGA1UEBhMC
VVMxCzAJBgNVBAGTAldBMRAwDgYDVQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAstC01BTSBDb25zb2x1MRIwEAYDVQQDEw1UZXRhbnQ2LsYWMxHZAAd
BgkqhkiG9w0BCQEWEG5vb25lQGFTtYXpva20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI1MjA0NTIxWjCBiDELMakGA1UEBhMCVVMxCzAJBgNVBAGTAldBMRAwDgYD
VQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAstC01BTSBDb25z
b2x1MRIwEAYDVQQDEw1UZXRhbnQ2LsYWMxHZAAdBgkqhkiG9w0BCQEWEG5vb25lQGFT
tYXpva20wZGZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMak0dn+a4GmWIWJ
21uUSfwfEvYSwTc2XADZ4nB+BLyGVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITx0USQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb30hjZnzcvQAaRHhd1QWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUHVvXyUntneD9+h8Mg9q6q+auNKyExzyLwax1Aoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJl1J00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp3780D8uTs7fLvJx79LjStB
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
-----END CERTIFICATE-----
```

Para obtener más información, consulte [Instalación de un certificado de CA raíz](#) en la Guía del AWS Private Certificate Authority usuario.

- 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
```

- 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
```

- 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

- 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 \  
    --signing-algorithm SHA256WITHRSA
```

```
--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. El siguiente ejemplo es para una EC2 instancia de 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.

```
$ passphrase=$(cat passphrase.txt | base64)
cat exported_cert.json | jq -r .PrivateKey > prv.key

cat exported_cert.json | jq -r .Certificate > cert.pem
```

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 EC2 instancia de Amazon que ejecute Amazon Linux 2.

Cómo instalar y configurar Libreswan

1. Conéctate a tu EC2 instancia 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 realizar la verificación 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. IPsec

```
$ sudo ipsec verify
```

Compruebe que la versión de Libreswan que ha instalado se esté ejecutando.

6. Inicialice la base de datos IPsec NSS.

```
$ sudo ipsec checknss
```

Cómo instalar los archivos de certificado en el cliente

1. Copia el [certificado que generaste](#) para el cliente en el directorio de trabajo de la EC2 instancia. 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 IPsec de configuración con 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
```


Empezará IPsec en el cliente después de realizar la configuración IPsec en su sistema de archivos.

Configuración IPsec en su sistema de archivos

En esta sección se proporcionan instrucciones sobre la instalación y configuración IPsec del certificado en el sistema de archivos de ONTAP. FSx

Cómo 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 ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando. 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 [Administrar sistemas de archivos con el 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, incluidos los del lado de ONTAP y del lado del cliente, en la gestión de ONTAP certificados CAs, a menos que ya estén instalados (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 dx -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 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 esté dentro de la ruta de búsqueda de la IPsec CA durante la autenticación, añada la administración de ONTAP certificados CAs al IPsec módulo 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 IPsec política 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 IPsec política que debe confirmar el sistema de archivos.

```
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
```

Comience IPsec en el cliente

Ahora IPsec que está configurado tanto en el sistema FSx de archivos de ONTAP como en el cliente, puede empezar IPsec en el cliente.

1. Conéctese al sistema cliente mediante SSH.
2. Empezar IPsec.

```
$ 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 IPsec configuración mostrando la conexión cifrada en el sistema de archivos FSx de ONTAP.

```
FSxID123:: > security ipsec show-ikesa -node FsxId123
FsxId08ac16c7ec2781a58:> security ipsec show-ikesa -node FsxId08ac16c7ec2781a58-01
```

Vserver	Policy Name	Local Address	Remote Address	Initator-SPI	State
dr	<i>policy-name</i>	198.19.254.13	172.31.77.6	551c55de57fe8976	ESTABLISHED
fsx	<i>policy-name</i>	198.19.254.38	172.31.65.193	4fd3f22c993e60c5	ESTABLISHED

2 entries were displayed.

Configuración IPsec para varios clientes

Cuando un número reducido de clientes necesita aprovechar el potencial IPsec, basta con utilizar una única entrada de SPD para cada cliente. Sin embargo, cuando cientos o incluso miles de clientes necesiten aprovecharlo IPsec, le recomendamos que utilice una configuración de IPsec varios clientes.

FSx ya que ONTAP admite la conexión de varios clientes de muchas redes a una única dirección IP de SVM si está habilitada IPsec. Para ello, puede utilizar la configuración subnet o la configuración Allow all clients, que se explican en los siguientes procedimientos:

Para configurarlo 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 en el caso de ONTAP, IPsec comprueba la validez del certificado en función del certificado CAs instalado en su almacén de confianza

local. FSx for ONTAP también admite la comprobación de la lista de certificados revocados (CRL).

1. Para acceder a la ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando. 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 [Administrar sistemas de archivos con el ONTAP CLI](#).

2. Utilice el comando `security ipsec policy create` NetApp ONTAP CLI de la siguiente manera, sustituyendo los *sample* valores 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 varios clientes mediante una configuración que permita a todos los clientes

Para permitir que cualquier cliente, independientemente de su dirección IP de origen, se conecte a la dirección IP IPsec habilitada para SVM, utilice el `0.0.0.0/0` comodín al especificar el `remote-ip-subnets` campo.

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 ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando. 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 [Administrar sistemas de archivos con el ONTAP CLI](#).

2. Utilice el comando `security ipsec policy create` NetApp ONTAP CLI de la siguiente manera, sustituyendo los *sample* valores 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
```

Gestión de identidad y acceso para Amazon FSx for NetApp ONTAP

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 quién puede autorizarse (tener permisos) para usar los recursos de Amazon FSx . El IAM es un Servicio de AWS servicio que puede utilizar sin coste adicional.

Temas

- [Público](#)
- [Autenticación con identidades](#)
- [Administración de acceso mediante políticas](#)
- [Cómo funciona Amazon FSx for NetApp ONTAP con IAM](#)
- [Ejemplos de políticas basadas en la identidad de Amazon for ONTAP FSx NetApp](#)
- [Solución de problemas de identidad y acceso a Amazon FSx for NetApp ONTAP](#)
- [Uso de roles vinculados a servicios para Amazon FSx](#)
- [Uso de etiquetas con Amazon FSx](#)

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realices en Amazon FSx.

Usuario del servicio: si utilizas el FSx servicio de Amazon para realizar tu trabajo, el administrador te proporcionará las credenciales y los permisos que necesitas. A medida que utilices más FSx funciones de Amazon para realizar tu trabajo, es posible que necesites permisos adicionales. Entender cómo se administra el acceso puede ayudarle a solicitar los permisos correctos al administrador. Si no puedes acceder a una función de Amazon FSx, consulta [Solución de problemas de identidad y acceso a Amazon FSx for NetApp ONTAP](#).

Administrador de servicios: si estás a cargo de FSx los recursos de Amazon en tu empresa, probablemente tengas acceso total a Amazon FSx. Es tu trabajo determinar a qué FSx funciones y recursos de Amazon deben acceder los usuarios de tu servicio. Luego, debe enviar solicitudes a su gestor 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 for NetApp ONTAP con IAM](#).

Administrador de IAM: si eres administrador de IAM, quizás te interese obtener más información sobre cómo puedes redactar políticas para gestionar el acceso a Amazon FSx. Para ver ejemplos de políticas FSx basadas en la identidad de Amazon que puedes usar en IAM, consulta. [Ejemplos de políticas basadas en la identidad de Amazon for ONTAP FSx NetApp](#)

Autenticación con identidades

La autenticación es la forma en que inicias sesión para AWS usar tus 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 gestor de IAM 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 la firma de solicitudes, consulte [AWS Signature Versión 4 para solicitudes 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 [Autenticación multifactor AWS en IAM](#) en 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 utiliza 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, consulta [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 utiliza AWS IAM Identity Center. 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, consulta [¿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 puedes iniciar sesión como grupo. Puedes usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos 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 de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte [Casos de uso para usuarios de IAM](#) en la Guía del usuario de IAM.

Roles de IAM

Un [rol de IAM](#) es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una persona determinada. Para asumir temporalmente un rol de IAM en el AWS Management Console, puede [cambiar de un rol de usuario a uno de IAM](#) (consola). Puedes asumir un rol llamando a una operación de AWS API AWS CLI o usando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulta [Métodos para asumir un rol](#) 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 de federación, consulte [Crear un rol para un proveedor de identidad de terceros \(federación\)](#) en la Guía de usuario de IAM. Si utiliza el 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, consulta [Conjuntos de permisos](#) en la Guía del usuario de AWS IAM Identity Center .
- **Permisos de usuario de IAM temporales:** un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- **Acceso entre cuentas:** puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. 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, consulta [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.
- **Acceso entre servicios:** algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realizas una llamada en un servicio, es habitual 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 AWS ellas, se te considera principal. 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:** puedes usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y realizan AWS CLI solicitudes a la AWS API. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo 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 que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte [Usar un rol de IAM para conceder permisos a las aplicaciones que se ejecutan en EC2 instancias de Amazon](#) 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. 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 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 utiliza 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 asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte [Creación de políticas de IAM](#) en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede 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 obtener más información sobre cómo elegir una política administrada o una política insertada, consulte [Elegir entre políticas administradas y políticas insertadas](#) en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los 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 () ACLs

Las listas de control de acceso (ACLs) controlan qué responsables (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs 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 compatibles. AWS WAF ACLs Para obtener más información ACLs, consulte la [descripción general de la 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). Puedes 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 (SCPs):** SCPs son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations es un servicio para agrupar y administrar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus 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 sobre Organizations SCPs, consulte las [políticas de control de servicios](#) en la Guía del AWS Organizations usuario.
- **Políticas de control de recursos (RCPs):** RCPs son políticas de JSON que puedes usar para establecer los permisos máximos disponibles para los recursos de tus cuentas sin actualizar las políticas de IAM asociadas a cada recurso que poseas. El RCP limita los permisos de los recursos en las cuentas de los miembros y puede afectar a los permisos efectivos de las identidades, incluidos los permisos Usuario raíz de la cuenta de AWS, independientemente de si pertenecen a su organización. Para obtener más información sobre Organizations e RCPs incluir una lista de Servicios de AWS ese apoyo RCPs, consulte [Políticas de control de recursos \(RCPs\)](#) en la Guía del AWS Organizations usuario.
- **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 se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la [lógica de evaluación de políticas](#) en la Guía del usuario de IAM.

Cómo funciona Amazon FSx for NetApp ONTAP con IAM

Antes de utilizar IAM para gestionar el acceso a Amazon FSx, consulta qué funciones de IAM están disponibles para su uso con Amazon FSx.

Funciones de IAM que puedes usar con Amazon FSx for ONTAP NetApp

Característica de IAM	FSx Soporte de Amazon
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
ACLs	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Sesiones de acceso directo (FAS)	Sí
Roles de servicio	No

Característica de IAM	FSx Soporte de Amazon
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo funcionan Amazon FSx y otros AWS servicios con la mayoría de las funciones de IAM, consulta [AWS los servicios que funcionan con IAM](#) en la Guía del usuario de IAM.

Políticas basadas en la identidad de Amazon FSx

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en 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 asociada. 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 de Amazon FSx basadas en la identidad, consulta. [Ejemplos de políticas basadas en la identidad de Amazon for ONTAP FSx NetApp](#)

Políticas basadas en recursos en Amazon FSx

Admite políticas basadas en recursos: no

Acciones políticas para Amazon FSx

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. 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 FSx las acciones de Amazon, consulta [Acciones definidas por Amazon FSx](#) en la Referencia de autorización de servicio.

Las acciones políticas en Amazon FSx usan el siguiente prefijo antes de la acción:

```
fsx
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [  
    "fsx:action1",  
    "fsx:action2"  
]
```

Para ver ejemplos de políticas de Amazon FSx basadas en la identidad, consulta. [Ejemplos de políticas basadas en la identidad de Amazon for ONTAP FSx NetApp](#)

Recursos de políticas para Amazon FSx

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes 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 \(ARN\)](#). Puedes 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, utiliza un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de los tipos de FSx recursos de Amazon y sus tipos ARNs, consulta [Recursos definidos por Amazon FSx](#) en la Referencia de autorización de servicio. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte [Acciones definidas por Amazon FSx](#).

Para ver ejemplos de políticas de Amazon FSx basadas en la identidad, consulta [Ejemplos de políticas basadas en la identidad de Amazon for ONTAP FSx NetApp](#).

Claves de condición de la política para Amazon FSx

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes 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. Puedes crear expresiones condicionales que utilizan [operadores de condición](#), tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

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 puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puedes 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, consulta [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 claves de FSx estado de Amazon, consulta [Claves de estado de Amazon FSx](#) en la Referencia de autorización de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte [Acciones definidas por Amazon FSx](#).

Para ver ejemplos de políticas de Amazon FSx basadas en la identidad, consulta. [Ejemplos de políticas basadas en la identidad de Amazon for ONTAP FSx NetApp](#)

Listas de control de acceso (ACLs) en Amazon FSx

Soporta ACLs: No

Control de acceso basado en atributos (ABAC) con Amazon FSx

Admite ABAC (etiquetas en las políticas): sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. 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 [Definición de permisos con la autorización de ABAC](#) en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte [Uso del control de acceso basado en atributos \(ABAC\)](#) en la Guía del usuario de IAM.

Para obtener más información sobre el etiquetado de FSx los recursos de Amazon, consulte [Etiquetado de 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 tus FSx recursos de Amazon](#).

Uso de credenciales temporales con Amazon FSx

Compatibilidad con credenciales temporales: sí

Algunos 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 obtener más información sobre el cambio de roles, consulte [Cambio de un usuario a un rol de IAM \(consola\)](#) 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 obtener más información, consulte [Credenciales de seguridad temporales en IAM](#).

Sesiones de acceso directo para Amazon FSx

Admite sesiones de acceso directo (FAS): sí

Cuando utilizas un usuario o un rol de IAM para realizar acciones en AWSél, se te 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](#).

Funciones de servicio para Amazon FSx

Compatible con roles de servicio: No

Funciones vinculadas a servicios para Amazon FSx

Admite roles vinculados a servicios: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información sobre la creación o la gestión de funciones FSx vinculadas a los servicios de Amazon, consulte. [Uso de roles vinculados a servicios para Amazon FSx](#)

Ejemplos de políticas basadas en la identidad de Amazon for ONTAP FSx NetApp

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar FSx los recursos de Amazon. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o la AWS API. 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 puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte [Creación de políticas de IAM \(consola\)](#) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por Amazon FSx, incluido el ARNs formato de cada uno de los tipos de recursos, consulte [Acciones, recursos y claves de condición de Amazon FSx](#) en la Referencia de autorización de servicio.

Temas

- [Prácticas recomendadas sobre las políticas](#)
- [Uso de la FSx consola de Amazon](#)
- [Cómo permitir a los usuarios consultar sus propios permisos](#)

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear, acceder o eliminar FSx los recursos de Amazon de tu cuenta. Estas acciones pueden generar costos adicionales para su

Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulta las [políticas administradas por AWS](#) o las [políticas administradas por AWS para funciones de tarea](#) en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta [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, consulta [Elementos de la política de JSON de IAM: Condición](#) en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte [Validación de políticas con el Analizador de acceso de IAM](#) en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte [Acceso seguro a la API con MFA](#) en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte [Prácticas recomendadas de seguridad en IAM](#) en la Guía del usuario de IAM.

Uso de la FSx consola de Amazon

Para acceder a la consola Amazon FSx for NetApp ONTAP, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirte enumerar y ver detalles sobre los FSx recursos de Amazon que tienes Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la AWS API AWS CLI o a la misma. En su lugar, permite el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la FSx consola de Amazon, adjunta también la política `AmazonFSxConsoleReadOnlyAccess` AWS gestionada a las entidades. Para obtener más información, consulte [Adición de permisos a un usuario](#) en la Guía del usuario de IAM:

Puedes consultar esta `AmazonFSxConsoleReadOnlyAccess` y otras políticas de servicios FSx gestionados de Amazon en [AWS políticas gestionadas de Amazon FSx para OpenZFS](#).

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 gestionadas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o AWS .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    }
  ]
}
```

```
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}
```

Solución de problemas de identidad y acceso a Amazon FSx for NetApp ONTAP

Utiliza la siguiente información para ayudarte a diagnosticar y solucionar los problemas habituales que puedes encontrar al trabajar con Amazon FSx e IAM.

Temas

- [No estoy autorizado a realizar ninguna acción en Amazon FSx](#)
- [No estoy autorizado a realizar tareas como: PassRole](#)
- [Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis FSx recursos de Amazon](#)

No estoy autorizado a realizar ninguna acción en Amazon FSx

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio `my-example-widget`, pero no tiene los permisos ficticios `fsx:GetWidget`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
fsx:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario mateojackson debe actualizarse para permitir el acceso al recurso *my-example-widget* mediante la acción *fsx:GetWidget*.

Si necesitas ayuda, ponte en contacto con tu AWS administrador. El gestor es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibes un error que indica que no estás autorizado a realizar la *iam:PassRole* acción, debes actualizar tus políticas para que puedas transferir una función a Amazon FSx.

Algunas te Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

El siguiente ejemplo de error se produce cuando un usuario de IAM denominado marymajor intenta utilizar la consola para realizar una acción en Amazon FSx. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir 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 necesitas ayuda, ponte en contacto con tu AWS administrador. El gestor es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis FSx recursos de Amazon

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 admiten políticas basadas en recursos o listas de control de acceso (ACLs), puedes usar esas políticas para permitir que las personas accedan a tus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si Amazon FSx admite estas funciones, consulte [Cómo funciona Amazon FSx for 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 usuario de su propiedad Cuenta de AWS en](#) la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulte [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 conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.

Uso de roles vinculados a servicios para Amazon FSx

Amazon FSx usa roles AWS Identity and Access Management vinculados a [servicios \(IAM\)](#). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Amazon. FSx Amazon predefine las funciones vinculadas al servicio FSx e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en tu nombre.

Un rol vinculado a un servicio facilita la configuración de Amazon FSx porque no tienes que añadir manualmente los permisos necesarios. Amazon FSx define los permisos de sus funciones vinculadas a servicios y, a menos que se defina lo contrario, solo Amazon FSx puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. Esto protege tus FSx recursos de Amazon porque no puedes eliminar inadvertidamente el permiso de acceso a los recursos.

Para obtener información acerca de otros servicios que admiten roles vinculados a servicios, consulte [Servicios de AWS que funcionan con IAM](#) y busque los servicios que muestran Sí en la columna Rol vinculado a un servicio. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

Permisos de roles vinculados a servicios para Amazon FSx

Amazon FSx usa 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 obtener actualizaciones de esta política, consulte [Amazon FSx ServiceRolePolicy](#)

Detalles de los permisos

Detalles de los permisos

Los permisos de los `AWSService RoleForAmazon FSx` roles se definen en la política `FSx ServiceRolePolicy AWS` gestionada de Amazon. `AWSServiceRoleForAmazonFSx` Tiene los siguientes permisos:

Note

Lo `AWSService RoleForAmazon FSx` utilizan todos los tipos de sistemas de FSx archivos de Amazon; algunos de los permisos enumerados no son aplicables a FSx ONTAP.

- `ds`— Permite FSx a Amazon ver, autorizar y desautorizar las aplicaciones de su AWS Directory Service directorio.
- `ec2`— Permite FSx a Amazon hacer lo siguiente:
 - Vea, cree y desasocie las interfaces de red asociadas a un sistema de FSx archivos de Amazon.
 - Vea una o más direcciones IP elásticas asociadas a un sistema de FSx archivos de Amazon.
 - Vea Amazon VPCs, los grupos de seguridad y las subredes asociados a un sistema de FSx archivos de Amazon.
 - Para proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una nube privada virtual (VPC).
 - Cree un permiso para que un usuario AWS autorizado realice determinadas operaciones en una interfaz de red.
- `cloudwatch`— Permite FSx a Amazon publicar puntos de datos métricos CloudWatch en el espacio de FSx nombres AWS/.
- `route53`— Permite FSx a Amazon asociar una Amazon VPC a una zona alojada privada.

```

{
  "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"
      }
    }
  }
]
```

Todas las actualizaciones de esta política están detalladas en [Amazon FSx actualiza las políticas AWS gestionadas](#).

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte [Permisos de roles vinculados a servicios](#) en la Guía del usuario de IAM.

Crear un rol vinculado a un servicio para Amazon FSx

No necesita crear manualmente un rol vinculado a servicios. Al crear un sistema de archivos en la AWS Management Console CLI de IAM o la API de IAM, Amazon FSx crea el rol vinculado al servicio automáticamente.

Important

Este rol vinculado a servicios puede aparecer en su cuenta si se ha completado una acción en otro servicio que utilice las características compatibles con este rol. Para obtener más información, consulte [Un nuevo rol ha aparecido en mi cuenta de IAM](#).

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando creas un sistema de archivos, Amazon vuelve a FSx crear el rol vinculado al servicio para ti.

Edición de un rol vinculado a un servicio para Amazon FSx

Amazon FSx no te permite editar el rol AWSService RoleForAmazon FSx vinculado al 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 [Edición de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Eliminar un rol vinculado a un servicio para Amazon FSx

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Sin embargo, debe eliminar todos los sistemas de archivo y copias de seguridad para poder eliminar el rol vinculado al servicio de forma manual.

Note

Si el FSx servicio de Amazon utiliza el rol cuando intentas eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM, la CLI de IAM o la API de IAM para eliminar el rol vinculado a servicios `AWSServiceRoleForAmazonFSx`. Para obtener más información, consulte [Eliminación de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Regiones compatibles con los roles vinculados a FSx los servicios de Amazon

Amazon FSx admite el uso de funciones vinculadas al servicio en todas las regiones en las que el servicio esté disponible. Para obtener más información, consulte [AWS Regiones y puntos de conexión](#).

Uso de etiquetas con Amazon FSx

Puedes usar etiquetas para controlar el acceso a FSx los recursos de Amazon e implementar el control de acceso basado en atributos (ABAC). Para aplicar etiquetas a FSx los recursos de Amazon durante la creación, los usuarios deben tener determinados permisos AWS Identity and Access Management (de IAM).

Conceder permisos para etiquetar recursos durante la creación

Con algunas acciones de la FSx API de Amazon que crean recursos, puedes especificar etiquetas al crear el recurso. Puede utilizar estas etiquetas de recursos para implementar el control de acceso

basado en atributos (ABAC). Para obtener más información, consulta [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Para que los usuarios puedan etiquetar recursos 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 (SVMs) 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 FSx los recursos de Amazon, consulte [Etiquetado de los recursos de Amazon FSx](#). Para obtener más información sobre el uso de etiquetas para controlar el acceso a FSx los recursos de Amazon, consulte [Uso de etiquetas para controlar el acceso a tus FSx recursos de Amazon](#).

Uso de etiquetas para controlar el acceso a tus FSx recursos de Amazon

Para controlar el acceso a FSx los recursos y acciones de Amazon, puedes usar políticas de IAM basadas en etiquetas. Puede proporcionar este control de dos maneras:

- Puedes controlar el acceso a FSx los recursos de Amazon en función de las etiquetas de esos recursos.
- Puede controlar qué etiquetas se pueden pasar en una condición de solicitud IAM.

Para obtener información sobre cómo utilizar las etiquetas para controlar el acceso a AWS los recursos, consulte [Controlar el acceso mediante etiquetas](#) en la Guía del usuario de IAM. Para obtener más información sobre cómo etiquetar FSx los recursos de Amazon en el momento de la creación, consulte [Conceder permisos para etiquetar recursos durante la creación](#). Para obtener más información acerca del etiquetado de recursos, consulte [Etiquetado de 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 un rol en un FSx recurso de Amazon, puedes usar etiquetas en el recurso. Por ejemplo, es posible que desee permitir o denegar acciones de la API específicas en un recurso del sistema de archivos en función del par clave-valor de la etiqueta del recurso.

Example 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 solo de los volúmenes de Amazon FSx para NetApp ONTAP con una etiqueta específica

Esta política permite a los usuarios crear copias de seguridad únicamente de FSx los volúmenes de 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"
        }
      }
    }
  ]
}

```

```
}  
  ]  
}
```

AWS políticas gestionadas de Amazon FSx para OpenZFS

Una política AWS gestionada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, 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 de AWS](#) en la Guía del usuario de IAM.

Amazon FSx ServiceRolePolicy

Permite FSx a Amazon gestionar AWS los recursos en tu nombre. Consulte [Uso de roles vinculados a servicios para Amazon FSx](#) para obtener más información.

AWS política gestionada: Amazon FSx DeleteServiceLinkedRoleAccess

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 FSx a Amazon eliminar su función vinculada a servicios para el acceso a Amazon S3, que solo utiliza Amazon FSx for Lustre.

Detalles de los permisos

Esta política incluye permisos que permiten `iam` FSx a Amazon ver, eliminar y ver el estado de eliminación de las funciones vinculadas al FSx servicio para el acceso a Amazon S3.

Para ver los permisos de esta política, consulta [Amazon FSx DeleteServiceLinkedRoleAccess](#) en la Guía de referencia de políticas AWS gestionadas.

AWS política gestionada: Amazon FSx FullAccess

Puedes adjuntar Amazon FSx FullAccess a tus entidades de IAM. Amazon FSx también vincula esta política a un rol de servicio que permite FSx a Amazon realizar acciones en tu nombre.

Proporciona acceso completo a Amazon FSx y acceso a los AWS servicios relacionados.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `fsx`— Permite a los directores tener acceso total para realizar todas las FSx acciones de Amazon, excepto `BypassSnaplockEnterpriseRetention`.
- `ds`— Permite a los directores ver información sobre los AWS Directory Service directorios.
- `ec2`
 - Permite que las entidades principales creen etiquetas en las condiciones especificadas.
 - Para proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una nube privada virtual (VPC).
- `iam`— Permite a los principios crear un rol vinculado a los FSx servicios de Amazon en nombre del usuario. Esto es necesario para que Amazon FSx pueda gestionar AWS los recursos en nombre del usuario.
- `firehose`: permite que las entidades principales escriban los registros en Amazon Data Firehose. Esto es necesario FSx para que los usuarios puedan supervisar el acceso al sistema de archivos de Windows File Server enviando los registros de acceso de auditoría a Firehose.
- `logs`: permite que las entidades principales creen grupos de registros, registren flujos y escriban eventos en los flujos de registro. Esto es necesario FSx para que los usuarios puedan supervisar el acceso al sistema de archivos del servidor de archivos de Windows enviando los registros de acceso de auditoría a CloudWatch Logs.

Para ver los permisos de esta política, consulta [Amazon FSx FullAccess](#) en la Guía de referencia de políticas AWS gestionadas.

AWS política gestionada: Amazon FSx ConsoleFullAccess

Puede adjuntar la política `AmazonFSxConsoleFullAccess` a las identidades de IAM.

Esta política otorga 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 los directores realizar todas las acciones en la consola FSx de administración de Amazon, excepto `BypassSnaplockEnterpriseRetention`.
- `cloudwatch`— Permite a los directores ver CloudWatch las alarmas y las métricas en la consola de FSx administración de Amazon.
- `ds`— Permite a los directores enumerar información sobre un AWS Directory Service directorio.
- `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 de 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.
 - Permite a los directores ver las interfaces de red elásticas asociadas a un sistema de FSx archivos de Amazon.
- `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`— Otorga permiso para crear un rol vinculado a un servicio que permita FSx a Amazon realizar acciones en nombre del usuario.

Para ver los permisos de esta política, consulta [Amazon FSx ConsoleFullAccess](#) en la Guía de referencia de políticas AWS gestionadas.

AWS política gestionada: Amazon FSx ConsoleReadOnlyAccess

Puede adjuntar la política `AmazonFSxConsoleReadOnlyAccess` a las identidades de IAM.

Esta política otorga permisos de solo lectura a Amazon FSx y los AWS servicios relacionados para que los usuarios puedan ver información sobre estos servicios en. AWS Management Console

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `fsx`— Permite a los directores ver información sobre los sistemas de FSx archivos de Amazon, incluidas todas las etiquetas, en Amazon FSx Management Console.
- `cloudwatch`— Permite a los directores ver CloudWatch las alarmas y las métricas en Amazon FSx Management Console.
- `ds`— Permite a los directores ver información sobre un AWS Directory Service directorio en Amazon FSx Management Console.
- `ec2`
 - Permite a los directores ver las interfaces de red, los grupos de seguridad, las subredes y la VPC asociada a un sistema de FSx archivos de Amazon en Amazon Management Console. 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.
 - Permite a los directores ver las interfaces de red elásticas asociadas a un sistema de FSx archivos de Amazon.
- `kms`— Permite a los directores ver los alias de las AWS Key Management Service claves en Amazon FSx Management Console.
- `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 los directores puedan ver la configuración de auditoría de acceso a los archivos existente FSx para un sistema de archivos del servidor de archivos de Windows.
- `firehose`: permite que las entidades principales describan los flujos de entrega de Amazon Data Firehose asociados a la cuenta que realiza la solicitud. Esto es necesario para que los directores puedan ver la configuración de auditoría de acceso a los archivos existente FSx para un sistema de archivos del servidor de archivos de Windows.

Para ver los permisos de esta política, consulta [Amazon FSx ConsoleReadOnlyAccess](#) en la Guía de referencia de políticas AWS gestionadas.

AWS política gestionada: Amazon FSx ReadOnlyAccess

Puede adjuntar la política AmazonFSxReadOnlyAccess a las identidades de IAM.

- `fsx`— Permite a los directores ver información sobre los sistemas de FSx archivos de Amazon, incluidas todas las etiquetas, en Amazon FSx Management Console.
- `ec2`: para proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una VPC.

Para ver los permisos de esta política, consulta [Amazon FSx ReadOnlyAccess](#) en la Guía de referencia de políticas AWS gestionadas.

Amazon FSx actualiza las políticas AWS gestionadas

Consulta los detalles sobre las actualizaciones de las políticas AWS gestionadas de Amazon FSx desde que este servicio comenzó a realizar el seguimiento de estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbete a la fuente RSS de la FSx [Historial de documentos de Amazon FSx for NetApp ONTAP](#) página de Amazon.

Cambio	Descripción	Fecha
Amazon FSx ConsoleFu llAccess : actualización de una política existente	Amazon FSx agregó un nuevo permiso <code>fsx:CreateAndAttachS3AccessPoint</code> que permite a los directores crear un S3 y adjuntarlo a un FSx volumen.	14 de abril de 2025
Amazon FSx ConsoleFu llAccess : actualización de una política existente	Amazon FSx agregó un nuevo permiso, <code>fsx:DescribeS3AccessPointAttachments</code> que permite a los directores enumerar todos los S3 dentro Cuenta de AWS de un Región de AWS	14 de abril de 2025

Cambio	Descripción	Fecha
Amazon FSx ConsoleFullAccess : actualización de una política existente	Amazon FSx agregó un nuevo permiso <code>fsx:UpdateS3AccessPointAttachments</code> que permite a los directores modificar un S3 existente.	14 de abril de 2025
Amazon FSx ConsoleFullAccess : actualización de una política existente	Amazon FSx agregó un nuevo permiso <code>fsx:DetachAndDeleteS3AccessPoint</code> que permite a los directores eliminar un S3.	14 de abril de 2025
Amazon FSx FullAccess : actualización de una política existente	Amazon FSx agregó un nuevo permiso <code>fsx:CreateAndAttachS3AccessPoint</code> que permite a los directores crear un S3 y adjuntarlo a un FSx volumen.	14 de abril de 2025
Amazon FSx FullAccess : actualización de una política existente	Amazon FSx agregó un nuevo permiso, <code>fsx:DescribeS3AccessPointAttachments</code> que permite a los directores enumerar todos los S3 dentro Cuenta de AWS de un Región de AWS	14 de abril de 2025
Amazon FSx FullAccess : actualización de una política existente	Amazon FSx agregó un nuevo permiso <code>fsx:UpdateS3AccessPointAttachments</code> que permite a los directores modificar un S3 existente.	14 de abril de 2025

Cambio	Descripción	Fecha
Amazon FSx FullAccess : actualización de una política existente	Amazon FSx agregó un nuevo permiso <code>fsx:DetachAndDeleteS3AccessPoint</code> que permite a los directores eliminar un S3.	14 de abril de 2025
Amazon FSx ConsoleReadOnlyAccess : actualización de una política existente	Amazon FSx agregó un nuevo permiso <code>ec2:DescribeNetworkInterfaces</code> que permite a los directores ver las interfaces de red elásticas asociadas a su sistema de archivos.	25 de febrero de 2025
Amazon FSx ConsoleFullAccess : actualización de una política existente	Amazon FSx agregó un nuevo permiso <code>ec2:DescribeNetworkInterfaces</code> que permite a los directores ver las interfaces de red elásticas asociadas a su sistema de archivos.	7 de febrero de 2025
Amazon FSx ServiceRolePolicy : actualización de una política existente	Amazon FSx agregó un nuevo permiso <code>ec2:GetSecurityGroupsForVpc</code> 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
Amazon FSx ReadOnlyAccess : actualización de una política existente	Amazon FSx agregó un nuevo permiso <code>ec2:GetSecurityGroupsForVpc</code> 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
Amazon FSx ConsoleReadOnlyAccess : actualización de una política existente	Amazon FSx agregó un nuevo permiso <code>ec2:GetSecurityGroupsForVpc</code> 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
Amazon FSx FullAccess : actualización de una política existente	Amazon FSx agregó un nuevo permiso <code>ec2:GetSecurityGroupsForVpc</code> 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
Amazon FSx ConsoleFullAccess : actualización de una política existente	Amazon FSx agregó un nuevo permiso <code>ec2:GetSecurityGroupsForVpc</code> 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
Amazon FSx 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 FSx para los sistemas de archivos OpenZFS.	20 de diciembre de 2023
Amazon FSx ConsoleFullAccess : 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 FSx para los sistemas de archivos OpenZFS.	20 de diciembre de 2023
Amazon FSx FullAccess : actualización de una política existente	Amazon FSx agregó un nuevo permiso para permitir a los usuarios realizar la replicación bajo demanda de volúmenes FSx para los sistemas de archivos OpenZFS.	26 de noviembre de 2023

Cambio	Descripción	Fecha
Amazon FSx ConsoleFullAccess : actualización de una política existente	Amazon FSx agregó un nuevo permiso para permitir a los usuarios realizar la replicación bajo demanda de volúmenes FSx para los sistemas de archivos OpenZFS.	26 de noviembre de 2023
Amazon FSx 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 FSx para los sistemas de archivos Multi-AZ de ONTAP.	14 de noviembre de 2023
Amazon FSx ConsoleFullAccess : 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 FSx para los sistemas de archivos Multi-AZ de ONTAP.	14 de noviembre de 2023
Amazon FSx FullAccess : actualización de una política existente	Amazon FSx ha añadido nuevos permisos que permiten FSx a Amazon gestionar las configuraciones de red de los sistemas de FSx archivos Multi-AZ de OpenZFS.	9 de agosto de 2023

Cambio	Descripción	Fecha
AWS política gestionada: Amazon FSxServiceRolePolicy : actualización a una política existente	Amazon FSx modificó el <code>cloudwatch:PutMetricData</code> permiso existente para que Amazon FSx publique CloudWatch las métricas en el espacio de AWS/FSx nombres.	24 de julio de 2023
Amazon FSx FullAccess : actualización de una política existente	Amazon FSx actualizó la política para eliminar el <code>fsx:*</code> permiso y añadir <code>fsx</code> acciones específicas.	13 de julio de 2023
Amazon FSx ConsoleFullAccess : actualización de una política existente	Amazon FSx actualizó la política para eliminar el <code>fsx:*</code> permiso y añadir <code>fsx</code> acciones específicas.	13 de julio de 2023
Amazon FSx ConsoleReadOnlyAccess : actualización de una política existente	Amazon FSx ha añadido nuevos permisos para permitir a los usuarios ver las métricas de rendimiento mejoradas y las acciones recomendadas FSx para los sistemas de archivos Windows File Server en la FSx consola de Amazon.	21 de septiembre de 2022
Amazon FSx ConsoleFullAccess : actualización de una política existente	Amazon FSx ha añadido nuevos permisos para permitir a los usuarios ver las métricas de rendimiento mejoradas y las acciones recomendadas FSx para los sistemas de archivos Windows File Server en la FSx consola de Amazon.	21 de septiembre de 2022

Cambio	Descripción	Fecha
Amazon FSx ReadOnlyAccess : comenzó la política de seguimiento	Esta política otorga acceso de solo lectura a todos los FSx recursos de Amazon y a las etiquetas asociadas a ellos.	4 de febrero de 2022
Amazon FSx DeleteServiceLinkedRoleAccess : comenzó la política de seguimiento	Esta política concede permisos administrativos que permiten FSx a Amazon eliminar su función vinculada a servicios para el acceso a Amazon S3.	7 de enero de 2022
Amazon FSx ServiceRolePolicy : actualización de una política existente	Amazon FSx ha añadido nuevos permisos para que Amazon pueda FSx gestionar las configuraciones de red de Amazon FSx para los sistemas de archivos NetApp ONTAP.	2 de septiembre de 2021
Amazon FSx FullAccess : actualización de una política existente	Amazon FSx ha añadido nuevos permisos para que Amazon pueda FSx crear etiquetas en las tablas de EC2 rutas para las llamadas restringidas.	2 de septiembre de 2021
Amazon FSx ConsoleFullAccess : actualización de una política existente	Amazon FSx ha añadido nuevos permisos para permitir a Amazon crear Amazon FSx FSx para los sistemas de archivos Multi-AZ de NetApp ONTAP.	2 de septiembre de 2021

Cambio	Descripción	Fecha
Amazon FSx ConsoleFu llAccess : actualización de una política existente	Amazon FSx ha añadido nuevos permisos para que Amazon pueda FSx crear etiquetas en las tablas de EC2 rutas para las llamadas restringidas.	2 de septiembre de 2021
Amazon FSx ServiceRo lePolicy : actualización de una política existente	Amazon FSx ha añadido nuevos permisos para que Amazon FSx pueda describir y escribir en las secuencias de registro de CloudWatch Logs. Esto es necesario para que los usuarios puedan ver los registros de auditoría de acceso a los archivos de FSx los sistemas de archivos del servidor de archivos de Windows mediante CloudWatc h registros.	8 de junio de 2021

Cambio	Descripción	Fecha
Amazon FSx ServiceRolePolicy : actualización de una política existente	Amazon FSx ha añadido nuevos permisos para que Amazon pueda 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 para Windows File Server mediante Amazon Data Firehose.	8 de junio de 2021
Amazon FSx FullAccess : actualización de 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 de FSx archivos del servidor de archivos de Windows mediante CloudWatch registros.	8 de junio de 2021

Cambio	Descripción	Fecha
Amazon FSx FullAccess: 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 para Windows File Server mediante Amazon Data Firehose.	8 de junio de 2021
Amazon FSx ConsoleFullAccess: actualización de una política existente	Amazon FSx ha añadido nuevos permisos para permitir 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 los directores puedan elegir un grupo de CloudWatch registros existente al configurar la auditoría de acceso a los archivos FSx para un sistema de archivos del servidor de archivos de Windows.	8 de junio de 2021

Cambio	Descripción	Fecha
Amazon FSx ConsoleFu llAccess : actualización de una política existente	Amazon FSx ha añadido nuevos permisos para que los responsables describan los flujos de entrega de Amazon Data Firehose asociados 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 FSx un sistema de archivos para Windows File Server.	8 de junio de 2021
Amazon FSx ConsoleRe adOnlyAccess : actualización de una política existente	Amazon FSx ha añadido nuevos permisos para permitir 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 los directores puedan ver la configuración de auditoría de acceso a los archivos existente FSx para un sistema de archivos del servidor de archivos de Windows.	8 de junio de 2021

Cambio	Descripción	Fecha
Amazon FSx ConsoleReadOnlyAccess : actualización de una política existente	Amazon FSx ha añadido nuevos permisos para que los responsables describan los flujos de entrega de Amazon Data Firehose asociados a la cuenta que realiza la solicitud. Esto es necesario para que los directores puedan ver la configuración de auditoría de acceso a los archivos existente FSx para un sistema de archivos del servidor de archivos de Windows.	8 de junio de 2021
Amazon FSx comenzó a rastrear 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

Accede a tus sistemas de archivos de Amazon FSx for NetApp ONTAP SVMs utilizando el nombre DNS o la dirección IP de uno de sus puntos de conexión, 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 actúa como un firewall virtual para los sistemas de archivos de ONTAP a FSx fin de 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 asociados y SVMs. 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 usar un grupo de seguridad para controlar el acceso a tu sistema de FSx archivos de Amazon, añade 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 tener las reglas de tráfico de red correctas en su grupo de seguridad para asignar el recurso compartido de FSx archivos de su sistema de archivos de Amazon a una carpeta de la instancia de procesamiento compatible.

Para obtener más información sobre las reglas de los grupos de [seguridad, consulte Reglas de grupos](#) de seguridad en la Guía del EC2 usuario de Amazon.

Creación de un grupo de seguridad de VPC

Para crear un grupo de seguridad para Amazon FSx

1. Abre la EC2 consola de Amazon 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. En el campo de origen, debe seleccionar Personalizado e introducir los grupos de seguridad o los intervalos de direcciones IP asociados a las instancias que necesitan acceder a su sistema de archivos FSx de ONTAP, incluidos:
 - Clientes de Linux, Windows y and/or macOS que acceden a los datos de su sistema de archivos a través de NFS, SMB o iSCSI.
 - Cualquier archivo de ONTAP systems/clusters que vaya a vincular a su sistema de archivos (por ejemplo, para usarlo SnapMirror, SnapVault o). FlexCache
 - Cualquier cliente que vaya a utilizar para acceder a la API REST, la CLI o ZAPIs (por ejemplo, una Harvest/Grafana instancia, NetApp Connector o NetApp BlueXP) de ONTAP.

Protocolo	Puertos	Rol
Todos los ICMP	Todos	Hacer ping a la instancia
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 a través de TCP con entramado de NetBIOS

Protocolo	Puertos	Rol
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 interclúster LIFs
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 el acceso de red al sistema de archivos a todos los clientes, puede eliminar todos los grupos de seguridad asociados a las interfaces elastic network del sistema de archivos y sustituirlos por un grupo que no tenga inbound/outbound reglas.

Validación de conformidad de Amazon FSx para NetApp ONTAP

Para saber si un programa de conformidad Servicio de AWS está incluido [Servicios de AWS en el ámbito de aplicación de programas de conformidad específicos](#), consulte [Alcance por programa](#) de de conformidad y elija el programa de conformidad 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:

- [Cumplimiento de seguridad y gobernanza](#): en estas guías se explican las consideraciones de arquitectura y se proporcionan pasos para implementar las características de seguridad y cumplimiento.
- [Referencia de servicios válidos de HIPAA](#): muestra una lista con los servicios válidos de HIPAA. No todos Servicios de AWS cumplen con los requisitos de la HIPAA.
- [AWS Recursos 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](#)— Este Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la [Referencia de controles de Security Hub](#).
- [Amazon GuardDuty](#): Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como la PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- [AWS Audit Manager](#)— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Amazon FSx para NetApp ONTAP y puntos finales de VPC de interfaz ()AWS PrivateLink

Puede mejorar el nivel de seguridad de su VPC configurando Amazon FSx para que utilice un punto de enlace de VPC de interfaz. Los puntos finales de VPC de interfaz cuentan con una tecnología que le permite acceder de forma privada a Amazon FSx APIs sin una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o una conexión. [AWS PrivateLink](#) AWS Direct Connect Las instancias de tu VPC no necesitan direcciones IP públicas para comunicarse con Amazon. FSx APIs El tráfico entre tu VPC y Amazon FSx no sale de la AWS red.

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 para el tráfico a la FSx API de Amazon. Amazon FSx admite puntos de enlace de VPC configurados con tipos de direcciones IP (IPv4 IPv4 y IPv6) de doble pila. Para obtener más información, consulte [Creación de un punto de conexión de VPC de interfaz](#) en la Guía del usuario de Amazon VPC.

Consideraciones sobre los puntos de enlace de FSx VPC de la interfaz de Amazon

Antes de configurar un punto de enlace de VPC de interfaz para Amazon FSx, asegúrese de revisar las [propiedades y limitaciones del punto de enlace de VPC de interfaz en](#) la Guía del usuario de Amazon VPC.

Puedes llamar a cualquiera de las operaciones de la FSx API de Amazon desde tu 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 Amazon FSx APIs, consulta [Acciones](#) en la referencia de la FSx API de Amazon.

Consideraciones sobre el emparejamiento de VPC

Puede conectar otros VPCs a la VPC con puntos finales de la VPC de interfaz mediante el emparejamiento de VPC. El emparejamiento de VPC es una conexión de red entre dos VPCs. Puede establecer una conexión de emparejamiento de VPC entre sus dos VPCs VPC o con una VPC de otra. Cuenta de AWS También VPCs puede estar en dos tipos diferentes. Regiones de AWS

El tráfico entre pares VPCs permanece en la AWS red y no atraviesa la Internet pública. Una vez VPCs interconectados, los recursos como las instancias de Amazon Elastic Compute Cloud (Amazon EC2) de ambas VPCs pueden acceder a la FSx API de Amazon a través de los puntos de enlace de la VPC de la interfaz creados en uno de los VPCs

Creación de un punto de enlace de VPC de interfaz para la API de Amazon FSx

Puede crear un punto de enlace de VPC para la FSx API de Amazon 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 enlace de VPC de interfaz para Amazon FSx, utilice una de las siguientes opciones:

- **com.amazonaws.*region*.fsx**— Crea un punto final para las operaciones de la FSx API de Amazon.
- **com.amazonaws.*region*.fsx-fips**— Crea un punto final para la FSx API de Amazon que cumple con la [Norma 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 habilitas el DNS privado para el punto de conexión, puedes realizar solicitudes de API a Amazon FSx con el punto de enlace de la VPC utilizando su nombre de DNS predeterminado Región de AWS, por ejemplo. `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 puntos de conexión de VPC para Amazon FSx

Para controlar el acceso a la FSx API de Amazon, puedes adjuntar una política AWS Identity and Access Management (IAM) a tu punto de conexión de VPC. La política especifica lo siguiente:

- La entidad principal que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos en los que se pueden llevar a cabo las acciones.

Para 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 NetApp ONTAP

La infraestructura AWS global se basa en distintas zonas Regiones de AWS 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 que ayudan a 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 de su sistema de archivos Amazon FSx for 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 for NetApp ONTAP. Amazon FSx guarda las copias de seguridad automatizadas de sus volúmenes de acuerdo con el período de retención de copias de seguridad que especifique. 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 [Protección de datos con copias de seguridad de volúmenes](#).

Instantáneas

Amazon FSx crea copias instantáneas de los volúmenes de Amazon FSx for NetApp ONTAP. 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 [Protección de los datos con instantáneas](#).

Zonas de disponibilidad

Los sistemas de archivos Amazon FSx for NetApp ONTAP están diseñados para proporcionar 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 replica FSx automáticamente sus datos para protegerlos de fallos de los componentes, supervisa continuamente 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 for 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 [Opciones de disponibilidad, durabilidad e implementación](#).

Sistemas de archivos Single-AZ

Los sistemas de archivos Amazon FSx for 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 [Opciones de disponibilidad, durabilidad e implementación](#).

Seguridad de infraestructuras en Amazon FSx para NetApp ONTAP

Como servicio gestionado, Amazon FSx for 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.

Utilizas 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 puedes utilizar [AWS Security Token Service](#) (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Utilice NetApp ONTAP Vscan con FSx ONTAP

Puede utilizar la función NetApp ONTAP's Vscan para ejecutar software antivirus de terceros compatible. Para obtener más información, consulte los siguientes recursos para cada una de las soluciones compatibles.

- Deep Instinct: [soluciones asociadas a Vscan](#) y documentación de [Deep Instinct](#) (1)
- SentinelOne — [Soluciones asociadas de Vscan](#) y [SentinelOne Singularity Cloud Data Security](#)
- Symantec: [soluciones asociadas a Vscan](#) y [motor de protección de Symantec](#)
- Trellix (anteriormente McAfee): [soluciones para socios de Vscan y documentación de productos de Trellix](#)
- Trend Micro: [soluciones asociadas a Vscan](#)

Note

¹ Debe iniciar sesión en el portal de Deep Instinct para ver su documentación.

Usuarios y roles de ONTAP

NetApp ONTAP incluye una sólida y extensible capacidad de control de acceso basado en roles (RBAC). Los roles de ONTAP definen las capacidades y los privilegios de los usuarios al utilizar la CLI y la API de REST de ONTAP. Cada rol define un nivel diferente de capacidades y privilegios administrativos. Al utilizar la API ONTAP REST y la CLI, se asignan funciones a los usuarios con el fin de controlar su acceso a FSx los recursos de ONTAP. Hay ONTAP funciones disponibles por separado FSx para los usuarios del sistema de archivos de ONTAP y para los usuarios de máquinas virtuales de almacenamiento (SVM).

Al crear un sistema de archivos FSx para ONTAP, se crea un ONTAP usuario predeterminado en el nivel del sistema de archivos y en el nivel de SVM. Puede crear usuarios adicionales del sistema de archivos y de la SVM, como así también puede crear roles de SVM adicionales para satisfacer las necesidades de la organización. En este capítulo, se explican los usuarios y roles de ONTAP y se proporcionan procedimientos detallados para crear usuarios y roles de SVM adicionales.

Roles y usuarios del administrador del sistema de archivos

El usuario predeterminado del sistema de archivos de ONTAP es `fsxadmin`, quien tiene el rol de `fsxadmin` asignado. Hay dos roles predefinidos que puede asignar a los usuarios del sistema de archivos, que se enumeran a continuación:

- **fsxadmin:** los administradores con este rol tienen derechos ilimitados en el sistema de ONTAP. Pueden configurar todos los recursos del sistema de archivos y de nivel SVM disponibles en FSx los sistemas de archivos ONTAP.
- **fsxadmin-readonly:** los administradores con este rol pueden ver todo en el nivel del sistema de archivos, pero no pueden realizar ningún cambio.

Este rol es adecuado para usarse con aplicaciones de supervisión, como NetApp Harvest, ya que tiene acceso de solo lectura a todos los recursos disponibles y sus propiedades, pero no puede realizar ningún cambio en ellos.

Puede crear usuarios adicionales del sistema de archivos y asignarles el rol `fsxadmin` o `fsxadmin-readonly`. No puede crear nuevos roles ni modificar los roles existentes. Para obtener más información, consulte [Creación de nuevos usuarios de ONTAP para la administración del sistema de archivos y la SVM](#).

En la siguiente tabla, se describe el nivel de acceso que tienen los roles de administrador del sistema de archivos a los comandos y directorios de comandos de la CLI y la API de REST de ONTAP.

Nombre del rol	Nivel de acceso	A los siguientes comandos o directorios de comandos
<code>fsxadmin</code>	<code>all</code>	Todos los directorios de comandos están disponibles en ONTAP FSx
<code>fsxadmin-readonly</code>	<code>all</code>	<code>security login</code> <code>password</code> Solo para administrar la propia cuenta de usuario, la contraseña local y la información clave

Nombre del rol	Nivel de acceso	A los siguientes comandos o directorios de comandos
	none	security
	solo lectura	Todos los demás directorios de comandos están disponibles en FSx ONTAP

Roles y usuarios de administrador de la SVM

Cada SVM tiene un dominio de autenticación independiente y sus propios administradores pueden administrarlo de forma independiente. Para cada SVM del sistema de archivos, el usuario predeterminado es vsadmin, al que se le ha asignado el rol vsadmin de forma predeterminada. Además del rol vsadmin, hay otros roles de SVM predefinidos que proporcionan permisos específicos que puede asignar a los usuarios de SVM. También puede crear roles personalizados que proporcionen el nivel de control de acceso que mejor se adapte a las necesidades de la organización.

Los roles predefinidos de los administradores de SVM y sus capacidades son las siguientes:

Nombre del 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 LUNs • Realice SnapLock operaciones, excepto la eliminación privilegiada • Configurar protocolos: NFS, SMB e iSCSI • Configurar los servicios: DNS, LDAP y NIS • Monitorear trabajos

Nombre del rol	Capacidades
	• 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 LUNs • 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 LUNs • 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 • Gestionar SnapMirror las relaciones y las copias instantáneas • Ver los volúmenes y la información de la red

Nombre del 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 • Vea los volúmenes y LUNs • Ver los servicios y protocolos

Para obtener más información sobre cómo crear un nuevo, consulte [Creación de roles de SVM](#).

Uso de un Active Directory para autenticar usuarios de ONTAP

Puede autenticar el acceso de los usuarios del dominio Windows Active Directory a un FSx sistema de archivos ONTAP y a un SVM. Debe realizar las siguientes tareas para que las cuentas de Active Directory puedan acceder a su sistema de archivos:

- Debe configurar el acceso del controlador de dominio de Active Directory a la SVM.

La SVM que use para configurar como puerta de enlace o túnel para el acceso al controlador de dominio de Active Directory debe tener el CIFS activado, estar unida a un Active Directory o ambas

opciones. Si no está habilitando el CIFS y solo va a unir la SVM de túnel a un Active Directory, corrobore que la SVM esté unida al Active Directory. Para obtener más información, consulte [Cómo funciona SVMs la unión a Microsoft Active Directory](#).

- Debe habilitar una cuenta de usuario de dominio de Active Directory para acceder al sistema de archivos.

Puede usar la autenticación por contraseña o la autenticación por clave pública SSH para los usuarios del dominio de Windows que acceden a la CLI o a la API de REST de ONTAP.

Para ver los procedimientos que describen cómo configurar la autenticación de Active Directory para los administradores de sistemas de archivos y la SVM, consulte [Configuración de la autenticación con Active Directory para usuarios de ONTAP](#).

Creación de nuevos usuarios de ONTAP para la administración del sistema de archivos y la SVM

Cada usuario de ONTAP está asociado a una SVM o al sistema de archivos. Los usuarios del sistema de archivos con el rol `fsxadmin` pueden crear nuevos roles y usuarios de SVM mediante el comando [security login create](#) de la CLI de ONTAP.

El comando `security login create` 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. Si lo desea, puede incluir un nombre de rol de control de acceso. Si se usa un nombre de grupo del Active Directory, el protocolo ligero de acceso a directorios (LDAP) o el servicio de información de red (NIS), el método de inicio de sesión da 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 comandos autorizados para grupos individuales.

Para obtener información sobre cómo crear un usuario nuevo de ONTAP, consulte [Creación de usuarios de ONTAP](#).

Temas

- [Creación de usuarios de ONTAP](#)
- [Creación de roles de SVM](#)
- [Configuración de la autenticación con Active Directory para usuarios de ONTAP](#)

- [Configuración de la autenticación de clave pública](#)
- [Actualización de los requisitos de contraseña para los roles del sistema de archivos y la SVM](#)
- [Se produce un error al actualizar la contraseña de la cuenta fsxadmin](#)

Creación de usuarios de ONTAP

Cómo crear un nuevo usuario de la SVM o del sistema de archivos (CLI de ONTAP)

Solo los usuarios del sistema de archivos con el rol `fsxadmin` pueden crear nuevos usuarios de la SVM y del sistema de archivos.

1. Para acceder a la ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando. 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 [Administrar sistemas de archivos con el ONTAP CLI](#).

2. Utilice el comando `security login create` ONTAP CLI para crear una nueva cuenta de usuario en su sistema FSx de archivos ONTAP o SVM.

Introduzca los datos de los marcadores de posición del ejemplo para definir las siguientes propiedades obligatorias:

- `-vserver`: especifica el nombre de la SVM en la que desea crear el nuevo rol o usuario de SVM. Si va a crear un rol o usuario del sistema de archivos, no especifique una SVM.
- `-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 autenticación de `domain` y las aplicaciones de `ontapi` y `ssh`.
- `-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 iniciar sesión. Entre los valores posibles se incluyen:
 - `dominio`: se usa para la autenticación con Active Directory

- contraseña: se usa para la autenticación con contraseña
- clave pública: se usa para la autenticación con clave pública
- `-role`: especifica el nombre del rol 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 usar uno o más de los siguientes parámetros con el comando:

- `[-comment]`: se usa para incluir una anotación o un comentario en 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 siguientes métodos:
 - contraseña: se usa para la autenticación con contraseña
 - clave pública: se usa para la autenticación con clave pública
 - nsswitch: se usa para la autenticación NIS o LDAP
 - nada: el valor predeterminado si no especifica uno

```
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
```

El siguiente comando crea un nuevo usuario del sistema de archivos `new_fsxadmin` con el rol `fsxadmin-readonly` asignado, usando SSH con una contraseña para iniciar sesión. Cuando se solicite, proporcione una contraseña para el usuario.

```
Fsx0123456:> security login create -user-or-group-name new_fsxadmin -application  
ssh -authentication-method password -role fsxadmin-readonly
```

```
Please enter a password for user 'new_fsxadmin':  
Please enter it again:
```

```
Fsx0123456:>
```

3. El siguiente comando crea un nuevo usuario de SVM `new_vsadmin` en la SVM de `fsx` con el rol `vsadmin_readonly`, configurado para usar SSH con una contraseña para iniciar sesión. Cuando se solicite, proporcione una contraseña para el usuario.

```
Fsx0123456::> security login create -vserver fsx -user-or-group-name new_vsadmin -
application ssh -authentication-method password -role vsadmin-readonly
```

Please enter a password for user 'new_vsadmin':

Please enter it again:

```
Fsx0123456::>
```

- El siguiente comando crea un nuevo usuario del sistema de archivos de solo lectura harvest2-user que la aplicación NetApp Harvest utilizará para recopilar métricas de rendimiento y capacidad. Para obtener más información, consulte [Supervisión de FSx los sistemas de archivos ONTAP mediante Harvest y Grafana](#).

```
Fsx0123456::> security login create -user-or-group-name harvest2-user -application
ssh -role fsxadmin-readonly -authentication-method password
```

Cómo ver la información de todos los usuarios del sistema de archivos y la SVM

- Utilice el siguiente comando para ver toda la información de inicio de sesión de su sistema de archivos y. SVMs

```
Fsx0123456::> security login show
```

Vserver: Fsx0123456

User/Group Name	Application	Authentication Method	Role Name	Acct Locked	Second Authentication Method
autosupport	console	password	autosupport	no	none
fsxadmin	http	password	fsxadmin	no	none
fsxadmin	ontapi	password	fsxadmin	no	none
fsxadmin	ssh	password	fsxadmin	no	none
fsxadmin	ssh	publickey	fsxadmin	-	none
new_fsxadmin	ssh	password	fsxadmin-readonly	no	none

Vserver: fsx

User/Group Name	Application	Authentication Method	Role Name	Acct Locked	Second Authentication Method

```

-----
new_vsadmin  ssh      password  vsadmin-readonly no      none
vsadmin      http     password  vsadmin      yes     none
vsadmin      ontapi   password  vsadmin      yes     none
vsadmin      ssh      password  vsadmin      yes     none
10 entries were displayed.

Fsx0123456::>

```

Creación de roles de SVM

Cada SVM que cree tiene un administrador de SVM predeterminado al que se le asigna el rol `vsadmin` predefinido. Además del conjunto de [roles de SVM predefinidas](#), puede crear nuevos roles de SVM. Si necesita crear nuevos roles para la SVM, use el comando `security login role create` de la CLI de ONTAP. Este comando está disponible para los administradores de sistemas de archivos que tengan el rol `fsxadmin`.

Cómo crear un nuevo rol de SVM (CLI de ONTAP)

1. Puede crear un nuevo rol de SVM mediante el comando [security login role create](#) de la ONTAP CLI:

```

Fsx0123456::> security login role create -vserver vs1.example.com -role vol_role -
cmddirname volume

```

2. Especifique los parámetros en el comando de la siguiente manera:
 - `-vserver` el nombre de la SVM
 - `-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`.

El siguiente comando crea un rol de control de acceso denominado “admin” para el servidor virtual `vs1.example.com`. El rol tiene acceso total al comando “volume”, pero solo dentro del agregado “aggr0”.

```
Fsx0123456::>security login role create -role admin -cmddirname volume -query "-aggr aggr0" -access all -vserver vs1.example.com
```

Configuración de la autenticación con Active Directory para usuarios de ONTAP

Use la CLI de ONTAP para configurar el uso de la autenticación de Active Directory para los usuarios del sistema de archivos y la SVM de ONTAP.

Debe ser un administrador del sistema de archivos con el rol `fsxadmin` para usar los comandos de este procedimiento.

Cómo configurar la autenticación de Active Directory para usuarios de ONTAP (CLI de ONTAP)

Los comandos de este procedimiento están disponibles para los usuarios del sistema de archivos con el rol `fsxadmin`.

1. Para acceder a la ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando. 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 [Administrar sistemas de archivos con el ONTAP CLI](#).

2. Use el comando [security login domain-tunnel create](#) como se muestra para establecer un túnel de dominio para autenticar a los usuarios de Windows Active Directory. *svm_name* Sustitúyalo por el nombre del SVM que está utilizando para el túnel de dominio.

```
FsxId0123456::> security login domain-tunnel create -vserver svm_name
```

3. Use el comando [security login create](#) para crear cuentas de usuario de dominio de Active Directory que accederán al sistema de archivos.

Especifique los parámetros en el comando de la siguiente manera:

- `-vserver`: el nombre de la SVM configurada con CIFS y está unida al Active Directory. Se usará como túnel para autenticar a los usuarios del dominio de Active Directory en el sistema de archivos, 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 usado para iniciar sesión. Entre los valores posibles se incluyen:
 - `dominio`: para la autenticación con 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`.

En el siguiente ejemplo, se crea una cuenta de usuario de dominio de Active Directory CORP\Admin para el sistema de archivos filesystem1.

```
FsxD012345::> security login create -vserver filesystem1 -username CORP\Admin -  
application ssh -authmethod domain -role fsxadmin
```

En el siguiente ejemplo, se crea la cuenta de usuario CORP\Admin con autenticación con clave pública.

```
FsxD0123456ab::> security login create -user-or-group-name "CORP\Admin" -  
application ssh -authentication-method publickey -role fsxadmin  
Warning: To use public-key authentication, you must create a public key for user  
"CORP\Admin".
```

Cree una clave pública para el usuario CORP\Admin mediante el siguiente comando:

```
FsxD0123456ab::> security login publickey create -username "CORP  
\Admin" -publickey "ecdsa-sha2-nistp256 SECRET_STRING_HERE_IS_REDACTED=  
cwaltham@b0be837a91bf.ant.amazon.com"
```

Cómo iniciar sesión en el sistema de archivos mediante SSH con credenciales de Active Directory

- 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.

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
<code>-vserver</code> (opcional)	El nombre de la SVM a la que accede la cuenta. Si va a configurar la autenticación con clave pública de SSH para los usuarios del sistema de archivos, no incluya <code>-vserver</code> .
<code>-username</code>	El nombre de usuario de la cuenta. El valor predeterminado, <code>admin</code> , es el nombre predeterminado del administrador del clúster.
<code>-index</code>	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.
<code>-publickey</code>	La clave pública de OpenSSH. Escriba la clave entre comillas.
<code>-role</code>	El rol de control de acceso que se asigna a la cuenta.
<code>-comment</code> (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.

Actualización de los requisitos de contraseña para los roles del sistema de archivos y la SVM

Puede actualizar los requisitos de contraseña de un sistema de archivos o un rol de SVM mediante el comando [security login role config modify](#) de la CLI de ONTAP. Este comando solo está disponible para las cuentas de administrador del sistema de archivos que tengan el rol `fsxadmin`. Al modificar los requisitos de contraseña, el sistema avisará si hay algún usuario con ese rol que se vea afectado por el cambio.

En el siguiente ejemplo, se modifica el requisito de longitud mínima de la contraseña a 12 caracteres para los usuarios con el rol `vsadmin-readonly` en la SVM de `fsx`. En este ejemplo, hay usuarios con este rol.

```
FsxId0123456::> security login role config modify -role vsadmin-readonly -vserver fsx -
passwd-minlength 12
```

El sistema muestra la siguiente advertencia debido a los usuarios existentes:

```
Warning: User accounts with this role exist. Modifications to the username/password
restrictions on this role could result in non-compliant user
accounts.
Do you want to continue? {y|n}:

FsxId0123456::>
```

Se produce un error al actualizar la contraseña de la cuenta **fsxadmin**

Al actualizar la contraseña del usuario **fsxadmin**, es posible que reciba un error si no cumple con los requisitos de contraseña configurados en el sistema de archivos. Puede consultar los requisitos de contraseña mediante el comando `security login role config show` de la CLI o la API de REST de ONTAP.

Cómo ver los requisitos de contraseña de un sistema de archivos o un rol de SVM

1. Para acceder a la ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando. 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 [Administrar sistemas de archivos con el ONTAP CLI](#).

2. El comando `security login role config show` devuelve los requisitos de contraseña para un sistema de archivos o un rol de SVM.

```
FsxId0123456:> security login role config show -role fsxadmin -  
fields password_requirement_fields
```

Para el parámetro `-fields`, especifique cualquiera o todo lo siguiente:

- `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:

```
FsxId0123456::> 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
```

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
FsxId0123456	fsxadmin	3	enabled	0	0	0	0	0	0
		unlimited		0		0		0	
		unlimited							

Cuotas

A continuación, puede obtener información sobre las cuotas cuando trabaje con Amazon FSx para NetApp ONTAP.

Temas

- [Cuotas que puede aumentar](#)
- [Cuotas de recursos para cada sistema de archivos](#)

Cuotas que puede aumentar

A continuación se muestran las cuotas de Amazon FSx para NetApp ONTAP por Región de AWS cada una Cuenta de AWS de ellas que puedes aumentar.

Recurso	Predeterminado/a	Descripción
ONTAP sistemas de archivos	100	El número máximo de sistemas de archivos de Amazon FSx for NetApp ONTAP que puedes crear en esta cuenta.
ONTAP Capacidad de almacenamiento en SSD	524.288	La cantidad máxima de capacidad de almacenamiento en SSD (en GiB) para todos los sistemas de archivos de Amazon FSx for NetApp ONTAP que puedes tener en esta cuenta.
ONTAP capacidad de rendimiento	10 240	La cantidad máxima de capacidad de procesamiento (en MBps) para todos los sistemas de archivos de Amazon FSx for NetApp

Recurso	Predeterminado/a	Descripción
		ONTAP que puede tener en esta cuenta.
ONTAP IOPS en SSD	1 000 000	La cantidad máxima de IOPS de SSD para todos los sistemas de archivos de Amazon FSx for NetApp ONTAP que puedes tener en esta cuenta.
ONTAP copias de seguridad	10 000	El número máximo de copias de seguridad por volumen iniciadas por el usuario para todos los sistemas de archivos de Amazon FSx for NetApp ONTAP que puede tener en un. Cuenta de AWS

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. En Crear caso, seleccione 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 FSx cuota que desea aumentar y el valor al que desea aumentarla, si lo 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

La siguiente tabla muestra las cuotas en 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	- Sistemas de archivos Single-AZ de segunda generación: 512 TiB por par de HA, hasta 1 PiB - Sistemas de archivos Multi-AZ de segunda generación: 512 TiB - Sistemas de archivos de primera generación: 192 TiB
El máximo de IOPS de SSD	Sistema de archivos de segunda generación: 200 000 por par de HA (hasta 12 pares) para Single-AZ 200 000 en total para Multi-AZ Sistemas de archivos de primera generación: 160 000 en la región este de EE. UU. (Ohio), región este de EE. UU. (Norte de Virginia), región oeste de EE. UU. (Oregón) y Europa (Irlanda)

Recurso	El límite por sistema de archivos • 80 000 en todos los demás Regiones de AWS lugares donde FSx ONTAP esté disponible
La capacidad de rendimiento mínima	• Sistemas de archivos de segunda generación (1 par HA): 384 MBps • Sistemas de archivos de segunda generación (2 o más pares de alta disponibilidad): 1.536 MBps por par de alta disponibilidad • Sistemas de archivos de primera generación: 128 MBps
La capacidad de rendimiento máxima	Sistema de archivos de segunda generación: • 73.728 1 MBps para Single-AZ • 6.144 para Multi-AZ MBps Sistemas de archivos de primera generación: • 4.096 MBps ² en la región EE.UU. Este (Ohio), Región EE.UU. Este (Norte de Virginia), Región EE.UU. Oeste (Oregón) y Europa (Irlanda) • 2.048 MBps en todos los demás Regiones de AWS lugares donde está disponible FSx ONTAP

Recurso	El límite por sistema de archivos
Número máximo de volúmenes	• Sistemas de archivos de segunda generación (1 par de HA): 500 • Sistemas de archivos de segunda generación (2 o más pares de HA): 1000 • Sistemas de archivos de primera generación: 500
Número máximo de instantáneas	1023 por volumen ³
Cantidad máxima de copias de seguridad	4091 por volumen ⁴

Recurso	El límite por sistema de archivos
Número máximo de SVMs	Sistemas de archivos de segunda generación con 1 par de HA: • 6 (384 MBps de la capacidad de rendimiento) • 6 (768 MBps de la capacidad de rendimiento) • 14 (1.536 de MBps la capacidad de rendimiento) • 14 (3.072 de la capacidad MBps de rendimiento) • 24 (6.144 de la capacidad MBps de rendimiento) Sistemas de archivos de segunda generación con 2 a 12 pares de HA: • 5 Sistemas de archivos de primera generación: • 6 (128 de capacidad de MBps rendimiento) • 6 (256 MBps capacidad de rendimiento) • 14 (512 de MBps capacidad de rendimiento) • 14 (capacidad de MBps rendimiento de 1.024) • 24 (capacidad de rendimiento de 2.048 MBps)

Recurso	El límite por sistema de archivos
	• 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
Cantidad máxima de rutas admitidas por sistema de archivos	50 5
Número máximo de conexiones de cliente por servidor de archivos ⁶	100 000

Note

¹ En un sistema de archivos Single-AZ de segunda generación con 12 pares de alta disponibilidad (6.144 MBps por par de alta disponibilidad). Para obtener más información, consulte [Administración de pares de alta disponibilidad \(HA\)](#).

² Para aprovisionar el 4% GBps de la capacidad de rendimiento, su sistema de archivos de primera generación FSx para ONTAP requiere una configuración máxima de IOPS de SSD (160 000) y una capacidad mínima de almacenamiento SSD de 5 120 GiB si es compatible. Región de AWS Para obtener más información sobre los que Regiones de AWS admiten una capacidad de rendimiento de 4.096 unidades, consulte. MBps [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 4091 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 del volumen.

⁵ Puede configurar hasta 50 rutas por sistema de archivos en cualquier momento. Cuando alcance este límite, debe eliminar una ruta existente antes de poder configurar una nueva

ruta. El número de rutas que tiene su sistema de archivos viene determinado por el número de rutas SVMs que tiene y el número de tablas de rutas asociadas a él. Puede determinar el número actual de rutas a un sistema de archivos mediante la siguiente ecuación: (1 más el número de SVMs en el sistema de archivos) * (tablas de rutas asociadas al sistema de archivos).

⁶ Una conexión de cliente se define como una conexión TCP única a un servidor de archivos determinado. Hay un servidor de archivos activo por cada par de alta disponibilidad en un sistema de archivos. Un cliente puede tener varias conexiones TCP a un servidor de archivos. Por ejemplo, si un cliente utiliza múltiples rutas.

Solución de problemas de Amazon FSx for NetApp ONTAP

Utilice las siguientes secciones como ayuda para solucionar los problemas de los sistemas de archivos FSx de ONTAP.

Temas

- [Su sistema de archivos está en un estado MISCONFIGURED](#)
- [No puede acceder al sistema de archivos](#)
- [La máquina virtual de almacenamiento \(SVM\) está en un estado MISCONFIGURED](#)
- [No puede unir una máquina virtual de almacenamiento \(SVM\) a Active Directory](#)
- [No puede eliminar una máquina virtual de almacenamiento o un volumen](#)
- [El volumen está en un MISCONFIGURED estado](#)
- [Su volumen tiene una capacidad de almacenamiento insuficiente](#)
- [Las copias de seguridad fallan por una capacidad de volumen insuficiente](#)
- [Solución de problemas de red](#)

Su sistema de archivos está en un estado **MISCONFIGURED**

Existen varias causas posibles por las que un sistema de archivos esté en estado MISCONFIGURED y cada una tiene su propia resolución, como se indica a continuación.

Temas

- [La cuenta de propietario de la VPC ha deshabilitado el uso compartido de VPC Multi-AZ](#)
- [No puede crear una SVM nueva en un sistema de archivos Multi-AZ](#)
- [El nivel de almacenamiento SSD de su sistema de archivos está lleno en más del 90%](#)

La cuenta de 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 VPC ha desactivado la compatibilidad con el uso compartido de VPC Multi-AZ para los sistemas de archivos ONTAP. FSx
- La cuenta propietaria ha dejado de compartir la subred de VPC.

Si la cuenta propietaria ha dejado de compartir la subred de VPC, aparecerá el siguiente mensaje en la consola de ese sistema de archivos:

The vpc ID *vpc-012345abcde* does not exist

Para resolver el problema, debe ponerse en contacto con la cuenta propietaria que compartió la subred de VPC con usted. Para obtener más información, consulte [Creación de sistemas de archivos FSx para ONTAP en subredes compartidas](#).

No puede crear una SVM nueva 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 VPC ha desactivado la compatibilidad con el uso compartido de VPC Multi-AZ para los sistemas de archivos ONTAP. FSx
- La cuenta propietaria ha dejado de compartir la subred de VPC.

Para resolver el problema, debe ponerse en contacto con la cuenta propietaria que compartió la subred de VPC con usted. Para obtener más información, consulte [Creación de sistemas de archivos FSx para ONTAP en subredes compartidas](#).

El nivel de almacenamiento SSD de su sistema de archivos está lleno en más del 90%

El nivel de almacenamiento SSD de su sistema de archivos Single-AZ o Multi-AZ está actualmente lleno en más del 90%. Le recomendamos que no utilice más del 80 % del nivel de almacenamiento en SSD de forma continua. Si no libera espacio en el nivel de almacenamiento SSD antes del siguiente período de mantenimiento del sistema de archivos, FSx ONTAP reducirá temporalmente el rendimiento del sistema de archivos mientras dure la operación de aplicación de parches. Esto se hace para garantizar que los procesos de mantenimiento en segundo plano puedan completarse en un período de tiempo razonable. Para evitarlo, reduzca la utilización de su nivel de almacenamiento SSD a menos del 90%. Puedes reducir el uso de la SSD de varias maneras, entre ellas:

- Aumentar la capacidad de almacenamiento en SSD de su sistema de archivos.
- Eliminando datos innecesarios.
- Eliminando las instantáneas de volumen innecesarias.

Para obtener más información, consulte [Administración de la capacidad de almacenamiento](#).

No puede acceder al sistema de archivos

En esta sección se describen los problemas y las soluciones relacionados con la imposibilidad de acceder al sistema de archivos.

Temas

- [A su sistema de archivos Multi-AZ le faltan etiquetas de tabla de rutas](#)
- [Su sistema de archivos tiene más de 50 rutas](#)
- [A su sistema de archivos le faltan rutas a uno o más servidores de archivos](#)
- [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 la VPC del sistema de archivos carece de las reglas de entrada requeridas](#)
- [El grupo de seguridad de la VPC de la instancia informática 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 no FSx puede actualizar la tabla de rutas para 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](#)

A su sistema de archivos Multi-AZ le faltan etiquetas de tabla de rutas

Amazon FSx administra las tablas de enrutamiento de VPC para sistemas de archivos Multi-AZ mediante la autenticación basada en etiquetas. En este momento, a una o más tablas de rutas asociadas a su sistema de archivos les faltan estas etiquetas de tabla de rutas. Estas tablas de rutas se etiquetan con `Key: AmazonFSx; Value: ManagedByAmazonFSx`. Si no agrega estas etiquetas manualmente antes del siguiente período de mantenimiento, los clientes de las subredes asociadas a las tablas de enrutamiento a los que les falten las etiquetas perderán temporalmente el acceso al sistema de archivos mientras dure la operación de aplicación de parches. Para evitarlo, añada manualmente las etiquetas de la tabla de rutas que faltan.

Para obtener más información, consulte [Actualizar sistemas de archivos](#).

Su sistema de archivos tiene más de 50 rutas

Su sistema de archivos tiene actualmente más de 50 rutas asociadas. Si no elimina algunas de estas rutas antes del siguiente período de mantenimiento programado del sistema de archivos, el proceso de conmutación por error puede tardar más de lo normal. Para evitarlo, reduzca el número de rutas a menos de 50. Las siguientes son medidas que puede tomar para reducir la cantidad de rutas asociadas a su sistema de archivos:

- Eliminar cualquier exceso de rutas
- Reducir el número de archivos SVMs asociados al sistema de archivos
- Reducir el número de tablas de rutas asociadas al sistema de archivos

Para obtener más información, consulte [Actualizar sistemas de archivos](#) y [Eliminación de máquinas virtuales de almacenamiento \(SVM\)](#).

A su sistema de archivos le faltan rutas a uno o más servidores de archivos

Actualmente, a su sistema de archivos le faltan rutas hacia uno o más servidores de archivos, y las tablas de rutas existentes no tienen espacio suficiente para agregar nuevas entradas en la tabla de rutas. Si no agrega las rutas que faltan antes del siguiente período de mantenimiento programado del sistema de archivos, todos los clientes conectados se desconectarán mientras dure la operación de aplicación de parches. Para evitarlo, añada las rutas que faltan.

Para obtener más información, consulte [Actualizar sistemas de archivos](#) y [Cuotas](#).

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. Crea un nuevo sistema de archivos y no modifiques ni elimines la interfaz de FSx red de Amazon. 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 desconecta FSx automáticamente cualquier dirección IP elástica, que es una dirección IP pública accesible desde Internet y 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 la 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 la VPC de la instancia informática 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 finales 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 principal de la VPC. Si lo desea, puede especificar una o más tablas de rutas para FSx que Amazon las utilice al crear su 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 [Actualizar sistemas de archivos](#).

Amazon no FSx puede actualizar la tabla de rutas para 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 se etiquetan con Key: AmazonFSx; Value: ManagedByAmazonFSx. Al crear o actualizar sistemas FSx de archivos Multi-AZ de ONTAP, le AWS CloudFormation recomendamos que añada la etiqueta manualmente. Key: AmazonFSx; Value: ManagedByAmazonFSx

Si no puede acceder al 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 [Actualizar sistemas 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, aparecerá el siguiente mensaje en la consola de ese sistema de archivos:

```
The vpc ID vpc-012345abcde does not exist
```

Debe comunicarse con la cuenta propietaria para que vuelvan a compartir la subred con usted.

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 [Acceder a sus FSx datos de ONTAP](#).

La máquina virtual de almacenamiento (SVM) está en un estado **MISCONFIGURED**

Existen varias causas posibles por las que una máquina virtual de almacenamiento entre en un MISCONFIGURED estado, cada una con su propia resolución, como se indica a continuación.

Su SVM tiene un volumen fuera de línea

El sistema de archivos contiene un volumen que está desconectado. Le recomendamos que mantenga los volúmenes en línea de forma continua. Si no pones este volumen en línea antes del siguiente período de mantenimiento de tu sistema de archivos, Amazon FSx lo pondrá en línea temporalmente mientras dure la operación de aplicación de parches. Para evitarlo, conecte el volumen o elimínelo.

Para volver a poner en línea un volumen sin conexión, usa la [volume online](#) ONTAP Comando CLI, como se muestra en el siguiente ejemplo. Si solo existe un SVM (Vserver), no es necesario que especifique el `-vserver` parámetro.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

Su SVM tiene un volumen fuera de línea con un LUN iSCSI o un espacio de nombres /TCP NVMe

El sistema de archivos contiene un volumen que se encuentra en un estado restringido. Le recomendamos que mantenga los volúmenes en línea de forma continua. Si no pones este volumen en línea antes del siguiente período de mantenimiento de tu sistema de archivos, Amazon FSx lo pondrá en línea temporalmente mientras dure la operación de aplicación de parches. Para evitarlo, conecte el volumen o elimínelo.

Para volver a poner en línea un volumen sin conexión, usa la [volume online](#) ONTAP Comando CLI, como se muestra en el siguiente ejemplo. Si solo existe un SVM (Vserver), no es necesario que especifique el `-vserver` parámetro.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

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 [Cómo funciona SVMs la unión 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.](#)
- [El SVM ya está unido a otro Active Directory](#)

- [Amazon no FSx puede conectarse a los controladores de dominio de Active Directory porque el nombre NetBIOS de la SVM ya está en uso](#)
- [Amazon no FSx puede comunicarse con tus controladores de dominio de Active Directory](#)
- [Amazon no FSx puede conectarse a Active Directory debido a que no se cumplen los requisitos de puerto o los permisos de la cuenta de servicio](#)
- [Amazon no FSx puede conectarse a los controladores de dominio de Active Directory porque las credenciales de la cuenta de servicio no son válidas](#)
- [Amazon no FSx puede conectarse a los controladores de dominio de Active Directory porque las credenciales de la cuenta de servicio son insuficientes](#)
- [Amazon no FSx puede comunicarse con sus servidores DNS o controladores de dominio de Active Directory](#)
- [Amazon no FSx puede comunicarse con su Active Directory debido a un nombre de dominio de Active Directory no válido.](#)
- [La cuenta de servicio no puede acceder al grupo de administradores especificado en la configuración de SVM Active Directory](#)
- [Amazon no FSx puede conectarse a los controladores de dominio de Active Directory porque la unidad organizativa especificada no existe o no es accesible](#)

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 [Conexión SVMs a Active Directory mediante la API AWS Management Console y AWS 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 con 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 [Conexión SVMs a Active Directory mediante la API AWS Management Console y AWS CLI](#) para volver a intentar unir el SVM a su AD nuevo.

Amazon no FSx 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 [Conexión SVMs a Active Directory mediante la API AWS Management Console y AWS 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 no FSx puede comunicarse con tus 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, asegúrate de que el tráfico de red esté permitido entre Amazon FSx y tus controladores de dominio. A continuación, vuelva a intentar unir el SVM a su Active Directory.

Para resolver este problema, siga estos pasos:

1. Revisa los requisitos descritos en [Requisitos de configuración de la red](#) y realiza los cambios necesarios para habilitar las comunicaciones de red entre Amazon FSx y tu AD.
2. Cuando Amazon FSx pueda comunicarse con tu AD, sigue el procedimiento descrito en [Conexión SVMs a Active Directory mediante la API AWS Management Console y AWS CLI](#) y vuelve a intentar unir tu SVM a tu AD.

Amazon no FSx puede conectarse a 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 su 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 FSx usuario de Amazon.

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 [Conexión SVMs a Active Directory mediante la API AWS Management Console y AWS CLI](#) y vuelva a intentar unir el SVM a su AD.

Amazon no FSx 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 las configuraciones de SVM Active Directory existentes mediante la AWS Management Console API AWS CLI, y](#) 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 no FSx puede conectarse a los controladores de dominio de Active Directory porque las credenciales de la cuenta de servicio son insuficientes

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 de 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 [Delegar permisos a tu cuenta de FSx servicio de Amazon](#).

Amazon no FSx puede comunicarse 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 no FSx puede acceder a los servidores DNS proporcionados ni a los controladores de dominio de tu 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 al ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando. 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 [Administrar sistemas de archivos con el 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 [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 al ONTAP CLI, establezca una sesión SSH en el puerto de administración del sistema de archivos Amazon FSx for NetApp ONTAP o SVM ejecutando el siguiente comando. 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 [Administrar sistemas de archivos con el 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 no FSx puede comunicarse con su 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 [Conexión SVMs a Active Directory mediante la API AWS Management Console y AWS 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 la 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 [Conexión SVMs a Active Directory mediante la API AWS Management Console y AWS CLI](#) y vuelva a intentar unir su SVM a un AD.

Amazon no FSx 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 FSx de archivos de ONTAP puede contener una o más máquinas virtuales de almacenamiento (SVMs) 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 FSx consola, la API y la CLI de Amazon. Solo puede eliminar volúmenes mediante la FSx consola, la API o la CLI de Amazon si el volumen tiene habilitadas las FSx copias de seguridad de Amazon.

Para ayudar a proteger sus datos y su configuración, Amazon FSx impide la eliminación de SVMs volúmenes en determinadas circunstancias. Si intentas eliminar un SVM o un volumen y tu solicitud de eliminación no se realiza correctamente, Amazon te FSx proporciona información en la AWS 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](#)
- [Eliminación de SVM: no se puede acceder a las tablas de enrutamiento](#)
- [Eliminación de SVM: relación entre pares](#)
- [Eliminación de SVM o volumen: SnapMirror](#)
- [Eliminación de SVM: LIF habilitado para Kerberos](#)
- [Eliminación de SVM: otro motivo](#)
- [Eliminación de volumen: relación FlexCache](#)

Identificar las eliminaciones fallidas

Al eliminar un volumen o un FSx SVM de Amazon, normalmente se observa la transición del Lifecycle estado del recurso hasta unos minutos antes de que el recurso desaparezca de la FSx consola, la CLI y la API de Amazon. DELETING

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 muestra FSx un icono de alerta en la consola junto al estado del CREATED ciclo de vida. Al seleccionar el icono de alerta, aparecerá el motivo de la eliminación incorrecta, como se indica en el siguiente ejemplo.

Lifecycle state

 Created 

Lifecycle transition message

Cannot delete storage virtual machine while it has non-root volumes.

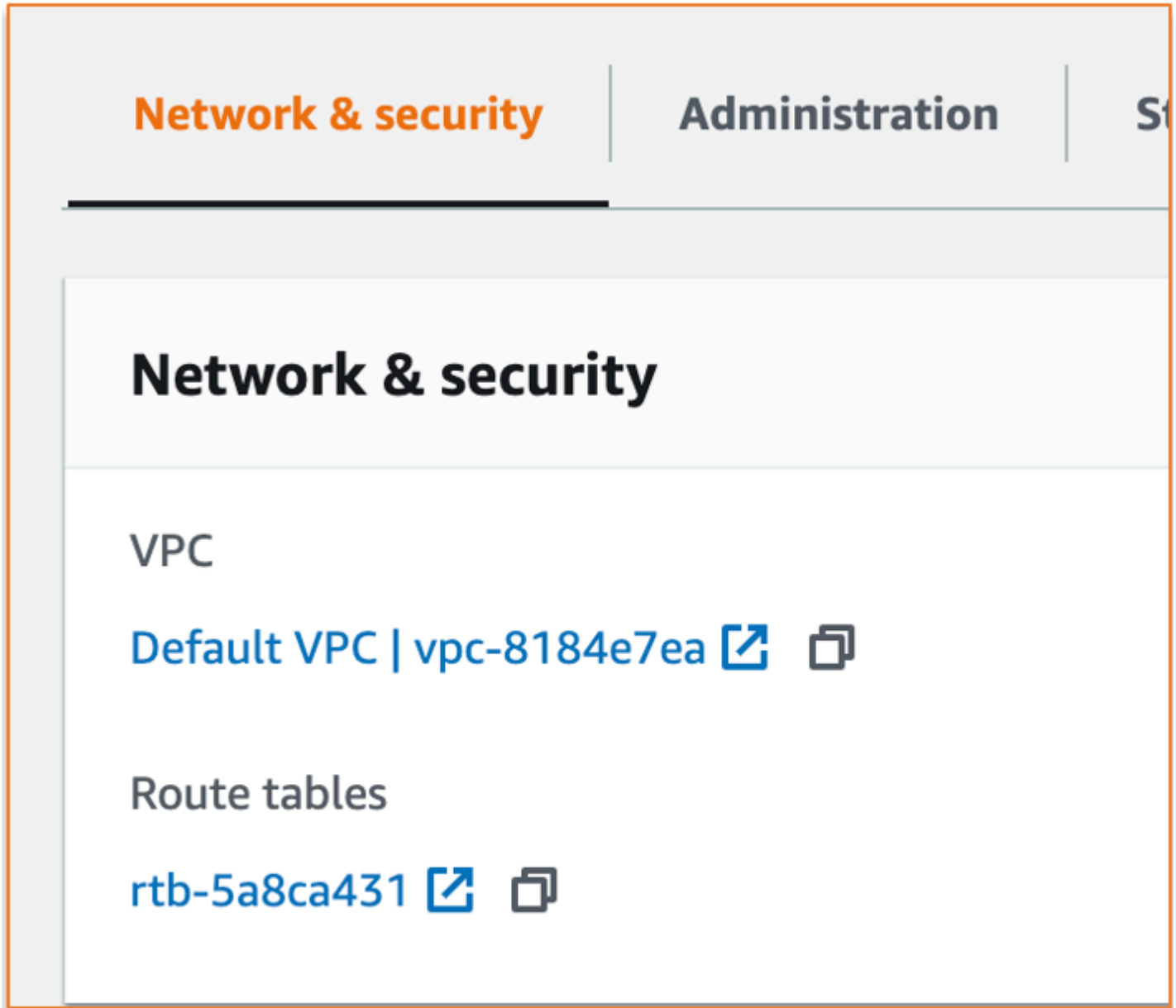
Los motivos más comunes por los FSx que Amazon impide la SVM y la eliminación de volúmenes se indican en las siguientes secciones, con step-by-step instrucciones sobre cómo resolver estos problemas.

Eliminación de SVM: no se puede acceder a las tablas de enrutamiento

Cada uno de FSx los sistemas de archivos de ONTAP crea una o más entradas en la tabla de rutas para proporcionar una conmutación por error automática y una recuperación por recuperación 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 las interfaces de ONTAP. Amazon FSx etiqueta cada tabla de rutas que está asociada a un sistema de archivos con una AmazonFSx etiqueta y, si se elimina esta etiqueta, puede impedir que Amazon FSx pueda eliminar los 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 Soporte.

Para encontrar las tablas de rutas de tu sistema de archivos en la FSx consola de Amazon, ve 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

Tags	
Search tags	
Key	Value
Name	Default
AmazonFSx	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 el objeto homólogo de SVMs vuelva insalubre. 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 [Administrar sistemas de archivos con el 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:

Vserver	Peer Vserver	Peer State	Peer Cluster	Peering Applications	Remote 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 (consulte [Eliminación 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 [Administrar sistemas de archivos con el ONTAP CLI](#).

Note

FSx Las copias de seguridad de Amazon SnapMirror se utilizan para crear point-in-time copias de seguridad incrementales de los volúmenes de su sistema de archivos. No puede eliminar esta SnapMirror relación para sus 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 Path	Type	Destination Path	Mirror State	Relationship Status	Total Progress	Healthy	Last 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 [Administrar sistemas de archivos con el 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 eliminar la SVM nuevamente 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

FSx para ONTAP, SVMs cree un objeto informático en su Active Directory cuando se una 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 [Administrar sistemas de archivos con el 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 [Administrar sistemas de archivos con el 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 .

El volumen está en un **MISCONFIGURED** estado

Existen varias causas posibles por las que un volumen ONTAP se deteriora, tal como se describe en los temas siguientes. MISCONFIGURED

Su volumen está lleno en más del 98%

Su sistema de archivos contiene actualmente un volumen que está lleno en más del 98%. Le recomendamos que no utilice su volumen de forma continua en más del 95%. Si no libera espacio en el volumen antes de la próxima ventana de mantenimiento de tu sistema de archivos, Amazon FSx desactivará el bloqueo oportunista del volumen y romperá los «oplocks» existentes. Amazon FSx volverá a habilitar los oplocks en el volumen una vez finalizado el proceso de aplicación de parches. Para evitarlo, reduzca la utilización de la capacidad de almacenamiento del volumen a menos del 98%. Algunas de las formas de lograrlo son las siguientes:

- Aumentar el tamaño del volumen.
- Eliminar datos innecesarios.
- Eliminar instantáneas innecesarias.

Para obtener más información, consulte [Actualización de la capacidad de almacenamiento y Eliminación de instantáneas](#).

El volumen sin conexión tiene un LUN iSCSI o un espacio de nombres / TCP NVMe

Actualmente, su sistema de archivos aloja un volumen que está fuera de línea y ese volumen contiene un LUN iSCSI, un espacio de nombres NVMe /TCP o ambos. Le recomendamos que mantenga los volúmenes en línea de forma continua. Si no pones este volumen en línea antes del siguiente período de mantenimiento de tu sistema de archivos, Amazon FSx lo pondrá en línea temporalmente mientras dure la operación de aplicación de parches. Para evitarlo, conecte el volumen o elimínelo.

Para volver a poner en línea un volumen sin conexión, usa la [volume online](#) ONTAP Comando CLI, como se muestra en el siguiente ejemplo. Si solo existe un SVM (Vserver), no es necesario que especifique el `-vserver` parámetro.

```
FsxID-abcdef123456:> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

Su volumen sin conexión es un FlexCache origen

El sistema de archivos contiene un volumen de FlexCache origen que está desconectado. Le recomendamos que mantenga los volúmenes en línea de forma continua. Si no pones este volumen en línea antes del siguiente período de mantenimiento de tu sistema de archivos, Amazon FSx lo pondrá en línea temporalmente mientras dure la operación de aplicación de parches. Durante este tiempo, es posible que los datos se vuelvan a escribir en el volumen de FlexCache origen con los datos del volumen de la memoria caché. Para evitarlo, conecte el volumen o elimínelo.

Para volver a poner en línea un volumen sin conexión, usa la [volume online](#) ONTAP Comando CLI, como se muestra en el siguiente ejemplo. Si solo existe un SVM (Vserver), no es necesario que especifique el `-vserver` parámetro.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

Su volumen sin conexión forma parte de un SnapMirror relación

Su sistema de archivos aloja actualmente un volumen que está fuera de línea y ese volumen es un SnapMirror origen o destino. Le recomendamos que mantenga los volúmenes en línea de forma continua. Si no pones este volumen en línea antes del siguiente período de mantenimiento de tu sistema de archivos, Amazon FSx lo pondrá en línea temporalmente mientras dure la operación de aplicación de parches y pausará la SnapMirror relación. Durante este tiempo, es posible que los datos se escriban en el SnapMirror volumen de destino con datos del SnapMirror volumen de origen. Para evitarlo, conecte el volumen o elimínelo.

Para volver a poner en línea un volumen sin conexión, usa la [volume online](#) ONTAP Comando CLI, como se muestra en el siguiente ejemplo. Si solo existe un SVM (Vserver), no es necesario que especifique el `-vserver` parámetro.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

El volumen restringido contiene un LUN iSCSI o un espacio de nombres / TCP NVMe

Su sistema de archivos aloja actualmente un volumen que se encuentra en un estado restringido y ese volumen contiene un LUN iSCSI, un espacio de nombres NVMe /TCP o ambos. Le recomendamos que mantenga los volúmenes en línea de forma continua. Si no pones este volumen en línea antes del siguiente período de mantenimiento de tu sistema de archivos, Amazon FSx lo pondrá en línea temporalmente mientras dure la operación de aplicación de parches. Para evitarlo, conecte el volumen a Internet o elimínelo.

Para volver a poner en línea un volumen sin conexión, usa la [volume online](#) ONTAP Comando CLI, como se muestra en el siguiente ejemplo. Si solo existe un SVM (Vserver), no es necesario que especifique el `-vserver` parámetro.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

Su volumen restringido es un origen FlexCache

El sistema de archivos contiene un volumen de FlexCache origen que se encuentra en un estado restringido. Le recomendamos que mantenga los volúmenes en línea de forma continua. Si no pones este volumen en línea antes del siguiente período de mantenimiento de tu sistema de archivos, Amazon FSx lo pondrá en línea temporalmente mientras dure la operación de aplicación de parches. Durante este tiempo, es posible que los datos se vuelvan a escribir en el volumen de FlexCache origen con los datos del volumen de la memoria caché. Para evitarlo, conecte el volumen o elimínelo.

Para volver a poner en línea un volumen sin conexión, usa la [volume online](#) ONTAP Comando CLI, como se muestra en el siguiente ejemplo. Si solo existe un SVM (Vserver), no es necesario que especifique el `-vserver` parámetro.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

Su volumen restringido forma parte de un SnapMirror relación

Su sistema de archivos aloja actualmente un volumen que se encuentra en estado restringido y ese volumen es un SnapMirror origen o destino. Le recomendamos que mantenga los volúmenes

en línea de forma continua. Si no pones este volumen en línea antes del siguiente período de mantenimiento de tu sistema de archivos, Amazon FSx lo pondrá en línea temporalmente mientras dure la operación de aplicación de parches y pausará la SnapMirror relación. Durante este tiempo, es posible que los datos se escriban en el SnapMirror volumen de destino con datos del SnapMirror volumen de origen. Para evitarlo, conecte el volumen o elimínelo.

Para volver a poner en línea un volumen sin conexión, usa la [volume online](#) ONTAP Comando CLI, como se muestra en el siguiente ejemplo. Si solo existe un SVM (Vserver), no es necesario que especifique el `-vserver` parámetro.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

Su volumen tiene una capacidad de almacenamiento 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 del 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 [Cómo 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 FSx consola de Amazon y la FSx API de Amazon. AWS CLI Para obtener más información sobre la actualización de un volumen con mayor capacidad, consulte [Actualización de volúmenes](#).

Como alternativa, puede aumentar la capacidad de almacenamiento de un volumen mediante el comando `volume modify` NetApp ONTAP CLI. Para obtener más información, consulte [Cómo 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 FSx para ONTAP, mediante el comando `volume autosize` NetApp CLI de ONTAP. Para obtener más información, consulte [Habilitación del ajuste de tamaño automático](#).

El almacenamiento principal de su sistema de archivos está lleno

Si el FSx almacenamiento principal del sistema de archivos de 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. Puedes ver la cantidad de capacidad de almacenamiento principal disponible en la pestaña Supervisión y rendimiento de la página de detalles del sistema de archivos de la FSx consola de Amazon. Para obtener más información, consulte [Supervisión de la utilización del almacenamiento en 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 almacenamiento en SSD e IOPS del sistema de archivos](#).

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.

Cuando elimina una instantánea, no se recupera la cantidad de almacenamiento equivalente al tamaño de la instantánea que se elimina. Puedes ver la cantidad de almacenamiento que puedes recuperar al eliminar una instantánea mediante el comando [compute-reclaimable -vserver](#) ONTAP Comando CLI, que utiliza sus datos para reemplazar *svm_name* *vol_name*, y *snapshot_name*.

```
fsid8970abc52::> volume snapshot compute-reclaimable -vserver svm_name -volume vol_name  
-snapshot snapshot_name  
A total of 667648 bytes can be reclaimed.
```

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 FSx de ONTAP puede quedarse sin capacidad de archivo cuando se agota el número de inodos o punteros de archivos 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 [Supervisión 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 [Cómo aumentar la cantidad máxima de archivos de un volumen \(CLI de ONTAP\)](#).

Las copias de seguridad fallan por una capacidad de volumen insuficiente

Las copias de seguridad diarias automáticas del volumen fallan y muestran 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 usar una o más de las siguientes opciones, según su situación:

- [Aumentar la capacidad de almacenamiento del volumen](#)
- [Aumentar la reserva de instantáneas del volumen](#)
- [Desactivar la eliminación automática de instantáneas](#)
- [No eliminar la instantánea de respaldo](#) mediante la CLI de ONTAP

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 lo siguiente NetApp ONTAP Comandos CLI:

- `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.

Cómo capturar el rastreo de un paquete desde su sistema de archivos

1. Para acceder mediante SSH al NetApp ONTAP En la CLI de su sistema de archivos, siga los pasos descritos en la [Uso de NetApp ONTAP CLI](#) sección de la Guía del usuario de Amazon FSx for 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:
 - *node_name* Sustitúyalo por el nombre del nodo (por ejemplo, FsxId01234567890abcdef-01).
 - *svm_name* Sustitúyalo por el nombre de la máquina virtual de almacenamiento (por ejemplo, fsx).
 - *junction_path_name* Sustitúyalo 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 el FSx caso de ONTAP, todo el tráfico de red utiliza la e0e interfaz.

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: *svm_name* /clus//*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: *_ _ .trc node-name port-name yyyymmdd_hhmmss*
- 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 el debug network dump](#) en ONTAP 9.10+ en el NetApp Knowledge Base.

Historial de documentos de Amazon FSx for NetApp ONTAP

- Versión de la API: 01-03-2018
- Última actualización de la documentación: 9 de junio de 2025

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
FSx para ONTAP es compatible con Amazon Elastic Service VMware	FSx for ONTAP ahora se puede utilizar como almacén de datos externo para Amazon EVS. Para obtener más información, consulte Uso de Amazon Elastic VMware Service con FSx ONTAP .	9 de junio de 2025
Se agregó Región de AWS soporte adicional	La segunda generación (Multi-AZ 2 y Single-AZ 2) FSx para los sistemas de archivos ONTAP ya está disponible en Asia Pacífico (Tokio) y Asia Pacífico (Bombay). Para obtener más información, consulte Disponibilidad por Región de AWS	2 de junio de 2025
Support agregado para el modo de FlexCache reescritura	FSx los volúmenes ONTAP ahora admiten FlexCache el modo de reescritura. Para obtener más información, consulte Replicar los datos con FlexCache	28 de mayo de 2025

[Amazon FSx ha actualizado la política de FSx FullAccess AWS gestión de Amazon](#)

La política FSx FullAccess gestionada por [Amazon](#) se actualizó para añadir los fsx:CreateAndAttachS3AccessPoint fsx:DetachAndDeleteS3AccessPoint permisos fsx:UpdateS3AccessPointAttachments, y fsx:DescribeS3AccessPointAttachments

28 de mayo de 2025

[Amazon FSx ha actualizado la política de FSx ConsoleFullAccess AWS gestión de Amazon](#)

La política FSx ConsoleFullAccess gestionada por [Amazon](#) se actualizó para añadir los fsx:CreateAndAttachS3AccessPoint fsx:DetachAndDeleteS3AccessPoint permisos fsx:UpdateS3AccessPointAttachments, y fsx:DescribeS3AccessPointAttachments

28 de mayo de 2025

[Se agregó Región de AWS soporte adicional](#)

FSx para los sistemas de archivos ONTAP ya están disponibles en Asia Pacífico (Tailandia) y México (Central). Para obtener más información, consulte [Disponibilidad por Región de AWS](#).

8 de mayo de 2025

[Ahora se admite la protección autónoma contra el ransomware \(ARP\)](#)

ONTAP ahora admite el ARP, una función NetApp impulsada por la IA que monitorea y protege contra los ataques de ransomware y malware. FSx Para obtener más información, consulte [Cómo proteger sus datos con la protección autónoma contra el ransomware](#)

7 de abril de 2025

[Un nuevo tema de la FSx guía del usuario de ONTAP describe cómo configurar un servidor SMB en un grupo de trabajo](#)

La [configuración de un servidor SMB en un grupo de trabajo](#) describe cómo configurar un servidor SMB en un grupo de trabajo en una SVM como alternativa a unir una SVM a un Microsoft Active Directory.

4 de marzo de 2025

[Amazon FSx ha actualizado la política de FSx ConsoleReadOnlyAccess AWS gestión de Amazon](#)

Amazon FSx actualizó la FSx ConsoleReadOnlyAccess política de Amazon para añadir el `ec2:DescribeNetworkInterfaces` permiso. Para obtener más información, consulta la FSx ConsoleReadOnlyAccess política de [Amazon](#).

25 de febrero de 2025

Ahora se Harvest admiten paneles adicionales	ONTAP ahora admite Harvest paneles adicionales, incluidos FSx los paneles que no están habilitados de forma predeterminada. También se ha añadido una lista de paneles que FSx ONTAP no admite. Para obtener más información, consulte Supervisión de FSx los sistemas de archivos ONTAP mediante Harvest y Grafana .	18 de febrero de 2025
Se ha añadido un tema nuevo FSx para los informes de facturación y uso de ONTAP a FSx la Guía del usuario de ONTAP	En el tema Informes de AWS facturación y uso FSx de ONTAP se explica cómo acceder a los informes de facturación y uso de los sistemas de archivos FSx de ONTAP en la consola. Administración de facturación y costos de AWS También incluye en ambos informes todos los tipos de uso específicos de ONTAP FSx .	13 de febrero de 2025
Support agregado para puntos finales de interfaz de VPC de doble pila para Amazon FSx	Ahora puede crear puntos de enlace de interfaz de VPC de doble pila para FSx Amazon IPv4 con direcciones IP IPv6 y nombres de DNS. Para obtener más información, consulte los puntos FSx finales de ONTAP y VPC de interfaz .	7 de febrero de 2025

[Support agregado para puntos finales de API de doble pila](#)

La API del FSx servicio de Amazon para crear y administrar sistemas de archivos tiene nuevos puntos finales de doble pila. Para obtener más información, consulta los [puntos de enlace de la API](#) en la Amazon FSx API Reference .

7 de febrero de 2025

[Amazon FSx ha actualizado la política de FSx ConsoleFullAccess AWS gestión de Amazon](#)

Amazon FSx actualizó la FSx ConsoleFullAccess política de Amazon para añadir el `ec2:DescribeNetworkInterfaces` permiso. Para obtener más información, consulta la FSx ConsoleFullAccess política de [Amazon](#).

7 de febrero de 2025

[Se ha publicado un nuevo tema, Replicar datos con FlexCache](#)

Se ha publicado un nuevo tema en el que se describe cómo replicar los datos de un sistema de archivos ONTAP local en un sistema de archivos ONTAP FSx para su uso. FlexCache Para obtener más información, consulte [Replicar](#) datos con. FlexCache

19 de diciembre de 2024

[Se agregó soporte para sistemas de archivos de segunda generación](#)

Ahora puede crear sistemas de archivos Single-AZ y Multi-AZ de segunda generación. Un solo par de alta disponibilidad (HA) ahora ofrece hasta un 6% de la capacidad GBps de rendimiento y 200 000 IOPS de SSD. Para obtener más información, consulte [Pares de alta disponibilidad \(HA\)](#).

9 de julio de 2024

[Se agregó soporte para leer datos de un volumen mientras se restaura desde una copia de seguridad](#)

Ahora puede montar un volumen con acceso de solo lectura a los datos del archivo mientras se restaura a partir de una copia de seguridad en sistemas de archivos de segunda generación. Para obtener más información, consulte [Restauración de copias de seguridad en un nuevo volumen](#).

9 de julio de 2024

[Se agregó soporte para ajustar la capacidad de rendimiento en los sistemas de archivos de segunda generación](#)

Ahora puede ajustar la capacidad de rendimiento de los sistemas de archivos de segunda generación luego de crearlos. Para obtener más información, consulte [Administración de la capacidad de rendimiento](#).

9 de julio de 2024

[Se agregó soporte para agregar pares de HA a sistemas de archivos Single-AZ de segunda generación](#)

Ahora puede agregar pares de HA a los sistemas de archivos Single-AZ de segunda generación luego de crearlos. Puede tener 12 pares de HA en total en un sistema de archivos Single-AZ de segunda generación. Para obtener más información, consulte [Agregar pares de alta disponibilidad \(HA\)](#).

9 de julio de 2024

[Support agregado para el protocolo Non-Volatile Memory Express over TCP \(NVMe/TCP\)](#)

Ahora puede utilizar el NVMe/TCP protocolo de transporte de datos en Amazon FSx para los sistemas de archivos NetApp ONTAP. Para obtener más información, consulte [Uso de protocolos de almacenamiento en bloques](#)

9 de julio de 2024

[Se agregó soporte para el rol fsxadmin-readonly de usuarios administrativos del sistema de archivos](#)

El rol fsxadmin-readonly ahora está disponible para los usuarios administrativos del sistema de archivos de ONTAP y se puede usar para aplicaciones de supervisión del sistema de archivos, como NetApp Harvest. Para obtener más información, consulte [Roles y usuarios de administrador del sistema de archivos](#).

30 de abril de 2024

[Se agregó soporte para la autenticación con clave pública de SSH para usuarios administrativos de dominios de Windows](#)

Ahora puede usar la autenticación con clave pública de SSH con los usuarios del sistema de archivos de dominio de Active Directory y de la SVM. Para obtener más información, consulte [Configuración de la autenticación de Active Directory para usuarios de ONTAP](#).

30 de abril de 2024

[Se agregó soporte para 12 pares de HA en sistemas de archivos de escalado horizontal](#)

Amazon FSx for NetApp ONTAP agregó soporte para 12 pares de alta disponibilidad en sistemas de archivos escalables. Los sistemas de archivos con 12 pares de alta disponibilidad pueden ofrecer hasta un 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 for NetApp ONTAP performance](#).

4 de marzo de 2024

[Se agregó soporte para el modo de escritura en la nube](#)

Amazon FSx for NetApp ONTAP agregó compatibilidad con el modo de escritura en la nube para volúmenes. Para obtener más información, consulte [Habilitar el modo de escritura en la nube en un volumen](#).

6 de febrero de 2024

[Support agregado para hacer copias de seguridad de FlexGroup volúmenes con AWS Backup](#)

Ahora puede utilizarlo AWS Backup para realizar copias de seguridad y restaurar FlexGroup volúmenes en sus sistemas FSx de archivos ONTAP. Para obtener más información, consulta [Uso AWS Backup con Amazon FSx](#).

11 de enero de 2024

[Amazon FSx actualizó las políticas FSx ServiceRolePolicy AWS gestionadas de Amazon FSx FullAccess FSx ConsoleFullAccess FSx ReadOnlyAccess FSx ConsoleReadOnlyAccess, Amazon, Amazon y Amazon](#)

Amazon FSx actualizó las FSx ServiceRolePolicy políticas de Amazon FSx FullAccess FSx ConsoleFullAccess FSxReadOnlyAccess, Amazon FSxConsoleReadOnlyAccess, Amazon y Amazon para añadir el `ec2:GetSecurityGroupsForVpc` permiso. Para obtener más información, consulta [Amazon FSx actualiza las políticas AWS gestionadas](#).

9 de enero de 2024

[Amazon FSx actualizó Amazon FSx FullAccess y las políticas FSx ConsoleFullAccess AWS gestionadas por Amazon](#)

Amazon FSx actualizó las FSx ConsoleFullAccess políticas de Amazon FSx FullAccess y Amazon para añadir la `ManageCrossAccountDataReplication` acción. Para obtener más información, consulta [Amazon FSx actualiza las políticas AWS gestionadas](#).

20 de diciembre de 2023

[Se agregó soporte para métricas de escalado 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 de escalado horizontal](#).

26 de noviembre de 2023

[Se agregó soporte para sistemas de archivos de escalado horizontal](#)

Amazon FSx for NetApp ONTAP agregó soporte para sistemas de archivos escalables que pueden ofrecer hasta un 36% GBps de la capacidad de rendimiento 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 for NetApp ONTAP performance](#).

26 de noviembre de 2023

[Support agregado para FlexGroup volúmenes](#)

Amazon FSx for NetApp ONTAP agregó soporte para FlexGroup volúmenes. Para obtener más información, consulte [Estilos de volumen](#).

26 de noviembre de 2023

[Se agregó compatibilidad de VPC compartidas con sistemas de archivos Multi-AZ](#)

Las cuentas de participantes no 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 FSx consola, la CLI y la API de Amazon. Para obtener más información, consulte [Creación de sistemas de archivos FSx para ONTAP en subredes compartidas](#)

26 de noviembre de 2023

[Amazon FSx actualizó Amazon FSx FullAccess y las políticas FSx ConsoleFullAccess AWS gestionadas por Amazon](#)

Amazon FSx actualizó las FSx ConsoleFullAccess políticas de Amazon FSx FullAccess y Amazon para añadir el `fsx:CopySnapshotAndUpdateVolume` permiso. Para obtener más información, consulta [Amazon FSx actualiza las políticas AWS gestionadas.](#)

26 de noviembre de 2023

[Amazon FSx actualizó Amazon FSx FullAccess y las políticas FSx ConsoleFullAccess AWS gestionadas por Amazon](#)

Amazon FSx actualizó las FSx ConsoleFullAccess políticas de Amazon FSx FullAccess y Amazon para añadir los `fsx:UpdateSharedVPCConfiguration` permisos `fsx:DescribeSharedVPCConfiguration` y. Para obtener más información, consulta [Amazon FSx actualiza las políticas AWS gestionadas.](#)

14 de noviembre de 2023

[Soporte añadido para la creación de roles y usuarios ONTAP adicionales](#)

Amazon FSx for 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 for NetApp ONTAP](#).

6 de septiembre de 2023

[Support agregado para CloudWatch métricas adicionales y un panel de monitoreo mejorado](#)

FSx para ONTAP ahora ofrece métricas de rendimiento adicionales y un panel de supervisión mejorado para mejorar la visibilidad de la actividad del sistema de archivos. Para obtener más información, consulte [Supervisión con CloudWatch](#).

17 de agosto de 2023

[Amazon FSx ha actualizado la política de FSx ServiceRolePolicy AWS gestión de Amazon](#)

Amazon FSx actualizó el `cloudwatch:PutMetricData` permiso en Amazon FSxServiceRolePolicy. Para obtener más información, consulta [Amazon FSx actualiza las políticas AWS gestionadas](#).

24 de julio de 2023

[Support agregado para usar NetApp System Manager directamente](#)

Puede gestionar sus sistemas FSx de archivos de ONTAP 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 los eventos del sistema FSx de archivos de ONTAP con la versión nativa de ONTAP de NetApp. Events Management System (EMS) Puede ver los eventos de EMS mediante la CLI de NetApp ONTAP. Para obtener más información, consulte [Supervisión de los eventos EMS FSx de ONTAP](#).

13 de julio de 2023

Soporte añadido para SnapLock

FSx porque ONTAP ahora admite SnapLock volúmenes. SnapLock permite proteger sus archivos mediante la transición a un estado de escritura una vez, lectura múltiple (WORM), lo que impide su modificación o eliminación durante un período de retención específico. FSx para ONTAP es compatible con los modos de retención Compliance y Enterprise con SnapLock. Para obtener más información, consulte [Trabajar con SnapLock](#).

13 de julio de 2023

Support agregado para el IPsec cifrado de datos en tránsito

FSx ya que ONTAP admite el uso del IPsec cifrado para cifrar los datos en tránsito entre los sistemas de archivos y los clientes conectados. Para obtener más información, consulte [Configuración IPsec mediante autenticación PSK y Configuración IPsec mediante autenticación mediante certificado](#).

13 de julio de 2023

Se ha incrementado el tamaño máximo del volumen

FSx para ONTAP, se actualizó el tamaño máximo de un volumen de 100 TB a 300 TB. Para obtener más información, consulte [Activar el tamaño automático del volumen](#).

13 de julio de 2023

[Amazon FSx ha actualizado la política de FSx FullAccess AWS gestión de Amazon](#)

Amazon FSx actualizó la FSx FullAccess política de Amazon para eliminar el `fsx:*` permiso y añadir `fsx` acciones específicas. Para obtener más información, consulta la FSx FullAccess política de [Amazon](#).

13 de julio de 2023

[Amazon FSx ha actualizado la política de FSx ConsoleFullAccess AWS gestión de Amazon](#)

Amazon FSx actualizó la FSx ConsoleFullAccess política de Amazon para eliminar el `fsx:*` permiso y añadir `fsx` acciones específicas. Para obtener más información, consulta la FSx ConsoleFullAccess política de [Amazon](#).

13 de julio de 2023

[Soporte añadido para unir máquinas virtuales de almacenamiento existentes a un Active Directory](#)

Puede unir las máquinas virtuales de almacenamiento existentes a un Active Directory mediante AWS Management Console la API AWS CLI y. Para obtener más información, consulte [Unir una SVM a un Active Directory](#).

13 de junio de 2023

[Support para caché de NVMe lectura agregado para sistemas de archivos Single-AZ](#)

NVMe La caché de lectura ahora es compatible con los sistemas de archivos Single-AZ creados después del 28 de noviembre GBps de 2022 con al menos un 2% de capacidad de rendimiento en las regiones EE.UU. Este (Ohio), EE.UU. Este (Norte de Virginia), Región EE.UU. Oeste (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 Multi-AZ FSx para los sistemas de archivos ONTAP especificando los puntos finales que estén dentro del rango de direcciones IP de su VPC. Para obtener más información, consulte [Creación de sistemas de archivos FSx para 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 de VPC a un sistema de archivos Multi-AZ FSx para ONTAP existente o desasociar (eliminar) una tabla de enrutamiento de VPC existente de un sistema de archivos Multi-AZ para ONTAP existente. FSx 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 EC2 las instancias de Amazon compatibles en la región EE.UU. Este (Ohio), la región EE.UU. Este (Norte de Virginia), la región EE.UU. Oeste (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 de DP (protección de datos) mediante la FSx consola de Amazon o la FSx API de Amazon. AWS CLI Puede utilizar los volúmenes DP como destino de una SnapVault relación NetApp SnapMirror o si desea 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 FSx API de Amazon la copia automática de 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 FSx consola de Amazon o la FSx API de Amazon. AWS CLI. 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 ya que ONTAP admite una capacidad MBps de procesamiento de 4096 unidades para los sistemas de archivos creados después del 28 de noviembre de 2022 en las regiones EE.UU. Este (Ohio), EE.UU. Este (Norte de Virginia), Oeste (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 for ONTAP ahora admite 160.000 IOPS de SSD para sistemas de archivos creados después del 28 de noviembre de 2022 en la región EE.UU. Este (Ohio), la región EE.UU. Este (Norte de Virginia), la región EE.UU. Oeste (Oregón) y Europa (Irlanda). Para obtener más información, consulte [Impacto de la capacidad de rendimiento en el rendimiento](#).

28 de noviembre de 2022

[Support añadido para el uso de ONTAP como almacén de datos externo FSx para Cloud on VMware AWS](#)

Puede utilizar ONTAP como almacén de datos externo FSx para centros de datos definidos por software en VMware AWS la nube (). SDDCs Este soporte adicional proporciona flexibilidad para aumentar o reducir el almacenamiento independientemente de los recursos de cómputo para las cargas de trabajo de Cloud on. VMware AWS Para obtener más información, consulte [Uso de VMware la nube con FSx 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 ahora FSx está integrado con AWS Backup](#)

Ahora puede utilizarlos AWS Backup para realizar copias de seguridad y restaurar sus sistemas de FSx archivos, además de utilizar las FSx copias de seguridad nativas de Amazon. Para obtener más información, consulta [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 sistemas de archivos Single-AZ FSx para ONTAP, que están diseñados para ofrecer 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 los puntos finales AWS PrivateLink de la interfaz de VPC](#)

Ahora puede usar los puntos de enlace de la VPC de la interfaz para acceder a la FSx API de Amazon desde su VPC sin enviar tráfico a través de Internet. Para obtener más información, consulte [Amazon FSx y los puntos de enlace de la 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 escalas de IOPS aprovisionadas](#)

Ahora puede aumentar la capacidad de almacenamiento en SSD y las IOPS aprovisionadas para los sistemas de archivos existentes FSx en ONTAP a medida que evolucionen sus requisitos de almacenamiento e IOPS. Para obtener más información, 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 ONTAP FSx 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 128 MBps y 256 MBps opciones de rendimiento del sistema de archivos. Para obtener más información, consulte [Impacto de la capacidad de rendimiento en el rendimiento](#).

30 de noviembre de 2021

[Amazon FSx for NetApp ONTAP ya está disponible de forma general](#)

FSx for ONTAP es un servicio totalmente gestionado que proporciona un almacenamiento de archivos altamente fiable, escalable, eficiente y rico en funciones integrado en NetApp el sistema de archivos ONTAP. Ofrece las funciones, el rendimiento, las capacidades y los sistemas APIs de NetApp archivos que ya conocemos, 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.