aws

Guía del usuario de Windows

Servidor FSx de archivos Amazon para Windows

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

Servidor FSx de archivos Amazon para Windows: Guía del usuario de Windows

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 FSx para Windows File Server? 1
FSx Recursos de Amazon 1
El acceso a los recursos compartidos de archivos 2
Seguridad y protección de datos 3
Disponibilidad y durabilidad 3
Gestión de sistemas de archivos 4
Flexibilidad de precio y rendimiento 4
Precios para Amazon FSx 4
Supuestos 4
Requisitos previos 5
Foros FSx de Amazon para Windows File Server 6
¿Es la primera vez que utilizas Amazon? FSx 6
FSx para las prácticas recomendadas de Windows 7
Prácticas recomendadas generales 7
Creación de un plan de monitoreo 7
Garantizar que sus sistemas de archivos dispongan de recursos suficientes 7
Prácticas recomendadas de seguridad 7
Seguridad de la red 8
Active Directory 8
Evite perder disponibilidad debido a una mala configuración de Active Directory 9
Windows ACLs 10
Configurar y ajustar el tamaño del sistema de archivos 10
Selección de un tipo de implementación 10
Selección de una capacidad de rendimiento 11
Aumentar la capacidad de almacenamiento y la capacidad de rendimiento 11
Modificación de la capacidad de rendimiento durante los períodos de inactividad 12
Introducción 13
Configuración de su Cuenta de AWS 14
..... 14
Paso 1. Configuración de un Active Directory 16
Paso 2: lanza una instancia de Windows en la EC2 consola de Amazon 17
Paso 3: Conectarse a la instancia 19
Paso 4: une la instancia a tu AWS Directory Service directorio 21
Paso 5. Crear el sistema de archivos 23

Paso 6. Asigne el recurso compartido de archivos a una EC2 instancia que ejecute Windows Server ... 29
Paso 7. Escribir datos en el recurso compartido de archivos ... 30
Paso 8. Hacer una copia de seguridad del sistema de archivos ... 31
Paso 9. Eliminar recursos ... 31
Acceso a sus datos ... 34
Clientes compatibles ... 34
Acceder a los datos desde el Nube de AWS ... 35
Acceder a los datos desde una VPC diferente, Cuenta de AWS o Región de AWS ... 37
Acceso a los datos en las instalaciones ... 37
Acceso a los datos mediante nombres de DNS predeterminados ... 38
Uso de la autenticación de Kerberos con nombres del DNS ... 39
Compatibilidad con espacios de nombres del sistema de archivos distribuido (DFS) ... 40
Acceso a los datos mediante alias del DNS ... 40
Uso de la autenticación de Kerberos y el cifrado con alias del DNS ... 41
Asociar alias del DNS con el sistema de archivos ... 42
Configure los nombres principales de servicio () para Kerberos SPNs ... 43
Actualizar o crear un registro CNAME del DNS ... 46
Aplicar la autenticación de Kerberos mediante objetos de política de grupo () GPOs ... 48
Acceso a los datos mediante recursos compartidos de archivos ... 49
Mapeo de recursos compartidos de archivos ... 50
Mapeo de un recurso compartido de archivos en una instancia de Amazon EC2 Windows ... 50
Montaje de un recurso compartido de archivos en una instancia de Amazon EC2 Mac ... 53
Montaje de un recurso compartido de archivos en una instancia de Amazon EC2 Linux ... 56
Monta automáticamente los recursos compartidos de archivos en una instancia de Amazon EC2 Linux ... 62
Administración de recursos compartidos de archivos ... 65
El FSx SmbShare comando New- falla cuando se trata de una confianza unidireccional ... 71
Disponibilidad y durabilidad ... 72
Elegir el tipo de implementación del sistema de archivos Single-AZ o Multi-AZ ... 73
Compatibilidad de características por tipo de implementación ... 73
Proceso de conmutación por error ... 74
La experiencia de conmutación por error en clientes de Windows ... 75
La experiencia de conmutación por error en clientes Linux ... 75
Prueba de conmutación por error en un sistema de archivos ... 75
Recursos del sistema de archivos Single-AZ y Multi-AZ ... 76

Subredes 76
Interfaces de red elástica del sistema de archivos 76
Uso de Active Directory 78
Usando AWS Managed Microsoft AD 79
Requisitos previos de red 80
Uso de un modelo de aislamiento de bosques de recursos 86
Ponga a prueba su configuración de Active Directory 86
Uso AWS Managed Microsoft AD en una cuenta o VPC diferente 87
Validar la conectividad con los controladores de dominio de Active Directory 88
Uso de un Active Directory autoadministrado 91
Requisitos previos 93
Prácticas recomendadas a la hora de utilizar un Active Directory autogestionado 99
Cuenta de FSx servicio de Amazon 101
Delegación de privilegios a Amazon FSx 101
Cómo validar la configuración del Active Directory 103
Únase FSx a un Active Directory autogestionado 107
Obtención de las direcciones IP para entradas manuales del DNS 118
Actualizar el Active Directory autoadministrado 119
Cambiar la cuenta de FSx servicio de Amazon 121
Supervisión de las actualizaciones del Active Directory autoadministrado 123
Rendimiento 126
El rendimiento del sistema de archivos 126
Consideraciones relativas al rendimiento adicional 128
Latencia 128
Rendimiento e IOPS 128
Rendimiento para un solo cliente 128
Rendimiento por ráfagas 129
Impacto de la capacidad de rendimiento y rendimiento 129
Elegir la capacidad de rendimiento 132
Configuración y rendimiento del almacenamiento 133
Rendimiento por ráfagas de HDD 134
Ejemplo: capacidad de almacenamiento y capacidad de rendimiento 135
Medir el rendimiento mediante métricas CloudWatch 136
Solución de problemas de rendimiento 136
Determine el rendimiento del sistema de archivos y los límites de IOPS 136
¿Qué son la E/S de red y la E/S de disco? ¿Por qué son diferentes? 137

¿Por qué el uso de la CPU o la memoria es alto, cuando la E/S de la red es baja? 137
¿Qué son las ráfagas? ¿Cuántas ráfagas utiliza el sistema de archivos? ¿Qué ocurre cuando se agotan los créditos de ráfaga? 138
Veo una advertencia en la página de Supervisión y rendimiento: ¿debo cambiar la configuración del sistema de archivos? 138
No pude ver las métricas por un momento, ¿debo preocuparme? 139
Administración de sistemas de archivos 140
Estado FSx del sistema de archivos de Amazon 141
Uso de Amazon FSx CLI para PowerShell 142
Inicio de una PowerShell sesión FSx remota de Amazon 144
Tareas de configuración únicas del sistema de archivos 145
Administración del consumo de almacenamiento 145
Activar las instantáneas para que los usuarios finales puedan recuperar archivos y carpetas de versiones anteriores 146
Aplicación del cifrado en tránsito 146
Solución de problemas de acceso a la Amazon FSx CLI en PowerShell 147
El grupo de seguridad del sistema de archivos carece de las reglas de entrada necesarias para permitir una conexión remota PowerShell 147
Tiene una confianza externa configurada entre el Microsoft Active Directory AWS administrado y su Active Directory local 147
Se produce un error de localización del idioma al intentar iniciar una sesión remota PowerShell 148
Periodo de mantenimiento 148
Cambio del periodo de mantenimiento semanal 149
Los alias del DNS 150
El estado del alias del DNS 152
Uso de alias del DNS con Kerberos 153
Visualización de alias del DNS existentes 153
Asociación de alias del DNS a los sistemas de archivos 154
La administración de los alias del DNS en los sistemas de archivos existentes 156
Sesiones de usuario y archivos abiertos 158
Uso de la GUI para administrar los usuarios y las sesiones 158
Se utiliza PowerShell para administrar las sesiones de usuario y abrir archivos 162
Administrar el almacenamiento 162
Optimizar costos de almacenamiento 163
Administrar la capacidad de almacenamiento 164

Administrar los tipos de almacenamiento ... 168
Cómo administrar IOPS de SSD ... 170
Deduplicación de datos ... 171
Cómo administrar cuotas de almacenamiento ... 176
Aumento de la capacidad de almacenamiento ... 177
Supervisión de los aumentos de almacenamiento ... 179
El aumento dinámico de la capacidad de almacenamiento ... 182
Cómo actualizar el tipo de almacenamiento ... 188
Supervisión de las actualizaciones de tipos de almacenamiento ... 189
Cómo actualizar las IOPS en SSD ... 190
La supervisión de las actualizaciones de IOPS de SSD aprovisionadas ... 191
Cómo administrar la deduplicación de datos ... 193
Cómo solucionar la deduplicación de datos ... 197
Uso de los espacios de nombres del DFS ... 199
Uso de los espacios de nombres del DFS ... 200
Mejora del rendimiento con particiones ... 200
Agrupar sistemas de archivos en un espacio de nombres ... 201
Partición de datos mediante los espacios de nombres del DFS para un rendimiento de escalado horizontal ... 203
Administración de la capacidad de rendimiento ... 205
Cómo funciona el escalado del rendimiento ... 206
Saber cuándo modificar la capacidad de rendimiento ... 207
Modificación de la capacidad de rendimiento ... 208
Supervisión de las actualizaciones de capacidad de rendimiento ... 209
Etiquetado de recursos ... 212
Conceptos básicos de etiquetas ... 212
Cómo etiquetar los recursos ... 213
Restricciones de las etiquetas ... 214
Permisos obligatorios para etiquetar recursos ... 214
Actualice un sistema de archivos mediante AWS CLI ... 214
Proteja sus datos ... 217
Protección de los datos con copias de seguridad ... 217
Trabajo con copias de seguridad diarias automáticas ... 219
Trabajo con copias de seguridad iniciadas por el usuario ... 220
Uso AWS Backup con Amazon FSx ... 220
Copiar copias de seguridad ... 222

Restauración de copias de seguridad en un nuevo sistema de archivos 224
Crear copias de seguridad iniciadas por el usuario 225
Eliminación de copias de seguridad 226
Tamaño de las copias de seguridad 227
Copiar copias de seguridad 228
Restauración de una copia de seguridad 229
Protección de datos con copias de redundancia 230
Prácticas recomendadas 231
Configuración de copias de redundancia 232
Configurar las copias de redundancia para que usen los ajustes predeterminados 237
Configuración de la cantidad máxima de almacenamiento de copias de redundancia 239
Visualización del almacenamiento de copias de redundancia 241
Creación de un programa de copias de redundancia personalizado 242
Visualización de la programación de copias de redundancia 244
Crear una copia de redundancia 245
Visualización de copias de redundancia existentes 245
Eliminar copias de redundancia 245
Eliminar una programación de copias de redundancia 247
Eliminación de una configuración de copias de redundancia 247
Solución de copias de redundancia 248
La replicación programada 249
Uso FSx para Windows File Server con Microsoft SQL Server 250
Uso de Amazon FSx para archivos de datos de Active SQL Server 250
Cree un recurso compartido de disponibilidad continua 251
Configure los ajustes de tiempo de espera de SMB 251
Uso de Amazon FSx como testigo del intercambio de archivos para pequeñas y medianas empresas 251
Migración a Amazon FSx 252
Migración de archivos a un servidor de archivos FSx de Windows 252
Las prácticas recomendadas de migración 253
Migración de archivos mediante AWS DataSync 253
Migración de archivos con Robocopy 257
La migración de configuraciones de recursos compartido de archivos 261
Migración de la configuración de DNS local al servidor de FSx archivos de Windows 263
Pasando FSx a Windows File Server 266
Preparándose para la transición a Amazon FSx 267

Configure SPNs para la autenticación Kerberos 267
Actualiza los registros CNAME de DNS para el sistema de FSx archivos de Amazon 271
Monitoreo de sistemas de archivos 273
Supervisión automatizada y manual 273
Herramientas automatizadas 274
Herramientas de supervisión manuales 274
Monitorización con Amazon CloudWatch 275
Métricas y dimensiones 277
Uso de CloudWatch métricas 282
Advertencias y recomendaciones de rendimiento 288
Acceso a métricas del sistema de archivos 290
Creación de CloudWatch alarmas 294
CloudTrail registros 297
FSx Información de Amazon en CloudTrail 298
Descripción de las entradas de los archivos de FSx registro de Amazon 299
Seguridad 302
Protección de los datos 303
Cifrado de datos 304
Cifrado en reposo 304
Cifrado en tránsito 306
Windows ACLs 308
Vínculos relacionados 309
Control de acceso al sistema de archivos con Amazon VPC 310
Grupos de seguridad de Amazon VPC 310
Red Amazon VPC ACLs 314
Registro del acceso de usuarios finales 315
Audite los destinos del registro de eventos 317
Migración de los controles de auditoría 318
Visualización de registros de eventos 318
Configuración de controles de auditoría de archivos y carpetas 326
Administrar la auditoría de acceso a los archivos 328
Identity and Access Management 333
Público 333
Autenticación con identidades 334
Administración de acceso mediante políticas 338
Cómo funciona Amazon FSx para Windows File Server con IAM 341

Ejemplos de políticas basadas en identidades 348
AWS políticas gestionadas 351
Solución de problemas 367
Uso de etiquetas con Amazon FSx 369
Cómo utilizar roles vinculados a servicios 375
Validación de la conformidad 381
Puntos de conexión de VPC de la interfaz 382
Consideraciones sobre los puntos de enlace de FSx VPC de la interfaz de Amazon 383
Creación de un punto de enlace de VPC de interfaz para la API de Amazon FSx 383
Creación de una política de puntos de conexión de VPC para Amazon FSx 384
Trabajar con otros servicios de 385
Uso de Amazon FSx con Amazon AppStream 2.0 385
Brindar almacenamiento persistente y personal a cada usuario 386
Proporcionar una carpeta compartida entre los usuarios 388
Uso del servidor FSx de archivos de Windows con Amazon Kendra 390
El rendimiento del sistema de archivos 390
Cuotas 391
Cuotas que puede aumentar 391
Cuotas de recursos para cada sistema de archivos 393
Consideraciones adicionales 394
Las cuotas específicas de Microsoft Windows 394
Solución de problemas 395
No puede acceder al sistema de archivos 395
Se modificó o eliminó la interface de red elástica del sistema de archivos 396
Se eliminó la dirección IP elástica que está adjunta a la interfaz de red elástica del sistema de archivos 396
El grupo de seguridad del sistema de archivos carece de las reglas de entrada o salida requeridas. 396
El grupo de seguridad de la instancia informática carece de las reglas de salida requeridas 396
La instancia informática no está unida a un Active Directory 396
El recurso compartido de archivos no existe 397
El usuario de Active Directory carece de los permisos necesarios 397
Permita que se eliminen los permisos de control total de las ACL de NTFS 397
No puede acceder a un sistema de archivos mediante un cliente en las instalaciones 398
El nuevo sistema de archivos no está registrado en el DNS 398

No se puede acceder al sistema de archivos con un alias del DNS 399
No se puede acceder al sistema de archivos con una dirección IP 400
Error al crear un sistema de archivos 401
Grupo de seguridad de VPC mal configurado 401
Nombres de grupos de administradores de sistemas de archivos duplicados 401
No se puede acceder a los servidores del DNS ni a los controladores de dominio 402
Credenciales de cuenta de servicio inválidas 404
Permisos de cuenta de servicio insuficientes 405
Se superó la capacidad de la cuenta de servicio 406
No se puede obtener acceso a la OU 406
El grupo de administradores del sistema de archivos es incorrecto 407
Amazon FSx perdió la conectividad en el dominio 408
La cuenta de servicio no tiene los permisos correctos 408
Se usan caracteres Unicode en los parámetros de creación 409
Se produce un error al pasar el tipo de almacenamiento a disco duro durante la restauración de una copia de seguridad 410
El sistema de archivos está mal configurado 411
Sistema de archivos mal configurado: Amazon no FSx puede acceder a los servidores DNS ni a los controladores de dominio de tu dominio. 412
Sistema de archivos desconfigurado: las credenciales de la cuenta de servicio no son válidas 413
Sistema de archivos desconfigurado: la cuenta de servicio proporcionada no tiene permiso para unir el sistema de archivos al dominio 414
Sistema de archivos desconfigurado: la cuenta de servicio no puede unir más equipos al dominio 414
Sistema de archivos desconfigurado: la cuenta de servicio no tiene acceso a la OU 415
No puede configurar el DFS-R en un sistema de archivos Multi-AZ o Single-AZ 2 415
Las actualizaciones del almacenamiento o la capacidad de rendimiento fallan 416
El aumento de la capacidad de almacenamiento fracasa porque Amazon no FSx puede acceder al sistema de archivos AWS KMS key 416
Se produce un error en la actualización del almacenamiento o la capacidad de rendimiento, porque el Active Directory autoadministrado está mal configurado 417
El aumento de la capacidad de almacenamiento falla debido a una capacidad de rendimiento insuficiente 417
Se produce un error al actualizar la capacidad de rendimiento a 8 MBps 417
Historial de documentos 418

..... cdxxxv

¿Qué es FSx para Windows File Server?

Amazon FSx for Windows File Server proporciona servidores de archivos Microsoft Windows totalmente gestionados, respaldados por un sistema de archivos Windows totalmente nativo. FSx para Windows File Server tiene las características, el rendimiento y la compatibilidad para trasladar fácilmente las aplicaciones empresariales a las Nube de AWS.

Amazon FSx admite un amplio conjunto de cargas de trabajo empresariales de Windows con un almacenamiento de archivos totalmente gestionado integrado en Microsoft Windows Server. Amazon FSx es compatible de forma nativa con las funciones del sistema de archivos de Windows y con el protocolo Server Message Block (SMB) estándar del sector para acceder al almacenamiento de archivos a través de una red. Amazon FSx está optimizado para aplicaciones empresariales en el mundo Nube de AWS, con compatibilidad nativa con Windows, rendimiento y funciones empresariales y latencias consistentes de menos de un milisegundo.

Con el almacenamiento de archivos en Amazon FSx, el código, las aplicaciones y las herramientas que utilizan los desarrolladores y administradores de Windows en la actualidad pueden seguir funcionando sin cambios. Las aplicaciones y cargas de trabajo de Windows ideales para Amazon FSx incluyen aplicaciones empresariales, directorios principales, servidores web, administración de contenido, análisis de datos, configuraciones de creación de software y cargas de trabajo de procesamiento multimedia.

Al tratarse de un servicio totalmente gestionado, FSx Windows File Server elimina la sobrecarga administrativa que supone configurar y aprovisionar servidores de archivos y volúmenes de almacenamiento. Además, Amazon FSx mantiene actualizado el software de Windows, detecta y corrige los fallos de hardware y realiza copias de seguridad. También proporciona una rica integración con otros AWS servicios como AWS IAM AWS Directory Service for Microsoft Active Directory WorkSpacesAWS Key Management Service, Amazon y AWS CloudTrail.

FSx para los recursos del servidor de archivos de Windows: sistemas de archivos, copias de seguridad y recursos compartidos de archivos

Los recursos principales de Amazon FSx son los sistemas de archivos y las copias de seguridad. Un sistema de archivos es el lugar donde se almacenan los archivos y las carpetas, y donde

uno accede a ellos. Un sistema de archivos se compone de uno o más servidores de archivos y volúmenes de almacenamiento de Windows. Al crear un sistema de archivos, se especifica la cantidad de capacidad de almacenamiento (en GiB), las IOPS de SSD y la capacidad de rendimiento (en pulgadas). MBps Puede modificar estas propiedades a medida que cambien sus necesidades una vez creado el sistema de archivos. Para obtener más información, consulte Administrar la capacidad de almacenamiento, Cómo administrar IOPS de SSD y Administración de la capacidad de rendimiento.

FSx en el caso del servidor de archivos de Windows file-system-consistent, las copias de seguridad son muy duraderas e incrementales. Para garantizar la coherencia del sistema de archivos, Amazon FSx utiliza el Volume Shadow Copy Service (VSS) de Microsoft Windows. Las copias de seguridad diarias y automáticas están activadas de forma predeterminada cuando se un sistema de archivos. También, puede realizar copias de seguridad adicionales de forma manual en cualquier momento. Para obtener más información, consulte Protección de los datos con copias de seguridad.

Un recurso compartido de archivos de Windows es una carpeta específica (y sus subcarpetas) del sistema de archivos a la que pueden acceder las instancias informáticas mediante SMB. El sistema de archivos ya incluye un recurso compartido de archivos de Windows predeterminado que se llama `\share`. Puede crear y administrar tantos recursos compartidos de archivos de Windows como desee con la herramienta de interfaz gráfica de usuario (GUI) de Carpetas compartidas de Windows. Para obtener más información, consulte Acceso a los datos mediante recursos compartidos de archivos.

Para acceder a los recursos compartidos de archivos, se utiliza el nombre o los alias del DNS del sistema de archivos asociados a él. Para obtener más información, consulte La administración de los alias del DNS.

El acceso a los recursos compartidos de archivos

FSx Se puede acceder a Amazon desde instancias de procesamiento con el protocolo SMB (compatibles con las versiones 2.0 a 3.1.1). Puede acceder a los recursos compartidos desde todas las versiones de Windows, empezando por Windows Server 2008 y Windows 7, y también desde las versiones vigentes de Linux. Puede mapear sus FSx archivos compartidos de Amazon en instancias de Amazon Elastic Compute Cloud (Amazon EC2) y en WorkSpaces instancias, instancias de Amazon AppStream 2.0 y VMware Cloud on AWS VMs.

Puede acceder a los recursos compartidos de archivos desde instancias informáticas en las instalaciones con AWS Direct Connect o AWS VPN. Además de acceder a los recursos compartidos

de archivos que se encuentran en la misma VPC, AWS cuenta y Región de AWS sistema de archivos, también puede acceder a los recursos compartidos desde instancias de procesamiento que se encuentran en una Amazon VPC, cuenta o Región de AWS Para ello, se utilizan puertas de enlace de tránsito o conexión de emparejamiento de las VPC. Para obtener más información, consulte Acceder a los datos desde el Nube de AWS.

Seguridad y protección de datos

Amazon FSx ofrece varios niveles de seguridad y conformidad para garantizar la protección de tus datos. Cifra automáticamente los datos en reposo (tanto para los sistemas de archivos como para las copias de seguridad) mediante claves que usted administra AWS Key Management Service (AWS KMS). Los datos en tránsito también se cifran de manera automática con claves de sesión SMB Kerberos. Una evaluación confirma que cumple con las certificaciones ISO, PCI-DSS y SOC, y los requisitos de la HIPAA.

Amazon FSx proporciona control de acceso a nivel de archivos y carpetas con listas de control de acceso de Windows (ACLs). Brinda control de acceso a nivel de sistema de archivos mediante grupos de seguridad de Amazon Virtual Private Cloud (Amazon VPC). Además, proporciona control de acceso a nivel de la API mediante políticas de acceso de AWS Identity and Access Management (IAM). Los usuarios que acceden a los sistemas de archivos se autentican con Microsoft Active Directory. Amazon FSx se integra AWS CloudTrail para monitorear y registrar tus llamadas a la API, lo que te permite ver las acciones realizadas por los usuarios en tus FSx recursos de Amazon.

Además, protege los datos, ya que realiza copias de seguridad muy duraderas del sistema de archivos de forma automática y diaria, y le permite realizar copias de seguridad adicionales en cualquier momento. Para obtener más información, consulte Seguridad en Amazon FSx.

Disponibilidad y durabilidad

FSx para Windows File Server ofrece sistemas de archivos con dos niveles de disponibilidad y durabilidad. Los archivos Single-AZ garantizan una disponibilidad alta dentro de una única zona de disponibilidad (AZ), ya que detectan y abordan automáticamente las fallas de los componentes. Además, los sistemas de archivos Multi-AZ proporcionan alta disponibilidad y soporte de conmutación por error en varias zonas de disponibilidad al aprovisionar y mantener un servidor de archivos en espera en una zona de disponibilidad independiente dentro de una región. AWS Para obtener más información acerca de las implementaciones de los sistemas de archivos Single-AZ y Multi-AZ, consulte Disponibilidad y durabilidad: sistemas de archivos Single-AZ y Multi-AZ..

Gestión de sistemas de archivos

Puede administrar FSx los sistemas de archivos del servidor de archivos de Windows mediante PowerShell comandos de administración remota personalizados o, en algunos casos, mediante la GUI nativa de Windows. Para obtener más información sobre la gestión de los sistemas de FSx archivos de Amazon, consulteAdministración FSx de sistemas de archivos de Windows.

Flexibilidad de precio y rendimiento

FSx para Windows File Server le ofrece la flexibilidad de precio y rendimiento al ofrecer tipos de almacenamiento tanto en unidades de estado sólido (SSD) como en unidades de disco duro (HDD). El almacenamiento en el disco duro está diseñado para una amplia gama de cargas de trabajo, incluidos los directorios principales, los recursos compartidos de usuarios y departamentos y los sistemas de administración de contenido. El almacenamiento de SSD está diseñado para las cargas de trabajo de mayor rendimiento y más sensibles a la latencia, incluidas las bases de datos, las cargas de trabajo de procesamiento multimedia y las aplicaciones de análisis de datos.

Con FSx Windows File Server, puede aprovisionar el almacenamiento del sistema de archivos, las IOPS de SSD y el rendimiento de forma independiente para lograr la combinación adecuada de costo y rendimiento. Puede modificar las capacidades de almacenamiento, IOPS de SSD y de rendimiento del sistema de archivos para adaptarlos a las necesidades cambiantes de carga de trabajo, de modo que solo pague por lo que necesita.

Precios para Amazon FSx

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

Supuestos

Para usar Amazon FSx, necesitas una AWS cuenta con una EC2 instancia, WorkSpaces instancia AppStream 2.0 o máquina virtual de Amazon que se ejecute en VMware la nube en AWS entornos del tipo compatible.

En esta guía, hacemos las siguientes suposiciones:

- Si utilizas Amazon EC2, asumimos que estás familiarizado con Amazon EC2. Para obtener más información sobre cómo usar Amazon EC2, consulte la documentación de Amazon Elastic Compute Cloud.
- Si lo está utilizando WorkSpaces, asumimos que está familiarizado con WorkSpaces. Para obtener más información sobre cómo usarlo WorkSpaces, consulta la Guía WorkSpaces del usuario de Amazon.
- Si utilizas VMware Cloud on AWS, asumimos que lo conoces. Para obtener más información, consulta VMware Cloud on AWS.
- Damos por sentado que conoce los conceptos de Microsoft Active Directory.

Requisitos previos

Para crear un sistema de FSx archivos de Amazon, necesitas lo siguiente:

- Una AWS cuenta con los permisos necesarios para crear un sistema de FSx archivos de Amazon y una EC2 instancia de Amazon. Para obtener más información, consulte Configuración de su Cuenta de AWS.
- Una EC2 instancia de Amazon que ejecuta Microsoft Windows Server en la nube privada virtual (VPC) basada en el servicio Amazon VPC que desea asociar a su sistema de archivos de Amazon. FSx Para obtener información sobre cómo crear una, consulte Introducción a las instancias de Amazon EC2 Windows en la Guía del EC2 usuario de Amazon.
- Amazon FSx trabaja con Microsoft Active Directory para realizar la autenticación de los usuarios y el control de acceso. Al crearlo, debe unir su sistema de FSx archivos de Amazon a un Active Directory de Microsoft. Para obtener más información, consulte Trabajar con Microsoft Active Directory.
- En esta guía, se da por sentado no cambió las reglas del grupo de seguridad predeterminado de su VPC en función del servicio Amazon VPC. Si lo has hecho, asegúrate de añadir las reglas necesarias para permitir el tráfico de red desde tu EC2 instancia de Amazon a tu sistema de FSx archivos de Amazon. Para obtener más información, consulta Seguridad en Amazon FSx.
- Instala y configura el AWS Command Line Interface (AWS CLI). Las versiones admitidas son 1.9.12 y posteriores. Para obtener más información, consulte Instalar, actualizar y desinstalar la AWS CLI en la Guía del usuario de AWS Command Line Interface .

> **Note**
>
> Puedes comprobar la versión AWS CLI que estás utilizando con el `aws --version` comando.

Foros FSx de Amazon para Windows File Server

Si tienes problemas al usar Amazon FSx, usa los foros.

¿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 estás preparado para crear tu primer sistema de FSx archivos de Amazon, prueba elPrimeros pasos con Amazon FSx para Windows File Server.
2. Para obtener más información acerca del rendimiento, consulte FSx para el rendimiento del servidor de archivos de Windows.
3. Para conocer los detalles FSx de seguridad de Amazon, consulteSeguridad en Amazon FSx.
4. Para obtener información sobre la FSx API de Amazon, consulta la referencia de la FSx API de Amazon.

Prácticas recomendadas FSx para Windows File Server

Le recomendamos que siga estas prácticas recomendadas cuando trabaje con Amazon FSx for Windows File Server.

Temas

- Prácticas recomendadas generales
- Prácticas recomendadas de seguridad
- Active Directory
- Configurar y ajustar el tamaño del sistema de archivos

Prácticas recomendadas generales

Creación de un plan de monitoreo

Puede usar las métricas del sistema de archivos para supervisar el uso del almacenamiento y el rendimiento, comprender los patrones de uso y activar notificaciones cuando el uso se acerque a los límites de almacenamiento o rendimiento del sistema de archivos. La supervisión de los sistemas de FSx archivos de Amazon junto con el resto del entorno de aplicaciones le permite depurar rápidamente cualquier problema que pueda afectar al rendimiento.

Garantizar que sus sistemas de archivos dispongan de recursos suficientes

La insuficiencia de recursos puede provocar un aumento de la latencia y de las colas de espera para las solicitudes de E/S, lo que puede parecer una falta de disponibilidad total o parcial del sistema de archivos. Para obtener más información sobre el monitoreo del rendimiento y el acceso a las advertencias y recomendaciones de rendimiento, consulte Advertencias y recomendaciones de rendimiento.

Prácticas recomendadas de seguridad

Recomendamos que siga estas prácticas recomendadas para administrar los controles de seguridad y acceso de su sistema de archivos. Para obtener información más detallada sobre cómo configurar Amazon FSx para cumplir sus objetivos de seguridad y conformidad, consulteSeguridad en Amazon FSx.

Seguridad de la red

No modifique ni elimine el ENI asociado a su sistema de archivos

Se accede a su sistema de FSx archivos de Amazon a través de una interfaz de red elástica (ENI) que reside en la nube privada virtual (VPC) asociada a su 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.

Uso de redes y grupos de seguridad ACLs

Puede usar grupos de seguridad y listas de control de acceso a la red (ACLs) para limitar el acceso a sus sistemas de archivos. En el caso de los grupos de seguridad de VPC, el grupo de seguridad predeterminado ya está agregado al sistema de archivos en la consola. Asegúrese de que el grupo de seguridad y la red de ACLs las subredes en las que ha creado el sistema de archivos permiten el tráfico en los puertos.

Active Directory

Al crear un sistema de FSx archivos de Amazon, puede unirlo a su dominio de Microsoft Active Directory para proporcionar autenticación de usuario y autorización de control de acceso a nivel de recursos compartidos, archivos y carpetas. Sus usuarios pueden usar sus cuentas de Active Directory existentes para conectarse a los recursos compartidos de archivos y acceder a los archivos y carpetas que contienen. Además, puede migrar la configuración de ACL de seguridad existente a Amazon FSx sin modificaciones. Amazon le FSx ofrece dos opciones para Active Directory: Microsoft Active Directory AWS administrado o Microsoft Active Directory autoadministrado.

Si utiliza un Microsoft Active Directory AWS administrado, le recomendamos que deje la configuración predeterminada del grupo de seguridad de Active Directory. Si modifica esta configuración, asegúrese de mantener una configuración de red que satisfaga los requisitos de la red. Para obtener más información, consulte Requisitos previos de red.

Si utiliza un Microsoft Active Directory autogestionado, dispone de opciones adicionales para configurar el sistema de archivos. Recomendamos las siguientes prácticas recomendadas para la configuración inicial cuando utilices Amazon FSx con tu Microsoft Active Directory autogestionado:

- Asigne subredes a un único sitio de Active Directory: si su entorno de Active Directory tiene una gran cantidad de controladores de dominio, utilice Sitios y servicios de Active Directory

para asignar las subredes que utilizan los sistemas de FSx archivos de Amazon a un único sitio de Active Directory con la máxima disponibilidad y fiabilidad. Asegúrese de que el grupo de seguridad de la VPC, la ACL de la red de la VPC, las reglas del firewall de Windows y cualquier otro control de enrutamiento de red que tenga en su infraestructura de Active Directory permitan la comunicación desde Amazon FSx en los puertos necesarios. DCs Esto permite que Windows vuelva a otro sitio DCs si no puede usar el sitio de Active Directory asignado. Para obtener más información, consulte Control de acceso al sistema de archivos con Amazon VPC.

- Usa una unidad organizativa (OU) independiente: usa una OU para tus sistemas de FSx archivos de Amazon que sea independiente de cualquier otra unidad organizativa que puedas tener.
- Configura tu cuenta de servicio con los privilegios mínimos requeridos: configura o delega la cuenta de servicio que proporcionaste a Amazon FSx con los privilegios mínimos requeridos. Para obtener más información, consulte Uso de un Active Directory de Microsoft autoadministrado.
- Compruebe continuamente la configuración de Active Directory: ejecute la herramienta de validación de Amazon FSx Active Directory en su configuración de Active Directory antes de crear el sistema de FSx archivos de Amazon para comprobar que la configuración es válida para su uso con Amazon FSx y detectar cualquier advertencia o error que pueda exponer la herramienta.

Evite perder disponibilidad debido a una mala configuración de Active Directory

Cuando utilices Amazon FSx con tu Microsoft Active Directory autogestionado, es importante tener una configuración de Active Directory válida no solo durante la creación del sistema de archivos, sino también para las operaciones y la disponibilidad continuas. Durante los eventos de recuperación ante fallos, los eventos de mantenimiento rutinario y las acciones de actualización de la capacidad de rendimiento, Amazon FSx vuelve a unir los recursos del servidor de archivos a su Active Directory. Si la configuración de Active Directory no es válida durante un evento, el sistema de archivos cambia al estado de Configuración incorrecta y corre el riesgo de dejar de estar disponible. Estas son algunas formas de evitar la pérdida de disponibilidad:

- Mantenga actualizada la configuración de Active Directory con Amazon FSx: si realiza cambios, como restablecer la contraseña de su cuenta de servicio, asegúrese de actualizar la configuración de todos los sistemas de archivos que utilicen esta cuenta de servicio.
- Supervise si hay errores de configuración de Active Directory: configure usted mismo las notificaciones de estado de configuración incorrecta para poder restablecer la configuración de Active Directory del sistema de archivos, si es necesario. Para ver un ejemplo en el que se utiliza

una solución basada en Lambda para lograrlo, consulte Supervisión del estado de los sistemas de FSx archivos de Amazon mediante Amazon y. EventBridge AWS Lambda

- Valide la configuración de Active Directory con regularidad: si quiere detectar de forma proactiva un error de configuración de Active Directory, le recomendamos que ejecute la herramienta de validación de Active Directory en función de su configuración de Active Directory de forma continua. Si recibe advertencias o errores al ejecutar la herramienta de validación, significa que su sistema de archivos corre el riesgo de configurarse incorrectamente.
- No muevas ni modifiques los objetos informáticos creados por FSx: Amazon FSx crea y gestiona objetos informáticos en tu Active Directory mediante la cuenta de servicio y los permisos que nos proporciones. Mover o modificar estos objetos informáticos puede provocar una configuración incorrecta del sistema de archivos.

Windows ACLs

Con Amazon FSx, utilizas las listas de control de acceso estándar de Windows (ACLs) para un control de acceso detallado a nivel de recursos compartidos, archivos y carpetas. Los sistemas de FSx archivos de Amazon verifican automáticamente las credenciales de los usuarios que acceden a los datos del sistema de archivos para hacer cumplir estos requisitos de Windows ACLs.

- No cambies los permisos de ACL de NTFS para el usuario de SYSTEM: Amazon FSx requiere que el usuario de SYSTEM tenga el control total de los permisos de ACL de NTFS en todas las carpetas de tu sistema de archivos. Si se cambian los permisos de ACL de NTFS para el usuario del SISTEMA, es posible que el sistema de archivos quede inaccesible y que las copias de seguridad futuras del sistema de archivos queden inutilizables.

Configurar y ajustar el tamaño del sistema de archivos

Selección de un tipo de implementación

Amazon FSx ofrece dos opciones de implementación: Single-AZ y Multi-AZ. Recomendamos utilizar sistemas de archivos Multi-AZ para la mayoría de las cargas de trabajo de producción que requieren una alta disponibilidad para los datos de archivos de Windows compartidos. Para obtener más información, consulte Disponibilidad y durabilidad: sistemas de archivos Single-AZ y Multi-AZ..

Selección de una capacidad de rendimiento

Configure su sistema de archivos con una capacidad de rendimiento suficiente para satisfacer no solo el tráfico esperado de su carga de trabajo, sino también los recursos de rendimiento adicionales necesarios para admitir las características que desea habilitar en su sistema de archivos. Por ejemplo, si está ejecutando la deduplicación de datos, la capacidad de rendimiento que seleccione debe proporcionar suficiente memoria para ejecutar la deduplicación en función del almacenamiento del que disponga. Si utiliza copias de redundancia, aumente la capacidad de rendimiento hasta un valor que sea al menos tres veces superior al valor que se espera que genere su carga de trabajo para evitar que Windows Server elimine las copias de redundancia. Para obtener más información, consulte Impacto de la capacidad de rendimiento en el rendimiento.

Aumentar la capacidad de almacenamiento y la capacidad de rendimiento

Aumente la capacidad de almacenamiento de su sistema de archivos cuando se esté agotando el espacio de almacenamiento gratuito o cuando espere que sus necesidades de almacenamiento superen el límite de almacenamiento actual. Recomendamos mantener al menos un 20% de la capacidad de almacenamiento libre en todo momento en su sistema de archivos. También recomendamos aumentar la capacidad de rendimiento en al menos un 20% antes de aumentar la capacidad de almacenamiento para compensar cualquier impacto en el rendimiento durante un aumento de almacenamiento. Puedes usar la FreeStorageCapacity CloudWatch métrica para monitorear la cantidad de almacenamiento gratuito disponible y entender su evolución. Para obtener más información, consulte Administrar la capacidad de almacenamiento.

También debe aumentar la capacidad de rendimiento de su sistema de archivos si su carga de trabajo está limitada por los límites de rendimiento actuales. Puede utilizar la página Supervisión y rendimiento de la FSx consola para ver cuándo las demandas de carga de trabajo se han acercado o superado los límites de rendimiento y determinar si su sistema de archivos está insuficientemente aprovisionado para su carga de trabajo.

Para minimizar la duración del escalado del almacenamiento y evitar la reducción del rendimiento de escritura, le recomendamos aumentar la capacidad de rendimiento del sistema de archivos antes de aumentar la capacidad de almacenamiento y, después, reducirla una vez finalizado el aumento de la capacidad de almacenamiento. La mayoría de las cargas de trabajo experimentan un impacto mínimo en el rendimiento durante el escalado del almacenamiento. Sin embargo, los sistemas de archivos con almacenamiento en disco duro y las cargas de trabajo que implican un gran número de usuarios finales, altos niveles de E/S o los conjuntos de datos con un gran número de archivos pequeños podrían experimentar una reducción temporal del rendimiento. Para obtener más

información, consulte Los aumentos de capacidad de almacenamiento y el rendimiento del sistema de archivos.

Modificación de la capacidad de rendimiento durante los períodos de inactividad

La actualización de la capacidad de rendimiento interrumpe la disponibilidad durante unos minutos en los sistemas de archivos Single-AZ y provoca la conmutación por error y por recuperación en los sistemas de archivos Multi-AZ. En el caso de los sistemas de archivos Multi-AZ, si hay tráfico continuo durante la conmutación por error y la conmutación por recuperación, cualquier cambio en los datos que se haya realizado durante este tiempo deberá sincronizarse entre los servidores de archivos. El proceso de sincronización de datos puede tardar varias horas en el caso de cargas de trabajo con un uso intensivo de escrituras y de IOPS. Si bien su sistema de archivos seguirá disponible durante este tiempo, recomendamos que programe períodos de mantenimiento y realice actualizaciones de la capacidad de rendimiento durante los períodos de inactividad cuando la carga de su sistema de archivos es mínima para reducir la duración de la sincronización de datos. Para obtener más información, consulte Administración de la capacidad de rendimiento.

Primeros pasos con Amazon FSx para Windows File Server

A continuación, puede obtener información sobre cómo empezar a utilizar FSx Windows File Server. Este ejercicio introductorio incluye los siguientes pasos.

1. Inscríbase en una cuenta Cuenta de AWS y cree un usuario administrativo en la cuenta.
2. Cree un Active Directory de Microsoft AD AWS administrado mediante AWS Directory Service. Unirá el sistema de archivos y su instancia informática al Active Directory.
3. Cree una instancia informática de Amazon Elastic Compute Cloud que ejecute Microsoft Windows Server. Usará esta instancia para acceder al sistema de archivos.
4. Cree un sistema de archivos de Amazon FSx para Windows File Server con la FSx consola de Amazon.
5. Asigne su sistema de archivos a su EC2 instancia
6. Escriba datos en el sistema de archivos.
7. Haga una copia de seguridad del sistema de archivos.
8. Limpie los recursos de que ha creado.

Temas

- Configuración de su Cuenta de AWS
- Paso 1. Configuración de un Active Directory
- Paso 2: lanza una instancia de Windows en la EC2 consola de Amazon
- Paso 3: Conectarse a la instancia
- Paso 4: une la instancia a tu AWS Directory Service directorio
- Paso 5. Crear el sistema de archivos
- Paso 6. Asigne el recurso compartido de archivos a una EC2 instancia que ejecute Windows Server
- Paso 7. Escribir datos en el recurso compartido de archivos
- Paso 8. Hacer una copia de seguridad del sistema de archivos
- Paso 9. Eliminar recursos

Configuración de su Cuenta de AWS

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

Inscríbete en una Cuenta de AWS

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

Para suscribirte a una Cuenta de AWS

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

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

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

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

Creación de un usuario con acceso administrativo

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

Proteja su Usuario raíz de la cuenta de AWS

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

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte 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 .

Paso 1. Configuración de un Active Directory

Con Amazon FSx, puede gestionar un almacenamiento de archivos totalmente gestionado para cargas de trabajo basadas en Windows. Del mismo modo, AWS Directory Service proporciona directorios totalmente gestionados para utilizarlos en la implementación de la carga de trabajo. Si tiene un dominio corporativo de Active Directory que se ejecuta AWS en una nube privada virtual (VPC) mediante EC2 instancias, puede habilitar la autenticación y el control de acceso basados en el usuario. Para ello, debe establecer una relación de confianza entre su Microsoft Active Directory AWS administrado y su dominio corporativo. Para la autenticación de Windows en Amazon FSx, solo necesita una confianza de bosques unidireccional, en la que el bosque AWS gestionado confíe en el bosque de dominio corporativo.

Su dominio corporativo asume la función de dominio de confianza y el dominio AWS Directory Service administrado asume la función de dominio de confianza. Las solicitudes de autenticación validadas viajan entre los dominios en una sola dirección, lo que permite que las cuentas de su dominio corporativo se autentiquen con los recursos compartidos en el dominio administrado. En este caso, Amazon solo FSx interactúa con el dominio gestionado. Luego, el dominio administrado transfiere las solicitudes de autenticación a su dominio corporativo.

> **Note**
>
> También puedes usar un tipo de confianza externa con Amazon FSx para los dominios de confianza.

Su grupo de seguridad de Active Directory debe habilitar el acceso entrante desde el grupo de seguridad del sistema de FSx archivos de Amazon.

Para crear un servicio de AWS directorio para Microsoft Active Directory

- Si aún no tiene uno, utilícelo AWS Directory Service para crear el directorio AWS administrado de Microsoft Active Directory. Para obtener más información, consulte Crear su Microsoft Active Directory AWS administrado en la Guía de AWS Directory Service administración.

  > **Important**
  >
  > Recuerde la contraseña que asigne al usuario administrador; la necesitará más adelante en este ejercicio de introducción. Si olvida la contraseña, debe repetir los pasos de este ejercicio con el nuevo AWS Directory Service directorio y el usuario administrador.

- Si ya tiene un Active Directory, cree una relación de confianza entre su Microsoft Active Directory AWS administrado y su Active Directory existente. Para obtener más información, consulte Cuándo crear una relación de confianza en la Guía de administración de AWS Directory Service .

Paso 2: lanza una instancia de Windows en la EC2 consola de Amazon

Puede lanzar una instancia de Windows mediante el procedimiento AWS Management Console que se describe en el siguiente procedimiento. El objetivo es ayudarlo a iniciar su primera instancia rápidamente, por lo que este ejercicio no cubre todas las opciones posibles. Para obtener más información sobre las opciones avanzadas, consulte Lanzamiento de una instancia.

Cómo lanzar una instancia

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de la consola, elija Iniciar instancia.
3. La página Choose an Amazon Machine Image (AMI) muestra una lista de configuraciones básicas, denominadas Amazon Machine Images (AMIs), que sirven como plantillas para la instancia. Seleccione la AMI para Windows Server 2016 Base o versiones posteriores. Tenga en cuenta que AMIs están marcadas como «Aptas para el nivel gratuito».
4. En la página Elegir un tipo de instancia, puede seleccionar la configuración de hardware de la instancia. Seleccione el tipo `t2.micro`, que es la opción predeterminada. Observe que este tipo de instancia es apta para la capa gratuita.

5. Elija Revisar y lanzar para dejar que el asistente rellene los demás valores de configuración automáticamente.
6. En la página Revisar el lanzamiento de la instancia, en los Grupos de seguridad, verá que el asistente ya le creó y seleccionó un grupo de seguridad. Puede usar este grupo de seguridad, o puede elegir el grupo de seguridad que creó durante la configuración inicial con los siguientes pasos:

   a. Elija Editar grupos de seguridad.

   b. En la página Configurar grupo de seguridad, asegúrese de que Seleccionar un grupo de seguridad existente está seleccionado.

   c. Seleccione el grupo de seguridad en la lista de grupos de seguridad existentes y, a continuación, elija Revisar y lanzar.
7. En la página Revisar el lanzamiento de la instancia, elija Iniciar.
8. Cuando se le solicite un par de claves, seleccione Elegir un par de claves existente y, a continuación, seleccione el par de claves que creó durante la configuración inicial.

   Como opción, puede crear un nuevo par de claves. Seleccione Crear un nuevo par de claves, escriba un nombre para el par de claves y elija Descargar par de claves. Esta es la única oportunidad para guardar el archivo de clave privada, así que asegúrese de descargarlo. Guarde el archivo de clave privada en un lugar seguro. Deberá proporcionar el nombre de su par de claves al lanzar una instancia, y la clave privada correspondiente cada vez que se conecte a dicha instancia.

   > ⚠ Warning
   >
   > No seleccione la opción Continuar sin un par de claves. Si lanza la instancia sin un par de claves, no podrá conectarse a ella.

   Cuando esté listo, seleccione la casilla de confirmación y después elija Iniciar instancias.
9. Verá una página de confirmación que indicará que la instancia se está lanzando. Elija View instances para cerrar la página de confirmación y volver a la consola.
10. Puede ver el estado del lanzamiento en la pantalla Instancias. La instancia tarda poco tiempo en lanzarse. Al lanzar una instancia, su estado inicial es `pending`. Una vez iniciada la instancia, el estado cambia a `running` y recibe un nombre del DNS público. (Si la columna DNS público

(IPv4) está oculta, selecciona Mostrar u ocultar columnas (el icono con forma de engranaje) en la esquina superior derecha de la página y, a continuación, selecciona DNS público (). IPv4

11. Puede que transcurran unos minutos hasta que la instancia esté lista para conectarse a ella. Compruebe que la instancia haya superado las comprobaciones de estado; puede ver esta información en la columna Status Checks.

> **Important**
>
> Anote el ID del grupo de seguridad que se creó al iniciar esta instancia. Lo necesitarás cuando crees tu sistema de FSx archivos de Amazon.

Ahora que la instancia está iniciada, puede conectarse a ella.

Paso 3: Conectarse a la instancia

Para conectarse a una instancia de Windows, deber recuperar la contraseña inicial del administrador y luego especificar esta contraseña cuando se conecte a la instancia mediante escritorio remoto.

El nombre de la cuenta de administrador depende del idioma del sistema operativo. Por ejemplo, en inglés, es Administrator, en francés es Administrateur, y en portugués es Administrador. Para obtener más información, consulte Nombres localizados para cuentas de administrador en Windows en Microsoft TechNet Wiki.

Si unió la instancia a un dominio, puede conectarse a la instancia con las credenciales del dominio que haya definido en AWS Directory Service. En la pantalla de inicio de sesión de Remote Desktop, no utilice el nombre del equipo local ni la contraseña generada. En su lugar, utilice el nombre de usuario completo del administrador y la contraseña de esta cuenta. Un ejemplo es **`corp.example.com\Admin`**.

La licencia del sistema operativo (OS) Windows Server permite dos conexiones remotas simultáneas para fines administrativos. La licencia de Windows Server está incluida en el precio de la instancia de Windows. Si necesita más de dos conexiones remotas simultáneas, debe comprar una licencia de Servicios de escritorio remoto (RDS). Si intenta realizar una tercera conexión, se produce un error. Para obtener más información, consulte Configurar el número de conexiones remotas simultáneas permitidas para una conexión.

Cómo conectarse a la instancia de Windows mediante un cliente RDP

1. En la EC2 consola de Amazon, selecciona la instancia y, a continuación, selecciona Connect.
2. En el cuadro de diálogo Conectar a la instancia, elija Obtener contraseña (transcurren unos minutos hasta que la contraseña esté disponible una vez iniciada la instancia).
3. Elija Examina) y desplácese hasta el archivo de clave privada que creó cuando lanzó la instancia. Seleccione el archivo y elija Abrir para copiar todo el contenido del archivo en el campo Contenido.
4. Elija Descifrar contraseña. La consola muestra la contraseña de administrador predeterminada para la instancia en el cuadro de diálogo Conectar a la instancia, y reemplaza el enlace a Obtener contraseña que se mostró anteriormente con la contraseña real.
5. Anote la contraseña de administrador predeterminada o cópiela en el portapapeles. La necesitará para conectarse a la instancia.
6. Elija Download Remote Desktop File. El navegador le pedirá que abra o guarde el archivo .rdp. Puede elegir cualquiera de las dos opciones. Cuando termine, puede elegir Cerrar para descartar el cuadro de diálogo Conectar a la instancia.
   - Si ha abierto el archivo .rdp, verá el cuadro de diálogo Conexión remota en escritorio.
   - Si ha guardado el archivo .rdp, desplácese hasta el directorio de descargas y abra el archivo .rdp para mostrar el cuadro de diálogo.
7. Es posible que aparezca una advertencia en la que se indique que se desconoce el publicador de la conexión remota. Puede seguir conectándose a la instancia.
8. Cuando se le pida, inicie sesión en la instancia con la cuenta de administrador del sistema operativo y la contraseña que anotó o copió anteriormente. Si la Conexión a escritorio remoto ya tiene una cuenta de administrador configurada, es posible que tenga que elegir la opción Usar otra cuenta y escribir el nombre de usuario y la contraseña manualmente.

   > **Note**
   >
   > A veces, al copiar y pegar el contenido se dañan los datos. Si aparece el error "Password Failed" (Error de contraseña) al iniciar sesión, pruebe a especificar la contraseña manualmente.

9. Debido a la naturaleza de los certificados autofirmados, es posible que aparezca una advertencia que indica que no se pudo autenticar el certificado de seguridad. Realice los pasos

siguientes para verificar la identidad del equipo remoto o simplemente elija Sí o Continuar para continuar si el certificado es de confianza.

a. Si usa Conexión a Escritorio remoto desde un equipo Windows, elija Ver certificado. Si usa Microsoft Remote Desktop en un Mac, elija Ver certificado.
b. Selecciona la pestaña Detalles y desplázate hacia abajo hasta la entrada Huella digital en un PC con Windows o la entrada SHA1Huellas digitales en un Mac. Este el identificador único del certificado de seguridad del equipo remoto.
c. En la EC2 consola de Amazon, selecciona la instancia, selecciona Acciones y, a continuación, selecciona Obtener registro del sistema.
d. En el resultado del log del sistema, busque una entrada llamada `RDPCERTIFICATE-THUMBPRINT`. Si este valor coincide con la huella digital o la huella dactilar del certificado, ha verificado la identidad del equipo remoto.
e. Si usa Conexión a Escritorio remoto desde un equipo Windows, vuelva al cuadro de diálogo Certificado y elija Aceptar. Si usa Escritorio remoto de Microsoft en un Mac, vuelva al cuadro de diálogo Verificar certificado y elija Continuar.
f. [Windows] Elija Sí en la ventana Conexión remota de escritorio para conectarse a la instancia.

Ahora que está conectado a la instancia, puede unirla al directorio de AWS Directory Service .

Paso 4: une la instancia a tu AWS Directory Service directorio

El siguiente procedimiento le muestra cómo unir manualmente una instancia de Amazon EC2 Windows existente a su AWS Directory Service directorio.

Para unir una instancia de Windows a su AWS Directory Service directorio

1. Conéctese a la instancia mediante un cliente de Protocolo de escritorio remoto.
2. Abre el cuadro de diálogo de IPv4 propiedades TCP/ de la instancia.

   a. Abra Conexiones de red.

   > **Tip**
   >
   > Puede abrir Conexiones de red directamente ejecutando lo siguiente en un símbolo del sistema en la instancia.

```
%SystemRoot%\system32\control.exe ncpa.cpl
```

b. Abra el menú contextual (haga clic con el botón) de cualquier conexión de red habilitada y, luego, elija Propiedades.

c. En el cuadro de diálogo de propiedades de conexión, abra (doble clic) Protocolo de Internet versión 4.

3. (Opcional) Seleccione Usar las siguientes direcciones de servidor DNS, cambie las direcciones del servidor DNS preferido y del servidor DNS alternativo por las direcciones IP de los servidores DNS AWS Directory Service proporcionados y, a continuación, pulse Aceptar.

4. Abra el cuadro de diálogo Propiedades del sistema de la instancia, seleccione la pestaña Nombre de equipo y elija Cambiar.

> **Tip**
>
> Puede abrir el cuadro de diálogo Propiedades del sistema directamente en un símbolo del sistema en la instancia.
>
> ```
> %SystemRoot%\system32\control.exe sysdm.cpl
> ```

5. En el cuadro Miembro de, elija Dominio, introduzca el nombre completo del AWS Directory Service directorio y pulse Aceptar.

6. Cuando se le solicite el nombre y la contraseña de administrador de dominio, ingrese el nombre de usuario y la contraseña de la cuenta de administrador.

> **Note**
>
> Puede introducir el nombre completo de su dominio o el NetBios nombre seguido de una barra invertida (\) y, a continuación, el nombre de usuario, en este caso, Admin. Por ejemplo, corp.example.com\Admin o corp\Admin.

7. Cuando reciba el mensaje de bienvenida al dominio, reinicie la instancia para que se apliquen los cambios.

8. Vuelva a conectarse a la instancia a través de RDP e inicie sesión en la instancia con el nombre de usuario y la contraseña del usuario administrador del AWS Directory Service directorio.

Ahora que tu instancia se ha unido al dominio, estás listo para crear tu sistema de FSx archivos de Amazon.

Paso 5. Crear el sistema de archivos

Cómo crear el sistema de archivos (consola)

1. Abre 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 FSx Windows File Server y, a continuación, elija Siguiente. Aparece la página Create file system.
4. En Método de creación, elija Creación estándar.

Detalles del sistema de archivos

1. En la sección Detalles del sistema de archivos, proporcione un nombre para el 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, espacio en blanco y números, además de los siguientes caracteres especiales: + - = . _ : /
2. En Tipo de implementación, elija Multi-AZ o Single-AZ.

   - Elija Multi-AZ para implementar un sistema de archivos que sea tolerante a la no disponibilidad de la zona de disponibilidad. Esta opción admite el almacenamiento en SSD y HDD.
   - Elija Single-AZ para implementar un sistema de archivos que se implemente en una sola zona de disponibilidad. Single-AZ 2 es la última generación de sistemas de archivos de zona de disponibilidad única y admite almacenamiento SSD y HDD.

   Para obtener más información, consulte Disponibilidad y durabilidad: sistemas de archivos Single-AZ y Multi-AZ..
3. En cuanto al tipo de almacenamiento, puede elegir entre SSD o HDD.

   FSx para Windows File Server ofrece tipos de almacenamiento en unidades de estado sólido (SSD) y unidades de disco duro (HDD). El almacenamiento de SSD está diseñado para las cargas de trabajo de mayor rendimiento y más sensibles a la latencia, incluidas las bases de datos, las cargas de trabajo de procesamiento multimedia y las aplicaciones de análisis de

datos. El almacenamiento de HDD está diseñado para una amplia gama de cargas de trabajo, que incluye los directorios principales, los recursos compartidos de archivos por usuarios y departamentos y los sistemas de administración de contenido. Para obtener más información, consulte Acerca de los tipos de almacenamiento.

4. Para las IOPS de SSD aprovisionadas, puede elegir entre el modo automático o el Aprovisionamiento por el usuario.

   Si elige el modo automático, FSx Windows File Server escala automáticamente las IOPS de su SSD para mantener 3 IOPS de SSD por GiB de capacidad de almacenamiento. Si elige el modo aprovisionado por el usuario, ingrese cualquier número entero entre 96 y 400 000. El escalado de IOPS de SSD por encima de 80 000 está disponible en el Este de EE. UU. (Norte de Virginia), Oeste de EE. UU. (Oregón), Este de EE. UU. (Ohio), Europa (Irlanda), Asia-Pacífico (Tokio), Asia-Pacífico (Tokio) y Asia-Pacífico (Singapur). Para obtener más información, consulte Cómo administrar IOPS de SSD.

5. En Capacidad de almacenamiento, introduzca la capacidad de almacenamiento de su sistema de archivos, en GiB. Si utiliza un almacenamiento SSD, introduzca cualquier número entero comprendido entre 32 y 65 536. Si utiliza un almacenamiento SSD, introduzca cualquier número entero comprendido entre 2000 y 65 536. Puede aumentar la capacidad de almacenamiento según sea necesario en cualquier momento después de crear el sistema de archivos. Para obtener más información, consulte Administrar la capacidad de almacenamiento.

6. En el campo Throughput capacity (Capacidad de rendimiento), mantenga la configuración predeterminada. Capacidad de rendimiento: velocidad constante a la que el servidor de archivos que aloja a su sistema de archivos puede servir datos. La configuración de capacidad de rendimiento recomendada se basa en la cantidad de capacidad de almacenamiento que elija. Si necesita una capacidad de rendimiento superior a la recomendada, elija Especificar la capacidad de rendimiento y, a continuación, elija un valor. Para obtener más información, consulte FSx para el rendimiento del servidor de archivos de Windows.

   > **Note**
   >
   > Si va a habilitar la auditoría del acceso a los archivos, debe elegir una capacidad de rendimiento de 32 o más. MBps Para obtener más información, consulte Registro del acceso de usuarios finales con auditoría de acceso a archivos.

Puede modificar la capacidad de rendimiento según sea necesario en cualquier momento después de crear el sistema de archivos. Para obtener más información, consulte Administración de la capacidad de rendimiento.

Red y seguridad

1. En la sección Red y seguridad, elija la VPC de Amazon que desea asociar con su sistema de archivos. Para este ejercicio de introducción, elija la misma Amazon VPC que eligió para su AWS Directory Service directorio y su instancia de Amazon EC2 .
2. En el caso de los Grupos de seguridad de VPC, el grupo de seguridad predeterminado de la VPC de Amazon predeterminada ya está agregado al sistema de archivos en la consola. Si no utiliza el grupo de seguridad predeterminado, asegúrese de que el grupo de seguridad que elija sea el mismo Región de AWS que el de su sistema de archivos. Para asegurarse de que puede conectar una EC2 instancia a su sistema de archivos, tendrá que añadir las siguientes reglas al grupo de seguridad que haya elegido:

   a. Agregue las siguientes reglas de entrada y salida para permitir los siguientes puertos.

Reglas	Puertos
UDP	53, 88, 123, 389, 464
TCP	53, 88, 135, 389, 445, 464, 636, 3268, 3269, 5985, 9389, 49152-65535

   Añada las direcciones IP o el grupo de seguridad de origen y destino IDs asociados a las instancias informáticas del cliente desde las que desea acceder al sistema de archivos.

   b. Añada reglas de salida para permitir que todo el tráfico entre en el Active Directory al que va a unir el sistema de archivos. Para ello, siga uno de estos pasos:

   - Permita que el tráfico saliente vaya al ID del grupo de seguridad asociado a su directorio de AD de AWS administrado.
   - Permita que el tráfico saliente llegue a las direcciones IP asociadas a los controladores de dominio de Active Directory autoadministrados.

> **Note**
>
> En algunos casos, es posible que haya modificado las reglas de su grupo de AWS Managed Microsoft AD seguridad con respecto a la configuración predeterminada. Si es así, asegúrate de que este grupo de seguridad tenga las reglas de entrada necesarias para permitir el tráfico desde tu sistema de FSx archivos de Amazon. Para obtener más información sobre las reglas de entrada necesarias, consulte los requisitos previos de AWS Managed Microsoft AD en la Guía de administración de AWS Directory Service .

Para obtener más información, consulte Control de acceso al sistema de archivos con Amazon VPC.

3. Los sistemas de archivos Multi-AZ tienen un servidor de archivos principal y uno en espera, cada uno en su propia zona de disponibilidad y subred. Si va a crear un sistema de archivos Multi-AZ (consulte el paso 5), elija el valor Subred preferida para el servidor de archivos principal y el valor Subred en espera para el servidor de archivos en espera.

   Si va a crear un sistema de archivos Single-AZ, elija la subred para el sistema de archivos.

Autenticación de Windows

- Para la autenticación de Windows, tiene las siguientes opciones:

  Elija Microsoft Active Directory AWS administrado si desea unir su sistema de archivos a un dominio de Microsoft Active Directory administrado por y AWS, a continuación, elija su AWS Directory Service directorio de la lista. Para obtener más información, consulte Trabajar con Microsoft Active Directory.

  Si desea unir el sistema de archivos a un dominio de Microsoft Active Directory autoadministrado, elija Microsoft Active Directory autoadministrado y proporcione los siguientes detalles para el Active Directory. Para obtener más información, consulte Uso de un Active Directory de Microsoft autoadministrado.

  - El nombre de dominio completo del dominio de Active Directory.

> **Important**
>
> En los sistemas de archivos Single-AZ 2 y en todos los sistemas de archivos Multi-AZ, el nombre de dominio de Active Directory no puede superar los 47 caracteres. Esta limitación se aplica tanto AWS Directory Service a los nombres de dominio de Active Directory como a los autogestionados.
>
> Amazon FSx requiere una conexión directa para el tráfico interno a tu dirección IP de DNS. No se admite la conexión a través de una puerta de enlace de Internet. En su lugar AWS Virtual Private Network, utilice el emparejamiento de VPC o la asociación AWS Direct Connect. AWS Transit Gateway

- Direcciones IP de los servidores DNS: IPv4 las direcciones de los servidores DNS de tu dominio

> **Note**
>
> El servidor DNS debe tener habilitados los EDNS (mecanismos de extensión para DNS). Si EDNS está deshabilitado, es posible que el sistema de archivos no pueda crearlo.

- Nombre de usuario de la cuenta de servicio: el nombre de usuario de la cuenta de servicio en su Active Directory actual. No incluya un prefijo o sufijo de dominio.
- Contraseña de la cuenta de servicio: la contraseña de la cuenta de servicio.
- (Opcional) Unidad organizativa (OU): nombre de ruta distinguido de la unidad organizativa a la que quiere unir su sistema de archivos.
- (Opcional) Grupo de administradores de sistemas de archivos delegados: nombre del grupo de Active Directory que puede administrar el sistema de archivos. El grupo predeterminado es 'Administradores de dominio'. Para obtener más información, consulte Cuenta de FSx servicio de Amazon.

Cifrado, auditoría y acceso (alias del DNS)

1. Para el cifrado, elija la clave de AWS KMS key cifrado utilizada para cifrar los datos del sistema de archivos en reposo. Puede elegir el aws/fsx predeterminado (predeterminado) administrado por AWS KMS una clave existente o una clave administrada por el cliente especificando el ARN de la clave. Para obtener más información, consulte Cifrado de datos en reposo.

2. Para la Auditoría: opcional, la auditoría de acceso a los archivos está deshabilitada de forma predeterminada. Para obtener información sobre cómo habilitar y configurar la auditoría de acceso a los archivos, consulte Registro del acceso de usuarios finales con auditoría de acceso a archivos.
3. En Acceso: opcional, introduzca los alias de DNS que desea asociar al sistema de archivos. Cada alias debe tener el formato del nombre de dominio completo (FQDN). Para obtener más información, consulte La administración de los alias del DNS.

Copia de seguridad y mantenimiento

Para obtener más información sobre las copias de seguridad diarias automáticas y la configuración de esta sección, consulte Protección de los datos con copias de seguridad.

1. La copia de seguridad diaria automática está habilitada de forma predeterminada. Puedes desactivar esta configuración si no quieres que Amazon realice FSx copias de seguridad de tu sistema de archivos automáticamente a diario.
2. Si las copias de seguridad automáticas están habilitadas, se producen dentro de un periodo de tiempo conocido como periodo de copia de seguridad. Puede usar el periodo predeterminado o elegir una hora de inicio del periodo de copia de seguridad automático que mejor se adapte al flujo de trabajo.
3. Para el período de retención de copias de seguridad automáticas, puedes usar la configuración predeterminada de 30 días o establecer un valor entre 1 y 90 días durante el cual Amazon FSx conservará las copias de seguridad automáticas diarias de tu sistema de archivos. Esta configuración no se aplica a las copias de seguridad iniciadas por el usuario ni a las copias de seguridad realizadas por AWS Backup.
4. En Etiquetas: opcional, 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. Para obtener más información, consulte Etiquetar tus recursos de Amazon FSx .

   Elija Siguiente.

Revisar la configuración y crear

1. Revise la configuración del sistema de archivos que se muestra en la página Create File System. Para su referencia, podrá ver qué configuración del sistema de archivos puede modificar después de crear el sistema de archivos. Seleccione Crear sistema de archivos.
2. Una vez que FSx Amazon haya creado el sistema de archivos, elige el ID del sistema de archivos en la lista del panel de Sistemas de archivos para ver los detalles. Seleccione Adjuntar y anote el nombre del DNS del sistema de archivos en la pestaña Red y seguridad. Lo necesitará en el siguiente procedimiento para asignar un recurso compartido a una EC2 instancia.

Paso 6. Asigne el recurso compartido de archivos a una EC2 instancia que ejecute Windows Server

Ahora puede montar su sistema de FSx archivos de Amazon en su EC2 instancia de Amazon basada en Microsoft Windows unida a su AWS Directory Service directorio. El nombre de su recurso compartido de archivos no es el mismo que el nombre de su sistema de archivos.

Para mapear un recurso compartido de archivos en una instancia de Amazon EC2 Windows mediante la GUI

1. Para poder montar un recurso compartido de archivos en una instancia de Windows, debe lanzar la EC2 instancia y unirla a la instancia a la AWS Directory Service for Microsoft Active Directory que se ha unido su sistema de archivos. Para realizar esta acción, elija uno de los siguientes procedimientos de la Guía de AWS Directory Service administración:
   - Únase sin problemas a una EC2 instancia de Windows
   - Cómo unir manualmente una instancia de Windows
2. Conecte con la instancia . Para obtener más información, consulte Conectarse a su instancia de Windows en la Guía del EC2 usuario de Amazon.
3. Cuando esté conectado, abra el Explorador de archivos.
4. En el panel de navegación, abra el menú contextual (haga clic derecho) de Red y, a continuación, elija Conectar a unidad de red.
5. Elija la letra de unidad que prefiera para Unidad.
6. Puedes mapear tu sistema de archivos con el nombre DNS predeterminado asignado por Amazon FSx o con el alias de DNS que elijas. Este procedimiento describe el mapeo de un

recurso compartido de archivos con el nombre DNS predeterminado. Si desea mapear un recurso compartido de archivos mediante un alias DNS, consulte Acceso a los datos mediante alias del DNS.

En Carpeta, introduzca el nombre DNS del sistema de archivos y el nombre del recurso compartido. Se llama la FSx acción de Amazon predeterminada`\share`. Puedes encontrar el nombre DNS en la FSx consola de Amazon https://console.aws.amazon.com/fsx/, en la sección Windows File Server > Red y seguridad o en la respuesta CreateFileSystem o comando de la DescribeFileSystems API.

- En el caso de un sistema de archivos Single-AZ unido a un Microsoft Active Directory AWS administrado, el nombre DNS tiene el siguiente aspecto.

```
fs-0123456789abcdef0.ad-domain.com
```

- En un sistema de archivos Single-AZ unido a un Active Directory autoadministrado y en cualquier sistema de archivos Multi-AZ, el nombre del DNS tiene el siguiente aspecto.

```
amznfsxaa11bb22.ad-domain.com
```

Por ejemplo, escriba `\\fs-0123456789abcdef0.ad-domain.com\share`.

7. Elija si el recurso compartido de archivos debe Volver a conectarse al iniciar sesión y, a continuación, seleccione Finalizar.

Paso 7. Escribir datos en el recurso compartido de archivos

Ahora que ha asignado el recurso compartido de archivos a la instancia, puede usarlo como cualquier otro directorio de su entorno Windows.

Para escribir datos en su recurso compartido de archivos

1. Abra el editor de texto del Bloc de notas.
2. Escriba contenido en el editor de texto. Por ejemplo: *Hello, World!*
3. Guarde el archivo en la letra de disco de la unidad de archivo compartido.
4. Con el Explorador de archivos, navegue hasta su recurso compartido de archivos y busque el archivo de texto que acaba de guardar.

Paso 8. Hacer una copia de seguridad del sistema de archivos

Ahora que has tenido la oportunidad de usar tu sistema de FSx archivos de Amazon y sus recursos compartidos de archivos, puedes hacer una copia de seguridad. De forma predeterminada, las copias de seguridad diarias se crean automáticamente durante el período de copia de seguridad de 30 minutos del sistema de archivos. Sin embargo, puede crear una copia de seguridad iniciada por el usuario en cualquier momento. Las copias de seguridad tienen costos adicionales asociados. Para obtener más información sobre los precios de copia de seguridad, consulte Precios.

Cómo crear una copia de seguridad del sistema de archivos desde la consola

1. Abre la FSx consola de Amazon en https://console.aws.amazon.com/fsx/.
2. En el panel de control de la consola, seleccione el nombre del sistema de archivos que ha creado para este ejercicio.
3. En la pestaña Descripción general de su sistema de archivos, seleccione Crear copia de seguridad.
4. En el cuadro de diálogo Crear copia de seguridad que se abre, proporcione un nombre para la copia de seguridad. Este nombre puede contener un máximo de 256 letras Unicode e incluir espacios en blanco, números y los siguientes caracteres especiales: + - = . _ : /
5. Elija Create backup.
6. Para ver todas las copias de seguridad en una lista, de forma que pueda restaurar el sistema de archivos o eliminar la copia de seguridad, seleccione Copias de seguridad.

Al crear una nueva copia de seguridad, su estado se establece en CREACIÓN mientras se está creando. Este proceso puede tardar unos minutos. Cuando la copia de seguridad está disponible para su uso, su estado cambia a DISPONIBLE.

Paso 9. Eliminar recursos

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

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. En la FSx consola de Amazon, elimina tu sistema de archivos. Todas las copias de seguridad automáticas se eliminan automáticamente. Sin embargo, debe eliminar las copias de seguridad que se han creado de forma manual. Los pasos siguientes describen este proceso:

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

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

   c. En Acciones, seleccione Eliminar sistema de archivos.

   d. En el cuadro de diálogo Eliminar el sistema de archivos que se abre, decida si desea crear una copia de seguridad final. Si lo hace, proporcione un nombre para la copia de seguridad final. También se eliminan todas las copias de seguridad que se creen automáticamente.

      > **Important**
      >
      > Se pueden crear nuevos sistemas de archivos a partir de las copias de seguridad. Le recomendamos que cree una copia de seguridad final como práctica recomendada. Si descubre que no la necesita después de un período de tiempo determinado, puede eliminar esta y otras copias de seguridad creadas manualmente.

   e. Introduzca el ID del sistema de archivos que desea eliminar en el cuadro ID del sistema de archivos.

   f. Seleccione Eliminar sistema de archivos.

   g. El sistema de archivos se está eliminando ahora y su estado en el panel de control cambia a ELIMINACIÓN. Una vez que se elimina el sistema de archivos, deja de aparecer en el panel de control.

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

   i. En el panel de control, seleccione las copias de seguridad que tengan el mismo ID del sistema de archivos que el sistema de archivos que ha eliminado y seleccione Eliminar copia de seguridad.

   j. Se abre el cuadro de diálogo Eliminar copias de seguridad. Deje marcada la casilla de verificación del ID de la copia de seguridad que ha seleccionado y elija Eliminar copias de seguridad.

Su sistema de FSx archivos de Amazon y las copias de seguridad automáticas relacionadas ahora se eliminan.

3. Para eliminar el AWS Directory Service directorio que creó para este ejercicio, consulte Eliminar el directorio en la Guía de AWS Directory Service administración.

Acceso a sus datos

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

Temas

- Clientes compatibles
- Acceder a los datos desde el Nube de AWS
- Acceso a los datos en las instalaciones
- Acceso a los datos mediante nombres de DNS predeterminados
- Compatibilidad con espacios de nombres del sistema de archivos distribuido (DFS)
- Acceso a los datos mediante alias del DNS
- Acceso a los datos mediante recursos compartidos de archivos
- Crear, actualizar y eliminar recursos compartidos de archivos

Clientes compatibles

FSx para Windows, File Server es compatible con las versiones 2.0 a 3.1.1 del protocolo Server Message Block (SMB), lo que le brinda la flexibilidad de conectarse a sus sistemas de archivos mediante una amplia variedad de instancias informáticas y sistemas operativos.

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

- Instancias de Amazon Elastic Compute Cloud (Amazon EC2), incluidas las instancias de Microsoft Windows, Mac, Amazon Linux y Amazon Linux 2. Para obtener más información, consulte Mapeo de recursos compartidos de archivos.
- Contenedores de Amazon Elastic Container Service (Amazon ECS). Para obtener más información, consulte FSx los volúmenes de Windows File Server en la Guía para desarrolladores de Amazon Elastic Container Service.
- WorkSpaces instancias: para obtener más información, consulta la entrada del AWS blog Using FSx for Windows File Server with Amazon WorkSpaces.
- Instancias de Amazon AppStream 2.0: para obtener más información, consulta la entrada del AWS blog Cómo usar Amazon FSx con Amazon AppStream 2.0.

- VMs ejecución en AWS entornos basados en VMware la nube: para obtener más información, consulte la entrada del AWS blog Cómo almacenar y compartir archivos con FSx el servidor de archivos de Windows en un AWS entorno de VMware nube.

Se admiten los siguientes sistemas operativos para su uso con Amazon FSx:

- Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 y Windows Server 2022.
- Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10 (incluidas las experiencias de escritorio de Windows 7 y Windows 10 WorkSpaces) y Windows 11.
- Linux, con la herramienta `cifs-utils`.
- macOS

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 FSx de archivos del servidor de archivos de Windows 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 un sistema de VPCs archivos diferente Cuentas de AWS o Regiones de AWS distinto del sistema de archivos. Además de los requisitos descritos en las siguientes secciones FSx para acceder a los recursos del servidor de archivos de Windows, también debe asegurarse de que el grupo de seguridad de VPC del sistema de archivos esté configurado de modo que el tráfico de datos y administración pueda fluir entre el sistema de archivos y los clientes. Para obtener más información acerca de las reglas de los grupos de seguridad obligatorios, consulte Control de acceso al sistema de archivos con Amazon VPC.

Puede acceder al sistema FSx de archivos Windows File Server desde clientes compatibles que estén en la misma VPC que su sistema de archivos.

La siguiente tabla ilustra los entornos desde los que Amazon FSx admite el acceso de los clientes en cada uno de los entornos compatibles, en función de cuándo se creó el sistema de archivos.

Clientes ubicados en...	Acceso a los sistemas de archivos creados antes del 22 de febrero de 2019	Acceso a los sistemas de archivos creados antes del 17 de diciembre de 2020	Acceso a los sistemas de archivos creados después del 17 de diciembre de 2020
Las subredes en las que se crea el sistema de archivos	✓	✓	✓
Los bloques de CIDR principales de la VPC en la que se creó el sistema de archivos	✓	✓	✓
Secundarios CIDRs de la VPC en la que se creó el sistema de archivos		Los clientes con direcciones IP dentro un rango de direcciones IP privadas de acuerdo con la norma RFC 1918: • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	Los clientes con direcciones IP fuera del siguiente rango de bloques de CIDR: 198.19.0.0/16
Otras redes CIDRs o redes interconectadas			

> **Note**
>
> En algunos casos, es posible que desee acceder a un sistema de archivos creado antes del 17 de diciembre de 2020 en las instalaciones con un rango de direcciones IP no privadas.

Para ello, cree un nuevo sistema de archivos a partir de una copia de seguridad del sistema de archivos. Para obtener más información, consulte Protección de los datos con copias de seguridad.

Acceder a los datos desde una VPC diferente, Cuenta de AWS o Región de AWS

Puede acceder al sistema de archivos del servidor de archivos de Windows desde clientes de soporte que estén ubicados en una VPC Región de AWS diferente o desde la que esté asociada a su sistema de archivos mediante pasarelas de tránsito o interconexión de VPC. FSx Cuenta de AWS Cuando utilizas una conexión de emparejamiento de VPC o una puerta de enlace de tránsito para conectarte VPCs, las instancias de cómputo que se encuentran en una VPC pueden acceder a los sistemas de archivos de FSx Amazon que se encuentran en otra VPC. Este acceso es posible incluso si VPCs pertenecen a una diferente Cuentas de AWS e incluso si residen en una diferente. VPCs Regiones de AWS

Una conexión de emparejamiento de VPC es una conexión de red entre dos VPCs que puedes usar para enrutar el tráfico entre ellas mediante direcciones privadas IPv4 o IP de versión 6 ()IPv6. Puedes usar la interconexión de VPC para conectarte VPCs dentro de la misma AWS región o entre regiones. AWS Para obtener más información sobre la conexión de emparejamiento de las VPC, consulte ¿Qué es una conexión de emparejamiento de VPC? en la Guía de conexión de emparejamiento de VPC de Amazon.

Una puerta de enlace de tránsito es un centro de tránsito de red que puedes usar para interconectar tus redes con VPCs las locales. Para obtener más información acerca del uso de puertas de enlace de tránsito de VPC, consulte Introducción a las Puertas de enlace de tránsito en la Guía de las Puertas de enlace de tránsito de Amazon VPC.

Después de configurar una conexión de emparejamiento de las VPC o puerta de enlace de tránsito, puede acceder al sistema de archivos con el nombre del DNS. Lo hace del mismo modo que lo hace desde las instancias informáticas de la VPC asociada.

Acceso a los datos en las instalaciones

FSx para Windows, File Server admite el uso de sus sistemas de archivos AWS Direct Connect o el acceso AWS VPN a ellos desde sus instancias informáticas locales. Con la compatibilidad con AWS

Direct Connect, FSx Windows File Server le permite acceder a su sistema de archivos a través de una conexión de red dedicada desde su entorno local. Con la compatibilidad con AWS VPN, FSx Windows File Server le permite acceder a su sistema de archivos desde sus dispositivos locales a través de un túnel seguro y privado.

Tras conectar el entorno local a la VPC asociada al sistema de archivos de FSx Amazon, puede acceder al sistema de archivos mediante su nombre de DNS o un alias de DNS. Lo hace del mismo modo que desde las instancias informáticas de la VPC. Para obtener más información sobre AWS Direct Connect, consulte la Guía del usuario de AWS Direct Connect. Para obtener más información acerca de establecer las conexiones de la AWS VPN , consulte las Conexiones de la VPN en la Guía del usuario de Amazon VPC.

> **Note**
>
> En algunos casos, es posible que desee acceder a un sistema de archivos creado antes del 17 de diciembre de 2020 en las instalaciones con un rango de direcciones IP no privadas. Para ello, cree un nuevo sistema de archivos a partir de una copia de seguridad del sistema de archivos. Para obtener más información, consulte Protección de los datos con copias de seguridad.

FSx for Windows File Server también admite el uso de Amazon FSx File Gateway para proporcionar un acceso fluido y de baja latencia a los recursos compartidos de archivos FSx de Windows File Server en la nube desde sus instancias informáticas locales. Para obtener más información, consulte la Guía del usuario de Amazon FSx File Gateway.

> **Note**
>
> Amazon FSx File Gateway ya no está disponible para nuevos clientes. Los clientes actuales de FSx File Gateway pueden seguir utilizando el servicio con normalidad. Para obtener información sobre funciones similares a las de FSx File Gateway, visite esta entrada de blog.

Acceso a los datos mediante nombres de DNS predeterminados

FSx para Windows, File Server proporciona un nombre de sistema de nombres de dominio (DNS) para cada sistema de archivos. FSx Para acceder al sistema de archivos del servidor de archivos de Windows, debe asignar una letra de unidad de su instancia de cómputo a su recurso compartido de

FSx archivos de Amazon mediante este nombre de DNS. Para obtener más información, consulte Acceso a los datos mediante recursos compartidos de archivos.

> **Important**
>
> Amazon FSx solo registra los registros DNS de un sistema de archivos si utilizas el DNS de Microsoft como DNS predeterminado. Si utilizas un DNS de terceros, debes configurar manualmente las entradas de DNS para tus sistemas de FSx archivos de Amazon. Para obtener información acerca de la elección de las direcciones IP correctas para usar en el sistema de archivos, consulte Obtención de las direcciones IP del sistema de archivos correctas para usarlas en las entradas manuales del DNS.

Para buscar el nombre del DNS:

- En la FSx consola de Amazon, selecciona Sistemas de archivos y, a continuación, selecciona Detalles. Consulte el nombre del DNS en la sección Red y seguridad.
- O bien, véalo en la respuesta del comando de la API CreateFileSystem o DescribeFileSystems.

Para todos los sistemas de archivos Single-AZ unidos a un Microsoft Active Directory AWS administrado, el nombre DNS tiene el siguiente formato: `fs-0123456789abcdef0.`*`ad-dns-domain-name`*

En todos los sistemas de archivos Single-AZ unidos a un Active Directory autoadministrado y en cualquier sistema de archivos Multi-AZ, el nombre del DNS tiene el siguiente formato: `amznfsxaa11bb22.`*`ad-domain`*`.com`

Uso de la autenticación de Kerberos con nombres del DNS

Te recomendamos que utilices la autenticación y el cifrado basados en Kerberos en tránsito con Amazon. FSx Kerberos brinda la autenticación más segura para los clientes que acceden a su sistema de archivos. Para habilitar la autenticación y el cifrado de los datos en tránsito basados en Kerberos para sus sesiones de SMB, utilice el nombre DNS del sistema de archivos proporcionado por Amazon FSx para acceder a su sistema de archivos.

Si tiene una confianza externa configurada entre su Microsoft Active Directory AWS administrado y su Active Directory local, para usar Amazon FSx Remote PowerShell con autenticación Kerberos, debe configurar una política de grupo local en el cliente para el orden de búsqueda en los bosques.

Para obtener más información, consulte Configuración del orden de búsqueda en los bosques de Kerberos (KFSO) en la documentación de Microsoft.

Compatibilidad con espacios de nombres del sistema de archivos distribuido (DFS)

FSx para Windows File Server admite el uso de espacios de nombres DFS de Microsoft. Use los espacios de nombres del DFS para organizar los recursos compartidos de archivos de varios sistemas de archivos en una estructura de carpetas común (un espacio de nombres). Esta, a su vez, se usa para acceder a todo el conjunto de datos de archivos. Puedes usar un nombre en tu espacio de nombres DFS para acceder a tu sistema de FSx archivos de Amazon configurando su destino de enlace para que sea el nombre DNS del sistema de archivos. Para obtener más información, consulte Agrupe varios sistemas FSx de archivos del servidor de archivos de Windows con espacios de nombres DFS.

Acceso a los datos mediante alias del DNS

FSx para Windows File Server proporciona un nombre DNS para cada sistema de archivos que puede usar para acceder a sus recursos compartidos de archivos. También puede acceder a sus recursos compartidos de archivos mediante nombres DNS distintos del nombre DNS predeterminado registrando los alias DNS de sus FSx sistemas de archivos del servidor de archivos de Windows.

Con los alias DNS, puedes mover tus datos de archivos compartidos de Windows a FSx Windows File Server y seguir usando los nombres DNS existentes para acceder a los datos de Amazon FSx. Los alias de DNS también le permiten usar nombres significativos que facilitan la administración de herramientas y aplicaciones para conectarse a sus sistemas de FSx archivos de Amazon. Puede asociar hasta 50 alias del DNS con un sistema de archivos en cualquier momento. Para obtener más información sobre cómo asociar y desasociar los alias DNS con un sistema de archivos FSx para Windows File Server, consulte. La administración de los alias del DNS

Para configurar el acceso a los sistemas de archivos del servidor de archivos de Windows mediante alias DNS, debe realizar los siguientes pasos: FSx

1. Asociar alias del DNS con el sistema de archivos.
2. Cree un registro CNAME del DNS para el sistema de archivos y los alias del DNS asociados con él.

Para obtener más información sobre el uso de los alias DNS con los sistemas FSx de archivos del servidor de archivos de Windows, consulte. La administración de los alias del DNS

Uso de la autenticación de Kerberos y el cifrado con alias del DNS

Te recomendamos que utilices la autenticación y el cifrado basados en Kerberos en tránsito con Amazon. FSx Kerberos brinda la autenticación más segura para los clientes que acceden a su sistema de archivos. Para habilitar la autenticación Kerberos para los clientes que acceden a Amazon FSx mediante un alias de DNS, debe añadir los nombres principales de servicio (SPNs) que correspondan al alias de DNS del objeto informático de Active Directory del sistema de FSx archivos de Amazon.

Para configurar la autenticación y el cifrado de Kerberos al acceder al sistema de archivos mediante alias del DNS, consulte Configure los nombres principales de servicio () para Kerberos SPNs.

Si lo desea, puede obligar a los clientes que acceden al sistema de archivos mediante un alias de DNS a utilizar la autenticación y el cifrado de Kerberos configurando los siguientes objetos de política de grupo (GPOs) en su Active Directory:

- Restringir el NTLM: tráfico de NTLM saliente a servidores remotos: utilice esta configuración de política para denegar o auditar el tráfico de NTLM saliente de un equipo a cualquier servidor remoto que ejecute el sistema operativo Windows.
- Restringir el NTLM: agregar excepciones del servidor remoto para la autenticación de NTLM: utilice esta configuración de política para crear una lista de excepciones de los servidores remotos en los que los dispositivos cliente puedan usar la autenticación de NTLM, si está establecida la configuración de política Seguridad de red: restringir NTLM: tráfico de NTLM saliente a servidores remotos.

Para aplicar la autenticación y el cifrado de Kerberos al acceder al sistema de archivos mediante alias del DNS, consulte Aplicar la autenticación de Kerberos mediante objetos de política de grupo () GPOs.

Para obtener más información sobre cómo configurar el sistema de archivos para que utilice alias de DNS, consulte los siguientes procedimientos:

- Asociar alias del DNS con el sistema de archivos
- Configure los nombres principales de servicio () para Kerberos SPNs
- Actualizar o crear un registro CNAME del DNS

- Aplicar la autenticación de Kerberos mediante objetos de política de grupo () GPOs

Asociar alias del DNS con el sistema de archivos

Puede asociar los alias DNS a los sistemas de archivos de Windows File Server existentes FSx al crear nuevos sistemas de archivos y al crear un nuevo sistema de archivos a partir de una copia de seguridad mediante la FSx consola, la CLI y la API de Amazon. Si va a crear un alias con un nombre de dominio diferente, ingrese el nombre completo, incluido el dominio principal, para asociar un alias.

Este procedimiento describe cómo asociar alias de DNS al crear un nuevo sistema de archivos mediante la FSx consola de Amazon. Para obtener información sobre la asociación de los alias del DNS a los sistemas de archivos existentes, y sobre el uso de la CLI y la API, consulte La administración de los alias del DNS.

Cómo asociar los alias del DNS al crear un nuevo sistema de archivos

1. Abre la FSx consola de Amazon en https://console.aws.amazon.com/fsx/.
2. Siga el procedimiento para crear un nuevo sistema de archivos, tal y como se describe en Paso 5. Crear el sistema de archivos de la sección Introducción.
3. En la sección Acceso (opcional) del asistente para Crear un sistema de archivos, escriba los alias del DNS que desee asociar al sistema de archivos.

   Siga las siguientes pautas cuando especifique los alias del DNS:

   - Formato de nombre de dominio completo (FQDN) *`hostname.domain`*, por ejemplo, `accounting.example.com`.
   - Puede contener caracteres alfanuméricos o guiones (-).
   - No puede empezar ni terminar con un guion.
   - Puede comenzar con un número.

   Para los nombres de alias de DNS, Amazon FSx almacena los caracteres alfabéticos como letras minúsculas (a-z), independientemente de cómo los especifiques: mayúsculas, minúsculas o las letras correspondientes en los códigos de escape.
4. En las Preferencias de mantenimiento, realice los cambios que desee.
5. En la sección Etiquetas (opcional), añada las etiquetas que necesite y, luego, seleccione Siguiente.

6. Revise la configuración del sistema de archivos que se muestra en la página Crear sistema de archivos. Seleccione Crear sistema de archivos para abrir el asistente de creación de sistemas de archivos.

Configure los nombres principales de servicio () para Kerberos SPNs

Te recomendamos que utilices la autenticación y el cifrado basados en Kerberos en tránsito con Amazon. FSx Kerberos brinda la autenticación más segura para los clientes que acceden a su sistema de archivos.

Para habilitar la autenticación Kerberos para los clientes que acceden a Amazon FSx mediante un alias de DNS, debe añadir los nombres principales de servicio (SPNs) que correspondan al alias de DNS del objeto informático de Active Directory del sistema de FSx archivos de Amazon. Un SPN sólo puede asociarse a un único objeto informático de Active Directory a la vez. Si ya SPNs tiene el nombre DNS configurado para el objeto informático de Active Directory del sistema de archivos original, debe eliminarlo primero.

Se requieren dos SPNs para la autenticación de Kerberos:

```
HOST/alias
HOST/alias.domain
```

Si el alias es`finance.domain.com`, se requieren SPNs los dos siguientes:

```
HOST/finance
HOST/finance.domain.com
```

> **Note**
>
> Deberá eliminar cualquier HOST existente SPNs que corresponda al alias DNS del objeto informático de Active Directory antes de crear un nuevo HOST SPNs para el objeto informático Active Directory (AD) del sistema de FSx archivos de Amazon. Los intentos SPNs de configurar tu sistema de FSx archivos de Amazon fallarán si existe un SPN para el alias de DNS en el AD.

En los procedimiento a continuación, se describe cómo instalar lo siguiente:

- Busca cualquier alias de DNS existente SPNs en el objeto informático de Active Directory del sistema de archivos original.
- Elimine el existente SPNs encontrado, si lo hubiera.
- Cree un nuevo alias de DNS SPNs para el objeto informático de Active Directory de su sistema de FSx archivos de Amazon.

Para instalar el módulo de PowerShell Active Directory necesario

1. Inicie sesión en una instancia de Windows unida al Active Directory al que está unido su sistema de FSx archivos de Amazon.
2. PowerShell Ábrela como administrador.
3. Instale el módulo PowerShell Active Directory mediante el siguiente comando.

```
Install-WindowsFeature RSAT-AD-PowerShell
```

Para buscar y eliminar el alias de DNS existente SPNs en el objeto informático de Active Directory del sistema de archivos original

Si ha configurado SPNs el alias DNS que ha asignado a otro sistema de archivos en un objeto informático de su Active Directory, primero debe eliminarlos SPNs antes de añadirlos SPNs al objeto informático del sistema de archivos.

1. Busque cualquier existente mediante los siguientes comandos. SPNs Sustituya *alias_fqdn* por el alias del DNS que asoció al sistema de archivos en el Paso 1.

```
## Find SPNs for original file system's AD computer object
$ALIAS = "alias_fqdn"
SetSPN /Q ("HOST/" + $ALIAS)
SetSPN /Q ("HOST/" + $ALIAS.Split(".")[0])
```

2. Elimine el HOST existente SPNs devuelto en el paso anterior mediante el siguiente script de ejemplo.
   - Sustituya *alias_fqdn* por el alias del DNS completo que asoció al sistema de archivos en el Paso 1.
   - Sustituya *file_system_DNS_name* por el nombre del DNS del sistema de archivos original.

```
## Delete SPNs for original file system's AD computer object
$Alias = "alias_fqdn"
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})

SetSPN /D ("HOST/" + ${Alias}) ${FSxAdComputer}.Name
SetSPN /D ("HOST/" + ${Alias}.Split(".")[0]) ${FSxAdComputer}.Name
```

3. Repita los pasos anteriores con cada alias del DNS que haya asociado al sistema de archivos en el Paso 1.

Para configurar SPNs en el objeto informático de Active Directory del sistema de FSx archivos de Amazon

1. Configura un nuevo FSx archivo SPNs para tu sistema de archivos de Amazon ejecutando los siguientes comandos.

   - *file_system_DNS_name*Sustitúyalo por el nombre DNS que Amazon FSx asignó al sistema de archivos.

     Para encontrar el nombre DNS de tu sistema de archivos en la FSx consola de Amazon, selecciona Sistemas de archivos, elige tu sistema de archivos y, a continuación, selecciona el panel Red y seguridad en la página de detalles del sistema de archivos.

     También puedes obtener el nombre DNS en la respuesta a la operación de la DescribeFileSystemsAPI.

   - Sustituya *alias_fqdn* por el alias del DNS completo que asoció al sistema de archivos en el Paso 1.

```
## Set SPNs for FSx file system AD computer object
$FSxDnsName = "file_system_DNS_name"
$Alias = "alias_fqdn"
$FileSystemHost = (Resolve-DnsName $FSxDnsName | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity $FileSystemHost)
```

```
##Use the following command to set both the full FQDN and Alias SPNs
Set-AdComputer -Identity $FSxAdComputer -Add @{"msDS-AdditionalDnsHostname" =
 @($Alias, $Alias.Split(".")[0])}
```

> **Note**
>
> Se producirá un error al configurar un SPN para tu sistema de FSx archivos de Amazon si existe un SPN para el alias DNS en el AD del objeto informático del sistema de archivos original. Para obtener información sobre cómo buscar y eliminar los existentes SPNs, consulta. Para buscar y eliminar el alias de DNS existente SPNs en el objeto informático de Active Directory del sistema de archivos original

2. Compruebe que los nuevos SPNs están configurados para el alias DNS mediante el siguiente script de ejemplo. Asegúrese de que la respuesta incluya dos HOST `HOST/`*`alias`* y SPNs`HOST/`*`alias_fqdn`*, tal como se describió anteriormente en este procedimiento.

   *`file_system_DNS_name`*Sustitúyelo por el nombre DNS que Amazon FSx asignó a su sistema de archivos. Para encontrar el nombre DNS de tu sistema de archivos en la FSx consola de Amazon, selecciona Sistemas de archivos, elige tu sistema de archivos y, a continuación, selecciona el panel Red y seguridad en la página de detalles del sistema de archivos.

   También puedes obtener el nombre DNS en la respuesta a la operación de la DescribeFileSystemsAPI.

   ```
   ## Verify SPNs on FSx file system AD computer object
   $FileSystemDnsName = "file_system_dns_name"
   $FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
   [0].Name.Split(".")[0]
   $FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})
   SetSpn /L ${FSxAdComputer}.Name
   ```

3. Repita los pasos anteriores con cada alias del DNS que haya asociado al sistema de archivos en el Paso 1.

Actualizar o crear un registro CNAME del DNS

Tras configurar correctamente el sistema SPNs de archivos, puede pasar a Amazon FSx sustituyendo cada registro DNS que se resolvió en el sistema de archivos original por un registro DNS que se resolviera en el nombre DNS predeterminado del sistema de FSx archivos de Amazon.

Los módulos `dnsserver` y `activedirectory` de Windows son necesarios para ejecutar los comandos que se presentan en esta sección.

Para instalar los PowerShell módulos necesarios

1. Inicie sesión en una instancia de Windows unida al mismo Active Directory al que está unido su sistema de FSx archivos de Amazon como usuario que sea miembro de un grupo que tenga permisos de administración de DNS (administradores del sistema de nombres de dominio AWS delegados en AWS Managed Microsoft AD y administradores de dominio u otro grupo al que haya delegado permisos de administración de DNS en su Active Directory autogestionado).

   Para obtener más información, consulte Conectarse a su instancia de Windows en la Guía del EC2 usuario de Amazon.
2. Abrir PowerShell como administrador.
3. El módulo del servidor PowerShell DNS es necesario para realizar las instrucciones de este procedimiento. Instálelo con el siguiente comando.

   ```
   Install-WindowsFeature RSAT-DNS-Server
   ```

Para actualizar o crear un nombre DNS personalizado para tu sistema de FSx archivos de Amazon

1. Conéctate a tu EC2 instancia de Amazon como un usuario que sea miembro de un grupo que tenga permisos de administración de DNS (administradores AWS delegados del sistema de nombres de dominio en Active Directory AWS gestionado y administradores de dominio u otro grupo al que hayas delegado permisos de administración de DNS en tu Active Directory autogestionado).

   Para obtener más información, consulte Conectarse a su instancia de Windows en la Guía del EC2 usuario de Amazon.
2. En el símbolo del sistema, ejecute lo siguiente. Este script migra todos los registros CNAME de DNS existentes a tu sistema de FSx archivos de Amazon. Si no se encuentra ninguno, se crea un nuevo registro CNAME de DNS para el alias de DNS *`alias_fqdn`* que se convierte en el nombre de DNS predeterminado de tu sistema de FSx archivos de Amazon.

   Para ejecutar el script:

   - Sustituya *`alias_fqdn`* por el alias del DNS que asoció al sistema de archivos.

- *file_system_DNS_name*Sustitúyalo por el nombre DNS que Amazon FSx ha asignado al sistema de archivos.

```
$Alias="alias_fqdn"
$FSxDnsName="file_system_dns_name"
$AliasHost=$Alias.Split('.')[0]
$ZoneName=((Get-WmiObject Win32_ComputerSystem).Domain)
$DnsServerComputerName = (Resolve-DnsName $ZoneName -Type NS | Where Type -eq 'A' |
 Select -ExpandProperty Name) | Select -First 1
Add-DnsServerResourceRecordCName -Name $AliasHost -ComputerName
 $DnsServerComputerName -HostNameAlias $FSxDnsName -ZoneName $ZoneName
```

3. Repita el paso anterior para cada alias del DNS que haya asociado al sistema de archivos en el Paso 1.

Ahora has añadido un valor CNAME de DNS para tu sistema de FSx archivos de Amazon con el alias de DNS. Ya puede usar el alias del DNS para acceder a sus datos.

> **Note**
>
> Al actualizar un registro CNAME de DNS para que apunte a un sistema de FSx archivos de Amazon que anteriormente apuntaba a otro sistema de archivos, es posible que los clientes no puedan conectarse con el sistema de archivos durante un breve período de tiempo. Cuando la caché del DNS del cliente se actualice, deberían poder conectarse mediante el alias del DNS. Para obtener más información, consulte No se puede acceder al sistema de archivos con un alias del DNS.

Aplicar la autenticación de Kerberos mediante objetos de política de grupo () GPOs

Puede aplicar la autenticación Kerberos al acceder al sistema de archivos configurando los siguientes objetos de política de grupo (GPOs) en su Active Directory:

- Restringir el NTLM: tráfico de NTLM saliente a servidores remotos: utilice esta configuración de política para denegar o auditar el tráfico de NTLM saliente de un equipo a cualquier servidor remoto que ejecute el sistema operativo Windows.

- Restringir el NTLM: agregar excepciones del servidor remoto para la autenticación de NTLM: utilice esta configuración de política para crear una lista de excepciones de los servidores remotos en los que los dispositivos cliente puedan usar la autenticación de NTLM, si está establecida la configuración de política Seguridad de red: restringir NTLM: tráfico de NTLM saliente a servidores remotos.

1. Inicie sesión en una instancia de Windows unida al Active Directory al que esté unido su sistema de FSx archivos de Amazon como administrador. Si va a configurar un Active Directory autoadministrado, aplique estos pasos directamente al Active Directory.
2. Elija Inicio, Herramientas administrativas y, a continuación, Administración de políticas de grupo.
3. Elija Objetos de política de grupo.
4. Si el objeto de política de grupo aún no existe, créelo.
5. Localice la política existente de Seguridad de red: restringir el tráfico NTLM: tráfico NTLM saliente a servidores remotos. (Si no existe tal política, cree una nueva). En la pestaña Configuración de seguridad local, abra el menú contextual (botón derecho) y elija Propiedades.
6. Seleccione Denegar todo.
7. Elija Aplicar para guardar la configuración de seguridad.
8. Para establecer excepciones para las conexiones NTLM a servidores remotos específicos del cliente, busque la sección Seguridad de red: restringir NTLM: agregar excepciones de servidor remoto.

   Abra el menú contextual (botón derecho) y elija Propiedades en la pestaña Configuración de seguridad local.
9. Ingrese los nombres de los servidores que desee añadir a la lista de excepciones.
10. Elija Aplicar para guardar la configuración de seguridad.

Acceso a los datos mediante recursos compartidos de archivos

Un recurso compartido de archivos de Microsoft Windows es una carpeta o directorio específico del sistema de archivos. Incluye todas las subcarpetas que puedan existir. Los clientes acceden a los recursos compartidos de archivos del sistema de archivos mediante el protocolo de bloque de mensajes del servidor (SMB). Su sistema de archivos del servidor de archivos FSx para Windows viene con un recurso compartido de archivos de Windows predeterminado, denominado`share`.

Puede crear y administrar tantos recursos compartidos de archivos como desee con la herramienta de interfaz gráfica de usuario (GUI) carpetas compartidas de Windows.

Los recursos compartidos de disponibilidad continua (CA) de Microsoft Windows ofrecen la ventaja principal de mantener el acceso ininterrumpido a los archivos compartidos incluso cuando se produce un error en un nodo de servidor de un clúster. El uso de los recursos compartidos de archivos de CA puede minimizar las interrupciones en las aplicaciones del servidor que almacenan sus archivos de datos en estos recursos compartidos de archivos durante los períodos de mantenimiento del sistema de archivos.

Para obtener más información sobre la creación y administración de recursos compartidos de archivos en el sistema FSx de archivos del servidor de archivos de Windows, incluidos los recursos compartidos de CA, consulteCrear, actualizar y eliminar recursos compartidos de archivos.

Mapeo de recursos compartidos de archivos

Para acceder a tus recursos compartidos de archivos, usa la funcionalidad Windows Map Network Drive para asignar una letra de unidad de tu instancia de cómputo a tu recurso compartido de FSx archivos de Amazon. El proceso de mapear un recurso compartido de archivos a una unidad de la instancia informática se conoce como montar un recurso compartido de archivos en Linux. Este proceso varía según el tipo de instancia informática y el sistema operativo. Una vez que se mapea el recurso compartido de archivos, las aplicaciones y los usuarios pueden acceder a los archivos y las carpetas del recurso compartido de archivos como si se tratara de archivos y carpetas locales.

Para obtener más información sobre el mapeo y el montaje de recursos compartidos para ingresar datos en el sistema de archivos, consulte los siguientes procedimientos:

- Mapeo de un recurso compartido de archivos en una instancia de Amazon EC2 Windows.
- Montaje de un recurso compartido de archivos en una instancia de Amazon EC2 Mac
- Montaje de un recurso compartido de archivos en una instancia de Amazon EC2 Linux

Mapeo de un recurso compartido de archivos en una instancia de Amazon EC2 Windows

Puede asignar un recurso compartido de archivos en una instancia de EC2 Windows FSx para acceder al sistema de archivos del servidor de archivos de Windows mediante el Explorador de archivos de Windows o la línea de comandos.

Para mapear un recurso compartido de archivos en una instancia de Amazon EC2 Windows (Explorador de archivos)

1. Lanza la instancia de EC2 Windows y conéctala al Active Directory de Microsoft al que has 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 su instancia de EC2 Windows. Para obtener más información, consulta Cómo conectarse a tu instancia de Windows en la Guía del EC2 usuario de Amazon.
3. Una vez lista la conexión, abra el Explorador de archivos.
4. En el panel de navegación, abra el menú contextual (botón derecho) para Red y elija Conectar a unidad de red.
5. En Unidad, seleccione una letra de unidad.
6. En Carpeta, escriba el nombre del DNS del sistema de archivos o un alias del DNS asociado al sistema de archivos y el nombre del recurso compartido.

   > **Important**
   >
   > El uso de una dirección IP en lugar del nombre del DNS podría provocar que no esté disponible durante el proceso de conmutación por error del sistema de archivos Multi-AZ. Además, los nombres o los alias del DNS asociados son necesarios para la autenticación basada en Kerberos en los sistemas de archivos Multi-AZ y Single-AZ.

   Puedes encontrar el nombre DNS del sistema de archivos y cualquier alias DNS asociado en la FSx consola de Amazon si eliges Servidor de archivos, red y seguridad de Windows. O bien, puede encontrarlos en la respuesta de la operación de CreateFileSystem o de las API de DescribeFileSystems. Para obtener más información acerca de alias del DNS, consulte La administración de los alias del DNS.

   - En el caso de un sistema de archivos Single-AZ unido a un Microsoft Active Directory AWS administrado, el nombre DNS tiene el siguiente aspecto.

     ```
     fs-0123456789abcdef0.ad-domain.com
     ```

- En un sistema de archivos Single-AZ unido a un Active Directory autoadministrado y en cualquier sistema de archivos Multi-AZ, el nombre del DNS tiene el siguiente aspecto.

```
amznfsxaa11bb22.ad-domain.com
```

Por ejemplo, para usar el nombre del DNS de un sistema de archivos Single-AZ, ingrese lo siguiente en Carpeta.

```
\\fs-0123456789abcdef0.ad-domain.com\share
```

Para usar el nombre del DNS de un sistema de archivos Multi-AZ, ingrese lo siguiente en Carpeta.

```
\\amznfsxaa11bb22.ad-domain.com\share
```

Para usar un alias del DNS asociado al sistema de archivos, ingrese lo siguiente en Carpeta.

```
\\fqdn-dns-alias\share
```

7. Elija una opción para Reconectarse al iniciar sesión, que indica si el recurso compartido de archivos debe volver a conectarse al iniciar sesión y, a continuación, seleccione Finalizar.

Para mapear un recurso compartido de archivos en una instancia de Amazon EC2 Windows (línea de comandos)

1. Lanza la instancia de EC2 Windows y conéctala al Active Directory de Microsoft al que has 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 su instancia de EC2 Windows como usuario de su AWS Managed Microsoft AD directorio. Para obtener más información, consulta Cómo conectarse a tu instancia de Windows en la Guía del EC2 usuario de Amazon.
3. Una vez lista la conexión, abra una ventana de símbolo del sistema.

4. Monte el recurso compartido de archivos con la letra de unidad que prefiera, el nombre del DNS del sistema de archivos y el nombre del recurso compartido. Para encontrar el nombre DNS en la FSx consola de Amazon, selecciona Servidor de archivos, red y seguridad de Windows. O bien, puede encontrarlos en la respuesta de la operación de `CreateFileSystem` o de las API de `DescribeFileSystems`.

   - En el caso de un sistema de archivos Single-AZ unido a un Microsoft Active Directory AWS administrado, el nombre DNS tiene el siguiente aspecto.

     ```
     fs-0123456789abcdef0.ad-domain.com
     ```

   - En un sistema de archivos Single-AZ unido a un Active Directory autoadministrado y en cualquier sistema de archivos Multi-AZ, el nombre del DNS tiene el siguiente aspecto.

     ```
     amznfsxaa11bb22.ad-domain.com
     ```

   A continuación, se muestra un ejemplo de comando para montar el recurso.

   ```
   $ net use H: \\amzfsxaa11bb22.ad-domain.com\share /persistent:yes
   ```

   En lugar del `net use` comando, también puede usar cualquier PowerShell comando compatible para montar un recurso compartido de archivos.

Montaje de un recurso compartido de archivos en una instancia de Amazon EC2 Mac

Puede montar un recurso compartido de archivos en una instancia de Amazon EC2 Mac que esté unida a su Active Directory o no unida FSx para acceder a su sistema de archivos de Windows File Server. Si la instancia no está unida al Active Directory, asegúrese de actualizar las opciones de DHCP configuradas para Amazon Virtual Private Cloud (Amazon VPC) en la que reside la instancia para incluir los servidores de nombres del DNS de su dominio del Active Directory. A continuación, vuelva a iniciar la instancia.

Para montar un recurso compartido de archivos en una instancia de Amazon EC2 Mac (GUI)

1. Lanza la instancia de EC2 Mac. Para ello, elige uno de los siguientes procedimientos de la Guía del EC2 usuario de Amazon:

   - Iniciar una instancia Mac mediante la consola
   - Inicie una instancia de Mac mediante el AWS CLI

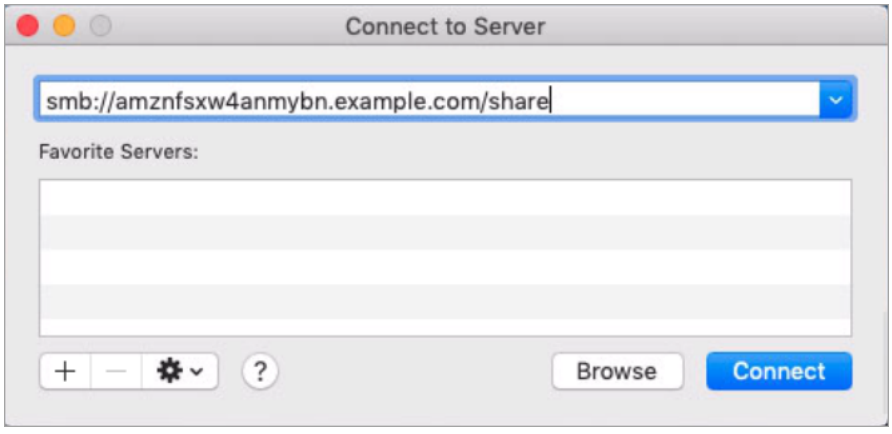
2. Conéctese a su instancia de EC2 Mac mediante Virtual Network Computing (VNC). Para obtener más información, consulte Conectarse a su instancia mediante VNC en la Guía del EC2 usuario de Amazon.

3. En tu instancia de EC2 Mac, conéctate a tu recurso compartido de FSx archivos de Amazon de la siguiente manera:

   a. Abra Finder, seleccione Ir y, a continuación, seleccione Conectar al servidor.

   b. En el cuadro de diálogo Conectar al servidor, escriba el nombre del DNS del sistema de archivos o un alias del DNS asociado al sistema de archivos y el nombre del recurso compartido. A continuación, elija Conectar.

      Puedes encontrar el nombre DNS del sistema de archivos y cualquier alias DNS asociado en la FSx consola de Amazon si eliges Servidor de archivos, red y seguridad de Windows. O bien, puede encontrarlos en la respuesta de la operación de CreateFileSystem o de las API de DescribeFileSystems. Para obtener más información acerca de alias del DNS, consulte La administración de los alias del DNS.

   c. En la siguiente pantalla, elija Conectar para continuar.

   d. Introduzca sus credenciales de Microsoft Active Directory (AD) para la cuenta de FSx servicio de Amazon, como se muestra en el siguiente ejemplo. A continuación, elija Conectar.

e. Si la conexión se ha realizado correctamente, podrás ver lo que has FSx compartido en Amazon en la sección Ubicaciones de la ventana del Finder.

Para montar un recurso compartido de archivos en una instancia de Amazon EC2 Mac (línea de comandos)

1. Lanza la instancia de EC2 Mac. Para ello, elige uno de los siguientes procedimientos de la Guía del EC2 usuario de Amazon:

   - Iniciar una instancia Mac mediante la consola
   - Inicie una instancia de Mac mediante el AWS CLI

2. Conéctese a su instancia de EC2 Mac mediante Virtual Network Computing (VNC). Para obtener más información, consulte Conectarse a su instancia mediante VNC en la Guía del EC2 usuario de Amazon.

3. Monte el sistema de recursos compartidos de archivos con el siguiente comando.

   ```
   mount_smbfs //file_system_dns_name/file_share mount_point
   ```

   Para encontrar el nombre DNS en la FSxconsola de Amazon, selecciona Windows File Server, Network & Security. O bien, puede encontrarlos en la respuesta de la operación de `CreateFileSystem` o de las API de `DescribeFileSystems`.

   - En el caso de un sistema de archivos Single-AZ unido a un Microsoft Active Directory AWS administrado, el nombre DNS tiene el siguiente aspecto.

```
fs-0123456789abcdef0.ad-domain.com
```

- En un sistema de archivos Single-AZ unido a un Active Directory autoadministrado y en cualquier sistema de archivos Multi-AZ, el nombre del DNS tiene el siguiente aspecto.

```
amznfsxaa11bb22.ad-domain.com
```

El comando montar utilizado en este procedimiento hace lo siguiente en los puntos indicados:

- *//file_system_dns_name/file_share*: especifica el nombre del DNS y el recurso compartido del sistema de archivos que se va a montar.
- *mount_point*— El directorio de la EC2 instancia en la que va a montar el sistema de archivos.

Montaje de un recurso compartido de archivos en una instancia de Amazon EC2 Linux

Puede montar un recurso compartido de archivos FSx para Windows File Server en una instancia de Amazon EC2 Linux que esté unida a su Active Directory o no esté unida para acceder a su sistema de archivos FSx para Windows File Server.

> **Note**
>
> - Los siguientes comandos especifican parámetros como el protocolo SMB, el almacenamiento en caché y el tamaño del búfer de lectura y escritura, únicamente a modo ilustrativo. Las elecciones de parámetros para el `cifs` comando de Linux, así como la versión del núcleo de Linux utilizada, pueden afectar al rendimiento y la latencia de las operaciones de red entre el cliente y el sistema de FSx archivos de Amazon. Para obtener más información, consulte la documentación `cifs` del entorno de Linux que utiliza.
> - Los clientes Linux no son compatibles con la conmutación por error automática basada en DNS. Para obtener más información, consulte La experiencia de conmutación por error en clientes Linux.

Para montar un recurso compartido de archivos en una instancia de Amazon EC2 Linux unida a un Active Directory

1. Si aún no tiene una instancia de EC2 Linux en ejecución unida a su Microsoft Active Directory, consulte Unirse manualmente a una instancia de Linux en la Guía de AWS Directory Service administración para obtener las instrucciones para hacerlo.
2. Conéctese a su instancia de EC2 Linux. Para obtener más información, consulta Conéctate a tu instancia de Linux en la Guía del EC2 usuario de Amazon.
3. Ejecute el comando siguiente, para instalar el paquete `cifs-utils`. Este paquete se utiliza para montar sistemas de archivos de red como Amazon FSx en Linux.

   ```
   $ sudo yum install cifs-utils
   ```

4. Cree el directorio **`/mnt/fsx`** de puntos de montaje. Aquí es donde montarás el sistema de FSx archivos de Amazon.

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

5. Autentíquese con kerberos con el siguiente comando.

   ```
   $ kinit
   ```

6. Monte el sistema de recursos compartidos de archivos con el siguiente comando.

   ```
   $ sudo mount -t cifs //file_system_dns_name/file_share mount_point --verbose -o
    vers=SMB_version,sec=krb5,cruid=ad_user,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=no
   file-server-Ip
   ```

   Para encontrar el nombre DNS en la FSxconsola de Amazon, selecciona Windows File Server, Network & Security. O bien, puede encontrarlos en la respuesta `CreateFileSystem` o en la operación `DescribeFileSystems` de la API.

   - En el caso de un sistema de archivos Single-AZ unido a un Microsoft Active Directory AWS administrado, el nombre DNS tiene el siguiente aspecto.

     ```
     fs-0123456789abcdef0.ad-domain.com
     ```

   - En un sistema de archivos Single-AZ unido a un Active Directory autoadministrado y en cualquier sistema de archivos Multi-AZ, el nombre del DNS tiene el siguiente aspecto.

```
amznfsxaa11bb22.ad-domain.com
```

Sustituya *CIFSMaxBufSize* por el valor más alto permitido por el núcleo. Para ello, ejecute el siguiente comando.

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

El resultado muestra que el tamaño máximo del búfer es 130048.

7. Compruebe que el sistema de archivos esté montado con el siguiente comando, que devuelve únicamente los sistemas de archivos del tipo Common Internet File System (CIFS).

```
$ mount -l -t cifs
//fs-0123456789abcdef0/share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=krb5,cache=cache_mode,username=user1@CORP.NETWORK.COM,ui
```

El comando montar utilizado en este procedimiento hace lo siguiente en los puntos indicados:

- *//file_system_dns_name/file_share*: especifica el nombre del DNS y el recurso compartido del sistema de archivos que se va a montar.
- *mount_point*— El directorio de la EC2 instancia en la que va a montar el sistema de archivos.
- `-t cifs vers=`*SMB_version*: especifica el tipo de sistema de archivos como CIFS y la versión del protocolo SMB. Amazon FSx para Windows File Server es compatible con las versiones 2.0 a 3.1.1 para SMB.
- `sec=krb5`: especifica el uso de la versión 5 de Kerberos para la autenticación.
- `cache=`*cache_mode*: establece el modo de caché. Esta opción de caché CIFS puede afectar al rendimiento, por lo que debería probar qué configuración funciona mejor con el núcleo y la carga de trabajo (y revisar la documentación de Linux). Se recomiendan las opciones `strict` y `none`, ya que `loose` puede provocar incoherencias en los datos, ya que tiene una semántica de protocolo más laxa.
- `cruid=`*ad_user*: establece el uid del propietario de la caché de credenciales del administrador del directorio de AD.

- */mnt/fsx*— Especifica el punto de montaje del recurso compartido de FSx archivos de Amazon en tu EC2 instancia.
- `rsize=`*`CIFSMaxBufSize`*`,wsize=`*`CIFSMaxBufSize`*: especifica el tamaño del búfer de lectura y escritura como el máximo que permite el protocolo CIFS. Sustituya *`CIFSMaxBufSize`* por el valor más alto permitido por el núcleo. Determine el `CIFSMaxBufSize` con el siguiente comando.

  ```
  $ modinfo cifs | grep CIFSMaxBufSize
  parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
   16384 Range: 8192 to 130048 (uint)
  ```

  El resultado muestra que el tamaño máximo del búfer es 130048.
- `ip=`*`preferred-file-server-Ip`*: establece la dirección IP de destino como la del servidor de archivos preferido del sistema de archivos.

  Puede recuperar la dirección IP del servidor de archivos preferido del sistema de archivos de la siguiente manera:

  - Desde la FSx consola de Amazon, en la pestaña Red y seguridad de la página de detalles del sistema de archivos.
  - En respuesta al comando `describe-file-systems` CLI o al comando DescribeFileSystemsAPI equivalente.

Para montar un recurso compartido de archivos en una instancia de Amazon EC2 Linux que no esté unida a Active Directory

El siguiente procedimiento monta un recurso compartido de FSx archivos de Amazon en una instancia de Amazon EC2 Linux que no está unida a su Active Directory (AD). En el caso de una instancia de EC2 Linux que no esté unida a su AD, solo puede montar un recurso compartido de archivos FSx para Windows File Server utilizando su dirección IP privada. Puedes obtener la dirección IP privada del sistema de archivos desde la FSx consola de Amazon, en la pestaña Red y seguridad, en Dirección IP del servidor de archivos preferido.

En este ejemplo, se utiliza la autenticación NTLM. Para ello, monte el sistema de archivos como un usuario que sea miembro del dominio de Microsoft Active Directory al que está unido el FSx sistema de archivos del servidor de archivos de Windows. Las credenciales de la cuenta de usuario se proporcionan en un archivo de texto que se crea en la EC2 instancia,`creds.txt`. Este archivo contiene el nombre de usuario, la contraseña y el dominio.

```
$ cat creds.txt
username=user1
password=Password123
domain=EXAMPLE.COM
```

Para lanzar y configurar la EC2 instancia de Amazon Linux

1. Lanza una EC2 instancia de Amazon Linux con la EC2consola de Amazon. Para obtener más información, consulta Cómo lanzar una instancia en la Guía del EC2 usuario de Amazon.
2. Conéctate a tu EC2 instancia de Amazon Linux. Para obtener más información, consulta Conéctate a tu instancia de Linux en la Guía del EC2 usuario de Amazon.
3. Ejecute el comando siguiente, para instalar el paquete `cifs-utils`. Este paquete se utiliza para montar sistemas de archivos de red como Amazon FSx en Linux.

   ```
   $ sudo yum install cifs-utils
   ```

4. Cree el **`/mnt/fsxx`** punto de montaje en el que planea montar el sistema de FSx archivos de Amazon.

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

5. Cree el archivo de credenciales `creds.txt` en el directorio `/home/ec2-user` con el formato mostrado anteriormente.
6. Configure los permisos del archivo `creds.txt` para que solo usted (el propietario) pueda leer y escribir en él con el siguiente comando.

   ```
   $ chmod 700 creds.txt
   ```

Cómo montar el sistema de archivos

1. Para montar un recurso compartido de archivo que no esté unido al Active Directory, utilice su dirección IP privada. Puedes obtener la dirección IP privada del sistema de archivos desde la FSx consola de Amazon, en la pestaña Red y seguridad, en la dirección IP del servidor de archivos preferido.
2. Monte el sistema de archivos con el siguiente comando.

```
$ sudo mount -t cifs //file-system-IP-address/file_share /mnt/fsx
 --verbose -o vers=SMB_version,sec=ntlmsspi,cred=/home/ec2-user/
creds.txt,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=none
```

Sustituya *CIFSMaxBufSize* por el valor más alto permitido por el núcleo. Para ello, ejecute el siguiente comando.

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

El resultado muestra que el tamaño máximo del búfer es 130048.

3. Compruebe que el sistema de archivo esté montado con el comando siguiente, que devuelve únicamente los sistemas de archivo CIFS.

```
$ mount -l -t cifs
//file-system-IP-address/file_share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=ntlmsspi,cache=cache_mode,username=user1,domain=CORP.EXA
```

El comando montar utilizado en este procedimiento hace lo siguiente en los puntos indicados:

- *//file-system-IP-address/file_share*: especifica la dirección IP y el recurso compartido del sistema de archivos que se va a montar.
- `-t cifs vers=`*SMB_version*: especifica el tipo de sistema de archivos como CIFS y la versión del protocolo SMB. Amazon FSx para Windows File Server es compatible con las versiones 2.0 a 3.1.1 para SMB.
- `sec=ntlmsspi`: especifica el uso de la interfaz de proveedor de soporte de seguridad de NT LAN Manager (NTLMSSPI) para la autenticación.
- `cache=`*cache_mode*: establece el modo de caché. Esta opción de caché CIFS puede afectar al rendimiento, por lo que debería probar qué configuración funciona mejor con el núcleo y la carga de trabajo (y revisar la documentación de Linux). Se recomiendan las opciones `strict` y `none`, ya que `loose` puede provocar incoherencias en los datos, ya que tiene una semántica de protocolo más laxa.
- `cred=/home/ec2-user/creds.txt`: especifica dónde obtener las credenciales de usuario.

- */mnt/fsx*— Especifica el punto de montaje del recurso compartido de FSx archivos de Amazon en tu EC2 instancia.
- `rsize=`*`CIFSMaxBufSize`*`,wsize=`*`CIFSMaxBufSize`*: especifica el tamaño del búfer de lectura y escritura como el máximo que permite el protocolo CIFS. Sustituya *`CIFSMaxBufSize`* por el valor más alto permitido por el núcleo. Determine el `CIFSMaxBufSize` con el siguiente comando.

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

Monta automáticamente los recursos compartidos de archivos en una instancia de Amazon EC2 Linux

Puede montar automáticamente su recurso compartido de archivos FSx para Windows File Server para acceder a su sistema de archivos FSx para Windows File Server cada vez que se reinicie la instancia de Amazon EC2 Linux en la que está montado. Para ello, añade una entrada al `/etc/fstab` archivo de la EC2 instancia. El archivo `/etc/fstab` contiene información sobre los sistemas de archivos. El comando mount -a, que se ejecuta durante el startup de la instancia, monta los sistemas de archivos enumerados en el archivo `/etc/fstab`.

En el caso de una instancia de Amazon EC2 Linux que no esté unida a Active Directory, solo puede montar un recurso compartido de archivos FSx para Windows File Server mediante su dirección IP privada. Puedes obtener la dirección IP privada del sistema de archivos desde la FSx consola de Amazon, en la pestaña Red y seguridad, en Dirección IP del servidor de archivos preferido.

El siguiente procedimiento utiliza la autenticación NTLM de Microsoft. El sistema de archivos se monta como un usuario que es miembro del dominio de Microsoft Active Directory al que está unido el sistema FSx de archivos del servidor de archivos de Windows. Puede recuperar las credenciales de la cuenta de usuario del archivo `creds.txt` mediante el siguiente comando.

```
$ cat creds.txt
username=user1
password=Password123
domain=EXAMPLE.COM
```

Para montar automáticamente un recurso compartido de archivos en una EC2 instancia de Amazon Linux que no esté unida a Active Directory

Para lanzar y configurar la EC2 instancia de Amazon Linux

1. Lanza una EC2 instancia de Amazon Linux con la EC2consola de Amazon. Para obtener más información, consulta Cómo lanzar una instancia en la Guía del EC2 usuario de Amazon.
2. Conecte con la instancia . Para obtener más información, consulta Conéctate a tu instancia de Linux en la Guía del EC2 usuario de Amazon.
3. Ejecute el comando siguiente, para instalar el paquete `cifs-utils`. Este paquete se utiliza para montar sistemas de archivos de red como Amazon FSx en Linux.

```
$ sudo yum install cifs-utils
```

4. Cree el directorio `/mnt/fsx`. Aquí es donde montarás el sistema de FSx archivos de Amazon.

```
$ sudo mkdir /mnt/fsx
```

5. Cree el archivo de credenciales `creds.txt` en el directorio `/home/ec2-user`.
6. Configure los permisos del archivo para que solo usted (el propietario) pueda leerlo con el siguiente comando.

```
$ sudo chmod 700 creds.txt
```

Cómo montar el sistema de archivos de forma automática

1. Para montar automáticamente un recurso compartido de archivos que no esté unido al Active Directory, utilice su dirección IP privada. Puedes obtener la dirección IP privada del sistema de archivos desde la FSx consola de Amazon, en la pestaña Red y seguridad, en Dirección IP del servidor de archivos preferido.
2. Para montar de manera automática el recurso compartido de archivos con su dirección IP privada, añada la siguiente línea al archivo `/etc/fstab`.

```
//file-system-IP-address/file_share /mnt/fsx cifs
 vers=SMB_version,sec=ntlmsspi,cred=/home/ec2-user/
creds.txt,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=none 0 0
```

Sustituya *CIFSMaxBufSize* por el valor más alto permitido por el núcleo. Para ello, ejecute el siguiente comando.

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

El resultado muestra que el tamaño máximo del búfer es 130048.

3. Pruebe la entrada `fstab` usando el comando `mount` con la opción 'fake' junto con las opciones 'all' y 'verbose'.

```
$ sudo mount -fav
home/ec2-user/fsx      : successfully mounted
```

4. Para montar el recurso compartido de archivos, reinicia la EC2 instancia de Amazon.
5. Cuando la instancia vuelva a estar disponible, compruebe que el sistema de archivos esté montado con el siguiente comando.

```
$ sudo mount -l -t cifs
//file-system-IP-address/file_share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=ntlmsspi,cache=cache_code,username=user1,domain=CORP.EXA
```

La línea que se añade al archivo `/etc/fstab` en este procedimiento hace lo siguiente en los puntos indicados:

- *//file-system-IP-address/file_share*— Especifica la dirección IP y el recurso compartido del sistema de FSx archivos de Amazon que estás montando.
- `/mnt/fsx`— Especifica el punto de montaje del sistema de FSx archivos de Amazon en la EC2 instancia.
- `cifs vers=`*SMB_version*: especifica el tipo de sistema de archivos como CIFS y la versión del protocolo SMB. Amazon FSx para Windows File Server es compatible con las versiones 2.0 a 3.1.1 para SMB.
- `sec=ntlmsspi`: especifica el uso de la Interfaz de proveedor de soporte de seguridad de NT LAN Manager para facilitar la autenticación de desafío-respuesta de NTLM.
- `cache=`*cache_mode*: establece el modo de caché. Esta opción de caché CIFS puede afectar al rendimiento, por lo que debería probar qué configuración funciona mejor con el núcleo

y la carga de trabajo (y revisar la documentación de Linux). Se recomiendan las opciones `strict` y `none`, ya que `loose` puede provocar incoherencias en los datos, ya que tiene una semántica de protocolo más laxa.

- `cred=/home/ec2-user/creds.txt`: especifica dónde obtener las credenciales de usuario.
- `_netdev`: indica al sistema operativo que el sistema de archivos reside en un dispositivo que requiere acceso a la red. Usar esta opción impide que la instancia monte el sistema de archivos hasta que esté activada el servicio de red en el cliente.
- `0`: Indica que `dump` debería hacer una copia de seguridad del sistema de archivos, si el valor no es cero. En el caso de Amazon FSx, este valor debería ser`0`.
- `0`: especifica el orden en que `fsck` comprueba los sistemas de archivos en el arranque. En el caso de los sistemas de FSx archivos de Amazon, este valor debe `0` indicar que no se `fsck` deben ejecutar al inicio.

Crear, actualizar y eliminar recursos compartidos de archivos

En este tema, se describe cómo administrar los recursos compartidos de archivos con las siguientes tareas.

- Crear un recurso compartido de archivos
- Modificación de un recurso compartido de archivos existente
- Eliminar un recurso compartido de archivos existente

Puede usar la GUI de carpetas compartidas nativa de Windows y la Amazon FSx CLI para la administración remota PowerShell para administrar los recursos compartidos de archivos en su sistema de archivos FSx para Windows File Server. Es posible que se produzcan retrasos al utilizar la GUI de carpetas compartidas (fsmgmt.msc) al abrir por primera vez el menú contextual de los recursos compartidos ubicados en un sistema de archivos diferente. Para evitar estos retrasos, utilícela PowerShell para gestionar los recursos compartidos de archivos ubicados en varios sistemas de archivos.

Microsoft Windows aplica reglas y limitaciones a la hora de asignar nombres a archivos y directorios. Para garantizar que pueda crear los datos y acceder a ellos correctamente, debe asignar un nombre a los archivos y directorios de acuerdo con estas directrices de Windows. Para obtener más información, consulte las Convenciones de nombres.

> **Warning**
>
> Amazon FSx requiere que el usuario del SISTEMA tenga permisos de ACL de NTFS de control total en todas las carpetas en las que cree un recurso compartido de archivos SMB. No cambie los permisos de las ACL de NTFS de este usuario en sus carpetas, ya que si lo hace, puede hacer que los recursos compartidos de archivos se vuelvan inaccesibles.

Administración de recursos compartidos de archivos con la Shared Folders GUI

Para gestionar los archivos compartidos en tu sistema de FSx archivos de Amazon, puedes usar la GUI de carpetas compartidas. La GUI de carpetas compartidas proporciona una ubicación central para administrar todas las carpetas compartidas de un servidor Windows. Los siguientes procedimientos describen cómo administrar los recursos compartidos de archivos.

Para conectar carpetas compartidas a su sistema FSx de archivos del servidor de archivos de Windows

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. En Microsoft Active Directory AWS administrado, este grupo se denomina FSx administradores AWS delegados. En el Microsoft Active Directory autoadministrado, este grupo se denomina Administradores de dominio o el nombre personalizado que le haya puesto cuando lo creó. Para obtener más información, consulte Conectarse a la instancia de Windows en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Windows.
3. Abra el menú Inicio y ejecute fsmgmt.msc con la opción Ejecutar como administrador. Al hacerlo, se abre la herramienta GUI de carpetas compartidas.
4. En Action, elija Connect to another computer.
5. Para otro ordenador, introduce el nombre del Sistema de nombres de dominio (DNS) de tu sistema de FSx archivos de Amazon, por ejemplo**`amznfsxabcd0123.corp.example.com`**.

Para encontrar el nombre DNS de tu sistema de archivos en la FSx consola de Amazon, selecciona Sistemas de archivos, elige tu sistema de archivos y, a continuación, consulta la sección Red y seguridad de la página de detalles del sistema de archivos. También puedes obtener el nombre DNS en la respuesta a la operación de la DescribeFileSystemsAPI.

6. Seleccione OK. 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. El recurso compartido predeterminado se llama `\share`. Puede hacerlo mediante las acciones siguientes:

- 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. 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:

  - Con la herramienta de carpetas compartidas: haga clic en “Examinar” cuando especifique la ruta de la carpeta local, y haga clic en “Crear nueva carpeta” para crear la carpeta local.
  - Uso de la línea de comandos:

    ```
    New-Item -Type Directory -Path \\amznfsxabcd0123.corp.example.com\D$\share
    \MyNewShare
    ```

- 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**
>
> Para los sistemas de archivos Single-AZ 2 y Multi-AZ, eliminar o modificar los recursos compartidos de archivos (incluida la actualización de los permisos, los límites de usuario y

otras propiedades) mediante la herramienta GUI de carpetas compartidas solo es posible si se conecta a fsmgmt.msc mediante el nombre DNS del sistema de archivos de Amazon. FSx La herramienta de la GUI de carpetas compartidas no admite estas acciones si se conecta con la dirección IP o el alias del DNS del sistema de archivos.

> **Note**
>
> Si utiliza la herramienta GUI de carpetas compartidas fsmgmt.msc FSx para acceder a los recursos compartidos ubicados en varios sistemas de archivos del servidor de archivos de Windows, es posible que se produzcan retrasos al abrir por primera vez el menú contextual de recursos compartidos de archivos de un recurso compartido ubicado en un sistema de archivos diferente. Para evitar estos retrasos, puede administrar los archivos compartidos de la manera que se describe a continuación. PowerShell

Administrar los archivos compartidos con PowerShell

Puede administrar los recursos compartidos de archivos mediante comandos de administración remota personalizados FSx para Windows File Server para. PowerShell Estos comandos pueden ayudarle a automatizar la administración de las tareas de recursos compartidos de archivos, como las siguientes:

- Migración de archivos compartidos de servidores de archivos existentes a Amazon FSx
- Sincronizar los archivos compartidos Regiones de AWS para la recuperación ante desastres
- Administrar de forma programática los flujos de trabajo continuos de archivos compartidos de recursos, como el aprovisionamiento de archivos compartidos en equipo

Para obtener información sobre cómo utilizar la Amazon FSx CLI para la administración remota en PowerShell, consulteUso de Amazon FSx CLI para PowerShell.

En la siguiente tabla se enumeran los PowerShell comandos de administración remota de Amazon FSx CLI que puede usar para administrar los recursos compartidos de archivos en FSx los sistemas de archivos de Windows File Server.

Comando para la administración compartida	Descripción
New-FSxSmbShare	Crea un recurso compartido de archivos nuevo.
Remove-FSxSmbShare	Elimina un recurso compartido de archivos.
Get-FSxSmbShare	Recupera los recurso compartido de archivos existentes.
Set-FSxSmbShare	Establece las propiedades de un recurso compartido.
Get-FSxSmbShareAccess	Recupera la lista de control de acceso (ACL) de un recurso compartido.
Grant-FSxSmbShareAccess	Agrega una entrada de permiso de control de acceso (ACE) para un administrador al descriptor de seguridad de un recurso compartido.
Revoke-FSxSmbShareAccess	Elimina todas las palabras «permitir ACEs un administrador» del descriptor de seguridad de un recurso compartido.
Block-FSxSmbShareAccess	Añade una ACE de denegación para un administrador con confianza al descriptor de seguridad de un recurso compartido.
Unblock-FSxSmbShareAccess	Elimina del descriptor de seguridad de un ACEs recurso compartido toda la información denegada a un administrador fiduciario.

La ayuda en línea de cada comando brinda una referencia de todas las opciones de comando. Para acceder a esta ayuda, ejecute el comando con un `-?`, por ejemplo, `New-FSxSmbShare -?`.

Pasar las credenciales a New- FSx SmbShare

Puede pasar las credenciales a New- para FSx SmbShare poder ejecutarlas en bucle y crear cientos o miles de recursos compartidos sin tener que volver a introducir las credenciales cada vez.

Prepare el objeto de credenciales necesario para crear los recursos compartidos de archivos en su servidor de archivos FSx para Windows File Server mediante una de las siguientes opciones.

- Para generar el objeto de credenciales de forma interactiva, utilice el siguiente comando.

```
$credential = Get-Credential
```

- Para generar el objeto de credenciales mediante un AWS Secrets Manager recurso, utilice el siguiente comando.

```
$credential = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
 $AdminSecret).SecretString
$FSxAdminUserCredential = (New-Object PSCredential($credential.UserName,(ConvertTo-
SecureString $credential.Password -AsPlainText -Force)))
```

Cómo crear un recurso compartido de disponibilidad continua (CA)

Puede crear recursos compartidos disponibles de forma continua (CA) mediante Amazon FSx CLI for Remote Management on PowerShell. Los recursos compartidos de CA creados en un sistema de archivos Multi-AZ FSx para Windows File Server son muy duraderos y están muy disponibles. Un sistema de archivos Amazon FSx Single-AZ se basa en un clúster de un solo nodo. Como resultado, los recursos compartidos de CA creados en un sistema de archivos Single-AZ son muy duraderos, pero no cuentan con una disponibilidad alta. Utilice el comando `New-FSxSmbShare` con la opción `-ContinuouslyAvailable` establecida en `$True` para especificar que el recurso compartido es de disponibilidad continua. El siguiente comando es un ejemplo para crear un recurso compartido de CA.

```
New-FSxSmbShare -Name "New CA Share" -Path "D:\share\new-share" -Description "CA share"
 -ContinuouslyAvailable $True
```

Puede modificar la opción `-ContinuouslyAvailable` en un recurso compartido de archivos existente mediante el comando `Set-FSxSmbShare`.

Determinar si un recurso compartido de archivos existente está disponible de forma continua

Use el siguiente comando para ver el valor de la propiedad continuamente disponible de un recurso compartido de archivos existente.

```
Invoke-Command -ComputerName powershell_endpoint -ConfigurationName FSxRemoteAdmin -
scriptblock { get-fsxsmbshare -name share_name }
```

Si la propiedad CA está habilitada, la salida incluirá la siguiente línea:

```
[...]
ContinuouslyAvailable : True
[...]
```

Si la propiedad CA no está habilitada, la salida incluirá la siguiente línea:

```
[...]
ContinuouslyAvailable : False
[...]
```

Para habilitar la disponibilidad continua en un recurso compartido de archivos existente, use el siguiente comando:

```
Invoke-Command -ComputerName powershell_endpoint -ConfigurationName FSxRemoteAdmin -
scriptblock { set-fsxsmbshare -name share_name -ContinuouslyAvailable $True}
```

El FSx SmbShare comando New- falla cuando se trata de una confianza unidireccional

Amazon FSx no admite la ejecución del `New-FSxSmbShare` PowerShell comando en los casos en los que tienes una confianza unidireccional y el dominio en el que reside el usuario no está configurado para confiar en el dominio asociado al sistema de FSx archivos de Amazon.

Puede resolver esta situación de alguna de las siguientes formas:

- El usuario que ejecuta el `New-FSxSmbShare` comando debe estar en el mismo dominio que el sistema de FSx archivos.
- Puede utilizar la interfaz gráfica de usuario de fsmgmt.msc para crear recursos compartidos en su sistema de archivos. Para obtener más información, consulte Administración de recursos compartidos de archivos con la Shared Folders GUI.

Disponibilidad y durabilidad: sistemas de archivos Single-AZ y Multi-AZ.

Amazon FSx para Windows File Server ofrece dos tipos de implementación de sistemas de archivos: Single-AZ y Multi-AZ. En las siguientes secciones, se proporciona información que le ayudará a elegir el tipo de implementación adecuado para las 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.

Los sistemas de archivos Single-AZ se componen de una única instancia del servidor de archivos de Windows y un conjunto de volúmenes de almacenamiento dentro de una única zona de disponibilidad (AZ). Con los sistemas de archivos Single-AZ, los datos se replican de manera automática para protegerlos de la falla de un solo componente en la mayoría de los casos. Amazon monitorea FSx continuamente los fallos de hardware y se recupera automáticamente de los fallos sustituyendo el componente de infraestructura averiado. Los sistemas de archivos Single-AZ suelen experimentar unos 30 minutos de inactividad durante los eventos de recuperación ante fallos y durante el período de mantenimiento planificado que se configura para el sistema de archivos. Con los sistemas de archivos Single-AZ, los fallos del sistema de archivos pueden ser irrecuperables en raras ocasiones, por ejemplo, debido a fallos de varios componentes o a un fallo imprevisto del servidor de archivos único que deja el sistema de archivos en un estado incongruente. En este caso, puede recuperar el sistema de archivos a partir de la copia de seguridad más reciente.

Los sistemas de archivos Multi-AZ se componen de un clúster de servidores de archivos Windows de alta disponibilidad repartidos en dos AZs (una zona de disponibilidad preferida y una zona de disponibilidad de reserva), que utilizan la tecnología de clústeres de conmutación por error de Windows Server (WSFC) y un conjunto de volúmenes de almacenamiento en cada uno de ellos. AZs Los datos se replican de forma sincrónica dentro de cada zona de disponibilidad individual y entre ambas. AZs En comparación con la implementación en una zona de disponibilidad única, las implementaciones en varias zonas de disponibilidad ofrecen una mayor durabilidad al replicar aún más los datos y una mayor disponibilidad durante el mantenimiento planificado del sistema y la interrupción no planificada del servicio al realizar la conmutación automática por error a la zona de disponibilidad en espera. AZs Gracias a esto, puede seguir accediendo a sus datos. Esto también ayuda a protegerlos contra los fallos de las instancias y las interrupciones en las zonas de disponibilidad.

Elegir el tipo de implementación del sistema de archivos Single-AZ o Multi-AZ

Se recomienda utilizar sistemas de archivos Multi-AZ para la mayoría de las cargas de trabajo de producción, dado el modelo de alta disponibilidad y durabilidad que ofrecen. La implementación en zonas de disponibilidad única está diseñada para ser una solución rentable para las cargas de trabajo de prueba y desarrollo, para ciertas cargas de trabajo de producción que tienen la replicación integrada en la capa de aplicación y no requieren redundancia adicional a nivel de almacenamiento, y para las cargas de trabajo de producción que tienen una disponibilidad y unas necesidades de objetivo de punto de recuperación (RPO) más reducidas. Las cargas de trabajo con disponibilidad y necesidades de RPO reducidas pueden tolerar la pérdida temporal de disponibilidad durante un máximo de 20 minutos, en caso de mantenimiento planificado del sistema de archivos o interrupciones imprevistas del servicio y, en raras ocasiones, la pérdida de actualizaciones de datos desde la última copia de seguridad.

También le recomendamos revisar el modelo de disponibilidad del sistema de archivos y asegurarse de que la carga de trabajo resista el comportamiento de recuperación esperado para el tipo de implementación que eligió durante eventos como el mantenimiento del sistema de archivos, los cambios en la capacidad de rendimiento y las interrupciones no planificadas del servicio.

Compatibilidad de características por tipo de implementación

En la siguiente tabla se resumen las características compatibles con los tipos de implementación de sistemas de archivos FSx de Windows File Server:

Tipo de implementación	Almacenamiento en SSD	Almacenamiento en HDD	Espacios de nombres de DFS	Replicación de DFS	Nombres del DNS personalizados	Recursos compartidos de CA
Single-AZ 1	✓		✓	✓	✓	
Single-AZ 2	✓	✓	✓		✓	✓*
Multi-AZ	✓	✓	✓		✓	✓*

> **Note**
>
> * Si bien puede crear recursos compartidos de disponibilidad continua (CA) en sistemas de archivos Single-AZ 2, debe usar recursos compartidos de CA en sistemas de archivos Multi-AZ para las implementaciones de alta disponibilidad de SQL Server.

Proceso de conmutación por error

Los sistemas de archivos Multi-AZ conmutan por error de forma automática desde el servidor de archivos preferido al servidor de archivos estándar si se da cualquiera de las siguientes condiciones:

- Ocurre una interrupción de una zona de disponibilidad.
- El servidor de archivos preferido deja de estar disponible.
- El servidor de archivos preferido se somete a un mantenimiento planificado.

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 de manera automática. Cuando los recursos de la subred preferida están disponibles, Amazon devuelve FSx automáticamente por error al servidor de archivos preferido de la subred preferida. Por lo general, una conmutación por error se completa en menos de 30 segundos, desde que se detecta el error en el servidor de archivos activo hasta que se activa el servidor de archivos que estaba en espera. La conmutación por recuperación a la configuración Multi-AZ original también se completa en menos de 30 segundos, y solo se produce una vez que el servidor de archivos de la subred preferida se recupera por completo.

Durante el breve período en el que el sistema de archivos se produce y se produce una falla, es posible que la E/S se detenga y que CloudWatch las métricas de Amazon no estén disponibles temporalmente. En el caso de los sistemas de archivos Multi-AZ, cualquier actividad de lectura y escritura de archivos que se produzca durante la conmutación por error y la conmutación por recuperación deberá sincronizarse entre los servidores de archivos principal y secundario. Este proceso puede tardar hasta varias horas en el caso de los sistemas de archivos con almacenamiento en disco duro y en las cargas de trabajo que requieren un uso intensivo de escrituras e IOPS. Recomendamos probar las repercusiones de las conmutaciones por error en la aplicación cuando el sistema de archivos tenga una carga más ligera.

La experiencia de conmutación por error en clientes de Windows

Al pasar por error de un servidor de archivos a otro, el nuevo servidor de archivos activo comienza a atender automáticamente todas las solicitudes de lectura y escritura del sistema de archivos. Cuando los recursos de la subred preferida estén disponibles, Amazon regresa FSx automáticamente al servidor de archivos preferido de la subred preferida. Como el nombre del DNS del sistema de archivos sigue siendo el mismo, las conmutaciones por error son transparentes para las aplicaciones de Windows, que reanudan las operaciones del sistema de archivos sin intervención manual. Por lo general, una conmutación por error se completa en menos de 30 segundos, desde que se detecta el error en el servidor de archivos activo hasta que se activa el servidor de archivos que estaba en espera. La conmutación por recuperación a la configuración Multi-AZ original también se completa en menos de 30 segundos, y solo se produce después de que el servidor de archivos de la subred preferida se recupera por completo.

La experiencia de conmutación por error en clientes Linux

Los clientes Linux no son compatibles con la conmutación por error automática basada en DNS. Por lo tanto, no se conectan de forma automática al servidor de archivos en espera durante una conmutación por error. Reanudarán de manera automática las operaciones del sistema de archivos cuando el sistema de archivos Multi-AZ haya hecho una conmutación por recuperación al servidor de archivos de la subred preferida.

Prueba de conmutación por error en un sistema de archivos

Puede probar la conmutación por error del sistema de archivos Multi-AZ modificando su capacidad de rendimiento. Cuando modificas la capacidad de procesamiento de tu sistema de archivos, Amazon FSx desactiva el servidor de archivos del sistema de archivos. Los sistemas de archivos Multi-AZ conmutan automáticamente por error al servidor secundario, mientras que Amazon FSx reemplaza primero el servidor de archivos del servidor preferido. Luego, el sistema de archivos devuelve 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. Una vez que la actualización haya finalizado correctamente, el sistema de archivos se transferirá por error al servidor secundario y al servidor principal. Para obtener más información sobre la modificación de la capacidad de rendimiento del sistema de archivos y la supervisión del progreso de la solicitud, consulte Administración de la capacidad de rendimiento.

Recursos del sistema de archivos Single-AZ y Multi-AZ

Los sistemas de archivos Single-AZ y Multi-AZ consumen las subredes y las interfaces de red elásticas de forma diferente, como se explica en las siguientes secciones.

Subredes

Cuando crea una nube privada virtual (VPC), abarca todas las zonas de disponibilidad (AZs) del. Región de AWS Las zonas de disponibilidad son ubicaciones diferentes diseñadas para quedar aisladas en caso de error en otras zonas de disponibilidad. Tras crear la VPC, podrá añadir una o varias subredes en cada zona de disponibilidad. La VPC predeterminada tiene una subred en cada zona de disponibilidad. Una subred es un rango de direcciones IP en su VPC. Una subred debe residir en una sola zona de disponibilidad.

FSx para Windows File Server, los sistemas de archivos Single-AZ requieren una subred que se especifica al crearlos. La subred que elija define la zona de disponibilidad en la que se crea el sistema de archivos.

Los sistemas de archivos Multi-AZ requieren dos subredes, una para el servidor de archivos preferido y otra para el servidor de archivos en espera. Las dos subredes que elija deben estar en zonas de disponibilidad diferentes dentro de la misma región. AWS

En el caso de AWS las aplicaciones internas, le recomendamos que lance sus clientes en la misma zona de disponibilidad que su servidor de archivos preferido para minimizar la latencia.

Interfaces de red elástica del sistema de archivos

Una interfaz de red elástica es un componente de red lógico en una VPC que representa una tarjeta de red virtual. Al crear un sistema de FSx archivos de Amazon, Amazon FSx aprovisiona una o más interfaces de red elásticas en la VPC que asocie a su sistema de archivos. La interfaz elastic network permite a los clientes comunicarse con el sistema de archivos y montarlo. Se considera que la interfaz de red elástica está dentro del ámbito de servicio de Amazon FSx, a pesar de formar parte de la VPC de su cuenta. Los sistemas de archivos Multi-AZ tienen dos interfaces de red elásticas, una para cada servidor de archivos. Los sistemas de archivos Single-AZ tienen una interfaz de red elástica.

> **Warning**
>
> No modifique ni elimine las interfaces de red elásticas asociadas a sus sistemas 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.

En la siguiente tabla se resume el uso de los recursos FSx para los sistemas de archivos Windows File Server Single-AZ y Multi-AZ:

Tipo de implementación del sistema de archivos	El número de subredes	El número de interfaces de red elásticas	El número de direcciones IP estáticas
Single-AZ 2	1	1	2
Single-AZ 1	1	1	1
Multi-AZ	2	2	4

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

> **Important**
>
> Amazon FSx no admite el acceso a los sistemas de archivos ni la exposición del sistema de archivos a la Internet pública. Si una dirección IP elástica, que es una dirección IP pública a la que se puede acceder desde Internet, se adjunta a la interfaz de red elástica de un sistema de archivos, Amazon la desconecta FSx automáticamente.

Trabajar con Microsoft Active Directory

Cuando crea un sistema de archivos FSx para Windows File Server, lo une a su dominio de Active Directory para proporcionar la autenticación de los usuarios y el control de acceso a nivel de archivos y carpetas. Amazon FSx trabaja con Microsoft Active Directory para integrarse con sus entornos Microsoft Windows existentes. Amazon FSx ofrece dos opciones FSx para utilizar el sistema de archivos de Windows File Server con Active Directory: Uso de Amazon FSx con AWS Directory Service for Microsoft Active Directory yUso de un Active Directory de Microsoft autoadministrado.

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.

Luego, sus usuarios pueden usar sus identidades de usuario existentes en Active Directory para autenticarse y acceder al sistema de archivos del FSx servidor de archivos de Windows. Los usuarios pueden usar sus identidades actuales para controlar el acceso a archivos y carpetas individuales. Además, puede migrar sus archivos y carpetas existentes junto con su configuración de lista de control de acceso de seguridad (ACL) a Amazon FSx sin ninguna modificación.

> **Note**
>
> Amazon FSx es compatible con los servicios de dominio de Active Directory de Microsoft Azure, que puede unir a un Active Directory de Microsoft Azure.

Tras crear una configuración de Active Directory unida para un sistema de archivos, solo podrá actualizar las siguientes propiedades:

- Credenciales de usuario de servicio
- Dirección IP del servidor DNS

No puede cambiar las siguientes propiedades del AD de Microsoft al que se ha unido después de crear el sistema de archivos:

- DomainName
- OrganizationalUnitDistinguishedName

- FileSystemAdministratorsGroup

Sin embargo, puede crear un nuevo sistema de archivos a partir de una copia de seguridad y cambiar estas propiedades en la configuración de integración de Microsoft Active Directory para el nuevo sistema de archivos. Para obtener más información, consulte Restauración de copias de seguridad en un nuevo sistema de archivos.

> **Note**
>
> Amazon FSx no admite Active Directory Connector ni Simple Active Directory.

Es posible que su servidor de archivos FSx para Windows quede mal configurado si se produce un cambio en la configuración de Active Directory que interrumpa la conexión con el sistema de archivos. Para devolver el sistema de archivos al estado Disponible, selecciona el botón Intentar recuperación en la FSx consola de Amazon o utiliza el `StartMisconfiguredStateRecovery` comando en la consola o FSx API de Amazon. Para obtener más información, consulte El sistema de archivos está mal configurado.

Temas

- Uso de Amazon FSx con AWS Directory Service for Microsoft Active Directory
- Uso de un Active Directory de Microsoft autoadministrado

Uso de Amazon FSx con AWS Directory Service for Microsoft Active Directory

AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) proporciona directorios de Active Directory reales, totalmente gestionados y de alta disponibilidad en la nube. Puede usar estos directorios de Active Directory en la implementación de la carga de trabajo.

Si su organización lo utiliza AWS Managed Microsoft AD para gestionar identidades y dispositivos, le recomendamos que integre su sistema de FSx archivos de Amazon con AWS Managed Microsoft AD. Al hacer esto, obtiene una solución llave en mano utilizando Amazon FSx con AWS Managed Microsoft AD. AWS gestiona el despliegue, el funcionamiento, la alta disponibilidad, la fiabilidad, la seguridad y la perfecta integración de los dos servicios, lo que le permite centrarse en gestionar su propia carga de trabajo de forma eficaz.

Para usar Amazon FSx con tu AWS Managed Microsoft AD configuración, puedes usar la FSx consola de Amazon. Cuando crees un nuevo sistema de archivos FSx para Windows File Server en la consola, selecciona AWS Managed Active Directory en la sección Autenticación de Windows. También elige el directorio específico que desee utilizar. Para obtener más información, consulte Paso 5. Crear el sistema de archivos.

Su organización puede gestionar las identidades y los dispositivos en un dominio de Active Directory autoadministrado (en las instalaciones o en la nube). Si es así, puede unir su sistema de FSx archivos de Amazon directamente a su dominio de Active Directory existente y autogestionado. Para obtener más información, consulte Uso de un Active Directory de Microsoft autoadministrado.

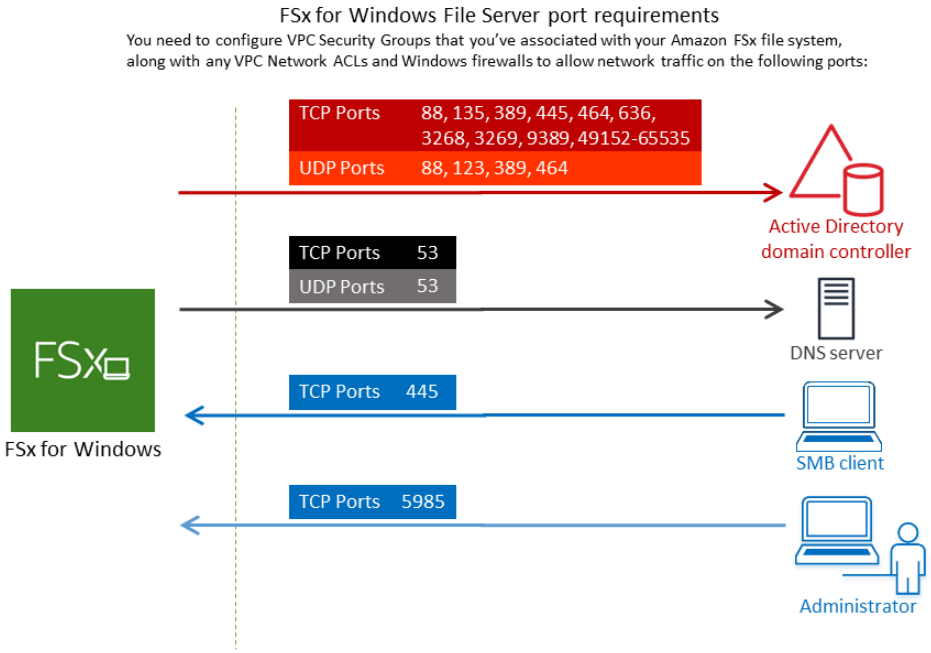
Además, también puede configurar su sistema para que se beneficie de un modelo de aislamiento de bosque de recursos. En este modelo, aísla sus recursos, incluidos los sistemas de FSx archivos de Amazon, en un bosque de Active Directory independiente del bosque en el que se encuentran sus usuarios.

> **Important**
>
> Para los sistemas de archivos Single-AZ 2 y todos los Multi-AZ, el nombre de dominio completo (FQDN) de Active Directory no puede superar los 47 caracteres.

Requisitos previos de red

Antes de crear un sistema de archivos de servidor de archivos FSx para Windows unido a su dominio de Active Directory administrado por AWS Microsoft, asegúrese de haber creado y configurado las siguientes configuraciones de red:

- En el caso de los grupos de seguridad de VPC, el grupo de seguridad predeterminado de la Amazon VPC predeterminada ya está agregado al sistema de archivos en la consola. Asegúrese de que el grupo de seguridad y la red ACLs de VPC de las subredes en las que va a crear el sistema de FSx archivos permitan el tráfico en los puertos y en las direcciones que se muestran en el siguiente diagrama.



En la siguiente tabla se identifica la función de cada puerto.

Protocolo	Puertos	Rol
TCP/UDP	53	Sisten de nombr de domin (DNS)
TCP/UDP	88	Auten ción de Kerbe

Protocolo	Puertos	Rol
TCP/UDP	464	Cambe stable contra a
TCP/UDP	389	Protoc ligero de acces a directo os (LD
UDP	123	Protoc de tiempo de red (NTP)

Protocolo	Puertos	Rol
TCP	135	Entorn de compu ón distrib do/ asigna dor de puntos de conex (DCE/ EPMA P)
TCP	445	Uso compa o de archiv SMB de Direct Servic

Protocolo	Puertos	Rol
TCP	636	Protoc ligero de acces a direct os sobre TLS/ SSL (
TCP	3268	Catálo global de Micros
TCP	3269	Catálo global de Micros media SSL
TCP	5985	WinRI 2.0 (Admi ración remot de Micros Windo

Protocolo	Puertos	Rol
TCP	9389	Servic web de Micros AD DS, Powe l
TCP	49152 - 65535	Puerto efíme para RPC

> **Important**
>
> Es necesario permitir el tráfico saliente del puerto TCP 9389 para las implementaciones de sistemas de archivos Single-AZ 2 y Multi-AZ.

> **Note**
>
> Si utilizas una red de VPC ACLs, también debes permitir el tráfico saliente en los puertos dinámicos (49152-65535) de tu sistema de archivos. FSx

- Si va a conectar su sistema de FSx archivos de Amazon a una VPC o cuenta AWS gestionada de Microsoft en una VPC o cuenta diferente, asegúrese de que haya conectividad entre esa VPC y la Amazon VPC en la que desee crear el sistema de archivos. Para obtener más información, consulte Uso de Amazon FSx AWS Managed Microsoft AD en una VPC o cuenta diferente.

> **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, las redes de VPC ACLs requieren que los puertos estén abiertos en ambas direcciones.

Utilice la herramienta Amazon FSx Network Validation para validar la conectividad con sus controladores de dominio de Active Directory.

Uso de un modelo de aislamiento de bosques de recursos

Une el sistema de archivos a una configuración de AWS Managed Microsoft AD . A continuación, debe establecer una relación de confianza forestal unidireccional entre un AWS Managed Microsoft AD dominio que cree y su dominio autogestionado de Active Directory existente. Para la autenticación de Windows en Amazon FSx, solo necesita una confianza de bosques unidireccional, en la que el bosque AWS gestionado confíe en el bosque de dominio corporativo.

Su dominio corporativo asume la función de dominio de confianza y el dominio AWS Directory Service administrado asume la función de dominio de confianza. Las solicitudes de autenticación validadas viajan entre los dominios en una sola dirección, lo que permite que las cuentas de su dominio corporativo se autentiquen con los recursos compartidos en el dominio administrado. En este caso, Amazon solo FSx interactúa con el dominio AWS gestionado. En un escenario de autenticación Kerberos, las solicitudes de autenticación que se originan en un cliente corporativo son validadas por el dominio corporativo, que las remite al dominio corporativo y AWS Managed Microsoft AD, finalmente, el cliente presenta su ticket de servicio al sistema de archivos del servidor de archivos de Windows. FSx Para obtener más información sobre las confianzas, consulte la publicación Todo lo que quería saber sobre las confianzas AWS Managed Microsoft AD en el blog AWS de seguridad.

Ponga a prueba su configuración de Active Directory

Antes de crear su sistema de FSx archivos de Amazon, le recomendamos que valide la conectividad con sus controladores de dominio de Active Directory mediante la herramienta Amazon FSx Network Validation. Para obtener más información, consulte Validar la conectividad con los controladores de dominio de Active Directory.

Los siguientes recursos relacionados pueden ayudarle AWS Directory Service for Microsoft Active Directory a FSx utilizar Windows File Server:

- ¿Qué AWS Directory Service contiene la Guía AWS Directory Service de administración
- Cree su Active Directory AWS administrado en la Guía AWS Directory Service de administración
- Cuándo crear una relación de confianza en la Guía de administración de AWS Directory Service

Uso de Amazon FSx AWS Managed Microsoft AD en una VPC o cuenta diferente

Puede unir su sistema FSx de archivos del servidor de archivos de Windows a un AWS Managed Microsoft AD directorio que se encuentre en una VPC diferente dentro de la misma cuenta mediante el emparejamiento de VPC. También puedes unir tu sistema de archivos a un AWS Managed Microsoft AD directorio que esté en una AWS cuenta diferente mediante el uso compartido de directorios.

> **Note**
>
> Solo puedes seleccionar uno AWS Managed Microsoft AD dentro del Región de AWS mismo sistema de archivos. Si desea usar una configuración de emparejamiento de VPC entre regiones, debe usar un Active Directory de Microsoft autoadministrado. Para obtener más información, consulte Uso de un Active Directory de Microsoft autoadministrado.

El flujo de trabajo para unir el sistema de AWS Managed Microsoft AD archivos a una VPC diferente consta de los siguientes pasos:

1. Configure su entorno de red.
2. Comparta su directorio.
3. Una su sistema de archivos al directorio compartido.

Para obtener más información, consulte Compartir su directorio en la Guía de administración de AWS Directory Service .

Para configurar su entorno de red, puede utilizar AWS Transit Gateway Amazon VPC y crear una conexión de emparejamiento de VPC. Además, asegúrese de que el tráfico de red esté permitido entre ambas. VPCs

Una puerta de enlace de tránsito es un centro de tránsito de red que puede usar para interconectar sus VPCs redes con las locales. Para obtener más información acerca del uso de puertas de enlace

de tránsito de VPC, consulte Introducción a las puertas de enlace de tránsito en la Guía de puertas de enlace de tránsito de Amazon VPC.

Una conexión de emparejamiento de VPC es una conexión de red entre dos. VPCs Esta conexión le permite enrutar el tráfico entre ellas mediante direcciones privadas del Protocolo de Internet versión 4 (IPv4) o del Protocolo de Internet versión 6 (IPv6). Puede utilizar el emparejamiento de VPC para conectarse VPCs dentro de la misma Región de AWS o entre ellas. 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.

Hay otro requisito previo al unir el sistema de archivos a un AWS Managed Microsoft AD directorio de una cuenta diferente a la del sistema de archivos. También debe compartir el Active Directory de Microsoft con la otra cuenta. Para ello, puede utilizar la función de uso compartido de directorios de Microsoft Active Directory AWS administrado. Para obtener más información, consulte Compartir su directorio en la Guía de administración de AWS Directory Service .

Validar la conectividad con los controladores de dominio de Active Directory

Antes de crear un sistema de archivos FSx para Windows File Server unido a su Active Directory, utilice la herramienta de validación de Amazon FSx Active Directory para validar la conectividad con su dominio de Active Directory. Puede utilizar esta prueba tanto si lo utiliza FSx para Windows File Server con Microsoft Active Directory AWS administrado como si utiliza una configuración de Active Directory autoadministrada. La prueba de conectividad de red del controlador de dominio (FSxADControllerconexión de prueba) no ejecuta el conjunto completo de comprobaciones de conectividad de red en todos los controladores de dominio del dominio. En su lugar utilice esta prueba para ejecutar la validación de la conectividad de red con un conjunto específico de controladores de dominio.

Cómo validar la conectividad con sus controladores de dominio de Active Directory

1. Lance una instancia de Amazon EC2 Windows en la misma subred y con los mismos grupos de seguridad de Amazon VPC que utilizará para FSx su sistema de archivos de Windows File Server. Para los tipos de implementación Multi-AZ, utilice la subred del servidor de archivos activo preferido.
2. Une tu instancia de EC2 Windows a tu Active Directory. Para obtener más información, consulte Cómo vincular una instancia de Windows de forma manual en la Guía de administración de AWS Directory Service .

3. Conéctese a su EC2 instancia. Para obtener más información, consulte Conectarse a su instancia de Windows en la Guía del EC2 usuario de Amazon.
4. Abre una PowerShell ventana de Windows (usando Ejecutar como administrador) en la EC2 instancia.

   Para comprobar si el módulo de Active Directory necesario para Windows PowerShell está instalado, utilice el siguiente comando de prueba.

   ```
   PS C:\> Import-Module ActiveDirectory
   ```

   Si lo anterior devuelve un error, instálelo con el siguiente comando.

   ```
   PS C:\> Install-WindowsFeature RSAT-AD-PowerShell
   ```
5. Descargue la herramienta de validación de red con el siguiente comando.

   ```
   PS C:\> Invoke-WebRequest "https://docs.aws.amazon.com/fsx/latest/WindowsGuide/
   samples/AmazonFSxADValidation.zip" -OutFile "AmazonFSxADValidation.zip"
   ```
6. Descomprima el archivo zip con el siguiente comando.

   ```
   PS C:\> Expand-Archive -Path "AmazonFSxADValidation.zip"
   ```
7. Añade el FSx ADValidation módulo Amazon a la sesión actual.

   ```
   PS C:\> Import-Module .\AmazonFSxADValidation
   ```
8. Establezca el valor de la dirección IP del controlador de dominio de Active Directory y ejecute la prueba de conectividad mediante los siguientes comandos:

   ```
   $ADControllerIp = '10.0.75.243'
   $Result = Test-FSxADControllerConnection -ADControllerIp $ADControllerIp
   ```
9. El siguiente ejemplo muestra cómo recuperar el resultado de la prueba, con los resultados de una prueba de conectividad correcta.

   ```
   PS C:\AmazonFSxADValidation> $Result
   ```

```
Name                           Value
----                           -----
TcpDetails                     {@{Port=88; Result=Listening; Description=Kerberos
 authentication}, @{Port=135; Resul...
Server                         10.0.75.243
UdpDetails                     {@{Port=88; Result=Timed Out; Description=Kerberos
 authentication}, @{Port=123; Resul...
Success                        True


PS C:\AmazonFSxADValidation> $Result.TcpDetails

Port Result    Description
---- ------    -----------
  88 Listening Kerberos authentication
 135 Listening DCE / EPMAP (End Point Mapper)
 389 Listening Lightweight Directory Access Protocol (LDAP)
 445 Listening Directory Services SMB file sharing
 464 Listening Kerberos Change/Set password
 636 Listening Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
3268 Listening Microsoft Global Catalog
3269 Listening Microsoft Global Catalog over SSL
9389 Listening Microsoft AD DS Web Services, PowerShell
```

El siguiente ejemplo muestra cómo se ejecuta la prueba y se obtiene un resultado fallido.

```
PS C:\AmazonFSxADValidation> $Result = Test-FSxADControllerConnection -
ADControllerIp $ADControllerIp
WARNING: TCP 9389 failed to connect. Required for Microsoft AD DS Web Services,
 PowerShell.
Verify security group and firewall settings on both client and directory
 controller.
WARNING: 1 ports failed to connect to 10.0.75.243. Check pre-requisites in
https://docs.aws.amazon.com/fsx/latest/WindowsGuide/self-managed-AD.html#self-
manage-prereqs

PS C:\AmazonFSxADValidation> $Result

Name                           Value
----                           -----
TcpDetails                     {@{Port=88; Result=Listening; Description=Kerberos
 authentication}, @{Port=135; Resul...
```

```
Server                          10.0.75.243
UdpDetails                      {@{Port=88; Result=Timed Out; Description=Kerberos
 authentication}, @{Port=123; Resul...
Success                         False
FailedTcpPorts                  {9389}


PS C:\AmazonFSxADValidation> $Result.FailedTcpPorts
9389
```

Windows socket error code mapping

https://msdn.microsoft.com/en-us/library/ms740668.aspx

> **Note**
>
> Como alternativa al procedimiento anterior, puede utilizar el `AWSSupport-ValidateFSxWindowsADConfig` manual de instrucciones para validar la configuración autogestionada de Active Directory. Para obtener más información, consulte `AWSSupport-ValidateFSxWindowsADConfig` en la Referencia del manual de procedimientos de automatización de AWS Systems Manager .

Uso de un Active Directory de Microsoft autoadministrado

Si su organización administra las identidades y los dispositivos mediante un Active Directory autogestionado de forma local o en la nube, puede unir un FSx sistema de archivos del servidor de archivos de Windows a su dominio de Active Directory en el momento de la creación.

Al unir el sistema de archivos al Active Directory autoadministrado, el sistema de archivos del servidor de archivos FSx para Windows reside en el mismo bosque de Active Directory (el contenedor lógico superior de una configuración de Active Directory que contiene dominios, usuarios y equipos) y en el mismo dominio de Active Directory que los usuarios y los recursos existentes (incluidos los servidores de archivos existentes).

> **Note**
>
> Puede aislar sus recursos, incluidos los sistemas de FSx archivos de Amazon, en un bosque de Active Directory distinto del bosque en el que residen sus usuarios. Para ello, una su sistema de archivos a un Microsoft Active Directory AWS administrado y establezca una relación de confianza en el bosque unidireccional entre un AWS Microsoft Active Directory administrado que cree y su Active Directory autoadministrado existente.

- Nombre de usuario y contraseña de una cuenta de servicio en su dominio de Active Directory, para FSx que Amazon los utilice para unir el sistema de archivos a su dominio de Active Directory.
- (Opcional) La unidad organizativa (OU) del dominio a la que desea unir el sistema de archivos.
- (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 archivos compartidos de Windows, administrar las listas de control de acceso (ACLs) en la carpeta raíz del sistema de archivos, hacerse con la propiedad de los 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.

  > **Note**
  >
  > El nombre del grupo de dominios que proporcione debe ser único en su Active Directory. FSx para Windows File Server no creará el grupo de dominios en las siguientes circunstancias:
  >
  > - Si ya existe un grupo con el nombre que especifique
  > - Si no especifica un nombre y ya existe un grupo denominado “Administradores de dominio” en el Active Directory.

Para obtener más información, consulte Unir un sistema de FSx archivos de Amazon a un dominio autogestionado de Microsoft Active Directory.

Temas

- Requisitos previos
- Prácticas recomendadas a la hora de utilizar un Active Directory autogestionado

- Cuenta de FSx servicio de Amazon
- Delegación de permisos a la cuenta o grupo FSx de servicio de Amazon
- Cómo validar la configuración del Active Directory
- Unir un sistema de FSx archivos de Amazon a un dominio autogestionado de Microsoft Active Directory
- Obtención de las direcciones IP del sistema de archivos correctas para usarlas en las entradas manuales del DNS
- Actualización de la configuración de un Active Directory autoadministrado
- Cambiar la cuenta de FSx servicio de Amazon
- Supervisión de las actualizaciones del Active Directory autoadministrado

Requisitos previos

Antes de unir un sistema FSx de archivos de Windows File Server a su dominio autogestionado de Microsoft Active Directory, revise los siguientes requisitos previos para asegurarse de que puede unir correctamente su sistema de FSx archivos de Amazon a su Active Directory autogestionado.

Configuraciones en las instalaciones

Estos son los requisitos previos para su Microsoft Active Directory autogestionado, ya sea local o basado en la nube, al que se unirá al sistema de FSx archivos de Amazon.

- Controladores de dominio del Active Directory:
  - Debe tener un nivel funcional de dominio en Windows Server 2008 R2 o superior.
  - Debe tener permisos de escritura.
  - Al menos uno de los controladores de dominio accesibles debe ser un catálogo global del bosque.
- El servidor DNS debe poder resolver los nombres de la siguiente manera:
  - En el dominio al que se va a unir al sistema de archivos
  - En el dominio raíz del bosque
- Las direcciones IP del servidor DNS y del controlador de dominio de Active Directory deben cumplir los siguientes requisitos, que varían en función de cuándo se creó el sistema de FSx archivos de Amazon:

Para los sistemas de archivos creados antes del 17 de diciembre de 2020	Para sistemas de archivos creados después del 17 de diciembre de 2020
Las direcciones IP deben estar en un rango de direcciones IP privadas según la norma RFC 1918: • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	Las direcciones IP pueden estar en cualquier rango, excepto: • Direcciones IP que entran en conflicto con las direcciones IP propiedad de Amazon Web Services en el Región de AWS que se encuentra el sistema de archivos. Para obtener una lista de las direcciones IP AWS propias por región, consulte los rangos de direcciones AWS IP. • Direcciones IP en el rango de bloques de CIDR de 198.19.0.0/16

Si necesita acceder a un FSx sistema de archivos del servidor de archivos de Windows creado antes del 17 de diciembre de 2020 utilizando un rango de direcciones IP no privadas, puede crear un nuevo sistema de archivos restaurando una copia de seguridad del sistema de archivos. Para obtener más información, consulte Restauración de una copia de seguridad en un nuevo sistema de archivos.

- El nombre de dominio del Active Directory autoadministrado debe cumplir los siguientes requisitos:
  - El nombre de dominio no está en formato de dominio de etiqueta única (SLD). Amazon FSx no admite dominios SLD.
  - En los sistemas de archivos Single-AZ 2 y en todos los sistemas de archivos Multi-AZ, el nombre de dominio no puede superar los 47 caracteres.
- Todos los sitios de Active Directory que haya definido deben cumplir los siguientes requisitos previos:
  - Las subredes de la VPC asociada al sistema de archivos deben definirse en un sitio del Active Directory.
  - No hay discrepancias entre las subredes de VPC y ninguna de las subredes del sitio de Active Directory.

Amazon FSx requiere conectividad con los controladores de dominio o los sitios de Active Directory que haya definido en su entorno de Active Directory. Amazon FSx ignorará cualquier controlador de dominio con TCP y UDP bloqueados en el puerto 389. Para el resto de los controladores de dominio de su Active Directory, asegúrese de que cumplen los requisitos de FSx conectividad de Amazon. Además, compruebe que cualquier cambio en su cuenta de servicio se propague a todos estos controladores de dominio.

> **Important**
>
> No muevas los objetos de ordenador que Amazon FSx cree en la unidad organizativa una vez creado el sistema de archivos. Si lo hace, el sistema de archivos no se configurará de manera correcta.

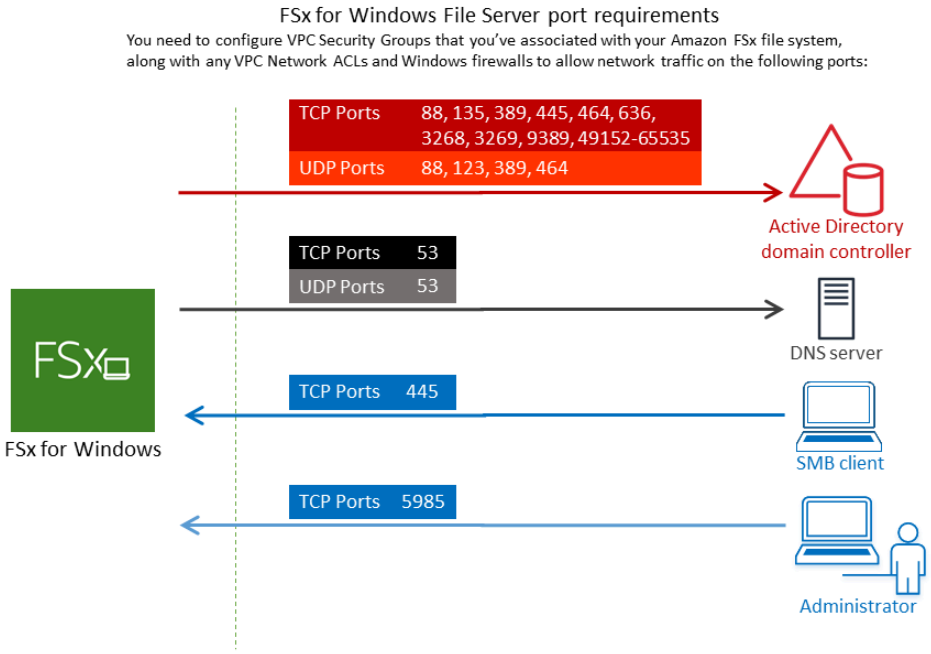
Puede validar la configuración de Active Directory, incluidas las pruebas de conectividad de varios controladores de dominio, mediante la herramienta de validación de Amazon FSx Active Directory. Para restringir la cantidad de controladores de dominio que requieren conectividad, también puede establecer una relación de confianza entre los controladores de dominio en las instalaciones y el AWS Managed Microsoft AD. Para obtener más información, consulte Uso de un modelo de aislamiento de bosques de recursos.

> **Important**
>
> Amazon FSx solo registra los registros DNS de un sistema de archivos si utilizas el DNS de Microsoft como servicio de DNS predeterminado. Si utiliza un DNS de terceros, tendrá que configurar las entradas de registro del DNS para el sistema de archivos de forma manual después de crearlo.

Configuraciones de red

En esta sección, se describen los requisitos de configuración de la red para unir un sistema de archivos al Active Directory autoadministrado. Le recomendamos encarecidamente que utilice la herramienta de validación de Amazon FSx Active Directory para probar la configuración de red antes de intentar unir su sistema de archivos a su Active Directory autogestionado.

- Asegúrese de que las reglas del firewall permitan el tráfico ICMP entre los controladores de dominio de Active Directory y Amazon FSx.
- La Conectividad debe estar configurada entre la Amazon VPC donde desea crear el sistema de archivos y el Active Directory autoadministrado. Puede configurar esta conectividad con AWS Direct Connect, AWS Virtual Private Network, el emparejamiento de VPC o AWS Transit Gateway.
- El grupo de seguridad de VPC predeterminado para su Amazon VPC predeterminada debe añadirse a su sistema de archivos mediante la consola de Amazon. FSx Asegúrese de que el grupo de seguridad y la red ACLs de VPC de las subredes en las que cree el sistema de archivos permitan el tráfico en los puertos y en la dirección que se muestra en el siguiente diagrama.



En la siguiente, tabla se identifican el protocolo, los puertos y la función.

Protocolo	Puertos	Rol
TCP/UDP	53	Sistema de nombres de dominio (DNS)
TCP/UDP	88	Autenticación de Kerberos
TCP/UDP	464	Cambiar/establecer contraseña

Protocolo	Puertos	Rol
TCP/UDP	389	Protocolo ligero de acceso a directorios (LDAP)
UDP	123	Protocolo de tiempo de red (NTP)
TCP	135	(Computación distribuida) Environment/End Point Mapper (DCE/EPMAP
TCP	445	Uso compartido de archivos SMB de Directory Services
TCP	636	Protocolo ligero de acceso a directorios sobre TLS/SSL (LDAP)
TCP	3268	Catálogo global de Microsoft
TCP	3269	Catálogo global de Microsoft mediante SSL
TCP	5985	WinRM 2.0 (Administración remota de Microsoft Windows)
TCP	9389	Servicios web Microsoft Active Directory DS, PowerShell **Important** Es necesario permitir el tráfico saliente en el puerto TCP 9389 para las implementaciones de sistemas de archivos Single-AZ 2 y Multi-AZ.
TCP	49152 - 65535	Puertos efímeros para RPC

Estas reglas de tráfico también deben reflejarse en los firewalls que se aplican a cada uno de los controladores de dominio, servidores DNS, FSx clientes y administradores de Active Directory. FSx

> **Note**
>
> Si utilizas una red de VPC ACLs, también debes permitir el tráfico saliente en los puertos dinámicos (49152-65535) de tu sistema de archivos.

> **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.

Permisos de cuentas de servicio

Debe tener una cuenta de servicio en el Microsoft Active Directory autoadministrado con permisos delegados para unir objetos de equipos al dominio del Active Directory autoadministrado. Una cuenta de servicio es una cuenta de usuario del Active Directory autoadministrado a la que se le delegó permiso para realizar determinadas tareas.

El siguiente es el conjunto mínimo de permisos que se deben delegar en la cuenta de FSx servicio de Amazon en la OU a la que se va a unir al sistema de archivos.

- Si usa el control delegado en la Microsoft Management Console (MMC) usuarios y computadoras del Active Directory:
  - Restablecer contraseñas
  - 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
- Si usa funciones avanzadas en la MMC usuarios y computadoras del Active Directory:
  - Modificar los permisos
  - Crear objetos de equipo
  - Eliminar objetos informáticos

Para obtener más información, consulte, en la documentación de Microsoft Windows Server, el tema Error: se deniega el acceso cuando los usuarios que no son administradores a los que se les delegó el control intentan unir los equipos a un controlador de dominio.

Para obtener más información sobre cómo establecer los permisos necesarios, consulte Delegación de permisos a la cuenta o grupo FSx de servicio de Amazon.

Prácticas recomendadas a la hora de utilizar un Active Directory autogestionado

Le recomendamos que siga estas prácticas recomendadas al unir un sistema de archivos de Amazon FSx para Windows File Server a su Microsoft Active Directory autogestionado. Estas prácticas recomendadas le ayudarán a mantener la disponibilidad continua e ininterrumpida del sistema de archivos.

Usa una cuenta de servicio independiente para Amazon FSx

Utilice una cuenta de servicio independiente para delegar los privilegios necesarios para que Amazon FSx gestione completamente los sistemas de archivos que están unidos a su Active Directory autogestionado. No recomendamos usar los administradores de dominio para este fin.

Uso de un grupo de Active Directory

Utilice un grupo de Active Directory para gestionar los permisos y las configuraciones de Active Directory asociados a la cuenta de FSx servicio de Amazon.

Segregar la unidad organizativa (OU)

Para facilitar la búsqueda y la administración de los objetos de su FSx ordenador de Amazon, le recomendamos que separe la unidad organizativa (OU) que utiliza FSx para sus sistemas de archivos de Windows File Server de otras cuestiones relacionadas con el controlador de dominio.

Conserve la configuración de Active Directory up-to-date

Es imprescindible que mantenga la configuración de Active Directory del sistema de archivos up-to-date con cualquier cambio. Por ejemplo, si el Active Directory autoadministrado usa una política de restablecimiento de contraseñas en función del tiempo, apenas se restablezca la contraseña, procure actualizar la contraseña de la cuenta de servicio en el sistema de archivos. Para obtener más información, consulte Actualización de la configuración de un Active Directory autoadministrado.

Cambiar la cuenta de FSx servicio de Amazon

Si actualiza el sistema de archivos con una cuenta de servicio nueva, debe tener los permisos y privilegios requeridos para unirse al Active Directory y tener permisos de control total sobre los objetos de equipos existentes asociados al sistema de archivos. Para obtener más información, consulte Cambiar la cuenta de FSx servicio de Amazon.

Asigne subredes a un único sitio de Microsoft Active Directory

Si su entorno de Active Directory tiene una gran cantidad de controladores de dominio, utilice Sitios y servicios de Active Directory para asignar las subredes que utilizan los sistemas de FSx archivos de Amazon a un único sitio de Active Directory con la máxima disponibilidad y fiabilidad. Asegúrese de que el grupo de seguridad de la VPC, la ACL de la red de la VPC, las reglas del firewall de Windows y cualquier otro control de enrutamiento de red que tenga en su infraestructura de Active Directory permitan la comunicación desde Amazon FSx en los puertos necesarios. DCs Esto permite a Windows volver a otros controladores de dominio si no puede usar el sitio de Active Directory asignado. Para obtener más información, consulte Control de acceso al sistema de archivos con Amazon VPC.

Usar reglas de grupos de seguridad para limitar el tráfico

Use las reglas de los grupos de seguridad para implementar el principio del privilegio mínimo en la nube privada virtual (VPC). Puede limitar el tipo de tráfico de red entrante y saliente permitido para el archivo mediante reglas de grupos de seguridad de VPC. Por ejemplo, recomendamos permitir el tráfico saliente únicamente a los controladores de dominio del Active Directory autoadministrado o dentro de la subred o el grupo de seguridad que esté usando. Para obtener más información, consulte Control de acceso al sistema de archivos con Amazon VPC.

No muevas los objetos informáticos creados por Amazon FSx

> **Important**
>
> No muevas los objetos de ordenador que Amazon FSx cree en la unidad organizativa una vez creado el sistema de archivos. Si lo hace, el sistema de archivos no se configurará de manera correcta.

Validar la configuración de Active Directory

Antes de intentar unir un sistema FSx de archivos de Windows File Server a Active Directory, le recomendamos encarecidamente que valide la configuración de Active Directory con la herramienta de validación de Amazon FSx Active Directory.

Cuenta de FSx servicio de Amazon

Los sistemas de FSx archivos de Amazon que están unidos a un Active Directory autogestionado requieren una cuenta de servicio válida durante toda su vida útil. Amazon FSx utiliza la cuenta de servicio para gestionar completamente sus sistemas de archivos y realizar tareas administrativas que requieren separar y volver a unir objetos informáticos a su dominio de Active Directory. Estas tareas incluyen reemplazar un servidor de archivos defectuoso y aplicar parches al software de Microsoft Windows Server. Para FSx que Amazon lleve a cabo estas tareas, la cuenta de FSx servicio de Amazon debe tener, como mínimo, el conjunto de permisos que se describe en Permisos de cuentas de servicio Delegado.

Aunque los miembros del grupo Administradores de dominio tienen privilegios suficientes para realizar estas tareas, te recomendamos encarecidamente que utilices una cuenta de servicio independiente para delegar los privilegios necesarios en Amazon FSx.

Para obtener más información sobre cómo delegar privilegios mediante las características de delegar control o características avanzadas del complemento MMC usuarios y computadoras de Active Directory, consulte Delegación de permisos a la cuenta o grupo FSx de servicio de Amazon.

Si actualiza el sistema de archivos con una cuenta de servicio nueva, esta debe tener los permisos y privilegios requeridos para unirse al Active Directory y tener permisos de control total sobre los objetos de equipos existentes asociados al sistema de archivos. Para obtener más información, consulte Cambiar la cuenta de FSx servicio de Amazon.

Delegación de permisos a la cuenta o grupo FSx de servicio de Amazon

La cuenta de FSx servicio o el grupo de administradores de Amazon deben tener los privilegios necesarios FSx para unirse a los sistemas de archivos de Windows File Server a su dominio autogestionado de Active Directory. Para delegar estos permisos, puede utilizar el control delegado o las funciones avanzadas del Active Directory User and Computers MMC complemento, tal y como se describe en los siguientes procedimientos.

Para asignar permisos mediante delegar control

Para asignar permisos a una cuenta o grupo de servicio mediante delegar control

1. Inicie sesión en el sistema como administrador de dominio del dominio del 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 Asistente de delegación de control, elija Siguiente.
6. Selecciona Añadir para añadir el nombre de tu cuenta de FSx servicio o grupo de Amazon y, a continuación, selecciona 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. 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

11. Elija Siguiente y, a continuación, elija Finalizar.
12. Cierre el complemento MMC Usuarios y equipos del Active Directory.

Para asignar permisos mediante características avanzadas

1. Inicie sesión en el sistema como administrador de dominio del dominio del Active Directory.
2. Abra el complemento MMC Usuarios y equipos del Active Directory.
3. Seleccione Ver en la barra de menús y asegúrese de que las Características avanzadas estén habilitadas (si la característica está habilitada, aparecerá una marca de verificación junto a ella).

4. En el panel de tareas, expanda el nodo del dominio.
5. Busque y abra (botón derecho) el menú contextual de la unidad organizativa que quiera modificar y, a continuación, elija Propiedades.
6. En el panel Propiedades de la unidad organizativa, seleccione la pestaña Seguridad.
7. En la pestaña Seguridad, seleccione Avanzado. Luego, elija Añadir.
8. En la página de entrada de permisos, selecciona Selecciona un responsable e introduce el nombre de tu cuenta de FSx servicio o grupo de Amazon. En Se aplica a:, seleccione Este objeto y todos los ordenadores descendientes. Compruebe que lo siguiente esté seleccionado:
   - Modificar los permisos
   - Crear objetos informáticos
   - Eliminar objetos informáticos
9. Seleccione Aplicar y, a continuación, Aceptar.
10. Cierre el complemento MMC Usuarios y equipos del Active Directory.

Cómo validar la configuración del Active Directory

Antes de crear un sistema de archivos FSx para Windows File Server unido a su Active Directory, le recomendamos que valide la configuración de Active Directory con la herramienta de validación de Amazon FSx Active Directory. Tenga en cuenta que para lograr validar la configuración de Active Directory es necesario tener conectividad a Internet saliente.

Cómo validar la configuración de Active Directory

1. Lance una instancia de Amazon EC2 Windows en la misma subred y con los mismos grupos de seguridad de Amazon VPC que utiliza para FSx su sistema de archivos de Windows File Server. Asegúrese de que la EC2 instancia tenga los permisos de `AmazonEC2ReadOnlyAccess` IAM necesarios. Puede validar los permisos de los roles de EC2 instancia mediante el simulador de políticas de IAM. Para obtener más información, consulte Probar las políticas de IAM con el simulador de política de IAM en la Guía del usuario de IAM.
2. Une tu instancia de EC2 Windows a tu Active Directory. Para obtener más información, consulte Cómo vincular una instancia de Windows de forma manual en la Guía de administración de AWS Directory Service .
3. Conéctese a su EC2 instancia. Para obtener más información, consulte Conectarse a su instancia de Windows en la Guía del EC2 usuario de Amazon.

4. Abre una PowerShell ventana de Windows (usando Ejecutar como administrador) en la EC2 instancia.

   Para comprobar si el módulo de Active Directory necesario para Windows PowerShell está instalado, utilice el siguiente comando de prueba.

   ```
   PS C:\> Import-Module ActiveDirectory
   ```

   Si lo anterior devuelve un error, instálelo con el siguiente comando.

   ```
   PS C:\> Install-WindowsFeature RSAT-AD-PowerShell
   ```

5. Descargue la herramienta de validación de red con el siguiente comando.

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

6. Descomprima el archivo zip con el siguiente comando.

   ```
   PS C:\> Expand-Archive -Path "AmazonFSxADValidation.zip"
   ```

7. Agregue el módulo `AmazonFSxADValidation` a la sesión actual.

   ```
   PS C:\> Import-Module .\AmazonFSxADValidation
   ```

8. Para establecer los parámetros necesarios, en el siguiente comando, tiene que sustituir:

   - Nombre de dominio de Active Directory (*DOMAINNAME.COM*)
   - Prepare el objeto `$Credential` para la contraseña de la cuenta de servicio mediante una de las siguientes opciones.
     - Para generar el objeto de credenciales de forma interactiva, utilice el siguiente comando.

       ```
       $Credential = Get-Credential
       ```

     - Para generar el objeto de credenciales mediante un AWS Secrets Manager recurso, utilice el siguiente comando.

```
$Secret = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
 $AdminSecret).SecretString
$Credential = (New-Object PSCredential($Secret.UserName,(ConvertTo-SecureString
 $Secret.Password -AsPlainText -Force)))
```

- Direcciones IP del servidor DNS (*IP_ADDRESS_1*,*IP_ADDRESS_2*)
- ID de subred para las subredes en las que planea crear su sistema de FSx archivos de Amazon (*SUBNET_1*,, por ejemplo*SUBNET_2*,`subnet-04431191671ac0d19`).

```
PS C:\>
$FSxADValidationArgs = @{
    # DNS root of ActiveDirectory domain
    DomainDNSRoot = 'DOMAINNAME.COM'

    # IP v4 addresses of DNS servers
    DnsIpAddresses = @('IP_ADDRESS_1', 'IP_ADDRESS_2')

    # Subnet IDs for Amazon FSx file server(s)
    SubnetIds = @('SUBNET_1', 'SUBNET_2')

    Credential = $Credential
}
```

9. (Opcional) Defina la unidad organizativa, el grupo de administradores delegados y habilite la validación de los permisos de la cuenta de servicio siguiendo las instrucciones del `README.md` archivo incluido antes de ejecutar la herramienta de validación. DomainControllersMaxCount

> **Note**
>
> El grupo `Domain Admins` tiene un nombre diferente si el sistema operativo no está en inglés. Por ejemplo, el nombre del grupo es `Administrateurs du domaine` en la versión francesa del sistema operativo. Si no especifica un valor, se utiliza el nombre predeterminado del grupo `Domain Admins`, y se produce un error en la creación del sistema de archivos.

10. Ejecute la herramienta de validación con este comando.

```
PS C:\> $Result = Test-FSxADConfiguration @FSxADValidationArgs
```

11. A continuación, hay un ejemplo de respuesta correcta de la prueba.

```
Test 1 - Validate EC2 Subnets ...
...
Test 17 - Validate 'Delete Computer Objects' permission ...

Test computer object amznfsxtestd53f deleted!
...
SUCCESS - All tests passed! Please proceed to creating an Amazon FSx file system.
 For your convenience, SelfManagedActiveDirectoryConfiguration of result can be
 used directly in CreateFileSystemWindowsConfiguration for New-FSXFileSystem
PS C:\AmazonFSxADValidation> $Result.Failures.Count
0
PS C:\AmazonFSxADValidation> $Result.Warnings.Count
0
```

A continuación, hay un ejemplo de respuesta con errores.

```
Test 1 - Validate EC2 Subnets ...
...
Test 7 - Validate that provided EC2 Subnets belong to a single AD Site ...

Name          DistinguishedName
     Site
----          -----------------
     ----
10.0.0.0/19   CN=10.0.0.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-
ad,DC=local   CN=SiteB,CN=Sites,CN=Configu...
10.0.128.0/19 CN=10.0.128.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-
ad,DC=local CN=Default-First-Site-Name,C...
10.0.64.0/19  CN=10.0.64.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-
ad,DC=local  CN=SiteB,CN=Sites,CN=Configu...



Best match for EC2 subnet subnet-092f4caca69e360e7 is AD site CN=Default-First-
Site-Name,CN=Sites,CN=Configuration,DC=te
st-ad,DC=local
Best match for EC2 subnet subnet-04431191671ac0d19 is AD site
 CN=SiteB,CN=Sites,CN=Configuration,DC=test-ad,DC=local
WARNING: EC2 subnets subnet-092f4caca69e360e7 subnet-04431191671ac0d19 matched to
 different AD sites! Make sure they
are in a single AD site.
```

```
...
9 of 16 tests skipped.
FAILURE - Tests failed. Please see error details below:

Name                           Value
----                           -----
SubnetsInSeparateAdSites       {subnet-04431191671ac0d19, subnet-092f4caca69e360e7}



Please address all errors and warnings above prior to re-running validation to
 confirm fix.
PS C:\AmazonFSxADValidation> $Result.Failures.Count
1
PS C:\AmazonFSxADValidation> $Result.Failures

Name                           Value
----                           -----
SubnetsInSeparateAdSites       {subnet-04431191671ac0d19, subnet-092f4caca69e360e7}


PS C:\AmazonFSxADValidation> $Result.Warnings.Count
0
```

Si recibe advertencias o errores al ejecutar la herramienta de validación, consulte la guía de solución de problemas que se incluye en el paquete de herramientas de validación (`TROUBLESHOOTING.md`) y Solución de problemas de Amazon FSx.

Unir un sistema de FSx archivos de Amazon a un dominio autogestionado de Microsoft Active Directory

Al crear un nuevo sistema de archivos FSx para Windows File Server, puede configurar la integración de Microsoft Active Directory para que se una a su dominio autogestionado de Microsoft Active Directory. Para ello, proporcione la siguiente información para su Microsoft Active Directory:

- El nombre de dominio completo (FQDN) del directorio en las instalaciones de Active Directory de Microsoft.

> **Note**
>
> FSx Actualmente, Amazon no admite dominios de etiqueta única (SLD).

- Las direcciones IP de los servidores DNS de su dominio.
- Credenciales de una cuenta de servicio en el dominio de Microsoft Active Directory en las instalaciones. Amazon FSx utiliza estas credenciales para unirse a su Active Directory autogestionado.

Si lo desea, también puede especificar lo siguiente:

- Una unidad organizativa (OU) específica del dominio al que quieres que se una tu sistema de FSx archivos de Amazon.
- El nombre del grupo de dominios a cuyos miembros se les conceden privilegios administrativos para el sistema de FSx archivos de Amazon. El nombre del grupo de dominios que proporcione debe ser único en el Active Directory.

Tras especificar esta información, Amazon FSx une su nuevo sistema de archivos a su dominio autogestionado de Active Directory mediante la cuenta de servicio que ha proporcionado.

> **Important**
>
> Amazon FSx solo registra los registros DNS de un sistema de archivos si el dominio de Active Directory al que se va a unir utiliza el DNS de Microsoft como DNS predeterminado. Si utilizas un DNS de terceros, tendrás que configurar manualmente las entradas de DNS para tus sistemas de FSx archivos de Amazon después de crear tu sistema de archivos. Para obtener más información acerca de la elección de las direcciones IP correctas para usar en el sistema de archivos, consulte Obtención de las direcciones IP del sistema de archivos correctas para usarlas en las entradas manuales del DNS.

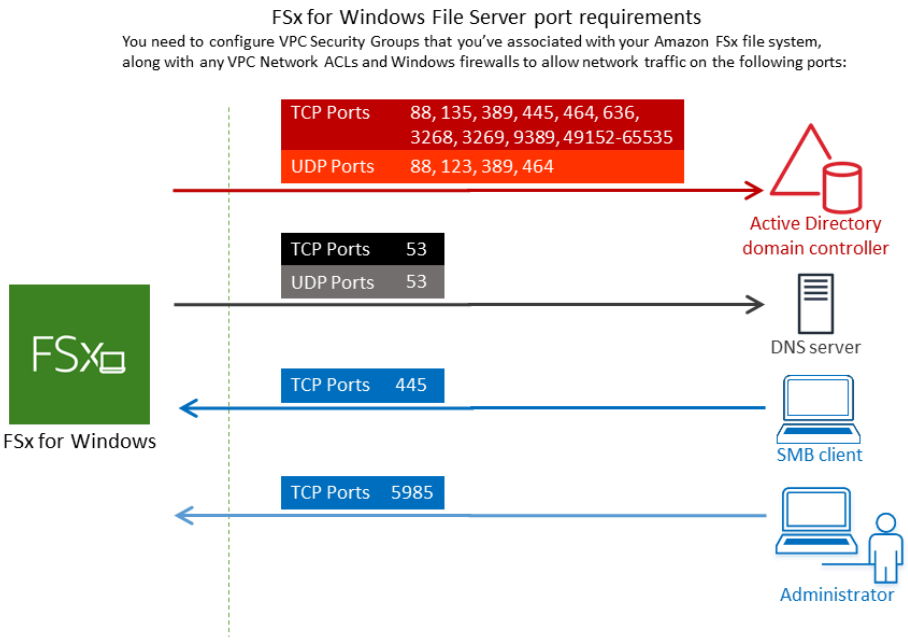
Antes de empezar

Asegúrese de haber completado Requisitos previos que se detalla en Uso de un Active Directory de Microsoft autoadministrado.

Para crear un sistema de archivos de servidor de archivos FSx para Windows unido a un Active Directory autogestionado (consola)

1. Abre 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. Selecciona FSx Windows File Server y, a continuación, selecciona Siguiente. Aparece la página Crear sistema de archivos.
4. Proporcione un nombre para el sistema de archivos. Puede utilizar un máximo de 256 letras Unicode, espacio en blanco y números, además de los siguientes caracteres especiales: + - = . _ : /
5. En Capacidad de almacenamiento, introduzca la capacidad de almacenamiento de su sistema de archivos, en GiB. Si utiliza un almacenamiento SSD, introduzca cualquier número entero comprendido entre 32 y 65 536. Si utiliza un almacenamiento SSD, introduzca cualquier número entero comprendido entre 2000 y 65 536. Puede aumentar la capacidad de almacenamiento según sea necesario en cualquier momento después de crear el sistema de archivos. Para obtener más información, consulte Administrar la capacidad de almacenamiento.
6. En el campo Throughput capacity (Capacidad de rendimiento), mantenga la configuración predeterminada. Capacidad de rendimiento: velocidad constante a la que el servidor de archivos que aloja a su sistema de archivos puede servir datos. La configuración de capacidad de rendimiento recomendada se basa en la cantidad de capacidad de almacenamiento que elija. Si necesita una capacidad de rendimiento superior a la recomendada, elija Especificar la capacidad de rendimiento y, a continuación, elija un valor. Para obtener más información, consulte FSx para el rendimiento del servidor de archivos de Windows.

   Puede modificar la capacidad de rendimiento según sea necesario en cualquier momento después de crear el sistema de archivos. Para obtener más información, consulte Administración de la capacidad de rendimiento.
7. Elija la VPC que desea asociar con su sistema de archivos. Para este ejercicio de introducción, elija la misma VPC que para su AWS Directory Service directorio e instancia de Amazon EC2.
8. Elija cualquier valor para las Zonas de disponibilidad y Subred.
9. En el caso de los grupos de seguridad de VPC, el grupo de seguridad predeterminado de la Amazon VPC predeterminada ya está agregado al sistema de archivos en la consola. Asegúrese de que el grupo de seguridad y la red ACLs de VPC de las subredes en las que va a crear el sistema de FSx archivos permitan el tráfico en los puertos y en las direcciones que se muestran en el siguiente diagrama.



En la siguiente tabla se identifica la función de cada puerto.

Protocolo	Puertos	Rol
TCP/UDP	53	Sisten de nombr de domin (DNS)
TCP/UDP	88	Auten ción de Kerbe

Protocolo	Puertos	Rol
TCP/UDP	464	Cambe stable contra a
TCP/UDP	389	Protoc ligero de acces a directo os (LD
UDP	123	Protoc de tiempo de red (NTP)

Protocolo	Puertos	Rol
TCP	135	Entorn de compu ón distrib do/ asigna dor de puntos de conex (DCE/ EPMA P)
TCP	445	Uso compa o de archiv SMB de Direct Servic

Protocolo	Puertos	Rol
TCP	636	Protoc ligero de acces a direct os sobre TLS/ SSL (
TCP	3268	Catálo global de Micros
TCP	3269	Catálo global de Micros media SSL
TCP	5985	WinRI 2.0 (Admi ración remot de Micros Windo

Protocolo	Puertos	Rol
TCP	9389	Servic web Micros Active Direct DS, Power
TCP	49152 - 65535	Puerto efíme para RPC

> **Important**
>
> Es necesario permitir el tráfico saliente del puerto TCP 9389 para las implementaciones de sistemas de archivos Single-AZ 2 y Multi-AZ.

> **Note**
>
> Si utilizas una red de VPC ACLs, también debes permitir el tráfico saliente en los puertos dinámicos (49152-65535) de tu sistema de archivos. FSx

- Reglas de salida para permitir que todo el tráfico se dirija a las direcciones IP asociadas a los servidores DNS y los controladores de dominio de su dominio autoadministrado de Microsoft Active Directory. Para obtener más información, consulte la documentación de Microsoft sobre la configuración del firewall para la comunicación con Active Directory.
- Asegúrese de que estas reglas de tráfico también estén reflejadas en los firewalls que se aplican a cada uno de los controladores de dominio, servidores DNS, clientes y administradores de Active Directory. FSx FSx

> **Note**
>
> Si tiene sitios de Active Directory definidos, debe asegurarse de que las subredes de la VPC asociadas a su sistema de archivos de FSx Amazon estén definidas en un sitio de Active Directory y de que no existan conflictos entre las subredes de su VPC y las subredes de sus otros sitios. Puede ver y cambiar esta configuración con el complemento MMC de sitios y servicios de Active Directory.

> **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.

10. Para Autenticación de Windows, elija Microsoft Active Directory autoadministrado.
11. Escriba un valor para Nombre de dominio completo para el directorio autoadministrado de Microsoft Active Directory.

> **Note**
>
> El nombre de dominio no debe tener el Formato de dominio de etiqueta única (SLD). FSx Actualmente, Amazon no admite dominios SLD.

> **Important**
>
> En los sistemas de archivos Single-AZ 2 y en todos los sistemas de archivos Multi-AZ, el nombre de dominio de Active Directory no puede superar los 47 caracteres.

12. Introduzca un valor para la unidad organizativa del directorio autoadministrado de Microsoft Active Directory.

> **Note**
>
> Asegúrese de que la cuenta de servicio que ha proporcionado tiene permisos delegados a la OU que especifique aquí o a la OU predeterminada si no especifica ninguno.

13. Introduzca al menos uno y no más de dos valores para Direcciones IP del servidor DNS del directorio autoadministrado de Microsoft Active Directory.
14. Introduzca un valor de cadena para Nombre de usuario de la cuenta de servicio de la cuenta de su dominio autoadministrado de Active Directory, por ejemplo `ServiceAcct`. Amazon FSx utiliza este nombre de usuario para unirse a su dominio de Microsoft Active Directory.

> **Important**
>
> NO incluya un prefijo de dominio (`corp.com\ServiceAcct`) o un sufijo de dominio (`ServiceAcct@corp.com`) al introducir el Nombre de usuario de la cuenta de servicio. NO utilice el nombre distintivo (DN) al introducir el Nombre de usuario de la cuenta de servicio (`CN=ServiceAcct,OU=example,DC=corp,DC=com`).

15. Introduzca un valor para Contraseña de la cuenta de servicio de la cuenta de su dominio autoadministrado de Active Directory. Amazon FSx usa esta contraseña para unirse a tu dominio de Microsoft Active Directory.
16. Vuelva a introducir la contraseña para confirmarla en Confirmar contraseña.
17. En el Grupo de administradores de sistemas de archivos delegados, especifique el grupo de `Domain Admins` o un grupo de administradores de sistemas de archivos delegados personalizado (si ha creado uno). El grupo que especifique debe tener la autoridad delegada para realizar tareas administrativas en el sistema de archivos. Si no proporcionas un valor, Amazon FSx utilizará el `Domain Admins` grupo Builtin. Ten en cuenta que Amazon FSx no admite tener un `Delegated file system administrators group` (ni el `Domain Admins` grupo ni el grupo personalizado que especifiques) que esté ubicado en el contenedor integrado.

> **Important**
>
> Si no proporciona un grupo de administradores de sistemas de archivos delegados, Amazon FSx intentará utilizar de forma predeterminada el `Domain Admins` grupo integrado en su dominio de Active Directory. Si se cambió el nombre de dicho grupo

integrado o si utiliza un grupo diferente para la administración del dominio, debe establecer ese nombre para el grupo aquí.

> **Important**
>
> NO incluya un prefijo de dominio (corp.com\ FSx Admins) ni un sufijo de dominio (FSxAdmins@corp.com) al proporcionar el parámetro de nombre de grupo.
> NO utilice el nombre distintivo (DN) para el grupo. Un ejemplo de nombre distintivo es CN= FSx Admins, OU=Example, DC=corp, DC=com.

Para crear un sistema de archivos de servidor de archivos FSx para Windows unido a un Active Directory autoadministrado ()AWS CLI

En el siguiente ejemplo, se crea un sistema de archivos de servidor de archivos FSx para Windows con un sistema `SelfManagedActiveDirectoryConfiguration` en la zona de `us-east-2` disponibilidad.

```
aws fsx --region us-east-2 \
create-file-system \
--file-system-type WINDOWS \
--storage-capacity 300 \
--security-group-ids security-group-id \
--subnet-ids subnet-id\
--windows-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",FileSystemAdmini
 \
UserName="FSxService",Password="password", \
   DnsIps=["10.0.1.18"]}',ThroughputCapacity=8
```

> **Important**
>
> No muevas los objetos de ordenador que Amazon FSx cree en la unidad organizativa una vez creado el sistema de archivos. Si lo hace, el sistema de archivos no se configurará de manera correcta.

Obtención de las direcciones IP del sistema de archivos correctas para usarlas en las entradas manuales del DNS

Amazon FSx solo registra los registros DNS de un sistema de archivos si utilizas el DNS de Microsoft como servicio de DNS predeterminado. Si utilizas un DNS de terceros, tendrás que configurar manualmente las entradas de DNS para tus sistemas de FSx archivos de Amazon. En esta sección, se describe cómo obtener las direcciones IP del sistema de archivos correctas para utilizarlas si tiene que añadir el sistema de archivos al DNS de forma manual. Tenga en cuenta que, una vez creado un sistema de archivos, las direcciones IP no cambian hasta que se elimina el sistema de archivos.

Cómo obtener las direcciones IP del sistema de archivos para usarlas en las entradas A del DNS

1. En el https://console.aws.amazon.com/fsx/, elige el sistema de archivos del que deseas obtener la dirección IP para que aparezca la página de detalles del sistema de archivos.
2. En la pestaña Red y seguridad, realice una de las siguientes acciones:

   - Para los sistemas de archivos Single-AZ 1:
     - En el panel de subred, elija la interfaz de red elástica que se muestra en Interfaz de red para abrir la página Interfaces de red en la EC2 consola de Amazon.
     - La dirección IP que debe utilizar el sistema de archivos Single-AZ 1 se muestra en la columna IPv4 IP privada principal.
   - Para los sistemas de archivos Single-AZ 2 o Multi-AZ:
     - En el panel Subred preferida, elija la interfaz de red elástica que se muestra en Interfaz de red para abrir la página Interfaces de red en la EC2 consola de Amazon.
     - La dirección IP de la subred preferida a utilizar se muestra en la columna IPv4 IP privada secundaria.
     - En el panel de subred Amazon FSx Standby, elija la interfaz de red elástica que se muestra en Interfaz de red para abrir la página Interfaces de red en la EC2 consola de Amazon.
     - La dirección IP que debe utilizar la subred en espera se muestra en la columna IPv4 IP privada secundaria.

> **Note**
>
> Si necesita configurar entradas de DNS para su PowerShell terminal remoto de Windows para sistemas de archivos Single-AZ 2 o Multi-AZ, debe usar la IPv4 dirección privada

principal para la interfaz de red elástica de su subred preferida. Para obtener más información, consulte Uso de Amazon FSx CLI para PowerShell.

Actualización de la configuración de un Active Directory autoadministrado

Para garantizar la disponibilidad continua e ininterrumpida de su sistema de FSx archivos de Amazon, debe actualizar la configuración de Active Directory del sistema de archivos cuando cambie alguna de las siguientes propiedades de Active Directory:

- Las direcciones IP del servidor del DNS
- Las credenciales de la cuenta de servicio del Active Directory autoadministrado

Al actualizar la configuración autogestionada de Active Directory para el sistema de FSx archivos de Amazon, el estado del sistema de archivos cambia de Disponible a Actualizado mientras se aplica la actualización. Compruebe que el estado vuelva a ser Disponible después de aplicar la actualización. Tenga en cuenta que la actualización puede tardar varios minutos en completarse. Para obtener más información, consulte Supervisión de las actualizaciones del Active Directory autoadministrado.

Si hay algún problema con la configuración actualizada del Active Directory autoadministrado, el estado del sistema de archivos cambia a Desconfigurado. Este estado muestra un mensaje de error y una acción correctiva recomendada junto a la descripción del sistema de archivos en la consola, la API y la CLI. Tras tomar las medidas correctivas recomendadas, compruebe que el estado del sistema de archivos cambie finalmente a Disponible.

> **Important**
>
> Si actualiza el sistema de archivos con una cuenta de servicio nueva, asegúrese de que la nueva tenga permisos de Control total sobre los objetos informáticos existentes asociados al sistema de archivos.

Para obtener información sobre cómo solucionar posibles problemas relacionados con las configuraciones del Active Directory autoadministrado, consulte El sistema de archivos está mal configurado.

Puede utilizar la AWS Management Console FSx API de Amazon o AWS CLI actualizar el nombre de usuario y la contraseña de la cuenta de servicio y las direcciones IP del servidor DNS de la

configuración autogestionada de Active Directory de un sistema de archivos. Puede realizar un seguimiento del progreso de una actualización de configuración de Active Directory autoadministrada en cualquier momento mediante la AWS Management Console CLI y la API. Para obtener más información, consulte Supervisión de las actualizaciones del Active Directory autoadministrado.

Cómo actualizar la configuración de Active Directory autoadministrado (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 de Windows para el que desee actualizar la configuración del Active Directory autoadministrado.
3. En la pestaña Red y seguridad, seleccione Actualizar para las direcciones IP del servidor del DNS, o para el nombre de usuario de la cuenta de servicio, según las propiedades del Active Directory que vaya a actualizar.
4. Escriba las nuevas direcciones IP del servidor DNS o las nuevas credenciales de la cuenta de servicio en el cuadro de diálogo que aparece.
5. Seleccione Actualizar para iniciar la actualización de la configuración del Active Directory.

   Puede supervisar el progreso de la actualización mediante el AWS Management Console o el AWS CLI.

Cómo actualizar la configuración del Active Directory autoadministrado (CLI)

- Para actualizar la configuración autogestionada de Active Directory de un sistema de archivos FSx para Windows File Server, utilice el AWS CLI comando update-file-system. Establezca los siguientes parámetros:
  - `--file-system-id` en el ID del sistema de archivos que va a actualizar.
  - `UserName` el nuevo nombre de usuario de la cuenta de servicio del Active Directory autoadministrado.
  - `Password` la nueva contraseña de la cuenta de servicio del Active Directory autoadministrado.
  - `DnsIps` las direcciones IP de los servidores de DNS del Active Directory autoadministrado.

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 \
  --windows-configuration
 'SelfManagedActiveDirectoryConfiguration={UserName=username,Password=password,\
    DnsIps=[192.0.2.0,192.0.2.24]}'
```

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200. El objeto `AdminstrativeActions` de la respuesta describe la solicitud y el estado.

Cambiar la cuenta de FSx servicio de Amazon

Si actualiza el sistema de archivos con una cuenta de servicio nueva, esta debe tener los permisos y privilegios requeridos para unirse al Active Directory y tiene permisos de control total sobre los objetos de equipos existentes asociados al sistema de archivos. Además, corrobore que la nueva cuenta de servicio forme parte de las cuentas de veracidad con la configuración de política de grupo habilitada como controlador de dominio: permitir la reutilización de las cuentas de equipo mientras se une a un dominio.

Recomendamos encarecidamente que use un grupo de Active Directory para administrar los permisos y las configuraciones del Active Directory asociados a la cuenta de servicio.

Al cambiar la cuenta de servicio de Amazon FSx, asegúrate de que las cuentas de servicio tengan la siguiente configuración:

- La nueva cuenta de servicio (o el grupo de Active Directory al cual pertenece) tiene permisos de control total sobre los objetos de equipo existentes asociados al sistema de archivos.
- Las cuentas de servicio nuevas y anteriores (o el grupo de Active Directory al que pertenecen) forman parte de las cuentas de veracidad (o del grupo de Active Directory de veracidad) con la configuración de políticas del grupo controlador de dominio: permitir la reutilización de las cuentas de equipo mientras se une a un dominio habilitada en todos los controladores de dominio del Active Directory.

Si las cuentas de servicio no cumplen estos requisitos, pueden darse las siguientes condiciones:

- En el caso de los sistemas de archivos Single-AZ, el sistema de archivos podría convertirse en MISCONFIGURED_UNAVAILABLE.
- En el caso de los sistemas de archivos Multi-AZ, es posible que el sistema de archivos esté MAL CONFIGURADO y que el nombre del RemotePowerShell terminal cambie.

Configuración de la política de grupo de un controlador de dominio

El siguiente procedimiento recomendado por Microsoft describe cómo usar la política de grupo del controlador de dominio para configurar la política de listas de permitidos.

Para configurar la política de listas de permitidos de un controlador de dominio

1. Instale las actualizaciones de Microsoft Windows del 12 de septiembre de 2023 o posteriores en todos los equipos miembros y controladores de dominio del Microsoft Active Directory autoadministrado.
2. En una política de grupo nueva o existente que se aplique a todos los controladores de dominio del Active Directory autoadministrado, configure los siguientes ajustes.

   a. Diríjase a Configuración de equipo > Políticas > Configuraciones de Windows > Configuraciones de seguridad > Políticas locales > Opciones de seguridad.

   b. Haga doble clic en Controlador de dominio: permitir la reutilización de la cuenta de equipo mientras se une al dominio.

   c. Seleccione Definir esta configuración de política y <Editar seguridad…>.

   d. Use el selector de objetos para agregar usuarios o grupos de creadores y propietarios de cuentas de equipo de veracidad al permiso Permitir. (Recomendamos encarecidamente la práctica de usar grupos para obtener permisos). No agregue la cuenta de usuario que realiza la unión al dominio.

   > **Warning**
   >
   > Limite la pertenencia a la política para los usuarios y cuentas de servicio de veracidad. No agregue a esta política usuarios autenticados, a otras personas ni a otros grupos grandes. En su lugar, agregue cuentas de servicio y usuarios de veracidad específicos a los grupos y agregue esos grupos a la política.

3. Espere a que se actualice la política de grupo o ejecute gpupdate /force en todos los controladores de dominio.
4. Compruebe que la clave de registro HKLM\ System\ CCS\ Control\ SAM — «ComputerAccountReuseAllowList» esté rellenada con el SDDL deseado. No modifique el registro manualmente.
5. Intente unirse a un equipo que tenga instaladas las actualizaciones del 12 de septiembre de 2023 o posteriores. Corrobore que una de las cuentas que figuran en la política sea

propietaria de la cuenta de equipo. Asegúrese también de que su registro no tenga la NetJoinLegacyAccountReuseclave habilitada (establecida en 1). Si se produce un error al unir dominios, revise **`c:\windows\debug\netsetup.log`**.

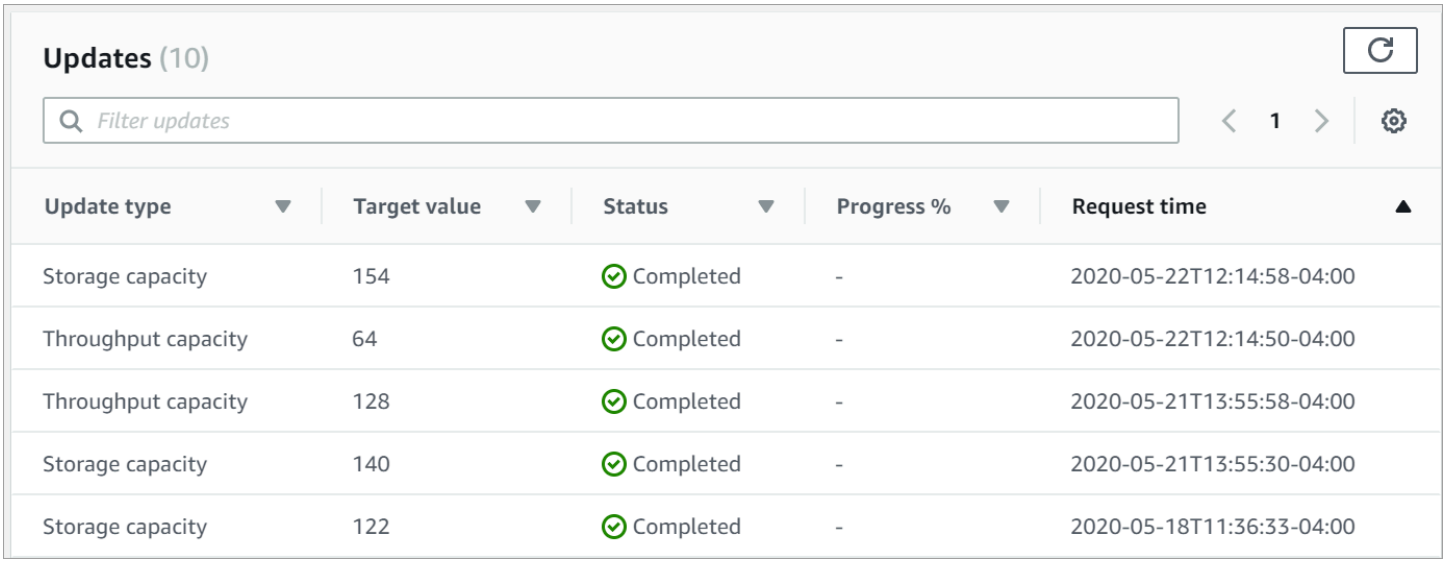
Supervisión de las actualizaciones del Active Directory autoadministrado

Puede supervisar el progreso de una actualización de configuración de Active Directory autogestionada mediante la API o la AWS Management Console AWS CLI, tal y como se describe en los siguientes procedimientos.

Al actualizar la configuración del Active Directory autoadministrado del sistema de archivos, el estado del sistema de archivos cambia de Disponible a Actualizando mientras se aplica la actualización. Una vez completada la actualización, el estado vuelve a ser Disponible. La actualización de una configuración del Active Directory puede tardar varios minutos en completarse.

Supervisión de las actualizaciones en la consola

En la pestaña Actualizaciones de la ventana de información del sistema de archivos, puede ver las 10 actualizaciones más recientes de cada tipo.



Para las actualizaciones del Active Directory autoadministrado, puede ver la siguiente información.

Tipo de actualización

Los tipos admitidos son los siguientes:

- Dirección IP del servidor DNS

- Las Credenciales de cuenta de servicio

Valor de destino

El valor deseado al que se debe actualizar la propiedad del sistema de archivos. En el caso de las actualizaciones de las credenciales de la cuenta de servicio, solo se muestra el nombre de usuario, y nunca se incluyen las contraseñas de las cuentas de servicio en este campo.

Estado

El estado de la actualización vigente. En el caso de las actualizaciones del Active Directory autoadministrado, 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 del sistema de archivos se completó correctamente.
- Error: no se pudo actualizar el sistema de archivos. Elija el signo de interrogación (?) para ver información sobre el error.

% de progreso

El progreso de la actualización del sistema de archivos se muestra como porcentaje completado.

Tiempo de solicitud

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

Supervisar las actualizaciones mediante la API AWS CLI y

Puede ver y supervisar las solicitudes de actualización del sistema de archivos que están en curso mediante el describe-file-systems AWS CLI comando y la acción de la DescribeFileSystemsAPI. La matriz de `AdministrativeActions` enumera las 10 acciones de actualización más recientes para cada tipo de acción administrativa.

El siguiente ejemplo muestra un extracto de la respuesta de un comando de la CLI describe-file-systems que muestra dos actualizaciones del sistema de archivos del Active Directory autoadministrado.

```
        {
            "OwnerId": "111122223333",
```

```
            .
            .
            .
            "StorageCapacity": 1000,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "RequestTime": 1581694766.757,
                    "Status": "PENDING",
                    "TargetFileSystemValues": {
                        "WindowsConfiguration": {
                            "SelfManagedActiveDirectoryConfiguration": {
                                "UserName": "serviceUser",
                            }
                        }
                    }
                },
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "RequestTime": 1619032957.759,
                    "Status": "FAILED",
                    "TargetFileSystemValues": {
                        "WindowsConfiguration": {
                            "SelfManagedActiveDirectoryConfiguration": {
                            "DnsIps": [
                                    "10.0.138.161"
                                ]
                            }
                        }
                    },
                    "FailureDetails": {
                        "Message": "Failure details message."
                    }
                }
            ],
        .
        .
        .
```

FSx para el rendimiento del servidor de archivos de Windows

FSx para Windows File Server ofrece opciones de configuración del sistema de archivos para satisfacer una variedad de necesidades de rendimiento. A continuación se presenta una descripción general del rendimiento del sistema de FSx archivos de Amazon, con un análisis de las opciones de configuración de rendimiento disponibles y consejos de rendimiento útiles.

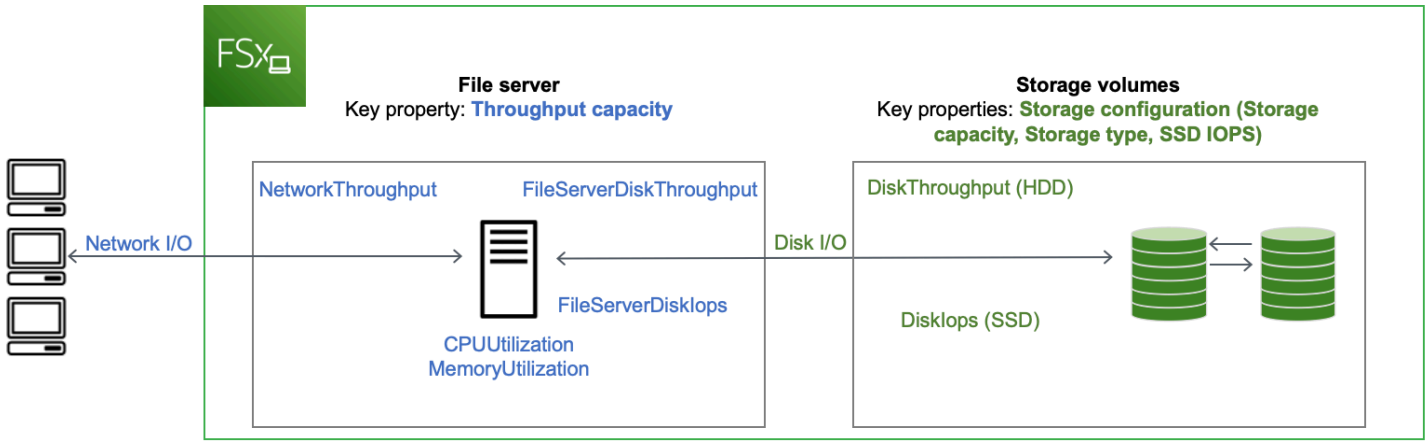
Temas

- El rendimiento del sistema de archivos
- Consideraciones relativas al rendimiento adicional
- Impacto de la capacidad de rendimiento en el rendimiento
- Elegir el nivel correcto de capacidad de rendimiento
- Impacto de la configuración del almacenamiento en el rendimiento
- Ejemplo: capacidad de almacenamiento y capacidad de rendimiento
- Medir el rendimiento mediante métricas CloudWatch
- Solución de problemas de rendimiento del sistema de archivos

El rendimiento del sistema de archivos

Cada sistema FSx de archivos del servidor de archivos de Windows consta de un servidor de archivos de Windows con el que se comunican los clientes y de un conjunto de volúmenes de almacenamiento, o discos, conectados al servidor de archivos. Cada servidor de archivos emplea un caché en memoria rápido para mejorar el rendimiento de los datos a los que se accede con más frecuencia.

El siguiente diagrama ilustra cómo se accede a los datos desde un sistema FSx de archivos del servidor de archivos de Windows.



Cuando un cliente accede a los datos almacenados en la caché en memoria, los datos se envían directamente al cliente solicitante como E/S de red. El servidor de archivos no necesita leerlos ni escribirlos en el disco. El rendimiento de este acceso a los datos viene determinado por los límites de E/S de la red y el tamaño de la caché en memoria.

Cuando un cliente accede a datos que no están en la memoria caché, el servidor de archivos los lee o los escribe en el disco como E/S del disco. A continuación, los datos se envían desde el servidor de archivos al cliente como E/S de red. El rendimiento de este acceso a los datos viene determinado por los límites de E/S de la red y los límites de E/S del disco.

El rendimiento de las E/S de la red y la caché en memoria del servidor de archivos vienen determinados por la capacidad de rendimiento del sistema de archivos. El rendimiento de E/S del disco se determina mediante una combinación de capacidad de rendimiento y configuración de almacenamiento. El rendimiento máximo de E/S del disco, que consiste en el rendimiento del disco y los niveles de IOPS del disco, que puede alcanzar el sistema de archivos es el menor de los siguientes:

- El nivel de rendimiento de E/S de disco que proporciona el servidor de archivos, en función de la capacidad de rendimiento que seleccione para el sistema de archivos.
- El nivel de rendimiento de E/S del disco proporcionado por su configuración de almacenamiento (la capacidad de almacenamiento, el tipo de almacenamiento y el nivel de IOPS de SSD que seleccione para su sistema de archivos).

Consideraciones relativas al rendimiento adicional

Por lo general, el rendimiento del sistema de archivos se mide por la latencia, el rendimiento y las operaciones de E/S por segundo (IOPS).

Latencia

FSx para Windows File Server, los servidores de archivos utilizan una caché rápida en memoria para lograr latencias consistentes de menos de un milisegundo para los datos a los que se accede activamente. Para los datos que no están en la caché en memoria, es decir, para las operaciones de archivos que deben gestionarse realizando E/S en los volúmenes de almacenamiento subyacentes, Amazon FSx proporciona latencias de operaciones de archivos de menos de milisegundos con almacenamiento en unidades de estado sólido (SSD) y latencias de milisegundos de un solo dígito con almacenamiento en unidades de disco duro (HDD).

Rendimiento e IOPS

Los sistemas de FSx archivos de Amazon proporcionan entre 2 GBps y 80 000 IOPS en todos los lugares donde Regiones de AWS Amazon FSx esté disponible, y 12 GBps de rendimiento y 400 000 IOPS en EE. UU. Este (Virginia del Norte), EE. UU. Oeste (Oregón), EE. UU. Este (Ohio), Europa (Irlanda), Asia Pacífico (Tokio) y Asia Pacífico (Singapur). La cantidad específica de rendimiento e IOPS que la carga de trabajo puede generar en el sistema de archivos depende de la capacidad de rendimiento, la capacidad de almacenamiento y el tipo de almacenamiento del sistema de archivos, junto con la naturaleza de la carga de trabajo, incluido el tamaño del conjunto de trabajo activo.

Rendimiento para un solo cliente

Con Amazon FSx, puede obtener todos los niveles de rendimiento e IOPS de su sistema de archivos desde un único cliente que accede a él. Amazon FSx admite la tecnología multicanal para pequeñas y medianas empresas. Esta función le permite ofrecer un GBps rendimiento múltiple y cientos de miles de IOPS para que un solo cliente acceda a su sistema de archivos. 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. Aunque hay un límite teórico para el número de conexiones SMB compatibles con Windows, este límite es de millones y prácticamente se puede tener un número ilimitado de conexiones SMB.

Rendimiento por ráfagas

Las cargas de trabajo basadas en archivos suelen tener picos de actividad. Estos picos se caracterizan por tener intervalos cortos e intensos de gran cantidad de E/S y varios intervalos de inactividad entre cada ráfaga. Para soportar cargas de trabajo con picos de actividad, además de las velocidades básicas que un sistema de archivos puede soportar las 24 horas del día, los 7 días de la semana, Amazon FSx ofrece la capacidad de alcanzar velocidades más altas durante períodos de tiempo tanto para las operaciones de E/S de red como de E/S de disco. Amazon FSx utiliza un mecanismo de créditos de E/S para asignar el rendimiento y las IOPS en función de la utilización media: los sistemas de archivos acumulan créditos cuando su rendimiento y su uso de IOPS están por debajo de sus límites de referencia, y pueden utilizar estos créditos cuando realizan operaciones de E/S.

Impacto de la capacidad de rendimiento en el rendimiento

La capacidad de rendimiento determina el rendimiento del sistema de archivos en las siguientes categorías:

- E/S de red: velocidad a la que el servidor de archivos puede entregar los datos de los archivos a los clientes que acceden a él.
- CPU y memoria del servidor de archivos: recursos disponibles para almacenar datos de archivos y realizar actividades en segundo plano, como la deduplicación de datos y la creación de copias de redundancia.
- E/S de disco: velocidad a la que el servidor de archivos admite la E/S entre el servidor de archivos y los volúmenes de almacenamiento.

En las tablas siguientes se proporcionan detalles sobre los niveles máximos de E/S de red (rendimiento e IOPS) y E/S de disco (rendimiento e IOPS) que se pueden gestionar con cada configuración de capacidad de rendimiento aprovisionada, y la cantidad de memoria disponible para almacenar en caché y respaldar actividades en segundo plano, como la deduplicación de datos y las copias de redundancia. Si bien puede seleccionar niveles de capacidad de rendimiento inferiores a 32 megabytes por segundo (MBps) cuando utiliza la API FSx o la CLI de Amazon, tenga en cuenta que estos niveles están pensados para cargas de trabajo de prueba y desarrollo, no para cargas de trabajo de producción.

> **Note**
>
> Tenga en cuenta que los niveles de capacidad de rendimiento de 4608 MBps o más solo se admiten en las siguientes regiones: EE.UU. Este (Norte de Virginia), EE.UU. Oeste (Oregón), EE.UU. Este (Ohio), Europa (Irlanda), Asia Pacífico (Tokio) y Asia Pacífico (Singapur).

E/S de red y memoria

FSx capacidad de rendimiento () MBps	Rendimiento de la red () MBps		IOPS de red	Memoria (GB)
	Referencia	Ráfaga (durante unos minutos al día)		
32	32	600	Miles	4
64	64	600	Decenas de miles	8
128	150	1250		8
256	300	1250	Cientos de miles	16
512	600	1250		32
1 024	1500	–		72
2048	3.125	–		144
4.608	9.375	–	Millones	192
6144	12.500	–		256
9216	18 750	–		384
12.288	21.250	–		512

E/S de disco

FSx capacidad de rendimiento () MBps	Rendimiento del disco () MBps		IOPS de disco	
	Referencia	Ráfaga (durante 30 minutos al día)	Referencia	Ráfaga (durante 30 minutos al día)
32	32	260	2K	12 K
64	64	350	4K	16 K
128	128	600	6 K	20 MIL
256	256	600	10,000	20 K
512	512	–	20 K	–
1 024	1 024	–	40 000	–
2048	2048	–	80 K	–
4.608	4.608	–	150 MIL	–
6144	6144	–	200,000	–
9216	9.216 [1]	–	300 K [1]	–
12.288	12.288 [1]	–	400 K [1]	–

> **Note**
>
> [1] Si tiene un sistema de archivos Multi-AZ con una capacidad de procesamiento de 9 216 o 12 288 MBps, el rendimiento se limitará a 9 000 MBps y 262 500 IOPS únicamente para el tráfico de escritura. De lo contrario, para el tráfico de lectura en todos los sistemas de archivos Multi-AZ, el tráfico de lectura y escritura en todos los sistemas de archivos Single-

AZ y todos los demás niveles de capacidad de rendimiento, su sistema de archivos admitirá los límites de rendimiento que se muestran en la tabla.

Elegir el nivel correcto de capacidad de rendimiento

Cuando crea un sistema de archivos mediante la consola de administración de Amazon Web Services, Amazon selecciona FSx automáticamente el nivel de capacidad de rendimiento recomendado para su sistema de archivos en función de la cantidad de capacidad de almacenamiento que configure. Si bien la capacidad de rendimiento recomendada debería ser suficiente para la mayoría de las cargas de trabajo, tiene la opción de anular la recomendación y configurar una cantidad específica de capacidad de rendimiento para satisfacer las necesidades de su carga de trabajo. Por ejemplo, si su carga de trabajo requiere dirigir el 1% GBps del tráfico al sistema de archivos, debe seleccionar una capacidad de rendimiento de al menos 1024. MBps La siguiente tabla proporciona el nivel de capacidad de rendimiento mínimo recomendado para un sistema de archivos en función de la cantidad de capacidad de almacenamiento aprovisionada.

Capacidad de almacenamiento SSD (GiB)	Capacidad de almacenamiento en disco duro (GiB)	Capacidad de rendimiento mínima recomendada () MBps
Hasta 640	Hasta 3.200	32
641—1280	3201—6.400	64
1281—2.560	6.401-12.800	128
2.561—5.120	12.801 — 25.600	256
5.121 — 10.240	25.601 — 51.200	512
10.241 a 20.480	> 51.200	1 024
> 20.480	N/D	2048

También debe tener en cuenta las características que planea habilitar en su sistema de archivos al decidir el nivel de rendimiento que desea configurar. Por ejemplo, la activación de copias de redundancia puede requerir que aumente su capacidad de rendimiento hasta un nivel hasta tres veces superior a la carga de trabajo prevista para garantizar que el servidor de archivos pueda

mantener las copias de redundancia con la capacidad de rendimiento de E/S disponible. Si habilita la deduplicación de datos, debe determinar la cantidad de memoria asociada a la capacidad de rendimiento del sistema de archivos y asegurarse de que esta cantidad de memoria es suficiente para el tamaño de los datos.

Puede aumentar o reducir la cantidad de capacidad de rendimiento en cualquier momento después de crearla. Para obtener más información, consulte Administración de la capacidad de rendimiento.

Puedes monitorizar el uso de los recursos de rendimiento del servidor de archivos por parte de tu carga de trabajo y obtener recomendaciones sobre qué capacidad de rendimiento seleccionar consultando la pestaña Monitoring & performance > Performance de tu FSx consola Amazon. Recomendamos realizar las pruebas en un entorno de preproducción para garantizar que la configuración que ha seleccionado cumpla con los requisitos de rendimiento de su carga de trabajo. En el caso de los sistemas de archivos Multi-AZ, también recomendamos probar el impacto del proceso de conmutación por error que se produce durante el mantenimiento del sistema de archivos, los cambios en la capacidad de rendimiento y la interrupción imprevista del servicio en la carga de trabajo, así como asegurarse de que se ha aprovisionado una capacidad de rendimiento suficiente para evitar que el rendimiento se vea afectado durante estos eventos. Para obtener más información, consulte Acceso a métricas del sistema de archivos.

Impacto de la configuración del almacenamiento en el rendimiento

La capacidad de almacenamiento, el tipo de almacenamiento y el nivel de IOPS de la SSD del sistema de archivos afectan al rendimiento de E/S del disco del sistema de archivos. Puede configurar estos recursos para ofrecer los niveles de rendimiento deseados para su carga de trabajo.

Puede aumentar la capacidad de almacenamiento y escalar las IOPS de las SSD en cualquier momento. Para obtener más información, consulte Administrar la capacidad de almacenamiento y Cómo administrar IOPS de SSD. También puede actualizar su sistema de archivos del tipo de almacenamiento HDD al tipo de almacenamiento SSD. Para obtener más información, consulte Administrar el tipo de almacenamiento del sistema de archivos.

El sistema de archivos proporciona los siguientes niveles predeterminados de rendimiento de disco e IOPS:

Tipo de almacenamiento	Rendimiento de disco (MBps por TiB de almacenamiento)	IOPS de disco (por TiB de almacenamiento)
SSD	750	3000 1
HDD	12 puntos de referencia; 80 ráfagas (hasta un máximo de 1 GBps por sistema de archivos)	12 de referencia; 80 de ráfaga

> **Note**
>
> [1]En el caso de los sistemas de archivos con almacenamiento en SSD, puede aprovisionar IOPS adicionales hasta una proporción máxima de 500 IOPS por GiB de almacenamiento y 400 000 IOPS por sistema de archivos.

Rendimiento por ráfagas de HDD

Para los volúmenes de almacenamiento en disco duro, Amazon FSx utiliza un modelo de cubos en ráfaga para mejorar el rendimiento. El tamaño del volumen determina el rendimiento de referencia del volumen, que es la velocidad a la que el volumen acumula créditos de rendimiento. El tamaño del volumen también determina el rendimiento de ráfaga del volumen, que es la velocidad a la que puede utilizar los créditos disponibles. Los volúmenes grandes presentan un rendimiento de referencia y de ráfaga superior. Cuantos más créditos tiene el volumen, más tiempo puede realizar E/S en el nivel de ráfaga.

El rendimiento disponible del volumen de almacenamiento de un HDD se expresa mediante la siguiente fórmula:

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

Para un volumen de disco duro de 1 TiB, el rendimiento de ráfaga está limitado a 80 MiBps, el depósito se llena de créditos a 12 MiBps y puede almacenar hasta 1 TiB de créditos.

Los volúmenes de almacenamiento en HDD pueden tener variaciones de rendimiento significativas en función de la carga de trabajo. Los picos repentinos de IOPS o del rendimiento pueden provocar

una degradación del rendimiento del disco. La métrica `DiskThroughputBalance` proporciona información sobre el saldo de créditos de expansión tanto para el rendimiento como para la utilización de las IOPS del disco. Por ejemplo, si la carga de trabajo supera los límites de referencia de IOPS en HDD (12 IOPS por TiB de almacenamiento), la utilización de las IOPS del disco (HDD) superará el 100 % y provocará el agotamiento del saldo de créditos de expansión, como puede ver en la métrica `DiskThroughputBalance`. Para que la carga de trabajo siga generando altos niveles de E/S, es posible que deba realizar una de las siguientes acciones:

- Reduzca las exigencias de E/S de la carga de trabajo para reponer el saldo de créditos de expansión.
- Aumente la capacidad de almacenamiento del sistema de archivos para proporcionar un nivel de referencia más alto de IOPS del disco.
- Actualice el sistema de archivos para que use el almacenamiento en SSD, que proporciona un nivel de referencia de IOPS del disco más alto para adaptarse mejor a los requisitos de la carga de trabajo.

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 que está configurado con 2 TiB de capacidad de almacenamiento en disco duro y 32 MBps de capacidad de rendimiento tiene los siguientes niveles de rendimiento:

- Rendimiento de red: 32 de MBps referencia y 600 de MBps ráfaga (consulte la tabla de capacidad de rendimiento)
- Rendimiento de disco: 24 de MBps referencia y 160 MBps ráfagas, que es el menor de los siguientes valores:
  - los niveles de rendimiento del disco de 32 bits de MBps referencia y 260 MBps ráfagas admitidos por el servidor de archivos, en función de la capacidad de rendimiento del sistema de archivos
  - los niveles de rendimiento del disco de 24 niveles de MBps referencia (12 MBps por TB * 2 TiB) y MBps 160 ráfagas (80 MBps por TiB * 2 TiB) compatibles con los volúmenes de almacenamiento, según el tipo y la capacidad de almacenamiento

Por lo tanto, su carga de trabajo al acceder al sistema de archivos podrá generar un rendimiento de hasta 32 MBps ráfagas de MBps referencia y 600 ráfagas para las operaciones de archivo realizadas con datos a los que se accede activamente almacenados en caché en la memoria caché del servidor de archivos, y hasta 24 de MBps referencia y 160 MBps ráfagas para las operaciones de archivos que deben ir hasta el disco, por ejemplo, debido a una pérdida de caché.

Medir el rendimiento mediante métricas CloudWatch

Puedes usar Amazon CloudWatch para medir y monitorear el rendimiento y las IOPS de tu sistema de archivos. Para obtener más información, consulte Monitorización con Amazon CloudWatch.

Solución de problemas de rendimiento del sistema de archivos

El rendimiento del sistema de archivos FSx del servidor de archivos de Windows depende de varios factores, como el tráfico que dirija al sistema de archivos, la forma en que lo aprovisione y los recursos que consuman las funciones que están habilitadas, como la deduplicación de datos o las instantáneas. Para obtener información sobre cómo entender el rendimiento del sistema de archivos, consulte FSx para el rendimiento del servidor de archivos de Windows.

Temas

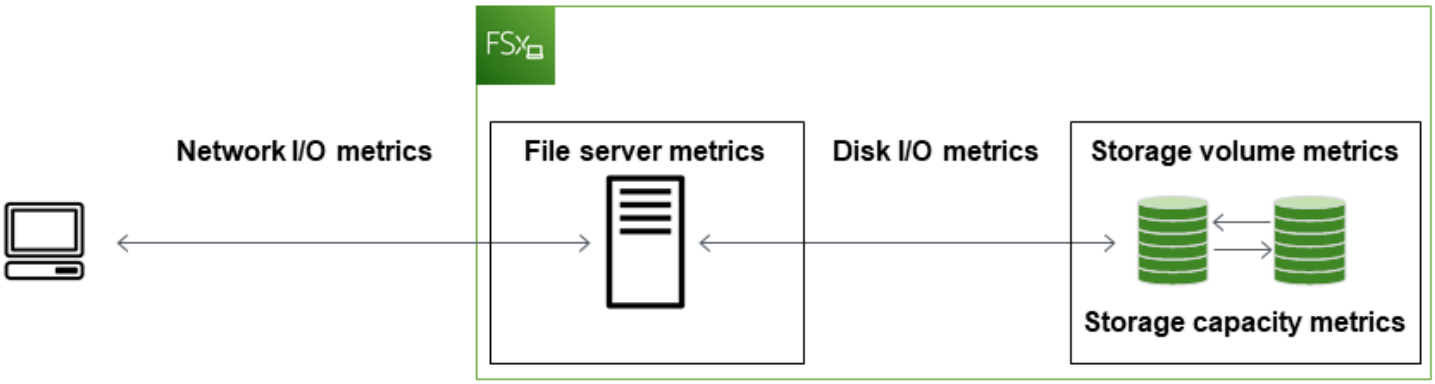
- ¿Cómo determino el rendimiento y los límites de IOPS de mi sistema de archivos?
- ¿Cuál es la diferencia entre las E/S de red y las de disco? ¿Por qué la E/S de red es diferente de la de disco?
- ¿Por qué el uso de la CPU o la memoria es alto, incluso cuando la E/S de la red es baja?
- ¿Qué son las ráfagas? ¿Cuántas ráfagas utiliza el sistema de archivos? ¿Qué ocurre cuando se agotan los créditos de ráfaga?
- Veo una advertencia en la página de Supervisión y rendimiento: ¿debo cambiar la configuración del sistema de archivos?
- No pude ver las métricas por un momento, ¿debo preocuparme?

¿Cómo determino el rendimiento y los límites de IOPS de mi sistema de archivos?

Para ver el rendimiento y los límites de IOPS de un sistema de archivos, consulte la tabla con los niveles de rendimiento según la cantidad de capacidad de rendimiento de aprovisionamiento.

¿Cuál es la diferencia entre las E/S de red y las de disco? ¿Por qué la E/S de red es diferente de la de disco?

Los sistemas de FSx archivos de Amazon incluyen uno o más servidores de archivos que proporcionan datos a través de la red a los clientes que acceden al sistema de archivos. Se trata de la E/S de la red. El servidor de archivos tiene una caché en memoria rápida para mejorar el rendimiento de los datos a los que se accede con mayor frecuencia. Los servidores de archivos también dirigen el tráfico a los volúmenes de almacenamiento que alojan los datos del sistema. Se trata de la E/S del disco. El siguiente diagrama ilustra la E/S de red y disco de un sistema de FSx archivos de Amazon.



Para obtener más información, consulte Monitorización con Amazon CloudWatch.

¿Por qué el uso de la CPU o la memoria es alto, incluso cuando la E/S de la red es baja?

El uso de la CPU y la memoria del servidor de archivos no solo depende del tráfico de red que tenga, sino también de las características que haya habilitado en el sistema de archivos. La forma en que configure y programe dichas características puede afectar al uso de la CPU y la memoria.

Las tareas de Desduplicación de datos en curso pueden consumir memoria. Puede modificar la configuración de las tareas de desduplicación para reducir los requisitos de memoria. Por ejemplo, puede restringir la optimización para que se solo ejecute en tipos de archivos o carpetas específicos, o puede establecer un mínimo para el tamaño y la antigüedad de los archivos que se van a optimizar. También, recomendamos establecer una configuración para que las tareas de desduplicación se ejecuten durante los períodos de inactividad, cuando la carga del sistema de archivos sea mínima. Para obtener más información, consulte Reducir los costos de almacenamiento con la dedduplicación de datos.

Si tiene habilitada la enumeración basada en el acceso, es posible que el uso de la CPU sea elevado cuando los usuarios finales consulten o enumeren recursos compartidos de archivos, o durante la fase de optimización de una tarea de escalado del almacenamiento. Para obtener más información, consulte Habilitar la enumeración basada en el acceso en un espacio de nombres en la Documentación de Microsoft Storage.

¿Qué son las ráfagas? ¿Cuántas ráfagas utiliza el sistema de archivos? ¿Qué ocurre cuando se agotan los créditos de ráfaga?

Las cargas de trabajo basadas en archivos suelen tener picos de actividad. Estos picos se caracterizan por tener intervalos cortos e intensos de gran cantidad de E/S e intervalos de inactividad entre cada ráfaga. Para soportar este tipo de cargas de trabajo, además de las velocidades básicas que puede soportar un sistema de archivos, Amazon FSx ofrece la capacidad de alcanzar velocidades más altas durante períodos de tiempo tanto para las operaciones de E/S de red como de E/S de disco.

Amazon FSx utiliza un mecanismo de créditos de E/S 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 para superar los límites de referencia (hasta los límites de ráfaga) cuando sea necesario. Para obtener más información sobre los límites y la duración de las ráfagas del sistema de archivos, consulte FSx para el rendimiento del servidor de archivos de Windows.

Veo una advertencia en la página de Supervisión y rendimiento: ¿debo cambiar la configuración del sistema de archivos?

La página Supervisión y rendimiento incluye advertencias que indican cuándo las demandas recientes de la carga de trabajo se acercaron o excedieron los límites de los recursos determinados según la configuración que haya establecido en el sistema de archivos. Esto no significa estrictamente que tenga que cambiar la configuración. Sin embargo, es posible que el sistema de archivos no esté lo suficientemente aprovisionado para la carga de trabajo, si no toma las medidas recomendadas.

Si la carga de trabajo que provocó la advertencia era atípica, y no espera que se prolongue, lo más seguro es no hacer nada, y supervisar de cerca el uso en el futuro. Sin embargo, si la carga de trabajo que provocó la advertencia es normal, y espera que continúe o incluso se intensifique, le recomendamos que tome las medidas recomendadas para aumentar el rendimiento del servidor de archivos (al aumentar la capacidad de rendimiento) o para aumentar el rendimiento del volumen de

almacenamiento (al aumentar la capacidad de almacenamiento o pasar de un almacenamiento en disco duro a uno en SSD).

> **Note**
>
> Algunos eventos del sistema de archivos pueden consumir los recursos de rendimiento de E/S del disco y, es posible que activen advertencias de rendimiento. Por ejemplo:
>
> - La fase de optimización del escalado de la capacidad de almacenamiento puede generar un aumento del rendimiento del disco, como se describe en Los aumentos de capacidad de almacenamiento y el rendimiento del sistema de archivos
> - En el caso de los sistemas de archivos Multi-AZ, los eventos como el escalado de la capacidad de rendimiento, la sustitución del hardware o la interrupción de la zona de disponibilidad provocan eventos de conmutación por error y de conmutación por recuperación. Cualquier cambio de datos que se produzca durante este tiempo se debe sincronizar entre los servidores de archivos principal y secundario, y Windows Server ejecuta una tarea de sincronización de datos que puede consumir recursos de E/S del disco. Para obtener más información, consulte Administración de la capacidad de rendimiento.

No pude ver las métricas por un momento, ¿debo preocuparme?

Los sistemas de archivos Single-AZ no estarán disponibles durante el mantenimiento del sistema de archivos, durante la sustitución de componentes de la infraestructura, y cuando una Zona de disponibilidad no esté disponible. Durante estos períodos, las métricas no estarán disponibles.

En una implementación Multi-AZ, Amazon aprovisiona y mantiene FSx automáticamente un servidor de archivos en espera en una zona de disponibilidad diferente. Si se produce un mantenimiento en el sistema de archivos o una interrupción imprevista del servicio, Amazon FSx realiza automáticamente la conmutación por error al servidor de archivos secundario, lo que te permite seguir accediendo a tus datos sin intervención manual. Durante el breve período en el que el sistema de archivos se interrumpe y se restaura, es posible que no se puedan ver las métricas por un momento.

Administración FSx de sistemas de archivos de Windows

Amazon FSx ofrece una amplia gama de capacidades administrativas que le ayudan a gestionar y hacer crecer fácilmente sus sistemas de archivos de Amazon FSx for Windows File Server para cumplir con los requisitos cambiantes de carga de trabajo y de los usuarios, así como con las necesidades normativas y de conformidad de su organización. La siguiente es una lista de algunas de las configuraciones del sistema de archivos que puede administrar mediante la AWS Management Console API AWS CLI y la API, la Amazon FSx CLI para la administración remota y las interfaces gráficas nativas de Microsoft Windows Server. PowerShell

- Capacidad de almacenamiento
- Tipo de almacenamiento
- IOPS en SSD
- Capacidad de rendimiento
- Los alias del DNS
- Deduplicación de datos
- Las copias de redundancia
- Cuotas de almacenamiento
- Auditoría de acceso a archivos
- Los recursos compartidos de archivos

En las siguientes secciones, se proporciona información acerca de las características administrativas y la configuración del sistema de archivos que están disponibles. Hemos incluido una guía para ayudarlo a determinar qué opciones son las mejores para su situación y las mejores prácticas, si corresponde.

Temas

- Estado FSx del sistema de archivos de Amazon
- Uso de Amazon FSx CLI para PowerShell
- Inicio de una PowerShell sesión FSx remota de Amazon
- Tareas únicas de configuración del sistema de archivos mediante Amazon FSx CLI para la administración remota en PowerShell
- Solución de problemas de acceso a la Amazon FSx CLI en PowerShell

- Ventana de mantenimiento del sistema de archivos
- Cambio del periodo de mantenimiento semanal
- La administración de los alias del DNS
- Sesiones de usuario y archivos abiertos
- Administrar el almacenamiento en FSx Windows File Server
- Uso de los espacios de nombres del DFS
- Administración de la capacidad de rendimiento
- Etiquetar tus recursos de Amazon FSx
- Actualice un sistema de archivos mediante AWS CLI

Estado FSx del sistema de archivos de Amazon

Puedes ver el estado de un sistema de FSx archivos de Amazon mediante la FSx consola de Amazon, el AWS CLI comando describe-file-systemso la operación de la API DescribeFileSystems.

Estado del sistema de archivos	Descripción
DISPONIBLE	El sistema de archivos se encuentra en buen estado y está accesible y disponible para su uso.
EN CREACIÓN	Amazon FSx está creando un nuevo sistema de archivos.
ELIMINANDO	Amazon FSx va a eliminar un sistema de archivos existente.
ACTUALIZANDO	El sistema de archivos está siendo objeto de una actualización iniciada por el cliente.
MISCONFIGURED	El sistema de archivos está deteriorado debido a un cambio en el entorno de Active Directory. Su sistema de archivos deja de estar disponibl e o corre el riesgo de perder la disponibilidad. Y, es posible que las copias de seguridad no se realicen correctamente. Para obtener más

Estado del sistema de archivos	Descripción
	información acerca de las zonas de disponibilidad, consulte El sistema de archivos está mal configurado.
MISCONFIGURED_UNAVAILABLE	El sistema de archivos no está disponible debido a un cambio en el entorno de su Active Directory. Para obtener más información acerca de las zonas de disponibilidad, consulte El sistema de archivos está mal configurado.
ERROR	• Al crear un nuevo sistema de archivos, Amazon no FSx ha podido crear el nuevo sistema de archivos. • El sistema de archivos no está disponible. • El sistema de archivos ha fallado y Amazon no FSx puede recuperarlo. • Amazon FSx no puede crear copias de seguridad.

Uso de Amazon FSx CLI para PowerShell

En este capítulo se describe cómo acceder a la Amazon FSx CLI para la administración remota y PowerShell realizar tareas administrativas del sistema de archivos FSx para los sistemas de archivos de Windows. También puede usar la interfaz gráfica de usuario (GUI) nativa de Microsoft Windows para realizar algunas tareas administrativas.

La Amazon FSx CLI para la administración remota PowerShell activa permite la administración del sistema de archivos para los usuarios del grupo de administradores del sistema de archivos. Para iniciar una PowerShell sesión remota en su FSx sistema de archivos del servidor de archivos de Windows, primero debe cumplir los siguientes requisitos previos:

- Debe poder conectarse a una instancia informática de Windows que tenga conectividad de red con el sistema de archivos del servidor de archivos de Windows. FSx
- Inicie sesión en la instancia informática de Windows como miembro del grupo de administradores del sistema de archivos. Si lo está utilizando AWS Managed Microsoft AD, ese es el grupo de

FSxadministradores AWS delegados. Si usa un Microsoft Active Directory autoadministrado, ese es el grupo de administradores de dominio o el grupo personalizado que especificó para la administración cuando creó el sistema de archivos. Para obtener más información, consulte Prácticas recomendadas a la hora de utilizar un Active Directory autogestionado.

- Corrobore que las reglas de entrada del grupo de seguridad de la VPC del sistema de archivos permitan el tráfico en el puerto 5985.

La Amazon FSx CLI para la administración remota PowerShell utiliza las siguientes características de seguridad:

- Las credenciales de usuario se autentican mediante la autenticación de Kerberos.
- Las comunicaciones de las sesiones de administración entre el cliente conectado y el sistema de archivos se cifran mediante Kerberos.

Tiene dos opciones para ejecutar comandos CLI de administración remota en su sistema de FSx archivos de Amazon:

- Puede establecer una PowerShell sesión remota de larga duración y ejecutar los comandos dentro de la sesión.
- Puede usarlo `Invoke-Command` para ejecutar un solo comando o un solo bloque de comandos sin establecer una sesión remota PowerShell de ejecución prolongada.

Si desea establecer y transferir variables como parámetros al comando de administración remota, tendrá que usar `Invoke-Command`.

> **Note**
>
> En el caso de los sistemas de archivos Multi-AZ, solo puede utilizar la Amazon FSx CLI para la gestión remota mientras el sistema de archivos utilice su servidor de archivos preferido. Para obtener más información, consulte Disponibilidad y durabilidad: sistemas de archivos Single-AZ y Multi-AZ..

Debe usar el PowerShell punto de conexión remoto de Windows del sistema de archivos para acceder al control remoto PowerShell. El punto de conexión de administración remota tiene el formato de `amznfsxctlyaa1k.`*`ActiveDirectory-DNS-name`*, por ejemplo,

`amznfsxctlyaa1k.corp.example.com`. Para encontrar el nombre del terminal, utilice la página AWS Management Console de detalles del sistema de archivos de la pestaña Red y seguridad. Utilice el AWS CLI `describe-file-systems`comando para ver la `RemoteAdministrationEndpoint` propiedad devuelta en la respuesta.

Puede usar el `Get-Command` cmdlet para recuperar información sobre los cmdlets, las funciones y los alias disponibles en. PowerShell Para obtener más información, consulte la documentación Get-Command de Microsoft.

También puede ejecutar Amazon FSx CLI para administración remota en PowerShell comandos de su sistema de archivos mediante el `Invoke-Command` cmdlet, con la siguiente sintaxis:

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName
 amznfsxctlyaa1k.corp.example.com -ConfigurationName FSxRemoteAdmin -scriptblock { fsx-
command}
```

Para obtener instrucciones sobre cómo iniciar una PowerShell sesión remota de larga duración en su sistema de archivos FSx de Windows File Server, consulte Inicio de una PowerShell sesión FSx remota de Amazon

Inicio de una PowerShell sesión FSx remota de Amazon

En este tema se proporcionan instrucciones para iniciar una PowerShell sesión remota de larga duración en el servidor FSx de archivos de Windows File Server.

Para iniciar una PowerShell sesión remota en el sistema de archivos

1. Conéctese a una instancia de procesamiento que tenga conectividad de red con su sistema de archivos como usuario que sea miembro del grupo de FSx administradores delegados que eligió al crear el sistema de archivos.
2. Abre una PowerShell ventana de Windows en la instancia de procesamiento.
3. En el PowerShell, introduce el siguiente comando para abrir una sesión remota de larga duración en tu sistema de FSx archivos de Amazon. *`Remote-PowerShell-Endpoint`*Reemplácelo por el PowerShell punto final remoto de Windows del sistema de archivos que desee administrar. Utilice `FsxRemoteAdmin` como nombre de la configuración de la sesión.

   ```
   PS C:\Users\delegateadmin> enter-pssession -ComputerName Remote-PowerShell-Endpoint
    -ConfigurationName FsxRemoteAdmin
   ```

```
[fs-0123456789abcdef0]: PS>
```

Si la instancia no forma parte del dominio de Amazon FSx Active Directory, se le solicitará que introduzca las credenciales de usuario en una ventana emergente. Introduzca las credenciales del usuario que es miembro del grupo de FSx administradores. Si su instancia está unida al dominio, no se le solicitarán credenciales.

> **Important**
>
> El PowerShell punto final remoto de Windows puede cambiar si utiliza una configuración autogestionada de Active Directory y cambia la cuenta de servicio sin la configuración adecuada de la política de grupo de Active Directory. Para obtener más información, consulte Cambiar la cuenta de FSx servicio de Amazon.

Tareas únicas de configuración del sistema de archivos mediante Amazon FSx CLI para la administración remota en PowerShell

Utilice la siguiente Amazon FSx CLI for Remote Management on PowerShell Commands para implementar rápidamente las tareas de administración del sistema de archivos siguiendo nuestras prácticas recomendadas.

Administración del consumo de almacenamiento

Use los siguientes comandos para administrar el consumo de almacenamiento del sistema de archivos.

- Para activar la deduplicación de los datos con el programa predeterminado, ejecute el siguiente comando.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Enable-FsxDedup }
```

Si lo desea, utilice el siguiente comando para que la deduplicación de datos entre en funcionamiento en sus archivos poco después de crearlos, sin que sea necesaria una antigüedad mínima para los archivos.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FSxDedupConfiguration -MinimumFileAgeDays 0 }
```

Para obtener más información, consulte Reducir los costos de almacenamiento con la dedduplicación de datos.

- Usa el siguiente comando para activar las cuotas de almacenamiento de los usuarios en el modo “Seguimiento”, que se utiliza únicamente con fines de elaboración de informes y no de cumplimiento.

```
$QuotaLimit = Quota limit in bytes
$QuotaWarningLimit = Quota warning threshold in bytes
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Enable-FSxUserQuotas -Track -DefaultLimit
 $Using:QuotaLimit -DefaultWarningLimit $Using:QuotaWarningLimit }
```

Para obtener más información, consulte Cómo administrar cuotas de almacenamiento.

Activar las instantáneas para que los usuarios finales puedan recuperar archivos y carpetas de versiones anteriores

Active las instantáneas con la programación predeterminada (de lunes a viernes a las 7 a. m. y a las 12 p. m.), de la siguiente manera.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxShadowStorage -Default }

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxShadowCopySchedule -Default -Confirm:$False}
```

Para obtener más información, consulte Configuración de copias de redundancia para que usen el almacenamiento y la programación predeterminados.

Aplicación del cifrado en tránsito

El siguiente comando aplica el cifrado a los clientes que se conectan a su sistema de archivos.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxSmbServerConfiguration -EncryptData $True -
RejectUnencryptedAccess $True -Confirm:$False}
```

Puede cerrar todas las sesiones abiertas y obligar a los clientes actualmente conectados a volver a conectarse mediante el cifrado.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Close-FSxSmbSession -Confirm:$False}
```

Para obtener más información, consulte Administración del cifrado en tránsito y Sesiones de usuario y archivos abiertos.

Solución de problemas de acceso a la Amazon FSx CLI en PowerShell

Existen varias causas posibles por las que no puede conectarse a su sistema de archivos mediante Remote PowerShell, cada una con su propia resolución, como se indica a continuación.

Para asegurarse primero de que puede conectarse correctamente al PowerShell punto final remoto de Windows, también puede realizar una prueba de conectividad básica. Por ejemplo, puede ejecutar el comando `test-netconnection endpoint -port 5985`.

El grupo de seguridad del sistema de archivos carece de las reglas de entrada necesarias para permitir una conexión remota PowerShell

El grupo de seguridad del sistema de archivos debe tener una regla de entrada que permita el tráfico en el puerto 5985 para poder establecer una sesión remota. PowerShell Para obtener más información, consulte Grupos de seguridad de Amazon VPC.

Tiene una confianza externa configurada entre el Microsoft Active Directory AWS administrado y su Active Directory local

Para utilizar Amazon FSx Remote PowerShell con autenticación Kerberos, debe configurar una política de grupo local en el cliente para el orden de búsqueda en los bosques. Para obtener más información, consulte la documentación de Microsoft sobre la Configuración del Orden de búsqueda en los bosques de Kerberos (KFSO).

Se produce un error de localización del idioma al intentar iniciar una sesión remota PowerShell

Debe agregar la siguiente `-SessionOption` (Opción de sesión) al comando `-SessionOption (New-PSSessionOption -uiCulture "en-US")`:

A continuación se muestran dos ejemplos que `-SessionOption` se utilizan al iniciar una PowerShell sesión remota en el sistema de archivos.

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName Windows Remote PowerShell
 Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {fsx-command} -SessionOption
 (New-PSSessionOption -uiCulture "en-US")
```

```
PS C:\Users\delegateadmin> Enter-Pssession -ComputerName Windows Remote PowerShell
 Endpoint -ConfigurationName FsxRemoteAdmin -SessionOption (New-PSSessionOption -
uiCulture "en-US")
```

Ventana de mantenimiento del sistema de archivos

Amazon FSx for Windows File Server realiza parches de software rutinarios para el software Microsoft Windows Server que administra. El período de mantenimiento especifica el día de la semana y la hora del día en que comienza este proceso de mantenimiento. Puede especificar el período de inicio de la ventana de mantenimiento durante la creación del sistema de archivos. Si no lo especifica, se asigna una ventana de inicio de mantenimiento predeterminada de 30 minutos. La duración del período de mantenimiento depende de varios factores, como el alcance del mantenimiento y el proceso de sincronización de cualquier actividad de lectura y escritura de archivos que se produzca durante el mantenimiento entre los servidores principal y secundario de los sistemas de archivos Multi-AZ. Para obtener más información, consulte Proceso de conmutación por error.

FSx para Windows File Server, le permite ajustar la hora de inicio del período de mantenimiento para adaptarla a la carga de trabajo y a los requisitos operativos. Puede cambiar la hora de inicio del período de mantenimiento con la frecuencia que necesite, siempre que la hora de inicio del período de mantenimiento esté programada al menos una vez cada 14 días. Si se publica un parche y no se ha programado un período de mantenimiento en un plazo de 14 días, FSx Windows File Server procederá al mantenimiento del sistema de archivos para garantizar su seguridad y fiabilidad. Para obtener más información sobre cómo ajustar la hora de inicio del período de mantenimiento del sistema de archivos, consulteCambio del periodo de mantenimiento semanal.

Mientras se estén aplicando los parches, es esperable que los sistemas de archivos Single-AZ no estén disponibles, por lo general durante menos de 20 minutos. Los sistemas de archivos Multi-AZ permanecen disponibles y realizan automáticamente la conmutación por error y la recuperación entre el servidor de archivos preferido y el servidor de archivos en espera. Para obtener más información, consulte Proceso de conmutación por error. Como la aplicación de parches en los sistemas de archivos Multi-AZ implica una conmutación por error y una recuperación entre los servidores de archivos, cualquier actividad de lectura y escritura de archivos que se produzca durante este tiempo debe sincronizarse entre el servidor de archivos preferido y el servidor de archivos en espera. Para reducir el tiempo de aplicación de parches, le recomendamos programar el período de mantenimiento durante los períodos de inactividad, cuando la carga del sistema de archivos sea mínima.

> **Note**
>
> Para garantizar la integridad de los datos durante las actividades de mantenimiento, Amazon FSx for Windows File Server completa cualquier operación de escritura pendiente en los volúmenes de almacenamiento subyacentes que alojan el sistema de archivos antes de que comience el mantenimiento.

Cambio del periodo de mantenimiento semanal

FSx para Windows File Server le permite ajustar cuándo comienza el período de mantenimiento del sistema de archivos para adaptarse a su carga de trabajo y requisitos operativos. Puedes usar la FSx API AWS Management Console AWS CLI, y Amazon para cambiar el momento en que comienza el período de mantenimiento semanal, tal como se describe en el siguiente procedimiento.

Para cambiar la hora de inicio del 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 Información del sistema de archivos.
4. Seleccione Administración para mostrar el panel de 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 Ajustes de administración.

Para cambiar la hora de inicio del período de mantenimiento semanal mediante el comando update-file-systemCLI, consulteActualice un sistema de archivos mediante AWS CLI.

La administración de los alias del DNS

Además del nombre predeterminado del Sistema de nombres de dominio (DNS) que FSx proporciona Amazon, también puedes asociar los alias DNS que desees a tus sistemas de archivos. Con los alias de DNS, puedes seguir utilizando los nombres de DNS existentes para acceder a los datos almacenados en Amazon FSx al migrar el almacenamiento del sistema de archivos de un entorno local a Amazon FSx, sin necesidad de actualizar ninguna herramienta o aplicación.

Puede asociar los alias DNS a sistemas de archivos nuevos y existentes FSx para Windows File Server y, cuando restaure una copia de seguridad en un nuevo sistema de archivos, utilice las teclas y. AWS Management Console AWS CLI Puede asociar hasta 50 alias del DNS con un sistema de archivos en cualquier momento.

> **Note**
>
> La compatibilidad con los alias de DNS está disponible en los sistemas FSx de archivos de Windows File Server creados después de las 12:00 p. m. ET del 9 de noviembre de 2020. Para usar los alias del DNS en un sistema de archivos creado antes de las 12:00 p. m. ET del 9 de noviembre de 2020, haga lo siguiente:
>
> 1. Realice una copia de seguridad del sistema de archivos existente. Para obtener más información, consulte Trabajo con copias de seguridad iniciadas por el usuario.
> 2. Restaure la copia de seguridad en un sistema de archivos nuevo. Para obtener más información, consulte Restauración de copias de seguridad en un nuevo sistema de archivos.
>
> Una vez que el sistema de archivos nuevo esté disponible, podrá utilizar los alias del DNS para acceder a él, con la información proporcionada en esta sección.

> **Note**
>
> La información que se presenta aquí da por sentado que trabaja exclusivamente en Active Directory y que no utiliza proveedores del DNS externos. Los proveedores del DNS de terceros pueden provocar un comportamiento inesperado.
> Amazon FSx solo registra los registros DNS de un sistema de archivos si el dominio de Active Directory al que se va a unir utiliza el DNS de Microsoft como DNS predeterminado. Si utilizas un DNS de terceros, tendrás que configurar manualmente las entradas de DNS para tus sistemas de FSx archivos de Amazon después de crearlo. Para obtener más información acerca de la elección de las direcciones IP correctas para usar en el sistema de archivos, consulte Obtención de las direcciones IP del sistema de archivos correctas para usarlas en las entradas manuales del DNS.

Puede asociar los alias de DNS a los sistemas FSx de archivos del servidor de archivos de Windows existentes al crear nuevos sistemas de archivos y al crear un nuevo sistema de archivos a partir de una copia de seguridad. Puede asociar hasta 50 alias del DNS con un sistema de archivos en cualquier momento.

Además de asociar los alias del DNS al sistema de archivos, para que los clientes se conecten a él con los alias del DNS, también debe hacer lo siguiente:

- Configure los nombres principales de los servicios (SPNs) para la autenticación y el cifrado de Kerberos.
- Configura un registro CNAME de DNS para el alias de DNS que se resuelva en el nombre de DNS predeterminado de tu sistema de FSx archivos de Amazon.

Para obtener más información, consulte Acceso a los datos mediante alias del DNS.

Un nombre de alias DNS FSx para su sistema de archivos del servidor de archivos de Windows debe cumplir los siguientes requisitos:

- Debe tener el formato del nombre de dominio completo (FQDN).
- Puede contener caracteres alfanuméricos o guiones (-).
- No puede empezar ni terminar con un guion.
- Puede comenzar con un número.

Para los nombres de alias de DNS, Amazon FSx almacena los caracteres alfabéticos como letras minúsculas (a-z), independientemente de cómo los especifiques: mayúsculas, minúsculas o las letras correspondientes en los códigos de escape.

Si intenta asociar un alias que ya está asociado al sistema de archivos, no tendrá ningún efecto. Si intentas desasociar un alias de un sistema de archivos que no está asociado al sistema de archivos, Amazon FSx responde con un error de solicitud incorrecta.

> **Note**
>
> Cuando Amazon FSx añade o elimina alias en un sistema de archivos, los clientes conectados se desconectan temporalmente y se vuelven a conectar automáticamente al sistema de archivos. El cliente debe volver a abrir todos los archivos que estaban abriendo los clientes que mapeaban un recurso compartido non-Continuously-Available (no perteneciente a CA) en el momento de la desconexión.

Temas

- El estado del alias del DNS
- Uso de alias del DNS con autenticación de Kerberos
- Visualización de los alias del DNS para sistemas de archivos y copias de seguridad
- Asociación de alias del DNS a los sistemas de archivos
- La administración de los alias del DNS en los sistemas de archivos existentes

El estado del alias del DNS

Los alias del DNS pueden tener uno de los siguientes valores de estado:

- Disponible: el alias DNS está asociado a un sistema de FSx archivos de Amazon.
- Creación: Amazon FSx está creando el alias de DNS y asociándolo al sistema de archivos.
- Eliminar: Amazon FSx desasociará el alias DNS del sistema de archivos y lo eliminará.
- No se pudo crear: Amazon no FSx pudo asociar el alias DNS al sistema de archivos.
- No se pudo eliminar: Amazon no FSx pudo desasociar el alias DNS del sistema de archivos.

Uso de alias del DNS con autenticación de Kerberos

Te recomendamos que utilices la autenticación y el cifrado basados en Kerberos en tránsito con Amazon. FSx Kerberos brinda la autenticación más segura para los clientes que acceden a su sistema de archivos. Para habilitar la autenticación Kerberos para los clientes que acceden a su sistema de FSx archivos de Amazon mediante un alias de DNS, debe configurar los nombres principales de servicio (SPNs) que se correspondan con el alias de DNS del objeto informático de Active Directory de su sistema de archivos.

Si ha configurado SPNs el alias DNS que ha asignado a otro sistema de archivos en un objeto informático de su Active Directory, primero debe eliminarlos SPNs antes de añadirlos SPNs al objeto informático del sistema de archivos. Para obtener más información, consulte Configure los nombres principales de servicio () para Kerberos SPNs.

Visualización de los alias del DNS para sistemas de archivos y copias de seguridad

Puede ver los alias DNS actualmente asociados a sus sistemas de archivos y copias FSx de seguridad del servidor de archivos de Windows mediante la API AWS Management Console, la y AWS CLI, tal y como se describe en los siguientes procedimientos.

Cómo ver los alias del DNS asociados a los sistemas de archivos

- Uso de la consola: elija un sistema de archivos para ver la página de información de los Sistemas de archivos. Seleccione la pestaña Red y seguridad para ver los Alias del DNS.
- Uso de la CLI o la API: utilice el comando `describe-file-system-aliases` CLI o la operación de DescribeFileSystemAliasesAPI.

Cómo ver los alias del DNS asociados a las copias de seguridad

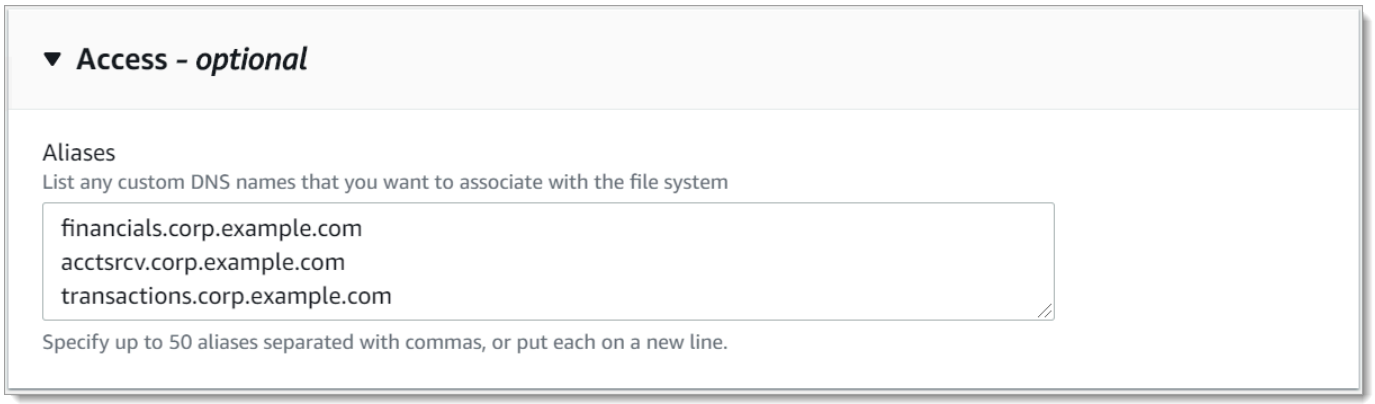
- Uso de la consola: en el panel de navegación, elija Copias de seguridad y, a continuación, elija la copia de seguridad que desea ver. En el panel de Resumen, consulte el campo de Alias del DNS.
- Uso de la CLI o la API: utilice el comando `describe-backups` CLI o la operación de DescribeBackupsAPI.

Asociación de alias del DNS a los sistemas de archivos

Puede asociar alias de DNS al crear un nuevo sistema de archivos FSx para el servidor de archivos de Windows desde cero o al restaurar una copia de seguridad en un nuevo sistema de archivos mediante la API AWS Management Console AWS CLI, que se describe a continuación.

Cómo asociar los alias del DNS cuando crea un nuevo sistema de archivos (consola)

1. Abre la FSx consola de Amazon en https://console.aws.amazon.com/fsx/.
2. Siga el procedimiento para crear un nuevo sistema de archivos que se describe en Paso 5. Crear el sistema de archivos en la sección Introducción.
3. En la sección Acceso (opcional) del asistente para Crear un sistema de archivos, escriba los alias del DNS que desee asociar al sistema de archivos.



4. Cuando el sistema de archivos esté disponible, podrá acceder a él mediante el alias de DNS configurando los nombres principales del servicio (SPNs) y actualizando o creando un registro CNAME de DNS para el alias. Para obtener más información, consulte Acceso a los datos mediante alias del DNS.

Para asociar alias de DNS al crear un nuevo sistema de FSx archivos Amazon (CLI)

1. Al crear un nuevo sistema de archivos, utilice la propiedad Alias con la operación de CreateFileSystemAPI para asociar los alias DNS al nuevo sistema de archivos.

```
aws fsx create-file-system \
  --file-system-type WINDOWS \
  --storage-capacity 2000 \
  --storage-type SSD \
  --subnet-ids subnet-123456 \
```

```
  --windows-configuration Aliases=[financials.corp.example.com,accts-
rcv.corp.example.com]
```

2. Cuando el sistema de archivos está disponible, puede acceder a él mediante el alias de DNS configurando los nombres principales del servicio (SPNs) y actualizando o creando un registro CNAME de DNS para el alias. Para obtener más información, consulte Acceso a los datos mediante alias del DNS.

Cómo agregar o eliminar alias del DNS al restaurar una copia de seguridad (CLI)

1. Al crear un nuevo sistema de archivos a partir de una copia de seguridad de un sistema de archivos existente, puede utilizar la propiedad Aliases con la operación de CreateFileSystemFromBackupAPI de la siguiente manera:

   - Todos los alias asociados a la copia de seguridad se asocian al sistema de archivos nuevo de forma predeterminada.
   - Para crear un sistema de archivos sin conservar ningún alias de la copia de seguridad, utilice la propiedad `Aliases` con un conjunto vacío.

     Para asociar los alias del DNS adicionales, utilice la propiedad `Aliases` e incluya tanto los alias originales asociados a la copia de seguridad como los nuevos que desee asociar.

   El siguiente comando CLI asocia dos alias al sistema de archivos que Amazon FSx está creando a partir de una copia de seguridad.

   ```
   aws fsx create-file-system-from-backup \
     --backup-id backup-0123456789abcdef0
     --storage-capacity 2000 \
     --storage-type HDD \
     --subnet-ids subnet-123456 \
     --windows-configuration Aliases=[transactions.corp.example.com,accts-
   rcv.corp.example.com]
   ```

2. Cuando el sistema de archivos está disponible, puede acceder a él mediante el alias de DNS configurando los nombres principales del servicio (SPNs) y actualizando o creando un registro CNAME de DNS para el alias. Para obtener más información, consulte Acceso a los datos mediante alias del DNS.

La administración de los alias del DNS en los sistemas de archivos existentes

Puede añadir y eliminar alias en los sistemas de archivos existentes FSx para Windows File Server mediante las teclas AWS Management Console y AWS CLI, tal y como se describe en los siguientes procedimientos.

Cómo administrar alias del DNS de un sistema de archivos (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 de Windows para el que desee administrar los alias del DNS.
3. En la pestaña Red y seguridad, seleccione Administrar para que los Alias del DNS muestren la ventana Administrar alias del DNS.

   - Para asociar alias del DNS: en el cuadro Asociar nuevos alias, escriba los alias del DNS que desee asociar. Elija Asociar.
   - Para desasociar los alias del DNS: en la lista de Alias actuales, elija los que desee desasociar. Elija Desasociar.

   Puede supervisar el estado de los alias que gestionó en la lista Alias actuales. Actualice la lista para actualizar el estado. Un alias tarda hasta 2,5 minutos en asociarse o desasociarse a un sistema de archivos.
4. Cuando el alias esté disponible, podrá acceder a su sistema de archivos mediante el alias de DNS configurando los nombres principales del servicio (SPNs) y actualizando o creando un registro CNAME de DNS para el alias. Para obtener más información, consulte Acceso a los datos mediante alias del DNS.

Cómo asociar alias del DNS a un sistema de archivos existente (CLI)

1. Utilice el comando `associate-file-system-aliases` CLI o la operación AssociateFileSystemAliasesAPI para asociar los alias DNS a un sistema de archivos existente.

   La siguiente solicitud de CLI asocia dos alias con el sistema de archivos especificado.

   ```
   aws fsx associate-file-system-aliases \
     --file-system-id fs-0123456789abcdef0 \
   ```

```
  --aliases financials.corp.example.com transfers.corp.example.com
```

La respuesta muestra el estado de los alias que Amazon FSx asocia al sistema de archivos.

```
{
    "Aliases": [
        {
            "Name": "financials.corp.example.com",
            "Lifecycle": CREATING
        },
        {
            "Name": "transfers.corp.example.com",
            "Lifecycle": CREATING
        }
    ]
}
```

2. Utilice el comando `describe-file-system-aliases` CLI (DescribeFileSystemAliases es la operación de API equivalente) para supervisar el estado de los alias que está asociando.
3. Cuando `Lifecycle` tiene el valor AVAILABLE (un proceso que puede tardar hasta 2,5 minutos), puede acceder al sistema de archivos mediante el alias de DNS configurando los nombres principales del servicio (SPNs) y actualizando o creando un registro CNAME de DNS para el alias. Para obtener más información, consulte Acceso a los datos mediante alias del DNS.

Cómo desasociar alias del DNS de sistemas de archivos (CLI)

- Utilice el comando `disassociate-file-system-aliases` CLI o la operación DisassociateFileSystemAliasesAPI para desasociar los alias DNS de un sistema de archivos existente.

  El siguiente comando desasocia un alias de un sistema de archivos.

  ```
  aws fsx disassociate-file-system-aliases \
    --file-system-id fs-0123456789abcdef0 \
    --aliases financials.corp.example.com
  ```

  La respuesta muestra el estado de los alias que Amazon FSx está desasociando del sistema de archivos.

```
{
    "Aliases": [
        {
            "Name": "financials.corp.example.com",
            "Lifecycle": DELETING
        }
    ]
}
```

Utilice el comando `describe-file-system-aliases` CLI (DescribeFileSystemAliases es la operación de API equivalente) para supervisar el estado de los alias. Se tarda hasta 2,5 minutos en eliminar el alias.

Sesiones de usuario y archivos abiertos

Puede supervisar las sesiones de los usuarios conectados y abrir archivos en su sistema FSx de archivos del servidor de archivos de Windows mediante la herramienta de carpetas compartidas. La herramienta de carpetas compartidas proporciona una ubicación central para supervisar quién está conectado al sistema de archivos y qué archivos están abiertos y quién los abre. Puede utilizar esta herramienta para hacer lo siguiente:

- Restaure el acceso a los archivos bloqueados.
- Al desconectar una sesión de usuario, se cierran todos los archivos abiertos por ese usuario.

Puede utilizar la herramienta GUI de carpetas compartidas nativa de Windows y la Amazon FSx CLI para la administración remota PowerShell para administrar las sesiones de usuario y abrir archivos en su FSx sistema de archivos de Windows File Server.

Uso de la GUI para administrar los usuarios y las sesiones

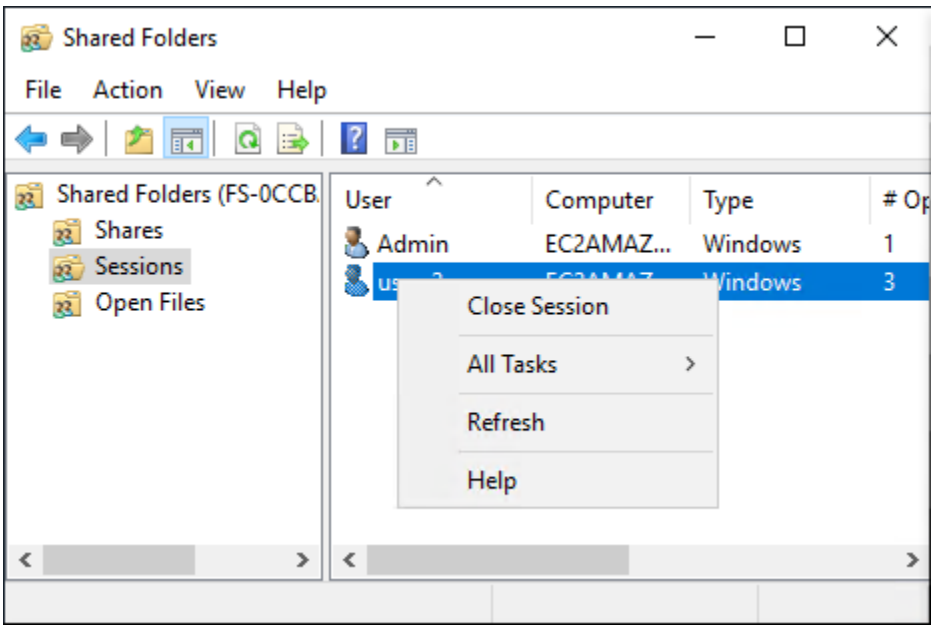
Los siguientes procedimientos detallan cómo puede administrar las sesiones de los usuarios y abrir archivos en su sistema de FSx archivos de Amazon mediante la herramienta de carpetas compartidas de Microsoft Windows.

Cómo lanzar la herramienta de carpetas compartidas

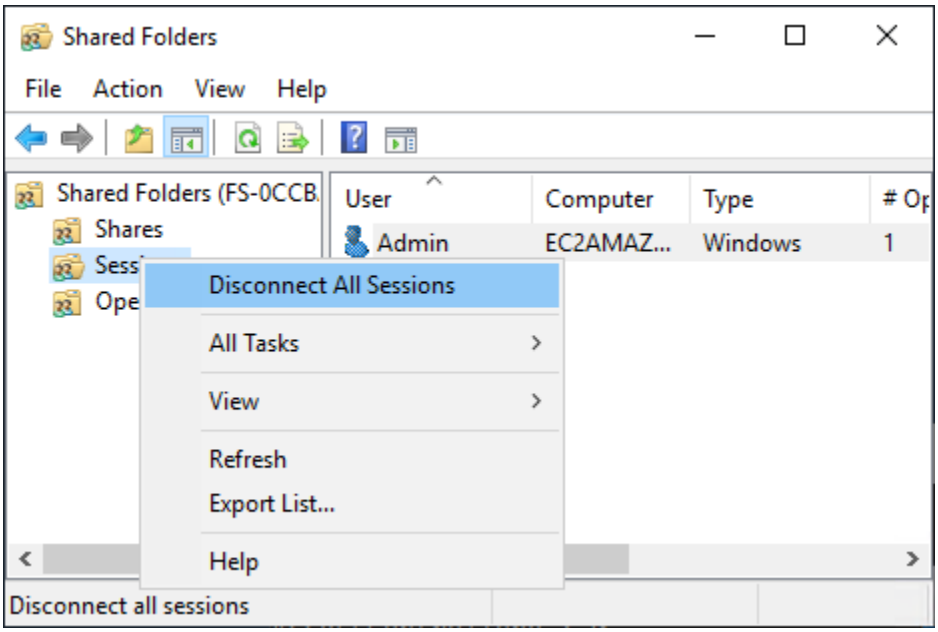
1. Lanza tu EC2 instancia de Amazon y conéctala al Active Directory de Microsoft al que está unido tu sistema de FSx archivos de Amazon. Para ello, elija uno de los procedimientos siguientes de la Guía de administración AWS Directory Service :
   - Únase sin problemas a una EC2 instancia de Windows
   - 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. En Microsoft Active Directory AWS administrado, este grupo se denomina FSx administradores AWS delegados. En el Microsoft Active Directory autoadministrado, este grupo se denomina Administradores de dominio o el nombre personalizado que le haya puesto cuando lo creó. Para obtener más información, consulte Conectarse a su instancia de Windows en la Guía del EC2 usuario de Amazon.
3. Abra el menú Inicio y ejecute fsmgmt.msc usando `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, introduce el nombre DNS de tu sistema de FSx archivos de Amazon, por ejemplo`fs-`*`012345678901234567`*`.`*`ad-domain`*`.com`.
6. Seleccione OK. A continuación, aparecerá una entrada para tu sistema de FSx archivos de Amazon en la lista de la herramienta Carpetas compartidas.

Cómo administrar las sesiones de usuario (GUI)

En la herramienta Carpetas compartidas, seleccione Sesiones para ver todas las sesiones de usuario que están conectadas a su sistema FSx de archivos del servidor de archivos de Windows. Si un usuario o una aplicación está accediendo a un recurso compartido de archivos en tu sistema de FSx archivos de Amazon, este complemento te muestra su sesión. Para desconectar sesiones, abra el menú contextual (haga clic con el botón derecho) de una sesión y elija Cifrado de sesión.



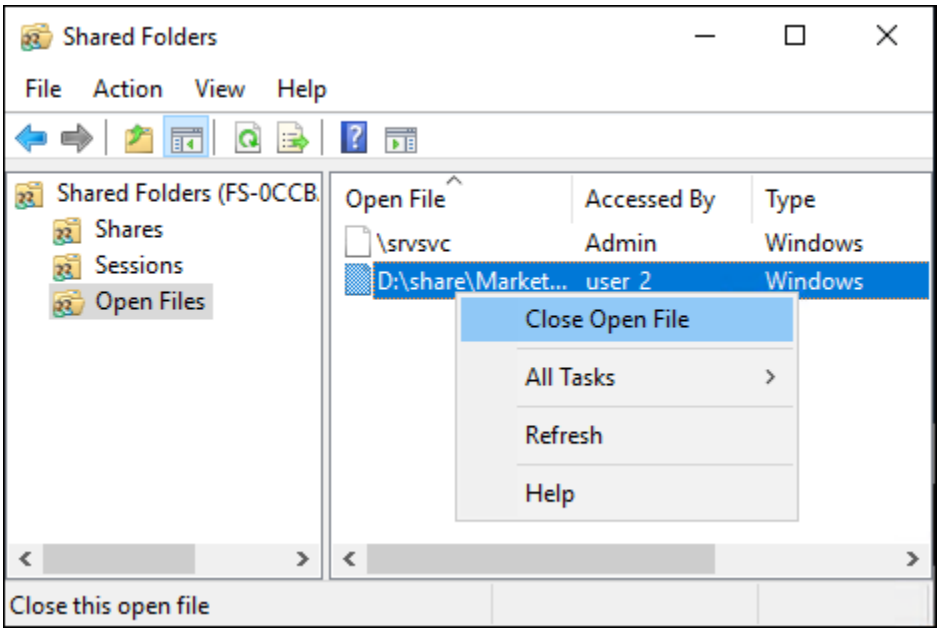
Para desconectar todas las sesiones abiertas, abra el menú contextual (haga clic con el botón derecho) de Sesiones, elija Desconectar todas las sesiones y confirme su acción.



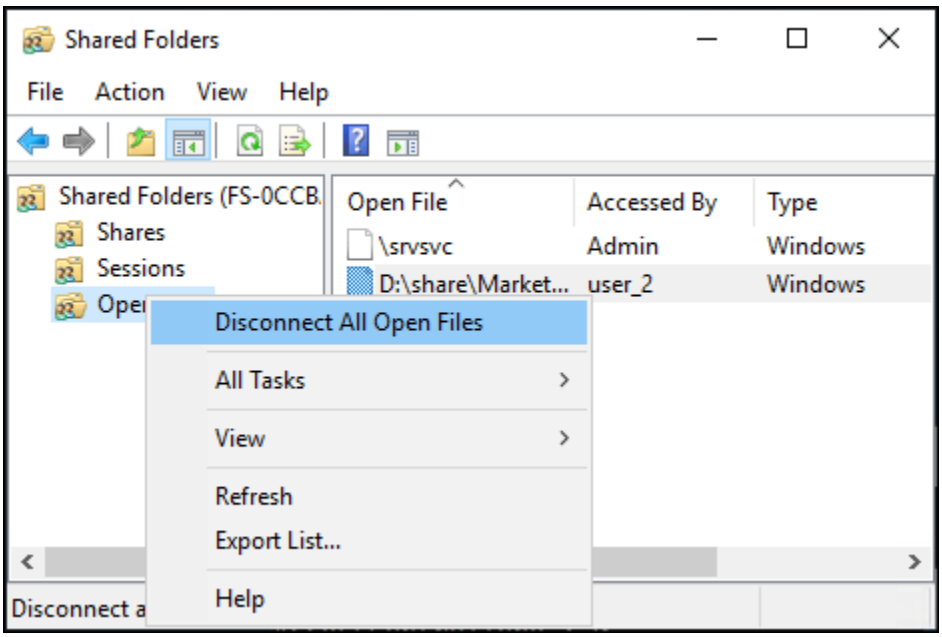
Cómo administrar los archivos abiertos (GUI)

En la herramienta Carpetas compartidas, elija Archivos abiertos para ver todos los archivos del sistema que están abiertos actualmente. La vista también muestra qué usuarios tienen abiertos los archivos o carpetas. Esta información puede resultar útil para averiguar por qué otros usuarios no pueden abrir determinados archivos. Para cerrar cualquier archivo que un usuario haya abierto,

basta con abrir el menú contextual (hacer clic con el botón derecho) correspondiente a la entrada del archivo en la lista y seleccionar Cerrar archivo abierto.



Para desconectar todos los archivos abiertos del sistema de archivos, utilice el menú contextual (haga clic con el botón derecho) de Archivos abiertos y seleccione Desconectar todos los archivos abiertos y confirme la acción.



Se utiliza PowerShell para administrar las sesiones de usuario y abrir archivos

Puede administrar las sesiones de usuario activas y abrir archivos en su sistema de archivos mediante Amazon FSx CLI para la administración remota de PowerShell. Para obtener información sobre cómo utilizar esta CLI, consulte Uso de Amazon FSx CLI para PowerShell.

A continuación, se muestran los comandos que puede utilizar para la administración de las sesiones de usuario y los archivos abiertos.

Comando	Descripción
Get-FSxSmbSession	Recupera información sobre las sesiones del bloque de mensajes del servidor (SMB) que están actualmente estableci das entre el sistema de archivos y los clientes asociados.
Close-FSxSmbSession	Finaliza una sesión SMB.
Get-FSxSmbOpenFile	Recupera información sobre los archivos que están abiertos para los clientes conectados al sistema de archivos.
Close-FSxSmbOpenFile	Cierra un archivo que está abierto para uno de los clientes del servidor SMB.

La ayuda en línea de cada comando brinda una referencia de todas las opciones de comando. Para acceder a esta ayuda, ejecute el comando con un -?, por ejemplo, Get-FSxSmbSession -?.

Administrar el almacenamiento en FSx Windows File Server

La configuración de almacenamiento del sistema de archivos incluye la cantidad de capacidad de almacenamiento aprovisionada, el tipo de almacenamiento y, si el tipo de almacenamiento es una unidad de estado sólido (SSD), la cantidad de IOPS en SSD. Puede configurar estos recursos junto con la capacidad de rendimiento del sistema de archivos, al crear uno y después de crearlo, para alcanzar el rendimiento deseado para la carga de trabajo. Aprenda a gestionar el almacenamiento de su sistema de archivos y el rendimiento relacionado con el almacenamiento mediante AWS Management Console AWS CLI, y la Amazon FSx CLI para la administración remota PowerShell explorando los siguientes temas.

Temas

- Optimizar costos de almacenamiento
- Administrar la capacidad de almacenamiento
- Administrar el tipo de almacenamiento del sistema de archivos
- Cómo administrar IOPS de SSD
- Reducir los costos de almacenamiento con la dedduplicación de datos
- Cómo administrar cuotas de almacenamiento
- Aumento de la capacidad de almacenamiento del sistema de archivos
- Supervisión de los aumentos de capacidad de almacenamiento
- Aumentar la capacidad de almacenamiento de un sistema de archivos FSx para Windows File Server de forma dinámica
- Actualización del tipo de almacenamiento de un sistema de archivos FSx para Windows
- Supervisión de las actualizaciones de tipos de almacenamiento
- Cómo actualizar las IOPS en SSD de un sistema de archivos
- La supervisión de las actualizaciones de IOPS de SSD aprovisionadas
- Cómo administrar la deduplicación de datos
- Cómo solucionar la deduplicación de datos

Optimizar costos de almacenamiento

Puede optimizar sus costes de almacenamiento mediante las opciones de configuración de almacenamiento disponibles en Windows FSx .

Opciones de tipo de almacenamiento: FSx para Windows, File Server ofrece dos tipos de almacenamiento, unidades de disco duro (HDD) y unidades de estado sólido (SSD), lo que le permite optimizar la relación costo/rendimiento para satisfacer sus necesidades de carga de trabajo. El almacenamiento en el disco duro está diseñado para una amplia gama de cargas de trabajo, incluidos los directorios principales, los recursos compartidos de usuarios y departamentos y los sistemas de administración de contenido. El almacenamiento de SSD está diseñado para las cargas de trabajo de mayor rendimiento y más sensibles a la latencia, incluidas las bases de datos, las cargas de trabajo de procesamiento multimedia y las aplicaciones de análisis de datos. Para obtener más información sobre los tipos de almacenamiento y el rendimiento del sistema de archivos, consulte FSx para el rendimiento del servidor de archivos de Windows.

Desduplicación de datos: los conjuntos de datos grandes suelen tener datos redundantes, lo cual aumenta los costos de almacenamiento de datos. Por ejemplo, los recursos compartidos de archivos por los usuarios pueden tener varias copias del mismo archivo, almacenadas por varios usuarios. Los recursos compartidos de desarrollo de software pueden contener muchos archivos binarios que permanecen inalterados de una compilación a otra. Puede reducir los costos de almacenamiento de datos activando la desduplicación de datos en el sistema de archivos. Cuando está activada, la desduplicación de datos reduce o elimina de forma automática los datos redundantes al almacenar las partes duplicadas del conjunto de datos solo una vez. Para obtener más información sobre la deduplicación de datos y cómo activarla fácilmente en su sistema de FSx archivos de Amazon, consulteReducir los costos de almacenamiento con la dedduplicación de datos.

Administrar la capacidad de almacenamiento

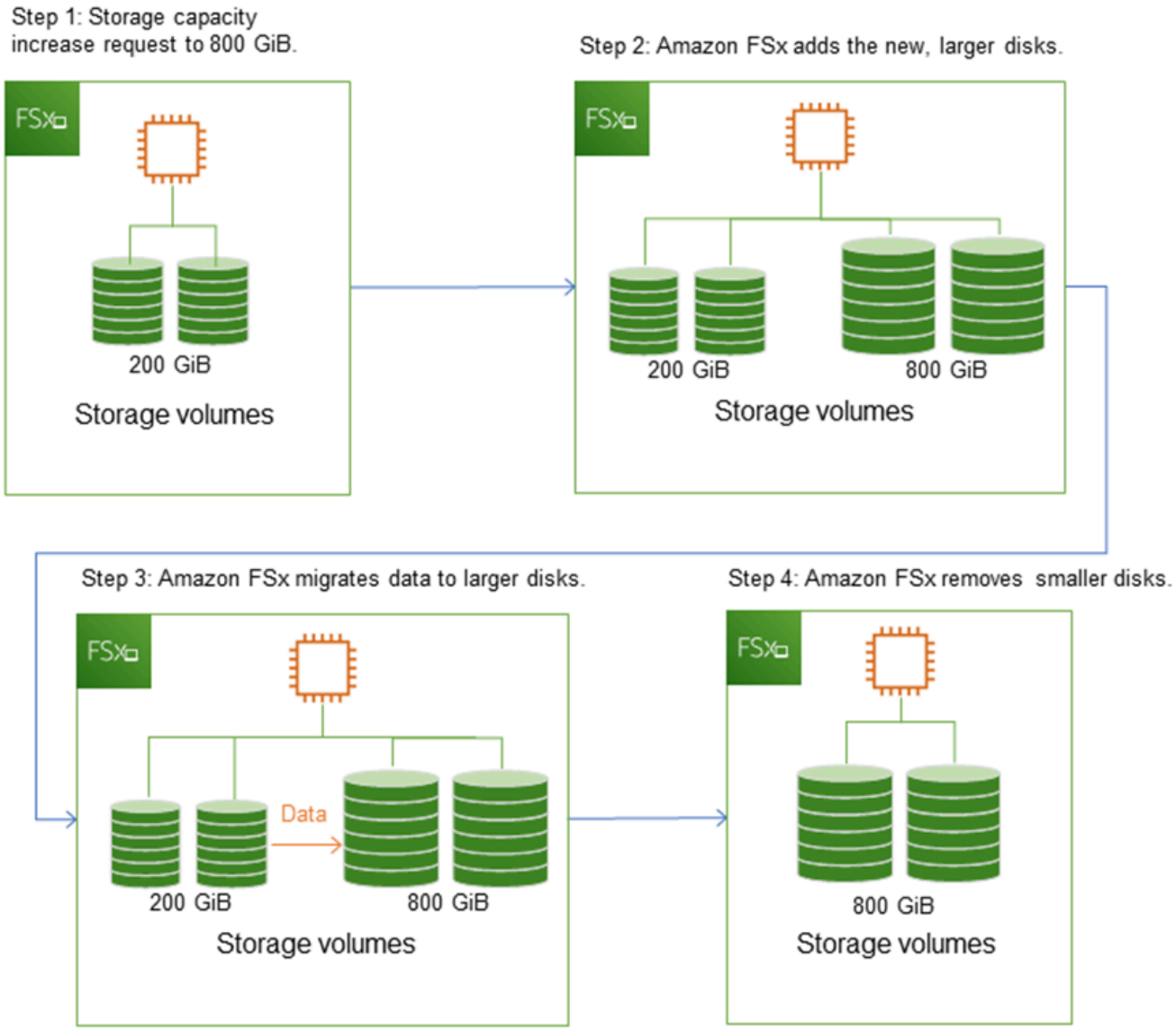
Puede aumentar FSx la capacidad de almacenamiento del sistema de archivos de Windows a medida que cambien sus requisitos de almacenamiento. Puedes hacerlo mediante la FSx consola de Amazon, la FSx API de Amazon o AWS Command Line Interface (AWS CLI). Los factores a tener en cuenta al planificar un aumento de la capacidad de almacenamiento incluyen saber cuándo es necesario aumentar la capacidad de almacenamiento, comprender cómo Amazon FSx procesa los aumentos de la capacidad de almacenamiento y hacer un seguimiento del progreso de una solicitud de aumento de almacenamiento. Solo se puede aumentar la capacidad de almacenamiento de un sistema de archivos; no se puede reducirla.

> **Note**
>
> No puede aumentar la capacidad de almacenamiento de los sistemas de archivos creados antes del 23 de junio de 2019, ni de los sistemas de archivos restaurados a partir de una copia de seguridad que pertenezcan a un sistema de archivos creado antes del 23 de junio de 2019.

Cuando aumentas la capacidad de almacenamiento de tu sistema de FSx archivos de Amazon, Amazon FSx añade un conjunto de discos nuevo y más grande a tu sistema de archivos entre bastidores. FSx A continuación, Amazon ejecuta un proceso de optimización del almacenamiento en segundo plano para migrar de forma transparente los datos de los discos antiguos a los nuevos. La optimización del almacenamiento puede tardar entre unas horas y varios días, según el tipo de almacenamiento y otros factores, con una implicancia que apenas se percibe en el rendimiento de la carga de trabajo. Durante esta optimización, el uso de las copias de seguridad aumenta temporalmente, ya que tanto los volúmenes de almacenamiento antiguos como los nuevos se

incluyen en las copias de seguridad a nivel del sistema de archivos. Se incluyen ambos conjuntos de volúmenes de almacenamiento para garantizar que Amazon FSx pueda realizar copias de seguridad y restaurarlas correctamente a partir de ellas, incluso durante la actividad de escalado del almacenamiento. El uso de las copias de seguridad vuelve al nivel de referencia anterior cuando los volúmenes de almacenamiento antiguos dejan de estar incluidos en el historial de copias de seguridad. Cuando la nueva capacidad de almacenamiento esté disponible, solo se le facturará la nueva capacidad de almacenamiento.

La siguiente ilustración muestra los cuatro pasos principales del proceso que Amazon FSx utiliza para aumentar la capacidad de almacenamiento de un sistema de archivos.



Puede realizar un seguimiento del progreso de la optimización del almacenamiento, los aumentos de la capacidad de almacenamiento de la SSD o las actualizaciones de IOPS de la SSD en cualquier momento mediante la FSx consola, la CLI o la API de Amazon. Para obtener más información, consulte Supervisión de los aumentos de capacidad de almacenamiento.

Lo que hay que saber sobre cómo aumentar la capacidad de almacenamiento de un sistema de archivos

Estos son algunos aspectos importantes que se deben tener en cuenta al aumentar la capacidad de almacenamiento:

- Solo aumentar: solo puede aumentar la capacidad de almacenamiento de un sistema de archivos; no puede reducirla.
- Aumento mínimo: cada aumento de la capacidad de almacenamiento debe tener un mínimo del 10 por ciento de la capacidad de almacenamiento actual del sistema de archivos, hasta el valor máximo permitido de 65 536 GiB.
- Capacidad de rendimiento mínima: para aumentar la capacidad de almacenamiento, un sistema de archivos debe tener una capacidad de rendimiento mínima de 16. MBps Esto se debe a que el paso de optimización del almacenamiento es un proceso que requiere un rendimiento intensivo.
- Tiempo entre aumentos: no puede realizar nuevos incrementos de la capacidad de almacenamiento en un sistema de archivos hasta 6 horas después de haber solicitado el último aumento, o hasta que se haya completado el proceso de optimización del almacenamiento, lo que sea más largo. La optimización del almacenamiento puede tardar en completarse desde unas horas hasta unos días. Para minimizar el tiempo que tarda en completarse la optimización del almacenamiento, recomendamos aumentar la capacidad de rendimiento del sistema de archivos antes de aumentar la capacidad de almacenamiento (la capacidad de rendimiento se puede volver a reducir una vez que se complete el escalado del almacenamiento), y aumentar la capacidad de almacenamiento cuando el tráfico en el sistema de archivos sea mínimo.

> **Note**
>
> Algunos eventos del sistema de archivos pueden consumir recursos de rendimiento de E/S del disco. Por ejemplo:
> La fase de optimización del escalado de la capacidad de almacenamiento puede generar un aumento del rendimiento del disco y, podría generar advertencias de rendimiento. Para obtener más información, consulte Advertencias y recomendaciones de rendimiento.

Saber cuándo aumentar la capacidad de almacenamiento

Aumente la capacidad de almacenamiento del sistema de archivos cuando se esté agotando la capacidad de almacenamiento libre. Utilice la `FreeStorageCapacity` CloudWatch métrica para supervisar la cantidad de almacenamiento libre disponible en el sistema de archivos. Puedes crear una CloudWatch alarma de Amazon en esta métrica y recibir una notificación cuando caiga por debajo de un umbral específico. Para obtener más información, consulte Monitorización con Amazon CloudWatch.

Te recomendamos que mantengas al menos un 20% de la capacidad de almacenamiento libre en todo momento en tu sistema de archivos. El uso de toda la capacidad de almacenamiento puede afectar negativamente al rendimiento y provocar incoherencias en los datos.

Puede aumentar de forma automática la capacidad de almacenamiento del sistema de archivos cuando la parte de esta que está libre caiga por debajo del umbral definido que especifique. Utilice la AWS AWS CloudFormation plantilla personalizada desarrollada para implementar todos los componentes necesarios para implementar la solución automatizada. Para obtener más información, consulte El aumento dinámico de la capacidad de almacenamiento.

Los aumentos de capacidad de almacenamiento y el rendimiento del sistema de archivos

La mayoría de las cargas de trabajo experimentan un impacto mínimo en el rendimiento mientras Amazon FSx ejecuta el proceso de optimización del almacenamiento en segundo plano una vez que la nueva capacidad de almacenamiento esté disponible. Sin embargo, los sistemas de archivos con almacenamiento en disco duro y las cargas de trabajo que implican un gran número de usuarios finales, altos niveles de E/S o conjuntos de datos con una gran cantidad de archivos pequeños podrían experimentar una reducción temporal del rendimiento. En estos casos, le recomendamos que primero aumente la capacidad de rendimiento del sistema de archivos antes de aumentar la capacidad de almacenamiento. Para estos tipos de cargas de trabajo, también recomendamos cambiar la capacidad de rendimiento durante los períodos de inactividad, cuando la carga del sistema de archivos sea mínima. Esto le permite seguir brindando el mismo nivel de rendimiento para satisfacer las necesidades de rendimiento de la aplicación. Para obtener más información, consulte Administración de la capacidad de rendimiento.

Administrar el tipo de almacenamiento del sistema de archivos

Puede cambiar el tipo de almacenamiento de su sistema de archivos de HDD a SSD mediante las AWS Management Console teclas y. AWS CLI Cuando cambie el tipo de almacenamiento a SSD,

tenga en cuenta que no podrá volver a actualizar la configuración del sistema de archivos hasta 6 horas después de haber solicitado la última actualización, o hasta que se complete el proceso de optimización del almacenamiento, lo que sea más largo. La optimización del almacenamiento puede tardar en completarse desde unas horas hasta unos días. Para minimizar este tiempo, se recomienda actualizar el tipo de almacenamiento cuando el tráfico en el sistema de archivos sea mínimo. Para obtener más información, consulte Actualización del tipo de almacenamiento de un sistema de archivos FSx para Windows.

No puede cambiar el tipo de almacenamiento del sistema de archivos de SSD a HDD. Si desea cambiar el tipo de almacenamiento de un sistema de archivos de SSD a HDD, tendrá que restaurar una copia de seguridad del sistema de archivos en un nuevo sistema de archivos que configure para usar el almacenamiento en HDD. Para obtener más información, consulte Restauración de copias de seguridad en un nuevo sistema de archivos.

Acerca de los tipos de almacenamiento

Puede configurar el sistema de archivos del servidor de archivos de Windows FSx para que utilice el tipo de almacenamiento de unidad de estado sólido (SSD) o unidad de disco duro magnético (HDD).

El almacenamiento SSD es adecuado para la mayoría de las cargas de trabajo de producción que tienen requisitos de alto rendimiento y sensibilidad a la latencia. Algunos ejemplos de estas cargas de trabajo son las bases de datos, el análisis de datos, el procesamiento multimedia y las aplicaciones empresariales. También recomendamos el SSD para casos de uso que involucren un gran número de usuarios finales, niveles altos de E/S o conjuntos de datos que tengan una gran cantidad de archivos pequeños. Por último, recomendamos que utilice el almacenamiento en SSD si planea habilitar las copias de redundancia. Puede configurar y escalar las IOPS de SSD para sistemas de archivos con almacenamiento en SSD, pero no en disco duro.

El almacenamiento en HDD está diseñado para una amplia gama de cargas de trabajo, que incluye los directorios principales, los recursos compartidos de archivos por usuarios y departamentos y los sistemas de administración de contenido. El almacenamiento en disco duro tiene un costo menor en comparación con el almacenamiento en SSD, pero con latencias más altas y niveles más bajos de rendimiento del disco e IOPS de disco por unidad de almacenamiento. Puede ser adecuado para recursos compartidos de usuarios de uso general y directorios principales con bajos requisitos de E/S, sistemas de administración de contenido (CMS) de gran tamaño en los que los datos se recuperan con poca frecuencia o conjuntos de datos con un número reducido de archivos grandes.

Para obtener más información, consulte Configuración y rendimiento del almacenamiento.

Cómo administrar IOPS de SSD

En el caso de los sistemas de archivos configurados con almacenamiento en SSD, la cantidad de IOPS en SSD determina la cantidad de E/S del disco disponible cuando el sistema de archivos tiene que leer y escribir datos en el disco, a diferencia de los datos que están en caché. Puede seleccionar y escalar la cantidad de IOPS en SSD independientemente de la capacidad de almacenamiento. La cantidad máxima de IOPS de SSD que puede aprovisionar depende de la cantidad de capacidad de almacenamiento y de capacidad de rendimiento que seleccione para los sistema de archivos. Si intenta aumentar las IOPS en SSD por encima del límite que admite la capacidad de rendimiento, es posible que tenga que aumentar la capacidad de rendimiento para llegar al nivel de IOPS en SSD. Para obtener más información, consulte FSx para el rendimiento del servidor de archivos de Windows y Administración de la capacidad de rendimiento.

Estos son algunos aspectos importantes que debe saber acerca de la actualización de IOPS en SSD aprovisionadas en un sistema de archivos:

- Al elegir un modo de IOPS, hay dos modos de IOPS entre los que elegir:
  - Automático: elige este modo y Amazon FSx escalará automáticamente las IOPS de tu SSD para mantener 3 IOPS de SSD por GiB de capacidad de almacenamiento, hasta 400 000 IOPS de SSD por sistema de archivos.
  - Aprovisionadas por el usuario: seleccione este modo para poder especificar la cantidad de IOPS en SSD dentro del rango de 96 a 400 000. Especifica un número entre 3 y 50 IOPS por GiB de capacidad de almacenamiento para todos los lugares donde Regiones de AWS Amazon FSx esté disponible, o entre 3 y 500 IOPS por GiB de capacidad de almacenamiento en EE. UU. Este (GiB), EE. UU. Oeste (Oregón), EE. UU. Este (Ohio), Europa (Irlanda), Asia Pacífico (Tokio) y Asia Pacífico (Singapur). Si elige el modo aprovisionado por el usuario y la cantidad de IOPS en SSD que especifique no es de al menos 3 IOPS por GiB, se produce un error en la solicitud. Para niveles más altos de IOPS de SSD aprovisionadas, paga por el promedio de IOPS por encima de 3 IOPS por GiB por sistema de archivos.
- Actualizaciones de la capacidad de almacenamiento: si aumentas la capacidad de almacenamiento de tu sistema de archivos y la cantidad requiere de forma predeterminada una cantidad de IOPS de SSD superior al nivel actual de IOPS de SSD aprovisionado por el usuario, Amazon cambia FSx automáticamente tu sistema de archivos al modo automático y tu sistema de archivos tendrá un mínimo de 3 IOPS de SSD por GiB de capacidad de almacenamiento.
- Actualizaciones de la capacidad de rendimiento: si aumentas tu capacidad de rendimiento y el máximo de IOPS de SSD que admite tu nueva capacidad de rendimiento es superior al nivel de

IOPS de SSD aprovisionado por el usuario, Amazon cambia FSx automáticamente tu sistema de archivos al modo automático.

- Tiempo entre aumentos de IOPS en SSD: no puede realizar más aumentos de IOPS en SSD, aumentos de la capacidad de rendimiento ni actualizaciones del tipo de almacenamiento en un sistema de archivos hasta 6 horas después de haber solicitado el último aumento. Asimismo, tampoco se puede realizar aumentos hasta que se haya completado el proceso de optimización del almacenamiento, lo que demore más. La optimización del almacenamiento puede tardar en completarse desde unas horas hasta unos días. Para minimizar el tiempo que tarda en completarse la optimización del almacenamiento, recomendamos escalar las IOPS de las SSD cuando el tráfico en el sistema de archivos sea mínimo.

> **Note**
>
> Tenga en cuenta que los niveles de capacidad de rendimiento de 4608 MBps o más solo se admiten en las siguientes regiones Regiones de AWS: EE. UU. Este (Norte de Virginia), EE. UU. Oeste (Oregón), EE. UU. Este (Ohio), Europa (Irlanda), Asia Pacífico (Tokio) y Asia Pacífico (Singapur).

Para obtener más información sobre cómo actualizar la cantidad de IOPS de SSD aprovisionadas FSx para su sistema de archivos Windows File Server, consulte. Cómo actualizar las IOPS en SSD de un sistema de archivos

Reducir los costos de almacenamiento con la dedduplicación de datos

La desduplicación de datos, que suele abreviarse como “Dedup”, ayuda a los administradores de almacenamiento a reducir los costos asociados a la duplicación de datos. Con FSx Windows File Server, puede usar la deduplicación de datos de Microsoft para identificar y eliminar los datos redundantes. Los conjuntos de datos grandes suelen tener datos redundantes, lo cual aumenta los costos de almacenamiento de datos. Por ejemplo:

- Los archivos compartidos por los usuarios pueden tener varias copias de los mismos archivos o de archivos similares.
- Los recursos compartidos de desarrollo de software pueden contener muchos archivos binarios que permanecen inalterados de una compilación a otra.

Puede reducir los costos de almacenamiento de datos activando la desduplicación de datos en el sistema de archivos. La deduplicación de datos reduce o elimina los datos redundantes al almacenar partes duplicadas del conjunto de datos solo una vez. Cuando activa la desduplicación de datos, la compresión de datos se activa de forma predeterminada, lo que comprime los datos después de la desduplicación para obtener un mayor ahorro. La desduplicación de datos optimiza las redundancias sin comprometer la fidelidad ni la integridad de los datos. La deduplicación de datos se ejecuta como un proceso en segundo plano que escanea y optimiza el sistema de archivos de forma continua y automática, y es transparente para los usuarios y los clientes conectados.

El ahorro de almacenamiento que puede lograr con la deduplicación de datos depende de la naturaleza del conjunto de datos, incluida la cantidad de duplicados que existan entre los archivos. Los ahorros típicos promedian entre un 50 y un 60 por ciento en el caso de los archivos compartidos de uso general. Dentro de las acciones, los ahorros oscilan entre el 30 y el 50 por ciento en los documentos de usuario y entre el 70 y el 80 por ciento en los conjuntos de datos de desarrollo de software. Puede medir los posibles ahorros en la deduplicación mediante el PowerShell comando `Measure-FSxDedupFileMetadata` remoto que se describe a continuación.

También puede personalizar la deduplicación de datos para que se adapte a sus necesidades de almacenamiento específicas. Por ejemplo, puede configurar la deduplicación para que se ejecute solo en determinados tipos de archivos o puede crear un cronograma de trabajo personalizado. Dado que los trabajos de desduplicación pueden consumir recursos del servidor de archivos, le recomendamos que supervise el estado de los trabajos de desduplicación mediante el comando `Get-FSxDedupStatus`.

Para obtener información sobre cómo configurar la desduplicación de datos en el sistema de archivos, consulte Cómo administrar la deduplicación de datos.

Para obtener información sobre cómo resolver problemas relacionados con la desduplicación de datos, consulte

Use la siguiente información como ayuda para solucionar algunos problemas comunes al configurar y usar la desduplicación de datos.

Temas

- La desduplicación de datos no funciona
- Los valores de desduplicación se establecen en 0 de forma inesperada
- Aunque se eliminan los archivos, no se libera espacio en el sistema de archivos

La desduplicación de datos no funciona

Para ver el estado actual de la deduplicación de datos, ejecute el `Get-FSxDedupStatus` PowerShell comando para ver el estado de finalización de los trabajos de deduplicación más recientes. Si una o más tareas fallan, es posible que no vea un aumento en la capacidad de almacenamiento libre del sistema de archivos.

La razón más común por la que fallan las tareas de desduplicación es la falta de memoria.

- Microsoft recomienda disponer de forma óptima de 1 GB de memoria por cada 1 TB de datos lógicos (o un mínimo de 350 MB por 1 TB de datos lógicos). Usa la tabla de FSx rendimiento de Amazon para determinar la memoria asociada a la capacidad de rendimiento de tu sistema de archivos y asegurarte de que los recursos de memoria son suficientes para el tamaño de tus datos. Si no es así, debe aumentar la capacidad de rendimiento del sistema de archivos hasta un nivel que cumpla con los requisitos de memoria de 1 GB por 1 TB de datos lógicos.
- Las tareas de desduplicación se configuran con la asignación de memoria predeterminada del 25% que recomienda Windows. Esto significa que, para un sistema de archivos con 32 GB de memoria, habrá 8 GB disponibles para la desduplicación. La asignación de memoria es configurable (mediante el comando `Set-FSxDedupSchedule` con el parámetro `-Memory`). Tenga en cuenta que el uso de una mayor asignación de memoria para la desduplicación puede afectar al rendimiento del sistema de archivos.
- Puede modificar la configuración de las tareas de desduplicación para reducir la cantidad de memoria requerida. Por ejemplo, puede restringir la optimización para que se solo ejecute en tipos de archivos o carpetas específicos, o puede establecer un mínimo para el tamaño y la antigüedad de los archivos que se van a optimizar. También, recomendamos establecer una configuración para que las tareas de desduplicación se ejecuten durante los períodos de inactividad, cuando la carga del sistema de archivos sea mínima.

También, es posible que se produzcan errores si las tareas de desduplicación no tienen tiempo suficiente para completarse. Es posible que tenga que cambiar la duración máxima de las tareas, como se describe en Cómo modificar un programa de deduplicación de datos.

Si las tareas de desduplicación estuvieron fallando durante un tiempo prolongado, y se cambiaron los datos del sistema de archivos durante este período, es posible que las tareas de desduplicación posteriores requieran más recursos para completarse correctamente por primera vez.

Los valores de desduplicación se establecen en 0 de forma inesperada

De manera inesperada, los valores del `SavedSpace` y la `OptimizedFilesSavingsRate` se encuentran en 0, en un sistema de archivos en el cual configuró la desduplicación de datos.

Esto puede ocurrir durante el proceso de optimización del almacenamiento cuando se aumenta la capacidad de almacenamiento del sistema de archivos. Al aumentar la capacidad de almacenamiento de un sistema de archivos, Amazon FSx cancela los trabajos de deduplicación de datos existentes durante el proceso de optimización del almacenamiento, que migra los datos de los discos antiguos a los nuevos discos de mayor tamaño. Amazon FSx reanuda la deduplicación de datos en el sistema de archivos una vez finalizado el trabajo de optimización del almacenamiento. Para obtener más información sobre el aumento de la capacidad de almacenamiento y la optimización, consulte Administrar la capacidad de almacenamiento.

Aunque se eliminan los archivos, no se libera espacio en el sistema de archivos

El comportamiento esperado de la desduplicación de datos es el siguiente: si los datos que se eliminaron eran una forma de ahorro de espacio realizado por la desduplicación, entonces realmente se liberará espacio en el sistema de archivos cuando se ejecute la recopilación de elementos no utilizados.

Una práctica que puede resultarle útil consiste en programar la ejecución de la recopilación de elementos no utilizados para inmediatamente después de eliminar un gran número de archivos. Una vez finalizada la recopilación de elementos no utilizados, puede volver a establecer la programación de dicha recopilación a la configuración original. Esto garantiza que pueda ver el espacio de que generan las eliminaciones de forma inmediata.

Use el siguiente procedimiento para configurar la recopilación de elementos no utilizados para que se ejecute en 5 minutos.

1. Para comprobar que la desduplicación de datos esté habilitada, utilice el comando `Get-FSxDedupStatus`. Para obtener más información acerca del comando y el resultado esperado, consulte Cómo visualizar la cantidad de espacio ahorrado.
2. Utilice lo siguiente para programar la ejecución de la recopilación de elementos no utilizados dentro de 5 minutos.

```
$FiveMinutesFromNowUTC = ((get-date).AddMinutes(5)).ToUniversalTime()
$DayOfWeek = $FiveMinutesFromNowUTC.DayOfWeek
$Time = $FiveMinutesFromNowUTC.ToString("HH:mm")
```

```
Invoke-Command -ComputerName ${RPS_ENDPOINT} -ConfigurationName FSxRemoteAdmin -
ScriptBlock {
    Set-FSxDedupSchedule -Name "WeeklyGarbageCollection" -Days $Using:DayOfWeek -
Start $Using:Time -DurationHours 9
}
```

3. Una vez que se haya ejecutado la recopilación de elementos no utilizados, y se haya liberado espacio, restablezca la programación a su configuración original.

.

Para obtener más información acerca de la deduplicación de datos, consulte la documentación Entender la deduplicación de datos de Microsoft.

> **Warning**
>
> No se recomienda ejecutar determinados comandos de Robocopy con la deduplicación de datos, ya que estos comandos pueden afectar a la integridad de los datos del Chunk Store. Para obtener más información, consulte la documentación de Interoperabilidad de deduplicación de datos de Microsoft.

Prácticas recomendadas para usar la desduplicación de datos

Estas son algunas prácticas recomendadas para utilizar la deduplicación de datos:

- Programe los trabajos de deduplicación de datos para que se ejecuten cuando el sistema de archivos esté inactivo: la programación predeterminada incluye un trabajo de `GarbageCollection` semanal a las 2:45 UTC los sábados. Este proceso puede tardar varias horas en completarse si su sistema de archivos está absorbiendo una gran cantidad de datos. Si este tiempo no es ideal para su carga de trabajo, programe este trabajo para que se ejecute en un momento en el que espere poco tráfico en su sistema de archivos.
- Configure una capacidad de rendimiento suficiente para que se complete la deduplicación de datos: las capacidades de rendimiento más altas proporcionan niveles de memoria más altos. Microsoft recomienda disponer de 1 GB de memoria por cada 1 TB de datos lógicos para ejecutar la deduplicación de datos. Usa la tabla de FSx rendimiento de Amazon para determinar la memoria asociada a la capacidad de rendimiento de tu sistema de archivos y asegurarte de que los recursos de memoria son suficientes para el tamaño de tus datos.

- Personalice la configuración de deduplicación de datos para que se adapte a sus necesidades de almacenamiento específicas y reduzca los requisitos de rendimiento: puede restringir la optimización para que se ejecute en tipos de archivos o carpetas específicos, o establecer un tamaño y una antigüedad mínimos de los archivos para la optimización. Para obtener más información, consulte Reducir los costos de almacenamiento con la dedduplicación de datos.

Cómo administrar cuotas de almacenamiento

Puede configurar las cuotas de almacenamiento de los usuarios en sus sistemas de archivos para limitar la cantidad de almacenamiento de datos que los usuarios pueden consumir. Después de establecer las cuotas, puede realizar un seguimiento del estado de las cuotas para controlar el uso y ver si los usuarios superan sus cuotas.

También puedes hacer cumplir las cuotas impidiendo que los usuarios que las alcancen escriban en el espacio de almacenamiento. Al aplicar las cuotas, un usuario que las supere recibirá un mensaje de error que indica que no hay suficiente espacio en disco.

Puede establecer estos umbrales para la configuración de las cuotas:

- Advertencia: se utiliza para comprobar si un usuario o un grupo se acerca a su límite de cuota y solo es relevante para el seguimiento.
- Límite: el límite de la cuota de almacenamiento de un usuario o grupo.

Puede configurar las cuotas predeterminadas que se aplican a los nuevos usuarios que acceden a un sistema de archivos y las cuotas que se aplican a usuarios o grupos específicos. También puedes ver un informe sobre la cantidad de almacenamiento que consume cada usuario o grupo y si está superando sus cuotas.

El consumo de almacenamiento a nivel de usuario se registra en función de la propiedad de los archivos. El consumo de almacenamiento se calcula utilizando el tamaño lógico de los archivos, no el espacio de almacenamiento físico real que ocupan los archivos. Se realiza un seguimiento de las cuotas de almacenamiento de los usuarios en el momento en que se escriben los datos en un archivo.

La actualización de las cuotas de varios usuarios requiere ejecutar el comando de actualización una vez para cada usuario u organizar a los usuarios en un grupo y actualizar la cuota de ese grupo.

Puede administrar las cuotas de almacenamiento de los usuarios en su sistema de archivos mediante la Amazon FSx CLI para la administración remota de PowerShell. Para obtener información sobre cómo utilizar esta CLI, consulte Uso de Amazon FSx CLI para PowerShell.

A continuación, encontrará comandos que puede utilizar para administrar las cuotas de almacenamiento de los usuarios.

Comando de cuotas de almacenamiento de usuario	Descripción
Enable-FSxUserQuotas	Comienza a rastrear o aplicar las cuotas de almacenamiento de los usuarios, o ambas.
Disable-FSxUserQuotas	Detiene el seguimiento y la aplicación de las cuotas de almacenamiento de los usuarios.
Get-FSxUserQuotaSettings	Recupera la configuración actual de cuota de almacenamiento de usuario para el sistema de archivos.
Get-FSxUserQuotaEntries	Recupera las entradas actuales de la cuota de almacenamiento de usuarios para usuarios individuales y grupos del sistema de archivos.
Set-FSxUserQuotas	Establezca la cuota de almacenamiento de usuarios para un usuario individual o un grupo. Los valores de cuota están expresados en bytes.

La ayuda en línea de cada comando brinda una referencia de todas las opciones de comando. Para acceder a esta ayuda, ejecute el comando con -?, por ejemplo, Enable-FSxUserQuotas -?.

Aumento de la capacidad de almacenamiento del sistema de archivos

Puede aumentar FSx la capacidad de almacenamiento del sistema de archivos del servidor de archivos de Windows a medida que cambien sus requisitos de almacenamiento. Utilice la FSx consola de Amazon AWS CLI, la o la FSx API de Amazon para aumentar la capacidad de almacenamiento de un sistema de archivos, tal y como se describe en los siguientes procedimientos. Para obtener más información, consulte Administrar la capacidad de almacenamiento.

Para aumentar la capacidad de almacenamiento de un sistema de archivos (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 de Windows al que desee aumentarle la capacidad de almacenamiento.
3. En Acciones, seleccione Actualizar almacenamiento. O bien, en el panel Resumen, seleccione Actualizar junto a la Capacidad de almacenamiento del sistema de archivos.

   Aparece la ventana Actualizar la capacidad de almacenamiento.
4. En Tipo de entrada, elija Porcentaje para ingresar la nueva capacidad de almacenamiento como un cambio porcentual con respecto al valor actual, o elija Absoluto para especificar el nuevo valor en GiB.
5. Especifique la Capacidad de almacenamiento deseada.

   > **Note**
   >
   > El valor de capacidad deseada debe ser al menos un 10 por ciento mayor que el valor actual, hasta un valor máximo de 65.536 GiB.
6. Seleccione Actualizar para iniciar la actualización de la capacidad de almacenamiento.
7. Puede supervisar el progreso de la actualización en la página de información de los Sistemas de archivos, en la pestaña Actualizaciones.

Para aumentar la capacidad de almacenamiento de un sistema de archivos (CLI)

Para aumentar la capacidad de almacenamiento de un sistema de archivos FSx para Windows File Server, utilice el AWS CLI comando update-file-system. Establezca los siguientes parámetros:

- `--file-system-id` en el ID del sistema de archivos que va a actualizar.
- `--storage-capacity` a un valor que sea al menos un 10 por ciento superior al valor actual.

Puede supervisar el progreso de la actualización mediante el AWS CLI comando describe-file-systems. Busque las `administrative-actions` en los resultados.

Para obtener más información, consulte AdministrativeAction.

Supervisión de los aumentos de capacidad de almacenamiento

Tras aumentar la capacidad de almacenamiento del sistema de archivos, puede supervisar el progreso del aumento de la capacidad de almacenamiento mediante la FSx consola de Amazon, la API o AWS CLI según se describe en los siguientes procedimientos.

Supervisión de los aumentos en la consola

En la pestaña Actualizaciones de la ventana de información del sistema de archivos, puede ver las 10 actualizaciones más recientes de cada tipo.

Para obtener información sobre las actualizaciones de capacidad de almacenamiento, puede ver la siguiente información.

Tipo de actualización

Los valores posibles son Capacidad de almacenamiento.

Valor de destino

El valor que desea alcanzar con la actualización de la capacidad de almacenamiento del sistema de archivos.

Estado

El estado de la actualización vigente. Para las actualizaciones de capacidad de almacenamiento, 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.
- Optimización actualizada: Amazon FSx ha aumentado la capacidad de almacenamiento del sistema de archivos. El proceso de optimización del almacenamiento ahora traslada los datos del sistema de archivos a los discos nuevos y de mayor tamaño.
- Finalizado: el aumento de la capacidad de almacenamiento se completó correctamente.
- Error: no se pudo aumentar la capacidad de almacenamiento. Elija el signo de interrogación (?) para ver información sobre la causa de un error en la actualización del almacenamiento.

% de progreso

El progreso del proceso de optimización del almacenamiento se ve reflejado por el porcentaje completado.

Tiempo de solicitud

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

La supervisión aumenta con la AWS CLI y la API

Puedes ver y monitorear la capacidad de almacenamiento del sistema de archivos, aumentar las solicitudes mediante el describe-file-systems AWS CLI comando y la acción de la DescribeFileSystemsAPI. La matriz de `AdministrativeActions` enumera las 10 acciones de actualización más recientes para cada tipo de acción administrativa. Al aumentar la capacidad de almacenamiento de un sistema de archivos, se generan dos `AdministrativeActions`: una acción de `FILE_SYSTEM_UPDATE` y una de `STORAGE_OPTIMIZATION`.

En el siguiente ejemplo se muestra un extracto de la respuesta de un comando de la CLI describe-file-systems. El sistema de archivos tiene una capacidad de almacenamiento de 300 GB y hay una acción administrativa pendiente para aumentar la capacidad de almacenamiento a 1000 GB.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 300,
            "AdministrativeActions": [
                {
                     "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                     "RequestTime": 1581694764.757,
                     "Status": "PENDING",
                     "TargetFileSystemValues": {
                         "StorageCapacity": 1000
                     }
                },
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
                    "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. Esto se muestra en el siguiente extracto de la respuesta de un comando de CLI describe-file-systems.

La propiedad `ProgressPercent` muestra el avance del proceso de optimización del almacenamiento. Una vez que el proceso de optimización del almacenamiento finaliza correctamente, el estado de la acción de `FILE_SYSTEM_UPDATE` cambia a `COMPLETED`, y la acción de `STORAGE_OPTIMIZATION` deja de aparecer.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 1000,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "RequestTime": 1581694764.757,
                    "Status": "UPDATED_OPTIMIZING",
                    "TargetFileSystemValues": {
                        "StorageCapacity": 1000
                }
                },
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
                    "Status": "IN_PROGRESS",
                    "ProgressPercent": 50,
                }
            ]
```

Si se produce un error en el aumento de la capacidad de almacenamiento, el estado de la acción `FILE_SYSTEM_UPDATE` cambia a `FAILED`. La propiedad `FailureDetails` otorga información sobre el error, como se muestra en el siguiente ejemplo.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 300,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "FailureDetails": {
                        "Message": "string"
                    },
                    "RequestTime": 1581694764.757,
                    "Status": "FAILED",
                    "TargetFileSystemValues":
                        "StorageCapacity": 1000
                }
            ]
```

Para obtener información acerca de la solución de acciones fallidas, consulte Las actualizaciones del almacenamiento o la capacidad de rendimiento fallan.

Aumentar la capacidad de almacenamiento de un sistema de archivos FSx para Windows File Server de forma dinámica

Como alternativa a aumentar FSx manualmente la capacidad de almacenamiento del sistema de archivos del servidor de archivos de Windows a medida que aumenta la cantidad de datos almacenados, puede utilizar una AWS CloudFormation plantilla para aumentar el almacenamiento automáticamente. La siguiente solución presentada en esta sección aumenta de manera dinámica la capacidad de almacenamiento de un sistema de archivos cuando la capacidad de almacenamiento libre cae por debajo del umbral definido que especifique.

Esta AWS CloudFormation plantilla implementa automáticamente todos los componentes necesarios para definir el umbral de capacidad de almacenamiento libre, 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 usa los siguientes parámetros:

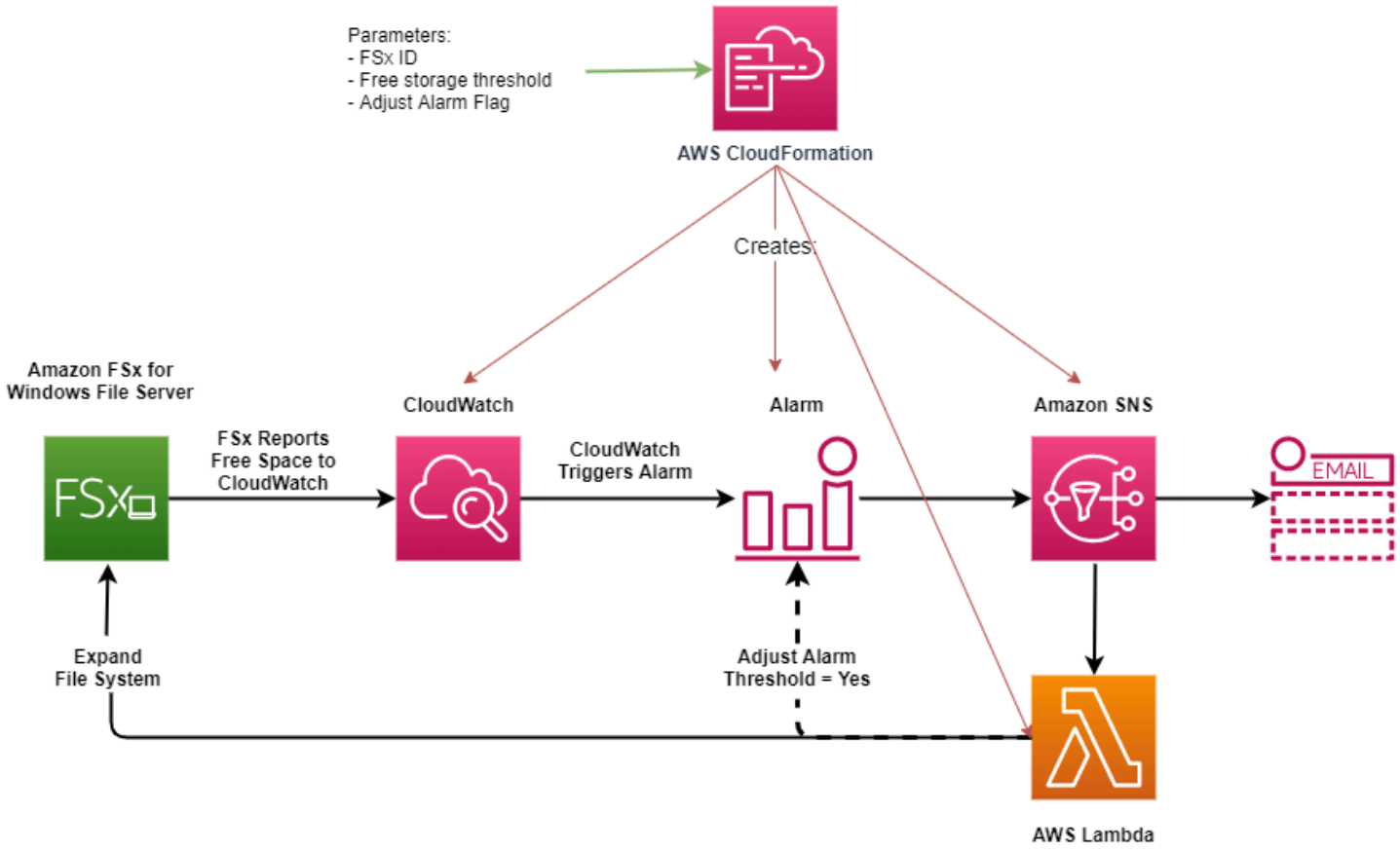
- El ID del sistema de archivos
- El umbral de la capacidad de almacenamiento libre (valor numérico)
- Unidad de medida (porcentaje [predeterminado] o GiB)
- El porcentaje en el que se debe aumentar la capacidad de almacenamiento (%)
- La dirección de correo electrónico de la suscripción a SNS
- Ajuste el umbral de alarma (Sí/No)

Temas

- Información general de la arquitectura
- AWS CloudFormation plantilla
- Implementación automatizada con AWS CloudFormation

Información general de la arquitectura

Al implementar esta solución, se crean los siguientes recursos en la AWS nube.



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 libre del sistema de archivos es inferior al umbral especificado y envía un mensaje a la cola de Amazon SNS.
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. La función de Lambda puede ajustar de manera opcional el umbral de capacidad de almacenamiento libre, para que sea igual a un porcentaje específico de la nueva capacidad de almacenamiento del sistema de archivos.
6. El estado de CloudWatch alarma original y los resultados de las operaciones de la función Lambda se envían a la cola de Amazon SNS.

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

AWS CloudFormation plantilla

Esta solución se utiliza AWS CloudFormation para automatizar la implementación de los componentes que se utilizan para aumentar automáticamente la capacidad de almacenamiento de un sistema de archivos FSx para Windows File Server. Para usar esta solución, descargue la AWS CloudFormation plantilla FSxIncrease Size.

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 libre inicial en base al cual se activa una alarma y se aumenta automáticamente la capacidad de almacenamiento del sistema de archivos, que está especificado en GiB o como porcentaje (%). Cuando se expresa como un porcentaje, la CloudFormation plantilla se vuelve a calcular en GiB para que coincida con CloudWatch la configuración de la alarma.

LowFreeDataStorageCapacityThresholdUnit

Está predeterminada en %. Especifica las unidades para la `LowFreeDataStorageCapacityThreshold`, ya sea en GiB o como porcentaje de la capacidad de almacenamiento actual.

AlarmModificationNotification

Está predeterminada en Sí. Si está establecida en Sí, el `LowFreeDataStorageCapacityThreshold` inicial, se incrementa proporcionalmente al valor de los umbrales de `PercentIncrease` para los umbrales de alarma subsiguientes.

Por ejemplo, cuando `PercentIncrease` se establece en 20 y AlarmModificationNotification se establece en Sí, el umbral de espacio libre disponible (`LowFreeDataStorageCapacityThreshold`) especificado en GiB aumenta un 20% para los eventos de aumento de la capacidad de almacenamiento posteriores.

EmailAddress

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

PercentIncrease

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

Implementación automatizada con AWS CloudFormation

El siguiente procedimiento configura e implementa una AWS CloudFormation pila para aumentar automáticamente la capacidad de almacenamiento de un sistema de archivos FSx para Windows File Server. Tarda alrededor de 5 minutos en implementarse.

> **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.

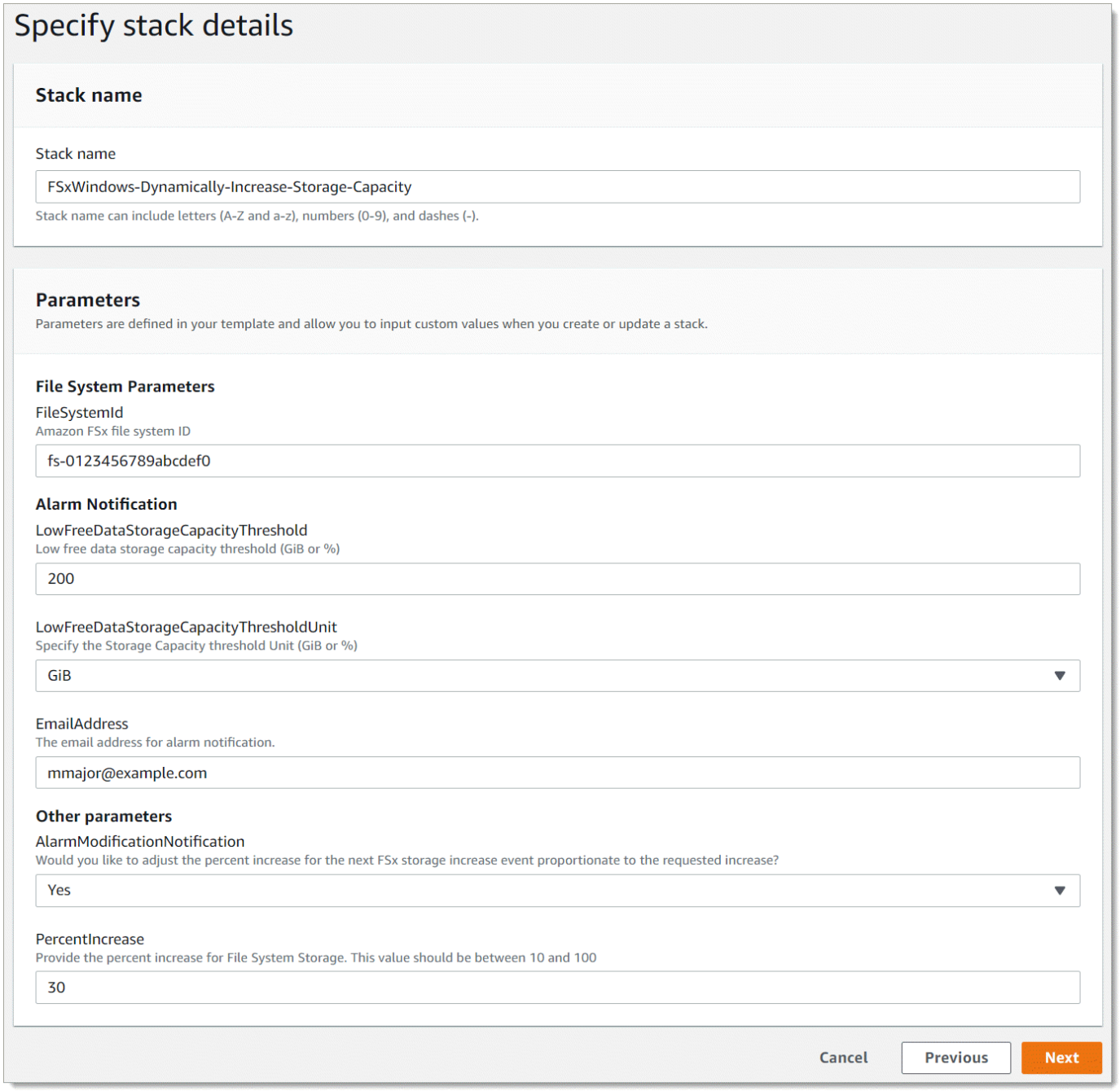
Antes de empezar, debe tener el ID del sistema de FSx archivos de Amazon que se ejecuta en una Amazon Virtual Private Cloud (Amazon VPC) en su AWS cuenta. Para obtener más información sobre la creación de FSx recursos de Amazon, consultePrimeros pasos con Amazon FSx para Windows File Server.

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

1. Descarga la AWS CloudFormation plantilla FSxIncrease Size. 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**
   >
   > 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 Especificar los detalles de la pila, ingrese los valores de la solución de aumento automático de la capacidad de almacenamiento.



3. Establezca un Nombre de pila.
4. En Parámetros, revise los parámetros de la plantilla y modifíquelos para adaptarlos a las necesidades del sistema de archivos. A continuación, elija Siguiente.
5. Ingrese cualquier ajuste de Opciones que desee para la solución personalizada y, luego, elija Siguiente.
6. En Revisar, revise y confirme la configuración. Debe seleccionar la casilla para aceptar que la plantilla crea recursos de IAM.

7. Elija Crear para implementar la pila.

Puede ver el estado de la pila en la AWS CloudFormation consola, en la columna Estado. Debería aparecer el estado CREATE_COMPLETE en alrededor de 5 minutos.

Cómo actualizar 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 .

Actualización del tipo de almacenamiento de un sistema de archivos FSx para Windows

Puede cambiar el tipo de almacenamiento de un sistema de archivos que usa almacenamiento en HDD para usar almacenamiento en SSD. Puedes usar la FSx consola de Amazon, la o la AWS CLI FSx API de Amazon para cambiar el tipo de almacenamiento de un sistema de archivos, tal y como se muestra en los siguientes procedimientos. Para obtener más información, consulte Administrar el tipo de almacenamiento del sistema de archivos.

Para actualizar el tipo de almacenamiento de un sistema de archivos (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 de Windows para el que desee actualizar el tipo de almacenamiento.
3. En Acciones, seleccione Actualizar el tipo de almacenamiento. O bien, en el panel Resumen, seleccione el botón Actualizar situado junto a la unidad de disco duro. Aparece la ventana Actualizar el tipo de almacenamiento.
4. En el tipo de almacenamiento deseado, elija SSD. Seleccione Actualizar para iniciar la actualización del tipo de almacenamiento.

   Puede supervisar el progreso de una actualización del tipo de almacenamiento con la consola y la CLI.

Para actualizar el tipo de almacenamiento de un sistema de archivos (CLI)

Para actualizar el tipo de almacenamiento de un sistema de archivos FSx para Windows File Server, utilice el AWS CLI comando update-file-system. Establezca los siguientes parámetros:

- `--file-system-id` al ID del sistema de archivos que desea actualizar.
- `--storage-type` a SSD. No puede cambiar del tipo de almacenamiento en SSD al tipo de almacenamiento en HDD.

Puede supervisar el progreso de la actualización mediante el AWS CLI comando describe-file-systems. Busque las `administrative-actions` en los resultados.

Para obtener más información, consulte AdministrativeAction.

Supervisión de las actualizaciones de tipos de almacenamiento

Tras actualizar el tipo de almacenamiento de tu sistema de archivos de HDD a SSD, puedes supervisar el progreso de la actualización del tipo de almacenamiento mediante la FSx consola de Amazon AWS CLI, la o la API, tal y como se describe en los siguientes procedimientos.

Supervisión de las actualizaciones del sistema de archivos en la consola

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

Para leer sobre las actualizaciones de los tipos de almacenamiento, puede ver la siguiente información.

Tipo de actualización

El valor posible es Tipo de almacenamiento.

Valor de destino

SSD

Estado

El estado de la actualización vigente. Para las actualizaciones de los tipos de almacenamiento, 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.
- Optimización actualizada: el rendimiento del almacenamiento en SSD está disponible para operaciones de escritura. La actualización pasa a un estado de optimización actualizada, que

normalmente dura unas horas, durante el cual las operaciones de lectura tendrán niveles de rendimiento entre HDD y SSD. Una vez completada la acción de actualización, el rendimiento de la nueva SSD estará disponible tanto para lecturas como para escrituras.

- Finalizado: la actualización del tipo de almacenamiento se completó correctamente.
- Error: no se pudo actualizar el tipo de almacenamiento. Elija el signo de interrogación (?) para ver la información.

% de progreso

Muestra el avance del proceso de optimización del almacenamiento según el porcentaje que se haya completado.

Tiempo de solicitud

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

Supervisar las actualizaciones con la API AWS CLI y

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

Cómo actualizar las IOPS en SSD de un sistema de archivos

En el caso de los sistemas de archivos configurados con almacenamiento en SSD, el nivel de IOPS en SSD aprovisionadas determina la cantidad de E/S del disco disponible cuando el sistema de archivos tiene que leer y escribir datos en el disco, a diferencia de los datos que están en caché. Puede actualizar las IOPS de SSD para un sistema de archivos mediante la FSx consola de Amazon AWS CLI, la o la FSx API de Amazon, tal y como se describe en los siguientes procedimientos. Para obtener más información sobre la administración de IOPS en SSD, consulte Cómo administrar IOPS de SSD.

Para actualizar las IOPS de SSD de un sistema de archivos (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 de Windows para el que desee actualizar las IOPS de SSD.

3. En Acciones, seleccione Actualizar las IOPS de SSD. O bien, en el panel de Resumen, seleccione el botón Actualizar situado junto a las IOPS de SSD aprovisionadas. Se abre la ventana Actualizar el aprovisionamiento de IOPS.
4. En Modo, seleccione Automático o Aprovisionado por el usuario. Si eliges Automático, Amazon aprovisiona FSx automáticamente 3 IOPS de SSD por GiB de capacidad de almacenamiento para tu sistema de archivos. Si elige Aprovisionado por el usuario, ingrese cualquier número entero entre 96 y 400 000.
5. Seleccione Actualizar para iniciar la actualización de las IOPS del SSD aprovisionadas.
6. Puede supervisar el progreso de la actualización en la página de información de los Sistemas de archivos, en la pestaña Actualizaciones.

Para actualizar las IOPS de SSD de un sistema de archivos (CLI)

Para actualizar las IOPS de SSD FSx para un sistema de archivos de Windows File Server, usa la propiedad. `--windows-configuration DiskIopsConfiguration` Esta propiedad tiene dos parámetros, `Iops` y `Mode`:

- Si desea especificar la cantidad de IOPS de SSD`Iops=`*`number_of_IOPS`*, utilice hasta un máximo de 400 000 en AWS las regiones compatibles y. `Mode=USER_PROVISIONED`
- Si quieres que Amazon FSx aumente las IOPS de tu SSD automáticamente, usa `Mode=AUTOMATIC` y no uses el `Iops` parámetro. Amazon mantiene FSx automáticamente 3 IOPS de SSD por GiB de capacidad de almacenamiento en su sistema de archivos, hasta un máximo de 400 000 en AWS las regiones compatibles.

Puede supervisar el progreso de la actualización mediante el AWS CLI comando. describe-file-systems Busque las `administrative-actions` en los resultados.

Para obtener más información, consulte AdministrativeAction.

La supervisión de las actualizaciones de IOPS de SSD aprovisionadas

Tras actualizar la cantidad de IOPS de SSD aprovisionadas para su sistema de archivos, puede supervisar el progreso de la actualización de las IOPS de SSD mediante la FSx consola de Amazon, la y la API AWS CLI, tal y como se describe en los siguientes procedimientos.

Supervisión de las actualizaciones en la consola

En la pestaña Actualizaciones de la ventana de información del sistema de archivos, puede ver las 10 actualizaciones más recientes de cada tipo.

Para ver las actualizaciones de las IOPS de SSD aprovisionadas, puede consultar la siguiente información.

Tipo de actualización

Los valores posibles son el Modo IOPS y las IOPS de SSD.

Valor de destino

El valor deseado para actualizar el modo IOPS del sistema de archivos y las IOPS del SSD.

Estado

El estado de la actualización vigente. Para las actualizaciones de las IOPS de SSD, 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.
- Optimización actualizada: el nuevo nivel de LAS IOPS está disponible para las operaciones de escritura de la carga de trabajo. La actualización pasa a un estado de Optimización actualizada, que suele durar unas horas. Durante este período, las operaciones de lectura de la carga de trabajo tienen un rendimiento de IOPS entre el nivel anterior y el nuevo. Una vez completada la acción de actualización, el nivel nuevo de IOPS estará disponible tanto para lecturas como para escrituras.
- Finalizado: la actualización de las IOPS de la SSD se completó correctamente.
- Error: se produjo un error en la actualización de las IOPS del SSD. Elija el signo de interrogación (?) para ver información sobre la causa de un error en la actualización del almacenamiento.

% de progreso

El progreso del proceso de optimización del almacenamiento se ve reflejado por el porcentaje completado.

Tiempo de solicitud

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

Supervisar las actualizaciones con la API AWS CLI y

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

Cómo administrar la deduplicación de datos

Puede administrar la configuración de deduplicación de datos de su sistema de archivos mediante Amazon FSx CLI para la administración remota en PowerShell. Para obtener más información sobre el uso de la administración remota de Amazon FSx CLI en PowerShell, consulteUso de Amazon FSx CLI para PowerShell.

Los siguientes son los comandos que puede usar para la deduplicación de datos.

Comando de deduplicación de datos	Descripción
Enable-FSxDedup	Permite la deduplicación de datos en el recurso compartido de archivos. La compresión de datos después de la deduplicación está habilitada de forma predeterminada cuando se habilita la deduplicación de datos.
Disable-FSxDedup	Deshabilita la deduplicación de datos en el recurso compartido de archivos.
Get-FSxDedupConfiguration	Recupera la información de configuración de la deduplicación, incluidos el tamaño y la antigüedad mínimos de los archivos para la optimización, los ajustes de compresión y los tipos de archivos y carpetas excluidos.
Set-FSxDedupConfiguration	Cambia los ajustes de configuración de la deduplicación, incluidos el tamaño y la antigüedad mínimos de los archivos para la optimización, los ajustes de compresión y los tipos de archivos y carpetas excluidos.

Comando de deduplicación de datos	Descripción
Get-FSxDedupStatus	Recupera el estado de la desduplicación e incluye propiedad es de solo lectura que describen los ahorros de optimización y el estado del sistema de archivos, los tiempos y el estado de finalización de los últimos trabajos de desduplicación del sistema de archivos.
Get-FSxDedupMetadata	Recupera los metadatos de optimización de la deduplicación.
Update-FSxDedupStatus	Calcula y recupera información actualizada sobre los ahorros en la deduplicación de datos.
Measure-FSxDedupFileMetadata	Mide y recupera el espacio de almacenamiento potencial que puede recuperar en su sistema de archivos si elimina un grupo de carpetas. Los archivos suelen tener fragmentos que se comparten en otras carpetas, y el motor de deduplicación calcula qué fragmentos son únicos y se eliminarían.
Get-FSxDedupSchedule	Recupera los programas de deduplicación que están definidos actualmente.
New-FSxDedupSchedule	Cree y personalice un programa de desduplicación de datos.
Set-FSxDedupSchedule	Cambie los ajustes de configuración de los programas de desduplicación de datos existentes.
Remove-FSxDedupSchedule	Elimine un programa de desduplicación.
Get-FSxDedupJob	Acceda el estado y la información de todos los trabajos de desduplicación actualmente en ejecución o en cola.
Stop-FSxDedupJob	Cancele uno o más trabajos de deduplicación de datos específicos.

La ayuda en línea de cada comando brinda una referencia de todas las opciones de comando. Para acceder a esta ayuda, ejecute el comando con -?, por ejemplo, Enable-FSxDedup -?.

Cómo habilitar la deduplicación de datos

Para habilitar la deduplicación de datos en un recurso compartido de archivos de Amazon FSx for Windows File Server, utilice el siguiente `Enable-FSxDedup` comando.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {Enable-FsxDedup }
```

Al habilitar la deduplicación de datos, se crean una programación y una configuración predeterminadas. Puede crear, modificar y eliminar programaciones y configuraciones mediante los siguientes comandos.

Puede usar el comando `Disable-FSxDedup` para deshabilitar completamente la deduplicación de datos en su sistema de archivos.

Cómo crear un programa de deduplicación de datos

Aunque el programa predeterminado funciona bien en la mayoría de los casos, puede crear un nuevo programa de desduplicación mediante el comando `New-FsxDedupSchedule` que se muestra a continuación. Las programaciones de deduplicación de datos utilizan la hora UTC.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {
New-FSxDedupSchedule -Name "CustomOptimization" -Type Optimization -Days Mon,Wed,Sat -
Start 08:00 -DurationHours 7
}
```

Este comando crea un programa denominado `CustomOptimization` que se ejecuta los lunes, miércoles y sábados, y comienza el trabajo a las 8:00 a. m. (UTC) todos los días, con una duración máxima de 7 horas, después de lo cual el trabajo se detiene si aún se está ejecutando.

Tenga en cuenta que la creación de nuevas programaciones de tareas de deduplicación personalizadas no anula ni elimina la programación predeterminada existente. Antes de crear un trabajo de deduplicación personalizado, puede que desee deshabilitar el trabajo predeterminado si no lo necesita.

Puede deshabilitar el programa de deduplicación predeterminado mediante el comando `Set-FsxDedupSchedule` que se muestra a continuación.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com
 -ConfigurationName FSxRemoteAdmin -ScriptBlock {Set-FSxDedupSchedule -Name
 “BackgroundOptimization” -Enabled $false}
```

Puede eliminar un programa de deduplicación mediante el comando `Remove-FSxDedupSchedule -Name "ScheduleName"`. Tenga en cuenta que el programa `BackgroundOptimization` de deduplicación predeterminado no se puede modificar ni eliminar y, en su lugar, será necesario inhabilitarlo.

Cómo modificar un programa de deduplicación de datos

Puede modificar un programa de deduplicación existente mediante el comando `Set-FsxDedupSchedule` que se muestra a continuación.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {
Set-FSxDedupSchedule -Name "CustomOptimization" -Type Optimization -Days
 Mon,Tues,Wed,Sat -Start 09:00 -DurationHours 9
}
```

Este comando modifica el programa `CustomOptimization` existente para que se ejecute los lunes, miércoles y sábados, y comienza el trabajo a las 9:00 a. m. (UTC) todos los días, con una duración máxima de 9 horas, después de lo cual el trabajo se detiene si aún se está ejecutando.

Para modificar la antigüedad mínima del archivo antes de optimizar la configuración, utilice el comando `Set-FSxDedupConfiguration`.

Cómo visualizar la cantidad de espacio ahorrado

Para ver la cantidad de espacio en disco que está ahorrando al ejecutar la desduplicación de datos, utilice el comando `Get-FSxDedupStatus` siguiente.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FsxRemoteAdmin -ScriptBlock {
Get-FSxDedupStatus } | select
 OptimizedFilesCount,OptimizedFilesSize,SavedSpace,OptimizedFilesSavingsRate

OptimizedFilesCount OptimizedFilesSize SavedSpace OptimizedFilesSavingsRate
------------------- ------------------ ---------- -------------------------
```

```
12587           31163594    25944826                83
```

> **Note**
>
> Los valores que se muestran en la respuesta del comando para los siguientes parámetros no son fiables y no debe utilizarlos: Capacidad FreeSpace, UsedSpace UnoptimizedSize, y SavingsRate.

Cómo solucionar la deduplicación de datos

Use la siguiente información como ayuda para solucionar algunos problemas comunes al configurar y usar la desduplicación de datos.

Temas

- La desduplicación de datos no funciona
- Los valores de desduplicación se establecen en 0 de forma inesperada
- Aunque se eliminan los archivos, no se libera espacio en el sistema de archivos

La desduplicación de datos no funciona

Para ver el estado actual de la deduplicación de datos, ejecute el `Get-FSxDedupStatus` PowerShell comando para ver el estado de finalización de los trabajos de deduplicación más recientes. Si una o más tareas fallan, es posible que no vea un aumento en la capacidad de almacenamiento libre del sistema de archivos.

La razón más común por la que fallan las tareas de desduplicación es la falta de memoria.

- Microsoft recomienda disponer de forma óptima de 1 GB de memoria por cada 1 TB de datos lógicos (o un mínimo de 350 MB por 1 TB de datos lógicos). Usa la tabla de FSx rendimiento de Amazon para determinar la memoria asociada a la capacidad de rendimiento de tu sistema de archivos y asegurarte de que los recursos de memoria son suficientes para el tamaño de tus datos. Si no es así, debe aumentar la capacidad de rendimiento del sistema de archivos hasta un nivel que cumpla con los requisitos de memoria de 1 GB por 1 TB de datos lógicos.
- Las tareas de desduplicación se configuran con la asignación de memoria predeterminada del 25% que recomienda Windows. Esto significa que, para un sistema de archivos con 32 GB de memoria, habrá 8 GB disponibles para la desduplicación. La asignación de memoria es

configurable (mediante el comando `Set-FSxDedupSchedule` con el parámetro `-Memory`). Tenga en cuenta que el uso de una mayor asignación de memoria para la desduplicación puede afectar al rendimiento del sistema de archivos.

- Puede modificar la configuración de las tareas de desduplicación para reducir la cantidad de memoria requerida. Por ejemplo, puede restringir la optimización para que se solo ejecute en tipos de archivos o carpetas específicos, o puede establecer un mínimo para el tamaño y la antigüedad de los archivos que se van a optimizar. También, recomendamos establecer una configuración para que las tareas de desduplicación se ejecuten durante los períodos de inactividad, cuando la carga del sistema de archivos sea mínima.

También, es posible que se produzcan errores si las tareas de desduplicación no tienen tiempo suficiente para completarse. Es posible que tenga que cambiar la duración máxima de las tareas, como se describe en Cómo modificar un programa de deduplicación de datos.

Si las tareas de desduplicación estuvieron fallando durante un tiempo prolongado, y se cambiaron los datos del sistema de archivos durante este período, es posible que las tareas de desduplicación posteriores requieran más recursos para completarse correctamente por primera vez.

Los valores de desduplicación se establecen en 0 de forma inesperada

De manera inesperada, los valores del `SavedSpace` y la `OptimizedFilesSavingsRate` se encuentran en 0, en un sistema de archivos en el cual configuró la desduplicación de datos.

Esto puede ocurrir durante el proceso de optimización del almacenamiento cuando se aumenta la capacidad de almacenamiento del sistema de archivos. Al aumentar la capacidad de almacenamiento de un sistema de archivos, Amazon FSx cancela los trabajos de deduplicación de datos existentes durante el proceso de optimización del almacenamiento, que migra los datos de los discos antiguos a los nuevos discos de mayor tamaño. Amazon FSx reanuda la deduplicación de datos en el sistema de archivos una vez finalizado el trabajo de optimización del almacenamiento. Para obtener más información sobre el aumento de la capacidad de almacenamiento y la optimización, consulte Administrar la capacidad de almacenamiento.

Aunque se eliminan los archivos, no se libera espacio en el sistema de archivos

El comportamiento esperado de la desduplicación de datos es el siguiente: si los datos que se eliminaron eran una forma de ahorro de espacio realizado por la desduplicación, entonces realmente se liberará espacio en el sistema de archivos cuando se ejecute la recopilación de elementos no utilizados.

Una práctica que puede resultarle útil consiste en programar la ejecución de la recopilación de elementos no utilizados para inmediatamente después de eliminar un gran número de archivos. Una vez finalizada la recopilación de elementos no utilizados, puede volver a establecer la programación de dicha recopilación a la configuración original. Esto garantiza que pueda ver el espacio de que generan las eliminaciones de forma inmediata.

Use el siguiente procedimiento para configurar la recopilación de elementos no utilizados para que se ejecute en 5 minutos.

1. Para comprobar que la desduplicación de datos esté habilitada, utilice el comando `Get-FSxDedupStatus`. Para obtener más información acerca del comando y el resultado esperado, consulte Cómo visualizar la cantidad de espacio ahorrado.
2. Utilice lo siguiente para programar la ejecución de la recopilación de elementos no utilizados dentro de 5 minutos.

```
$FiveMinutesFromNowUTC = ((get-date).AddMinutes(5)).ToUniversalTime()
$DayOfWeek = $FiveMinutesFromNowUTC.DayOfWeek
$Time = $FiveMinutesFromNowUTC.ToString("HH:mm")

Invoke-Command -ComputerName ${RPS_ENDPOINT} -ConfigurationName FSxRemoteAdmin -
ScriptBlock {
    Set-FSxDedupSchedule -Name "WeeklyGarbageCollection" -Days $Using:DayOfWeek -
Start $Using:Time -DurationHours 9
}
```

3. Una vez que se haya ejecutado la recopilación de elementos no utilizados, y se haya liberado espacio, restablezca la programación a su configuración original.

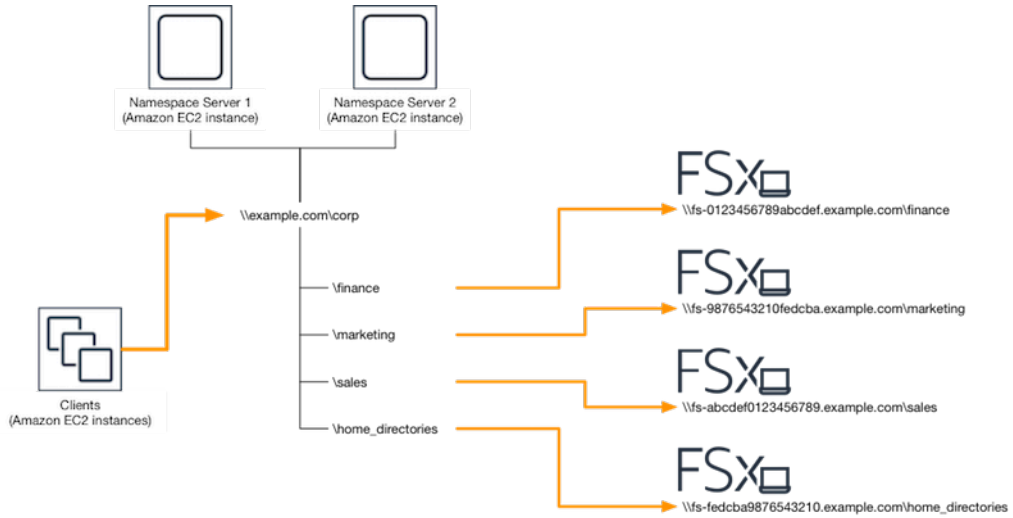
Uso de los espacios de nombres del DFS

Los espacios de nombres del sistema de archivos distribuidos (DFS) son un servicio de roles de Windows Server que se usa para agrupar carpetas compartidas ubicadas en distintos servidores en uno o más espacios de nombres estructurados de forma lógica. Esto permite ofrecer a los usuarios una vista virtual de las carpetas compartidas, en la que una única ruta dirige a los archivos ubicados en varios sistemas de archivos, como se muestra en el siguiente diagrama. Además de organizar y unificar el acceso a los recursos compartidos de archivos en varios sistemas de archivos,

Agrupe varios sistemas FSx de archivos del servidor de archivos de Windows con espacios de nombres DFS

Puede usar los espacios de nombres del Sistema de archivos distribuido (DFS) de Microsoft para agrupar los archivos compartidos en varios FSx sistemas de archivos del servidor de archivos de Windows en una estructura de carpetas o espacio de nombres común. Con los espacios de nombres del DFS, puede escalar el almacenamiento de archivos más allá de la capacidad de almacenamiento máxima de un sistema de archivos (64 TiB) único para conjuntos de datos de archivos grandes, hasta cientos de petabytes. En esta sección se muestra cómo configurar los espacios de nombres DFS en varios sistemas de archivos del servidor de archivos de Windows. FSx

Los espacios de nombres del sistema de archivos distribuidos (DFS) son un servicio de roles de Windows Server que se usa para agrupar carpetas compartidas ubicadas en distintos servidores en uno o más espacios de nombres estructurados de forma lógica. Esto permite ofrecer a los usuarios una vista virtual de las carpetas compartidas, en la que una única ruta dirige a los archivos ubicados en varios sistemas de archivos, como se muestra en el siguiente diagrama. Además de organizar y unificar el acceso a los recursos compartidos de archivos en varios sistemas de archivos,



Para obtener información sobre step-by-step el procedimiento de agrupación de sistemas de archivos FSx de Windows mediante espacios de nombres DFS, consulte. Agrupar varios sistemas de archivos en un único espacio de nombres

Mejora del rendimiento con particiones

El servidor de archivos de Amazon FSx para Windows admite el uso del Sistema de archivos distribuido (DFS) de Microsoft. Al usar los espacios de nombres DFS, puede escalar el rendimiento

(tanto de lectura como de escritura) para atender cargas de trabajo intensivas de E/S al distribuir los datos de sus archivos en varios sistemas de archivos de Amazon. FSx Al mismo tiempo, aún puede presentar una vista unificada en un espacio de nombres común para las aplicaciones. Esta solución implica dividir los datos de los archivos en conjuntos de datos o particiones más pequeños y almacenarlos en diferentes sistemas de archivos. Las aplicaciones que acceden a los datos desde varias instancias pueden alcanzar niveles de rendimiento altos al leer y escribir en estos fragmentos en paralelo.

En el caso de los sistemas de archivos de Windows File Server, puede utilizar la solución incluida Partición de datos mediante los espacios de nombres del DFS para un rendimiento de escalado horizontal para distribuir el acceso de lectura y escritura a sus datos de manera uniforme entre sus múltiples datos. FSx

Agrupar varios sistemas de archivos en un único espacio de nombres

En este procedimiento, creará un único espacio de nombres basado en un dominio (`example.com\corp`) en dos servidores de espacios de nombres, a fin de consolidar los recursos compartidos de archivos almacenados en varios sistemas de archivos de Windows (finanzas, marketing, ventas, FSx home_directories). También configurará cuatro recursos compartidos de archivos en el espacio de nombres, cada uno de los cuales redirigirá a los usuarios de forma transparente a recursos compartidos alojados en sistemas de archivos de Windows independientes. FSx Esto permite a los usuarios acceder a los recursos compartidos de archivos mediante un espacio de nombres común en lugar de tener que especificar los nombres del DNS de cada uno de los sistemas de archivos que alojan los recursos compartidos de archivos.

> **Note**
>
> Amazon FSx no se puede añadir a la raíz de la ruta de acceso compartido de DFS.

Para agrupar varios sistemas de archivos en un espacio de nombres del DFS común

1. Si aún no tiene servidores de espacio de nombres DFS en ejecución, puede lanzar un par de servidores de espacio de nombres DFS de alta disponibilidad mediante la plantilla Setup-DFSN-Servers.template. AWS CloudFormation Para obtener más información sobre la creación de una pila, consulte Creación de una AWS CloudFormation pila en la consola en la Guía del usuario. AWS CloudFormation AWS CloudFormation

2. Conéctese a uno de los servidores del espacio de nombres de DFS iniciado en el paso anterior como usuario del grupo de Administradores delegados de AWS . Para obtener más información, consulte Conectarse a su instancia de Windows en la Guía del EC2 usuario de Amazon.
3. Abra la consola de administración de DFS para acceder a ella. Abra el menú Inicio y ejecute dfsmgmt.msc. Esto abre la herramienta GUI de administración de DFS.
4. Seleccione Acción y, a continuación, Nuevo espacio de nombres, escriba el nombre del equipo del primer servidor de espacio de nombres de DFS que inició como Servidor y, a continuación, seleccione Siguiente.
5. En Nombre, escriba el espacio de nombres que corresponda (por ejemplo, corporación).
6. Seleccione Editar configuración y establezca los permisos adecuados según los requisitos. Elija Next (Siguiente).
7. Deje seleccionada la opción de espacio de nombres predeterminado basado en el dominio, y la opción Habilitar el modo Windows Server 2008, y ,por último, elija Siguiente.

   > **Note**
   >
   > El modo Windows Server 2008 es la opción más reciente que está disponible para los espacios de nombres.

8. Revise la configuración de los espacios de nombres y, a continuación, seleccione Crear.
9. Mantenga seleccionado el espacio de nombre recién creado en Nombres de espacios de la barra de navegación. Luego, elija Acción y, a continuación, Agregar servidor de espacios de nombres.
10. Escriba el nombre del equipo del segundo Servidor de espacio de nombres de DFS que inició para el Servidor de espacio de nombres.
11. Seleccione Editar configuración, establezca los permisos adecuados según los requisitos, y elija Aceptar.
12. Abra el menú contextual (botón derecho) del espacio de nombres que acaba de crear, elija Nueva carpeta, escriba el nombre de la carpeta (por `finance` ejemplo, en Nombre) y pulse Aceptar.
13. Escriba el nombre del DNS del recurso compartido de archivos al que desee que apunte la carpeta del espacio de nombres del DFS en formato UNC (por ejemplo, `\\fs-0123456789abcdef0.example.com\finance`) en Ruta a la carpeta de destino y pulse Aceptar.
14. Si el recurso compartido no existe:

a. Seleccione Sí para crearlo.

b. En el cuadro de diálogo Crear uso compartido, seleccione Examinar.

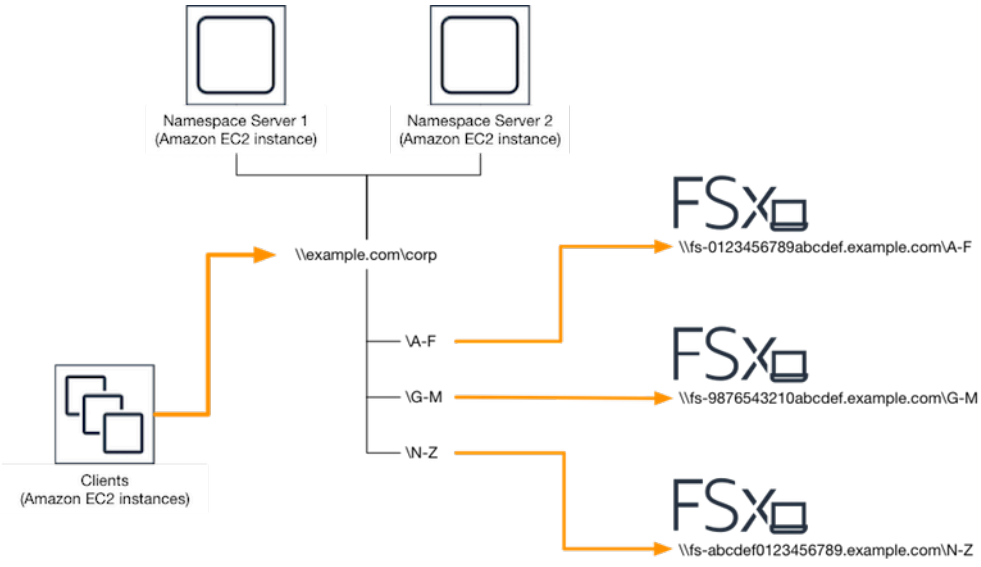
c. Seleccione una carpeta existente o cree una nueva en D$ y elija Aceptar.

d. Defina los permisos de uso compartido adecuados y elija Aceptar.

15. En el cuadro de diálogo Nueva carpeta, seleccione Aceptar. La nueva carpeta se creará en el espacio de nombres.
16. Repita los últimos cuatro pasos para las demás carpetas que desee compartir en el mismo espacio de nombres.

Partición de datos mediante los espacios de nombres del DFS para un rendimiento de escalado horizontal

El siguiente procedimiento lo guía a través de la creación de una solución DFS en Amazon FSx para obtener un rendimiento escalable. En este ejemplo, los datos almacenados en el espacio de *corp* nombres se dividen alfabéticamente. Los archivos de datos “A-F”, “G-M” y “N-Z” se almacenan en diferentes recursos compartidos de archivos. Según el tipo de datos, el tamaño de las E/S y el patrón de acceso a las E/S, usted debe decidir cuál es la mejor manera de particionar los datos en varios recursos compartidos de archivos. Elija una convención de partición que distribuya la E/S de manera uniforme entre todos los recursos compartidos de archivos que vaya a utilizar. Tenga en cuenta que cada espacio de nombres admite hasta 50 000 recursos compartidos de archivos y cientos de petabytes de capacidad de almacenamiento en total.



Cómo configurar los espacios de nombres del DFS para un rendimiento de escalado horizontal

1. Si aún no tiene servidores de espacio de nombres DFS en ejecución, puede lanzar un par de servidores de espacio de nombres DFS de alta disponibilidad mediante la plantilla Setup-DFSN-Servers.template. AWS CloudFormation Para obtener más información sobre la creación de una pila, consulte Creación de una AWS CloudFormation pila en la consola en la Guía del usuario. AWS CloudFormation AWS CloudFormation
2. Conéctese a uno de los servidores del espacio de nombres de DFS iniciado en el paso anterior como usuario del grupo de Administradores delegados de AWS . Para obtener más información, consulte Conectarse a su instancia de Windows en la Guía del EC2 usuario de Amazon.
3. Acceda a la consola de administración del DFS. Abra el menú Inicio y ejecute dfsmgmt.msc. Esto abre la herramienta GUI de administración de DFS.
4. Seleccione Acción y, a continuación, Nuevo espacio de nombres, escriba el nombre del equipo del primer servidor de espacio de nombres de DFS que inició como Servidor y, a continuación, seleccione Siguiente.
5. En Nombre, escriba el espacio de nombres que corresponda (por ejemplo, corporación).
6. Seleccione Editar configuración y establezca los permisos adecuados según los requisitos. Elija Next (Siguiente).
7. Deje seleccionada la opción de espacio de nombres predeterminado basado en el dominio, y la opción Habilitar el modo Windows Server 2008, y ,por último, elija Siguiente.

   > **Note**
   >
   > El modo Windows Server 2008 es la opción más reciente que está disponible para los espacios de nombres.

8. Revise la configuración de los espacios de nombres y, a continuación, seleccione Crear.
9. Mantenga seleccionado el espacio de nombre recién creado en Nombres de espacios de la barra de navegación. Luego, elija Acción y, a continuación, Agregar servidor de espacios de nombres.
10. Escriba el nombre del equipo del segundo Servidor de espacio de nombres de DFS que inició para el Servidor de espacio de nombres.
11. Seleccione Editar configuración, establezca los permisos adecuados según los requisitos, y elija Aceptar.

12. Abra el menú contextual (botón derecho) del espacio de nombres que acaba de crear, elija Nueva carpeta, escriba el nombre de la carpeta de la primera partición (por `A-F` ejemplo, en Nombre) y pulse Añadir.
13. Escriba el nombre del DNS del recurso compartido de archivos que aloja esta partición en formato UNC (por ejemplo`\\fs-0123456789abcdef0.example.com\A-F`) en Ruta a la carpeta de destino y elija Aceptar.
14. Si el recurso compartido no existe:
    a. Seleccione Sí para crearlo.
    b. En el cuadro de diálogo Crear uso compartido, seleccione Examinar.
    c. Seleccione una carpeta existente o cree una nueva en D$ y elija Aceptar.
    d. Defina los permisos de uso compartido adecuados y elija Aceptar.
15. Ahora que ya añadió la carpeta de destino de la partición, elija Aceptar.
16. Repita los últimos cuatro pasos para las demás particiones que desee agregar al mismo espacio de nombres.

Administración de la capacidad de rendimiento

Puede aumentar o disminuir la capacidad de rendimiento del sistema de archivos para gestionar su rendimiento en cualquier momento. La capacidad de rendimiento es una de las dimensiones que determina la velocidad a la que el servidor de archivos que aloja el sistema de archivos FSx del servidor de archivos de Windows puede almacenar los datos. Los niveles más altos de capacidad de rendimiento también vienen con niveles más altos de operaciones de E/S por segundo (IOPS) y más memoria para el almacenamiento en caché en el servidor de archivos. Para obtener más información, consulte FSx para el rendimiento del servidor de archivos de Windows.

Temas

- Cómo funciona el escalado del rendimiento
- Saber cuándo modificar la capacidad de rendimiento
- Modificación de la capacidad de rendimiento
- Supervisión de las actualizaciones de capacidad de rendimiento

Cómo funciona el escalado del rendimiento

Cuando modificas la capacidad de procesamiento de tu sistema de archivos, Amazon FSx cambia el servidor de archivos del sistema de archivos por uno con más o menos rendimiento entre bastidores. En el caso de los sistemas de archivos Multi-AZ, el cambio a un nuevo servidor de archivos desencadena una conmutación por error y una recuperación automáticas, mientras que Amazon FSx cambia el servidor de archivos preferido y el secundario. Los sistemas de archivos Single-AZ estarán disponible durante unos minutos mientras se intercambia el servidor de archivos durante el escalado de la capacidad de rendimiento. Se le facturará la nueva cantidad de capacidad de rendimiento una vez que esté disponible para el sistema de archivos.

> **Note**
>
> Durante una operación de mantenimiento en el back end, es posible que se retrasen las modificaciones del sistema (incluidas las modificaciones a la capacidad de rendimiento). Las operaciones de mantenimiento pueden provocar que las modificaciones del sistema se pongan en cola para ser procesadas.

En el caso de los sistemas de archivos Multi-AZ, el escalado de la capacidad de rendimiento produce una conmutación por error y una recuperación automáticas, mientras que FSx Amazon cambia el servidor de archivos preferido y el secundario. Durante las sustituciones de servidores de archivos, que se producen durante la ampliación de la capacidad de procesamiento, así como durante el mantenimiento del sistema de archivos y una interrupción imprevista del servicio, cualquier tráfico continuo al sistema de archivos será atendido por el servidor de archivos restante. Cuando el servidor de archivos reemplazado vuelva a estar en línea, FSx para Windows ejecutará un trabajo de resincronización para garantizar que los datos se vuelvan a sincronizar con el servidor de archivos recién reemplazado.

FSx para Windows está diseñado para minimizar el impacto de esta actividad de resincronización en la aplicación y los usuarios. Sin embargo, el proceso de resincronización implica sincronizar datos en bloques grandes. Esto significa que un bloque de datos grande puede requerir que se sincronicen aunque solo se actualice una pequeña parte. Por lo tanto, la cantidad de resincronización depende no solo de la cantidad de pérdida de datos, sino también de la naturaleza de tal pérdida en el sistema de archivos. Si su carga de trabajo contiene muchas escrituras e IOPS, el proceso de sincronización de datos puede tardar más y requerir recursos de rendimiento adicionales.

El sistema de archivos seguirá disponible durante este tiempo, pero, para reducir la duración de la sincronización de datos, le recomendamos que modifique la capacidad de rendimiento durante los períodos de inactividad, ya que la carga del sistema de archivos es mínima. También, le recomendamos asegurarse de que el sistema de archivos tenga una capacidad de rendimiento suficiente para ejecutar la sincronización además de la carga de trabajo, a fin de reducir la duración de la sincronización de datos. Por último, le recomendamos probar las repercusiones de las conmutaciones por error mientras el sistema de archivos tenga una carga más ligera.

Saber cuándo modificar la capacidad de rendimiento

Amazon FSx se integra con Amazon CloudWatch, lo que le permite supervisar los niveles de uso del rendimiento continuo de su sistema de archivos. El desempeño (rendimiento e IOPS) que puede usar el sistema de archivos depende de las características específicas de la carga de trabajo, además de la capacidad de rendimiento, la capacidad de almacenamiento y el tipo de almacenamiento del sistema de archivos. Puede utilizar CloudWatch las métricas para determinar cuáles de estas dimensiones debe cambiar para mejorar el rendimiento. Para obtener más información, consulte Monitorización con Amazon CloudWatch.

FSx para Windows File Server proporciona alertas de rendimiento basadas en los valores de CloudWatch las métricas de su sistema de archivos en el panel de supervisión y rendimiento de la página de detalles del sistema de archivos de la FSx consola de Amazon. Esto incluye la capacidad de rendimiento y otras métricas del sistema de archivos que pueden beneficiarse del aumento de la capacidad de rendimiento. Para obtener más información, consulte Advertencias y recomendaciones de rendimiento.

Configure su sistema de archivos con una capacidad de rendimiento suficiente para satisfacer no solo el tráfico esperado de su carga de trabajo, sino también los recursos de rendimiento adicionales necesarios para admitir las funciones que habilita en su sistema de archivos. Por ejemplo, si está ejecutando la deduplicación de datos, la capacidad de rendimiento que seleccione debe proporcionar suficiente memoria para ejecutar la deduplicación en función del almacenamiento del que disponga. Si utiliza copias de redundancia, aumente la capacidad de rendimiento hasta un valor que sea al menos tres veces superior al valor que se espera que genere su carga de trabajo para evitar que Windows Server elimine las copias de redundancia. Para obtener más información, consulte Impacto de la capacidad de rendimiento en el rendimiento.

Modificación de la capacidad de rendimiento

Puede aumentar o disminuir la capacidad de procesamiento de su sistema de archivos mediante la FSx consola de Amazon, la AWS Command Line Interface (AWS CLI) o la FSx API de Amazon, tal y como se describe en los siguientes procedimientos.

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 Sistemas de archivos y elija el sistema de archivos de Windows para el que desee aumentar la capacidad de rendimiento.
3. En Acciones, seleccione Actualizar rendimiento.

   O bien, en el panel Resumen, seleccione Actualizar junto a la capacidad de rendimiento del sistema de archivos.

   Aparece la ventana Actualizar la capacidad de rendimiento.
4. Seleccione el valor nuevo para la capacidad de rendimiento de la lista.
5. Seleccione Actualizar para iniciar la actualización de la capacidad de rendimiento.

   > **Note**
   >
   > Los sistemas de archivos Multi-AZ realizan conmutaciones por error y por recuperación cuando actualiza el escalado del rendimiento y están totalmente disponibles. Los sistemas de archivos Single-AZ experimentan un período de inactividad muy breve durante la actualización.
6. Puede supervisar el progreso de la actualización en la página de información de los Sistemas de archivos, en la pestaña Actualizaciones.

   Puedes monitorizar el progreso de la actualización mediante la FSx consola de Amazon AWS CLI, la y la API. Para obtener más información, consulte Supervisión de las actualizaciones de capacidad de rendimiento.

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

Para aumentar o disminuir 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; los valores válidos son 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4608, 6144, 9216, 12288. MBps

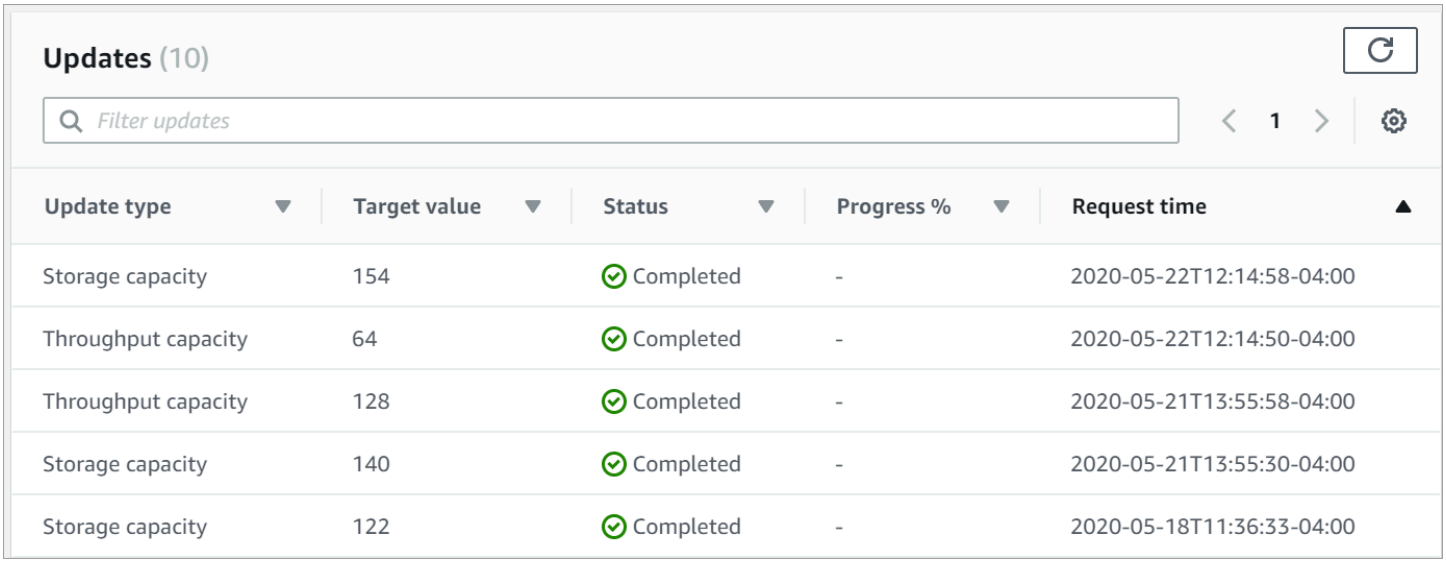
Puedes monitorizar el progreso de la actualización mediante la FSx consola de Amazon AWS CLI, la y la API. Para obtener más información, consulte Supervisión de las actualizaciones de capacidad de rendimiento.

Supervisión de las actualizaciones de 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.

Supervisión de los cambios en la capacidad de rendimiento en la consola

En la pestaña Actualizaciones de la ventana de Información del sistema de archivos, puede ver las 10 acciones de actualización más recientes de cada tipo de acción de actualización.



Para ver las acciones de actualización de la capacidad de rendimiento, puede consultar la siguiente información.

Tipo de actualización

El valor posible es la Capacidad de rendimiento.

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.
- Optimización actualizada: Amazon FSx ha actualizado los recursos de E/S de red, CPU y memoria del sistema de archivos. El nuevo nivel de rendimiento de E/S de disco está disponible para las operaciones de escritura. En las operaciones de lectura, el rendimiento de E/S del disco se situará entre el nivel anterior y el nuevo hasta que el sistema de archivos deje de estar en este estado.
- Finalizado: la actualización de la capacidad de rendimiento se completó correctamente.
- Error: se produjo un error en la actualización de la capacidad de rendimiento. Elija el signo de interrogación (?) para ver detalles sobre el motivo por el que se produjo un error en la actualización del rendimiento.

Tiempo de solicitud

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

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-systemsCLI y la acción de la DescribeFileSystemsAPI. La matriz de `AdministrativeActions` enumera las 10 acciones de actualización más recientes para cada tipo de acción administrativa. Al modificar la capacidad de rendimiento de un sistema de archivos, se genera una acción administrativa de `FILE_SYSTEM_UPDATE`.

En el siguiente ejemplo se muestra un extracto de la respuesta de un comando de la CLI `describe-file-systems`. El sistema de archivos tiene una capacidad de rendimiento de 8 MBps y la capacidad de rendimiento objetivo de 256. MBps

```
.
```

```
.
.
    "ThroughputCapacity": 8,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "WindowsConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

Cuando Amazon FSx termine de procesar la acción correctamente, el estado cambiará 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": {
          "WindowsConfiguration": {
            "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. Para obtener información acerca de la solución de acciones fallidas, consulte Las actualizaciones del almacenamiento o la capacidad de rendimiento fallan.

Etiquetar tus recursos de Amazon FSx

Para ayudarle a administrar sus sistemas de archivos y otros FSx recursos del servidor de archivos de Windows, puede asignar sus propios metadatos a cada recurso en forma de etiquetas. Las etiquetas le permiten clasificar AWS los recursos de diferentes maneras, por ejemplo, por propósito, propietario o entorno. Esto es útil cuando tiene muchos recursos del mismo tipo: puede identificar rápidamente un recurso específico en función de las etiquetas que le haya asignado. En este tema se describe qué son las etiquetas y cómo crearlas.

Temas

- Conceptos básicos de etiquetas
- Cómo etiquetar los recursos
- Restricciones de las etiquetas
- Permisos obligatorios para etiquetar recursos

Conceptos básicos de etiquetas

Una etiqueta es una etiqueta que se asigna a un AWS recurso. Cada etiqueta está formada por una clave y un valor opcional, ambos definidos por el usuario.

Las etiquetas te permiten 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 archivos de Windows File Server de FSx tu cuenta que te ayude a realizar un seguimiento del propietario y del 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 eficaz de etiquetado de recursos, consulta el AWS documento técnico Mejores prácticas de etiquetado.

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. 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 usa la API de servidor FSx de archivos de Windows, la AWS CLI o un AWS SDK, puede usar la acción de la `TagResource` API para aplicar etiquetas a los recursos existentes. Además, algunas acciones de creación de recursos le permiten especificar etiquetas para un recurso al crear dicho recurso. Si no se pueden aplicar etiquetas durante la creación del recurso, el proceso de creación del recurso se revierte. Esto garantiza que los recursos se creen con etiquetas o, de lo contrario, no se creen y que ningún recurso se quede jamás sin etiquetar. Al etiquetar los recursos en el momento de su creación, se eliminar la necesidad de ejecutar scripts de etiquetado personalizados tras la creación del recurso. Para obtener más información acerca de cómo habilitar a los usuarios para etiquetar recursos al crearlos, consulte Conceder permisos para etiquetar recursos durante la creación.

Cómo etiquetar los recursos

Puedes etiquetar FSx los recursos del servidor de archivos de Windows 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. La consola puede organizar los recursos según la etiqueta de nombre, pero esta etiqueta no tiene ningún significado semántico FSx para el servicio de servidor de archivos de Windows.

Puede aplicar permisos a nivel de recursos basados en etiquetas en sus políticas de IAM a las acciones de la API del servidor de archivos de Windows que admiten el etiquetado en el momento de la creación FSx para implementar un control pormenorizado sobre los usuarios y grupos que pueden etiquetar los recursos en el momento de la creación. Sus recursos están debidamente protegidos frente a la creación; las etiquetas se aplican inmediatamente a los recursos, por lo que cualquier permiso de nivel de recursos basado en etiquetas que controle el uso de los recursos es efectivo inmediatamente. Se puede realizar un seguimiento y un registro más precisos de los recursos. Puede establecer el etiquetado obligatorio de los nuevos recursos y controlar qué claves y valores de etiquetas se usan en ellos.

También puede aplicar permisos a nivel de recursos a las acciones de la API del servidor de archivos de Windows `TagResource` y a las mismas en sus políticas de IAM `UntagResource` FSx para controlar qué valores y claves de etiquetas se configuran en los recursos existentes.

Para obtener más información acerca del etiquetado de recursos para facturación, consulte Uso de etiquetas de asignación de costos en la Guía del usuario de AWS Billing .

Restricciones de las etiquetas

Se aplican las siguientes restricciones básicas a las etiquetas:

- Número máximo de etiquetas por recurso: 50
- Para cada recurso, cada clave de etiqueta debe ser única y solo puede tener un valor.
- Longitud máxima de la clave: 128 caracteres Unicode en UTF-8
- Longitud máxima del valor: 256 caracteres Unicode en UTF-8
- Los caracteres permitidos FSx para las etiquetas del servidor de archivos de Windows son: letras, números y espacios representables en UTF-8, y los siguientes caracteres: + - =. _:/@.
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas.
- El `aws:` prefijo está reservado para su uso. AWS Si la etiqueta tiene una clave de etiqueta con este prefijo, no puede editar ni eliminar la clave o el valor de la etiqueta. Las etiquetas que tengan el prefijo `aws:` no cuentan para el límite de etiquetas por recurso.

No puede eliminar un recurso basándose únicamente en sus etiquetas; debe especificar el identificador del recurso. Por ejemplo, para eliminar un sistema de archivos etiquetado con una clave de etiqueta llamada `DeleteMe`, debe utilizar la acción `DeleteFileSystem` con el identificador de recurso del sistema de archivos, como fs-1234567890abcdef0.

Al etiquetar recursos públicos o compartidos, las etiquetas que asigne están disponibles solo para usted Cuenta de AWS; ninguna otra persona Cuenta de AWS tendrá 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 obligatorios para etiquetar recursos

Para obtener más información sobre los permisos necesarios para etiquetar los FSx recursos de Amazon en el momento de la creación, consulteConceder 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, consulteUso de etiquetas para controlar el acceso a tus FSx recursos de Amazon.

Actualice un sistema de archivos mediante AWS CLI

Hay tres elementos que puede actualizar siguiendo los procedimientos de esta explicación. Todos los demás elementos del sistema de archivos que desee actualizar lo puede hacer desde la consola.

En estos procedimientos se presupone que la tiene AWS CLI instalada y configurada en su equipo local. Para obtener más información, consulte la Instalar y Configurar en la Guía del usuario de AWS Command Line Interface .

- AutomaticBackupRetentionDays— el número de días que desea conservar las copias de seguridad automáticas para su sistema de archivos.
- DailyAutomaticBackupStartTime— la hora del día en hora universal coordinada (UTC) en la que desea que comience la ventana 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.
- WeeklyMaintenanceStartTime— 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.

Los siguientes procedimientos describen cómo actualizar el sistema de archivos con la AWS CLI.

Cómo actualizar el tiempo por el que se retienen las copias de seguridad automáticas del sistema de archivos

1. Abra el símbolo del sistema o el terminal en su equipo.
2. Ejecute el siguiente comando y sustituya el identificador del sistema de archivos por el identificador de su sistema de archivos y el número de días por el que desea retener las copias de seguridad automáticas.

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration AutomaticBackupRetentionDays=30
```

Cómo actualizar el período de copia de seguridad diaria del sistema de archivos

1. Abra el símbolo del sistema o el terminal en su equipo.
2. Ejecute el siguiente comando y sustituya el ID del sistema de archivos por el ID de su sistema de archivos y la hora en que desea iniciar el período.

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration DailyAutomaticBackupStartTime=01:00
```

Cómo actualizar el período de mantenimiento semanal del sistema de archivos

1. Abra el símbolo del sistema o el terminal en su equipo.
2. Ejecute el siguiente comando y sustituya el ID del sistema de archivos por el ID de su sistema de archivos y la fecha y la hora en las que desee iniciar el período.

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration WeeklyMaintenanceStartTime=1:01:30
```

Cómo proteger los datos con copias de seguridad, copias de redundancia y replicación programada

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

- FSx Las copias de seguridad nativas de Amazon respaldan sus necesidades de retención y cumplimiento de las copias de seguridad dentro de Amazon FSx.
- AWS Backup las copias de seguridad de sus sistemas de FSx archivos de Amazon forman parte de una solución de copia de seguridad centralizada y automatizada en todos AWS los servicios en la nube y en las instalaciones.
- Las copias de redundancia de Windows permiten a los usuarios deshacer fácilmente los cambios en los archivos y comparar las versiones de los archivos mediante la restauración de los archivos a versiones anteriores.
- AWS DataSync la replicación programada de su sistema de FSx archivos de Amazon en un segundo sistema de archivos proporciona protección y recuperación de datos.

Temas

- Protección de los datos con copias de seguridad
- Protección de los datos con copias de redundancia
- Replicación programada mediante AWS DataSync

Protección de los datos con copias de seguridad

Puede proteger los datos de su sistema de archivos del servidor FSx de archivos de Windows realizando copias de seguridad periódicas del sistema de archivos. Amazon te FSx ofrece varias opciones para realizar copias de seguridad de tus sistemas de archivos. Puede usar copias de seguridad diarias automáticas para realizar una copia de seguridad todos los días. Puede realizar una copia de seguridad iniciada por el usuario a partir del sistema de archivos en cualquier momento. También puede utilizarlos AWS Backup como parte de una solución de copia de seguridad centralizada para sus AWS recursos. Estas soluciones de copia de seguridad pueden ayudarlo a cubrir sus necesidades de retención de datos, de empresa y de cumplimiento.

Le recomendamos que utilice las copias de seguridad diarias automáticas que están habilitadas de forma predeterminada en su sistema de archivos y que utilice una solución AWS Backup de copia de seguridad centralizada en todos los sistemas Servicios de AWS. AWS Backup le permite configurar planes de respaldo adicionales con diferentes frecuencias (por ejemplo, varias veces al día, diariamente o semanalmente) y períodos de retención diferentes.

Con Amazon FSx file-system-consistent, las copias de seguridad son muy duraderas e incrementales. Cada copia de seguridad contiene toda la información necesaria para crear un nuevo sistema de archivos y restaurar de forma efectiva una point-in-time instantánea del sistema de archivos. Para garantizar la coherencia del sistema de archivos, Amazon FSx utiliza el Volume Shadow Copy Service (VSS) de Microsoft Windows. Para garantizar una alta durabilidad, Amazon FSx almacena las copias de seguridad en Amazon Simple Storage Service (Amazon S3).

Las FSx copias de seguridad de Amazon son incrementales, ya sea que se generen mediante la función de copia de seguridad diaria automática o la función de copia de seguridad iniciada por el usuario. Esto significa que solo se guardan los datos del sistema de archivos que han cambiado luego de la copia de seguridad más reciente. Esto disminuye el tiempo necesario para crear la copia, y ahorra costos de almacenamiento, ya que no se duplican los datos.

En algún momento del proceso de la copia de seguridad, es posible que la E/S del almacenamiento se suspenda brevemente, por lo general durante unos segundos. Como el servicio VSS necesita vaciar cualquier escritura de la caché en el disco antes de reanudar la E/S, la pausa puede prolongarse si la carga de trabajo tiene una gran cantidad de operaciones de escritura por segundo (`DataWriteOperations`). La mayoría de los usuarios finales y las aplicaciones experimentarán esta suspensión de E/S como una breve pausa de E/S. Es posible que las aplicaciones tengan una sensibilidad diferente a los ajustes de tiempo de espera según cómo estén configuradas.

Crear copias de seguridad periódicas para su sistema de archivos es una práctica recomendada que complementa la replicación que Amazon FSx for Windows File Server realiza para su sistema de archivos. FSx Las copias de seguridad de Amazon ayudan a satisfacer sus necesidades de cumplimiento y retención de copias de seguridad. Trabajar con las FSx copias de seguridad de Amazon es fácil, ya sea para crear copias de seguridad, copiar una copia de seguridad, restaurar un sistema de archivos a partir de una copia de seguridad o eliminar una copia de seguridad. Tenga en cuenta que para ver el uso de una copia de seguridad de un solo sistema de archivos, necesitará habilitar las etiquetas de esa copia de seguridad específica, y habilitar los informes de facturación basados en etiquetas.

Temas

- Trabajo con copias de seguridad diarias automáticas
- Trabajo con copias de seguridad iniciadas por el usuario
- Uso AWS Backup con Amazon FSx
- Copiar copias de seguridad
- Restauración de copias de seguridad en un nuevo sistema de archivos
- Crear copias de seguridad iniciadas por el usuario
- Eliminación de copias de seguridad
- Tamaño de las copias de seguridad
- Replicar copias de seguridad dentro de la misma cuenta
- Restauración de una copia de seguridad en un nuevo sistema de archivos

Trabajo con copias de seguridad diarias automáticas

De forma predeterminada, Amazon FSx realiza una copia de seguridad automática diaria de tu sistema de archivos. Estas copias de seguridad diarias automáticas se producen durante el período de copias de seguridad diarias que se estableció al crear el sistema de archivos. Al elegir la ventana de copia de seguridad diaria, le recomendamos que elija una hora del día que le resulte conveniente y que esté fuera del horario normal de funcionamiento de las aplicaciones que utilizan el sistema de archivos. También recomendamos elegir un período de copia de seguridad fuera del período de mantenimiento, ya que es posible que las copias de seguridad automatizadas no se realicen si el sistema de archivos está realizando un mantenimiento continuo.

Las copias de seguridad diarias automáticas se guardan durante un período de tiempo determinado, conocido como período de retención. Al crear un sistema de archivos en la FSx consola de Amazon, el período de retención diario automático predeterminado de las copias de seguridad es de 30 días. El período de retención predeterminado es diferente en la FSx API y la CLI de Amazon. Puede asignar al período de retención de copia de seguridad un valor de entre 0 días y 90 días. Si se establece que el período de retención sea 0 (cero) días, se desactivan las copias de seguridad automáticas y diarias. Si se elimina el sistema de archivos, también se eliminan las copias de seguridad automáticas y diarias.

> **Note**
>
> Si se establece el período de retención en 0 días, nunca se realizará una copia de seguridad automática del sistema de archivos. Le recomendamos encarecidamente que utilice copias

de seguridad diarias automáticas para los sistemas de archivos que tengan algún nivel de funcionalidad crítica asociado.

Puede usar uno de ellos AWS SDKs para cambiar la ventana de respaldo y el período de retención de la copia de seguridad de sus sistemas de archivos. AWS CLI Utilice la operación API `UpdateFileSystem` o el comando CLI `update-file-system`. Para obtener más información, consulte Actualice un sistema de archivos mediante AWS CLI.

> **Important**
>
> Si se reduce el período de retención de las copias de seguridad automáticas diarias, se eliminarán permanentemente las copias de seguridad fuera del nuevo período de retención. Asegúrese de que ya no necesita estas copias de seguridad antiguas antes de continuar.

Trabajo con copias de seguridad iniciadas por el usuario

Con Amazon FSx, puedes realizar copias de seguridad manuales de tus sistemas de archivos en cualquier momento. Puedes hacerlo mediante la FSx consola de Amazon, la API o AWS Command Line Interface (AWS CLI). Las copias de seguridad de los sistemas de FSx archivos de Amazon iniciadas por los usuarios nunca caducan y están disponibles durante el tiempo que desees conservarlas. Las copias de seguridad iniciadas por los usuarios se conservan incluso después de eliminar el sistema de archivos del que se hizo la copia de seguridad. Solo puede eliminar las copias de seguridad iniciadas por el usuario mediante la FSx consola, la API o la CLI de Amazon. Amazon nunca los elimina automáticamente FSx. Para obtener más información, consulte Eliminación de copias de seguridad.

Si se inicia una copia de seguridad mientras se está modificando el sistema de archivos (por ejemplo, durante una actualización de la capacidad de rendimiento o durante el mantenimiento del sistema), la solicitud de copia de seguridad queda en cola y se reanudará cuando se complete la actividad.

Para obtener información sobre cómo realizar copias de seguridad iniciadas por el usuario a partir de los sistemas de archivos, consulte Crear copias de seguridad iniciadas por el usuario.

Uso AWS Backup con Amazon FSx

AWS Backup es una forma sencilla y rentable de proteger sus datos mediante la realización de copias de seguridad de los sistemas de FSx archivos de Amazon. AWS Backup es un servicio de

copias de seguridad unificado diseñado para simplificar la creación, copia, restauración y eliminación de copias de seguridad y, al mismo tiempo, mejorar la elaboración de informes y la auditoría. AWS Backup facilita el desarrollo de una estrategia de respaldo centralizada para garantizar el cumplimiento legal, reglamentario y profesional. AWS Backup también simplifica la protección AWS de sus volúmenes de almacenamiento, bases de datos y sistemas de archivos al proporcionar un lugar central donde puede hacer lo siguiente:

- Configure y audite los AWS recursos de los que desea hacer una copia de seguridad.
- Automatizar la programación de copias de seguridad.
- Establecer políticas de retención.
- Copie las copias de seguridad en todas AWS las regiones y AWS cuentas.
- 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 realizadas desde la AWS Backup consola tienen el mismo nivel de coherencia y rendimiento del sistema de archivos, y las mismas opciones de restauración que las copias de seguridad realizadas a través de la FSx consola de Amazon. Las copias de seguridad de AWS Backup las que se toman son incrementales en relación con cualquier otra FSx copia de seguridad de Amazon que realices, ya sea iniciada por el usuario o automática.

Si se utilizan AWS Backup para gestionar estas copias de seguridad, se obtienen funciones adicionales, como opciones de retención ilimitadas y la posibilidad de crear copias de seguridad programadas con una frecuencia de hasta una hora. Además, AWS Backup conserva las copias de seguridad inmutables incluso después de eliminar el sistema de archivos de origen. Esto protege contra la eliminación accidental o malintencionada.

Las copias de seguridad realizadas por se AWS Backup consideran copias de seguridad iniciadas por el usuario y se incluyen en la cuota de copias de seguridad iniciadas por el usuario de Amazon. FSx Puede ver y restaurar las copias de seguridad realizadas AWS Backup en la FSx consola, la CLI y la API de Amazon. Sin embargo, no puedes eliminar las copias de seguridad realizadas AWS Backup en la FSx consola, la CLI o la API de Amazon. Para obtener más información sobre cómo AWS Backup realizar copias de seguridad de los sistemas de FSx archivos de Amazon, consulte Trabajar con Amazon FSx File Systems en la Guía para AWS Backup desarrolladores.

Copiar copias de seguridad

Puedes usar Amazon FSx para copiar manualmente las copias de seguridad de la misma AWS cuenta a otra AWS región (copias entre regiones) o dentro de la misma AWS región (copias dentro de la región). Solo puede realizar copias entre regiones dentro de la misma partición. AWS Puedes crear copias de seguridad iniciadas por el usuario mediante la FSx consola o la API de Amazon. AWS CLI Cuando crea una copia de seguridad iniciada por el usuario, tiene el tipo`USER_INITIATED`.

También puedes utilizarlas AWS Backup para copiar copias de seguridad entre AWS regiones y AWS cuentas. AWS Backup es un servicio de administración de copias de seguridad totalmente gestionado que proporciona una interfaz central para los planes de copia de seguridad basados en políticas. Con la gestión entre cuentas, puede utilizar automáticamente políticas de copia de seguridad para aplicar planes de copia de seguridad en las cuentas de su organización.

Las copias de seguridad entre regiones son particularmente valiosas para la recuperación de desastres entre regiones. Las copias de seguridad se toman y se copian en otra AWS región para, en caso de que se produzca un desastre en la AWS región principal, poder restaurarlas a partir de las copias de seguridad y recuperar rápidamente la disponibilidad en la otra AWS región. También puede utilizar copias de seguridad para clonar el conjunto de datos de archivos en otra AWS región o dentro de la misma AWS región. Puede realizar copias de seguridad en la misma AWS cuenta (entre regiones o dentro de una región) mediante la FSx consola de Amazon o la AWS CLI API de Amazon FSx . También puede utilizar AWS Backup para realizar copias de seguridad, a pedido o en función de políticas.

Las copias de seguridad entre cuentas son valiosas para acatar los requisitos de cumplimiento normativo que se necesitan para hacer copias de seguridad en una cuenta aislada. También proporcionan un nivel adicional de protección de datos para evitar la eliminación accidental o malintencionada de las copias de seguridad, la pérdida de credenciales o el peligro de AWS KMS las claves. Las copias de seguridad multicuenta permiten realizar copias de seguridad agrupadas (copiar copias de seguridad de varias cuentas principales a una cuenta de copia de seguridad aislada) y distribuidas (copiar copias de seguridad de una cuenta principal a varias cuentas de copias de seguridad aisladas).

Puede realizar copias de seguridad multicuenta si utiliza el AWS Backup AWS Organizations soporte. Las políticas definen los límites de las cuentas para las copias multicuentas. AWS Organizations Para obtener más información sobre cómo AWS Backup realizar copias de seguridad entre

cuentas, consulta Cómo crear copias de seguridad Cuentas de AWS en la Guía para AWS Backup desarrolladores.

Limitaciones de las copias de seguridad

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

- Las copias de seguridad entre regiones solo se admiten entre dos AWS regiones comerciales, entre las regiones de China (Pekín) y China (Ningxia) y entre las regiones (EE. UU. Este) y AWS GovCloud AWS GovCloud (EE. UU. Oeste), pero no entre esos conjuntos de regiones.
- Las copias de seguridad entre regiones no son compatibles con las regiones registradas.
- Puede realizar copias de seguridad regionales dentro de cualquier región. AWS
- La copia de seguridad de origen debe tener el estado de `AVAILABLE` antes de poder copiarla.
- No puede eliminar una copia de seguridad de origen si se está copiando. Es posible que transcurra un breve intervalo entre el momento en que la copia de seguridad de destino esté disponible y el momento en que se le permita eliminar la copia de seguridad de origen. Debe tener en cuenta este retraso si vuelve a intentar eliminar una copia de seguridad de origen.
- Puede tener hasta cinco solicitudes de copias de seguridad en curso para una sola AWS región de destino por cuenta.

Permisos para copias de seguridad entre regiones

Se utiliza una declaración de política de IAM para conceder permisos para realizar una operación de copia de seguridad. Para comunicarse con la AWS región de origen y solicitar una copia de seguridad entre regiones, el solicitante (rol de IAM o usuario de IAM) debe tener acceso a la copia de seguridad de origen y a la región de origen. AWS

La política se utiliza para conceder permisos a la acción `CopyBackup` para la operación de copia de seguridad. Las acciones se especifican en el campo `Action` de la política y el valor del recurso se especifica en el campo `Resource` de la política.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "fsx:CopyBackup",
            "Resource": "arn:aws:fsx:*:111111111111:backup/*"
```

```
        }
    ]
}
```

Para obtener más información general sobre las políticas de IAM, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.

Copias completas e incrementales

Al copiar una copia de seguridad a una AWS región de destino o AWS cuenta de destino diferente de la copia de seguridad de origen, la primera copia es una copia de seguridad completa, incluso si utiliza la misma clave KMS para cifrar las copias de origen y destino de la copia de seguridad.

Después de la primera copia de seguridad, todas las copias de seguridad posteriores que se envíen a la misma región de destino dentro de la misma AWS cuenta son incrementales, siempre y cuando no se hayan eliminado todas las copias de seguridad previamente copiadas en esa región y se haya utilizado la misma clave. AWS KMS Si no se cumple alguna de las condiciones, la operación de copia genera una copia de seguridad completa (no incremental).

Para obtener información sobre cómo realizar copias de seguridad de los sistemas de archivos, consulte Replicar copias de seguridad dentro de la misma cuenta.

Restauración de copias de seguridad en un nuevo sistema de archivos

Puede utilizar una copia de seguridad disponible para crear un nuevo sistema de archivos y restaurar de forma efectiva una point-in-time instantánea de otro sistema de archivos. Puede restaurar una copia de seguridad mediante la consola o una de las AWS SDKs. AWS CLI La restauración de una copia de seguridad en un nuevo sistema de archivos lleva el mismo tiempo que la creación de un nuevo sistema de archivos. Los datos restaurados a partir de la copia de seguridad se cargan de forma diferida en el sistema de archivos, durante el cual se experimentará una latencia ligeramente superior.

Para garantizar que los usuarios puedan seguir accediendo al sistema de archivos restaurado, corrobore que el dominio del Active Directory que está asociado al sistema de archivos restaurado sea el mismo que el del original. O bien, procure que el dominio del Active Directory del sistema de archivos original tenga veracidad. Para obtener más información acerca de Active Directory, consulte Trabajar con Microsoft Active Directory.

Para obtener información sobre cómo restaurar una copia de seguridad en un sistema de archivos nuevo FSx para Windows, consulteRestauración de una copia de seguridad en un nuevo sistema de archivos.

> **Note**
>
> Solo puede restaurar la copia de seguridad de un sistema de archivos nuevo con el mismo tipo de implementación y la misma capacidad de almacenamiento que el original. Puede aumentar la capacidad de almacenamiento del sistema de archivos nuevo una vez que esté disponible. Para obtener más información, consulte Administrar la capacidad de almacenamiento.

Puede cambiar cualquiera de las siguientes configuraciones del sistema de archivos cuando restaure una copia de seguridad en un nuevo sistema de archivos:

- Tipo de almacenamiento
- Capacidad de rendimiento
- VPC
- Zona de disponibilidad
- Subred
- Grupos de seguridad de la VPC
- Configuración del Active Directory
- AWS KMS clave de cifrado
- Hora de inicio de la copia de seguridad automática y diaria
- El período de mantenimiento semanal

Crear copias de seguridad iniciadas por el usuario

Además de las copias de seguridad automáticas diarias del sistema de archivos, puedes crear una copia de seguridad del sistema de archivos iniciada por el usuario en cualquier momento mediante la FSx consola de Amazon, tal y como se describe en el siguiente procedimiento.

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

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

2. En el panel de la consola, elija el nombre del sistema de archivos del que desea hacer una copia de seguridad.
3. En Actions, elija Create backup.
4. En el cuadro de diálogo Create backup que se abre, proporciona un nombre para la copia de seguridad. Los nombres de las copias de seguridad pueden tener un máximo de 256 caracteres Unicode, incluidas letras, espacios en blanco, números y caracteres especiales . + - = _ : /
5. Elija Create backup.

Ya ha creado la copia de seguridad de su sistema de archivos. Puedes encontrar una tabla con todas tus copias de seguridad en la FSx consola de Amazon seleccionando Backups en la barra de navegación de la izquierda. La nueva copia de seguridad iniciada por el usuario es de tipo `USER_INITIATED` y su estado es `CREATING` hasta que se convierte en `AVAILABLE`. Para obtener más información, consulte Trabajo con copias de seguridad iniciadas por el usuario.

Eliminación de copias de seguridad

Puede eliminar cualquier copia de seguridad diaria automática o iniciada por el usuario de su sistema de archivos mediante la FSx consola, la CLI o la API de Amazon, tal como se describe en los siguientes procedimientos. Para eliminar las copias de seguridad realizadas por AWS Backup, que tienen el tipo AWS Backup, debe utilizar la AWS Backup consola, la CLI o la API. Eliminar una copia de seguridad es una acción permanente e irrecuperable. También se eliminan todos los datos de una copia de seguridad eliminada. No elimine una copia de seguridad a menos que esté seguro de que no la necesitará de nuevo en el futuro.

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 Delete backups que se abre, confirme que el ID de la copia de seguridad identifica la copia de seguridad que desea eliminar.
5. Confirme que la casilla de la copia de seguridad que desea eliminar está marcada.
6. Elija Delete backups.

La copia de seguridad y todos los datos incluidos se eliminarán ahora de forma permanente e irrecuperable.

Tamaño de las copias de seguridad

El tamaño de las copias de seguridad lo determina el almacenamiento utilizado en el sistema de archivos, en lugar de la capacidad total de almacenamiento aprovisionada. El tamaño de las copias de seguridad dependerá de la capacidad de almacenamiento utilizada, de la cantidad de datos perdidos en el sistema de archivos. En función de cómo queden distribuidos los datos en los volúmenes de almacenamiento del sistema de archivos y de la frecuencia con la que cambie dicha distribución, el uso total de copias de seguridad puede ser mayor o menor que la capacidad de almacenamiento utilizada. Cuando se elimina una copia de seguridad, solo se borran los datos que son únicos de dicha copia de seguridad.

Para proporcionar copias de seguridad duraderas e incrementales, Amazon FSx realiza copias de seguridad de los datos a nivel de bloque. file-system-consistent Los datos de los volúmenes de almacenamiento del sistema de archivos pueden almacenarse en varios bloques, según el patrón en el que se hayan escrito o sobrescrito. Como resultado, es posible que el tamaño total de la copia de seguridad utilizada no coincida con el tamaño exacto de los archivos y directorios del sistema de archivos. Puedes consultar el uso y el coste generales de las copias de seguridad en el AWS Billing panel de control o AWS Cost Management Console.

Usa etiquetas para organizar tu AWS factura y reflejar tu propia estructura de costos. Para ello, inscríbase para recibir su Cuenta de AWS factura con los valores clave de las etiquetas incluidos. A continuación, para ver los costos de los recursos combinados, organice la información de facturación de acuerdo con los recursos con los mismos valores de clave de etiquetas. Por ejemplo, puede etiquetar varios recursos con un nombre de aplicación específico y luego organizar su información de facturación para ver el costo total de la aplicación en distintos servicios. Para obtener más información, consulte Uso de etiquetas de asignación de costos en la Guía del usuario de AWS Billing .

> **Note**
>
> Al aumentar la capacidad de almacenamiento, el proceso de migración de datos del conjunto anterior de discos de almacenamiento al nuevo conjunto de discos de almacenamiento, de mayor tamaño, puede provocar un aumento temporal del uso de las copias de seguridad hasta que se eliminen las copias de seguridad asociadas al conjunto anterior de discos de almacenamiento. Si el almacenamiento del sistema de archivos solo se utilizó parcialmente

antes de aumentar la capacidad de almacenamiento, el tamaño de los datos que se deben migrar a los nuevos discos puede ser mayor que el tamaño de los datos que existen en los discos de almacenamiento originales. Esto puede provocar un aumento en el uso de las copias de seguridad hasta el nuevo nivel de capacidad de almacenamiento. Debe tener en cuenta el impacto del aumento de la capacidad de almacenamiento en la planificación de las copias de seguridad.

Replicar copias de seguridad dentro de la misma cuenta

Puede usar AWS Management Console y AWS CLI para copiar manualmente las copias de seguridad de la misma AWS cuenta a otra Región de AWS (copias entre regiones) o dentro de la misma Región de AWS (copias dentro de una región) mediante los siguientes procedimientos.

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

1. Abre la FSx consola de Amazon en https://console.aws.amazon.com/fsx/.
2. En el panel de navegación, elija Backups.
3. En la tabla Backups, elija la copia de seguridad que desee copiar y, a continuación, elija Copy backup.
4. En la sección Settings, realice lo siguiente:
   - En la lista de regiones de destino, selecciona una AWS región de destino en la que copiar la copia de seguridad. El destino puede estar en otra AWS región (copia entre regiones) o dentro de la misma AWS región (copia dentro de la región).
   - (Opcional) Seleccione Copy Tags para copiar las etiquetas de la copia de seguridad de origen a la copia de seguridad de destino. Si selecciona Copy Tags y también las añade en el paso 6, se fusionarán todas las etiquetas.
5. Para el cifrado, elija la clave de AWS KMS cifrado para cifrar la copia de seguridad copiada.
6. Para Tags, introduzca una clave y un valor para añadir etiquetas a la copia de seguridad. Si añade etiquetas aquí y también seleccionó Copy Tags en el paso 4, todas las etiquetas se fusionarán.
7. Elija Copy backup.

La copia de seguridad se copia en la misma AWS cuenta a la AWS región seleccionada.

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

- Use el comando `copy-backup` CLI o la operación de CopyBackupAPI para copiar una copia de seguridad en la misma AWS cuenta, ya sea en una AWS región o dentro de una AWS región.

  El siguiente comando copia una copia de seguridad con un identificador `backup-0abc123456789cba7` de la región `us-east-1`.

  ```
  aws fsx copy-backup \
    --source-backup-id backup-0abc123456789cba7 \
    --source-region us-east-1
  ```

  La respuesta muestra la descripción de la copia de seguridad copiada.

  Puede ver sus copias de seguridad en la FSx consola de Amazon o mediante programación mediante el comando `describe-backups` CLI o la operación de DescribeBackupsAPI.

Restauración de una copia de seguridad en un nuevo sistema de archivos

Puede restaurar una copia de seguridad del sistema de archivos para crear un nuevo sistema de archivos mediante la AWS Management Console CLI y la API, tal y como se describe en el siguiente procedimiento.

Cómo restaurar un sistema de archivos a partir de una copia

1. Abre la FSx consola de Amazon en https://console.aws.amazon.com/fsx/.
2. En el panel de la consola, elija Backups en el menú de la izquierda.
3. En la tabla Backups, elija la copia de seguridad que desee restaurar y, a continuación, elija Restore backup.

   Al hacerlo, se abrirá el asistente de creación del sistema de archivos. Este asistente es idéntico al de creación de sistemas de archivos estándar, excepto que el Tipo de implementación y la Capacidad de almacenamiento ya están configurados y no se pueden cambiar. Sin embargo, puede cambiar la capacidad de rendimiento, la VPC asociada y otros ajustes, así como el tipo de almacenamiento. El tipo de almacenamiento está configurado en SSD de forma predeterminada, pero puede cambiarlo a HDD con las siguientes condiciones:

   - El tipo de implementación del sistema de archivos es Multi-AZ o Single-AZ 2.

- La capacidad de almacenamiento es de al menos 2000 GiB.

4. Siga los pasos del asistente al igual que cuando crea un sistema de archivos nuevo.
5. Elija Review and create.
6. Revisa la configuración que has elegido para tu sistema de FSx archivos de Amazon y, a continuación, selecciona Crear sistema de archivos.

   Amazon FSx está creando un nuevo sistema de archivos y, una vez que su estado cambie a`AVAILABLE`, podrás utilizar el sistema de archivos de forma normal.

Protección de los datos con copias de redundancia

Una copia de redundancia de Microsoft Windows es una copia de un sistema de archivos de Windows en un momento dado. Con las copias de redundancia habilitadas, los usuarios pueden recuperar rápidamente los archivos borrados o modificados que estén almacenados en la red y comparar las versiones de los archivos. Los administradores de almacenamiento pueden programar fácilmente la realización periódica de instantáneas mediante PowerShell los comandos de Windows.

Las copias de redundancia se almacenan junto con los datos del sistema de archivos y consumen la capacidad de almacenamiento del sistema de archivos para las porciones de archivos modificados. Todas las copias de redundancia almacenadas en el sistema de archivos se incluyen en copias de seguridad del sistema de archivos.

> **Note**
>
> De forma predeterminada, las instantáneas no están FSx activadas en el servidor de archivos de Windows. Para proteger los datos de las copias de redundancia en el sistema de archivos, debe habilitarlas y programarlas en el sistema de archivos. Para obtener más información, consulte Configuración de copias de redundancia para que usen el almacenamiento y la programación predeterminados.

> **Warning**
>
> Las copias de redundancia no sustituyen a las copias de seguridad. Si habilita las copias de redundancia, asegúrese de seguir realizando copias de seguridad periódicas.

Temas

- Prácticas recomendadas para usar copias de redundancia
- Configuración de copias de redundancia
- Configuración de copias de redundancia para que usen el almacenamiento y la programación predeterminados
- Configuración de la cantidad máxima de almacenamiento de copias de redundancia
- Visualización del almacenamiento de copias de redundancia
- Creación de un programa de copias de redundancia personalizado
- Visualización de la programación de copias de redundancia
- Crear una copia de redundancia
- Visualización de copias de redundancia existentes
- Eliminar copias de redundancia
- Eliminar una programación de copias de redundancia
- Eliminar el almacenamiento de las copias de redundancia, la programación y todas las copias de redundancia
- Solución de copias de redundancia

Prácticas recomendadas para usar copias de redundancia

Puede habilitar las copias de redundancia para sus sistemas de archivos para permitir a los usuarios finales ver y restaurar archivos o carpetas individuales a partir de una copia de redundancia anterior en el Explorador de archivos de Windows. Amazon FSx utiliza la función de instantáneas proporcionada por Microsoft Windows Server. Utilice estas prácticas recomendadas para las copias de redundancia:

- Asegúrese de que su sistema de archivos tenga suficientes recursos de rendimiento: Microsoft Windows utiliza un copy-on-write método para registrar los cambios desde el punto de captura de pantalla más reciente, y esta copy-on-write actividad puede provocar hasta tres operaciones de E/S por cada operación de escritura de archivos.
- Utilice almacenamiento SSD y aumente la capacidad de rendimiento: dado que Windows requiere un alto nivel de rendimiento de E/S para mantener copias de redundancia, le recomendamos utilizar almacenamiento SSD y aumentar la capacidad de rendimiento hasta un valor que triplique la carga de trabajo prevista. Esto ayuda a garantizar que su sistema de archivos disponga

de recursos suficientes para evitar problemas como la eliminación no deseada de copias de redundancia.

- Conserve solo el número de copias de redundancia que necesite: si tiene un gran número de copias de redundancia (por ejemplo, más de 64 de las copias de redundancia más recientes) o copias de redundancia que ocupan una gran cantidad de espacio de almacenamiento (a escala de TB) en un solo sistema de archivos, los procesos como la conmutación por error y la conmutación por recuperación pueden tardar más tiempo. Esto se debe a la FSx necesidad de que Windows ejecute comprobaciones de coherencia en el almacenamiento de instantáneas. También es posible que experimente una mayor latencia en las operaciones de E/S debido a la FSx necesidad de que Windows realice copy-on-write alguna actividad mientras mantiene las instantáneas. Para minimizar el impacto de las copias de redundancia en la disponibilidad y el rendimiento, elimine manualmente las copias de redundancia que no utilice o configure los scripts para que eliminen automáticamente las copias de redundancia antiguas del sistema de archivos.

> **Note**
>
> Durante los eventos de conmutación por error en los sistemas de archivos Multi-AZ, FSx Windows realiza una comprobación de coherencia que requiere escanear el almacenamiento de instantáneas del sistema de archivos antes de que el nuevo servidor de archivos activo entre en funcionamiento. La duración de la comprobación de coherencia depende del número de copias de redundancia del sistema de archivos y del almacenamiento consumido. Para evitar el retraso de los eventos de conmutación por error o conmutación por recuperación, le recomendamos que mantenga menos de 64 copias de redundancia en el sistema de archivos, y que siga los pasos que se indican a continuación para supervisar y eliminar con habitualidad las copias más antiguas.

Configuración de copias de redundancia

Puede activar y programar instantáneas periódicas en su sistema de archivos mediante PowerShell los comandos de Windows definidos por Amazon FSx. Los siguientes son tres ajustes principales a la hora de configurar las instantáneas en el sistema FSx de archivos del servidor de ficheros de Windows:

- Configurar la cantidad máxima de almacenamiento que pueden consumir las copias de redundancia en el sistema de archivos

- (Opcional) Configurar la cantidad máxima de copias de redundancia que pueden almacenarse en el sistema de archivos El valor predeterminado es 20.
- (Opcional) Configurar un programa para definir momentos e intervalos con los que se realizarán copias de redundancia, por ejemplo, de forma diaria, semanal y mensual

Puede almacenar un máximo de 500 copias de redundancia por sistema de archivos en cualquier momento; sin embargo, recomendamos mantener menos de 64 copias de redundancia en cualquier momento para garantizar la disponibilidad y el rendimiento. Cuando alcance este límite, la siguiente copias de redundancia que tome sustituirá a la más antigua. Del mismo modo, cuando se alcanza la cantidad máxima de almacenamiento de copias de redundancia, se eliminan una o más de las más antiguas para dejar suficiente espacio de almacenamiento para la siguiente.

Para obtener información sobre cómo habilitar y programar rápidamente instantáneas periódicas mediante la FSx configuración predeterminada de Amazon, consulteConfiguración de copias de redundancia para que usen el almacenamiento y la programación predeterminados.

Las consideraciones a la hora de asignar el almacenamiento de copias de redundancia

Una copias de redundancia es una copia a nivel de bloque de los cambios en los archivos que se hayan realizado desde la última copia de redundancia. No se copia todo el archivo, solo los cambios. Por lo tanto, las versiones anteriores de los archivos no suelen ocupar tanto espacio de almacenamiento como el archivo actual. La cantidad de espacio de volumen que se utiliza para los cambios puede variar en función de la carga de trabajo. Cuando se modifica un archivo, el espacio de almacenamiento utilizado por las copias de redundancia depende de la carga de trabajo. Al determinar cuánto espacio de almacenamiento desea asignar a las copias de redundancia, debe tener en cuenta los patrones de uso del sistema de archivos de la carga de trabajo.

Al habilitar las copias de redundancia, puede especificar la cantidad máxima de almacenamiento que pueden consumir en el sistema de archivos. El límite predeterminado es del 10 por ciento del sistema de archivos. Se recomienda aumentar el límite si los usuarios añaden o modifican archivos con frecuencia. Si el límite es demasiado pequeño, es posible que las copias de redundancia más antiguas se eliminen con más frecuencia de lo que los usuarios podrían esperar.

Puede establecer el almacenamiento de copias de redundancia como ilimitado (`Set-FsxShadowStorage -Maxsize "UNBOUNDED"`). Sin embargo, una configuración ilimitada puede provocar que un gran número de copias de redundancia consuma el almacenamiento del sistema de archivos. Esto podría provocar que no disponga de suficiente capacidad de almacenamiento para

las cargas de trabajo. Si establece un almacenamiento ilimitado, asegúrese de escalar la capacidad de almacenamiento a medida que se alcancen los límites de copias de redundancia. Para obtener información sobre cómo configurar el almacenamiento de copias de redundancia para un tamaño específico o de forma ilimitada, consulte Configuración de la cantidad máxima de almacenamiento de copias de redundancia.

Tras activar las copias de redundancia, puede controlar la cantidad de espacio de almacenamiento que ocupan. Para obtener más información, consulte Visualización del almacenamiento de copias de redundancia.

Consideraciones al establecer la cantidad máxima de copias de redundancia

Al habilitar las copias de redundancia, puede especificar la cantidad máxima de copias de redundancia almacenadas en el sistema de archivos. El límite predeterminado es 20 y, para minimizar el impacto de las copias de redundancia en la disponibilidad y el rendimiento, Microsoft recomienda configurar la cantidad máxima de copias de redundancia en menos de 64. Dado que Windows requiere un alto nivel de rendimiento de E/S para mantener copias de redundancia, recomendamos usar un almacenamiento en SSD y aumentar la capacidad de rendimiento hasta un valor que triplique la carga de trabajo prevista. Esto ayuda a garantizar que su sistema de archivos disponga de recursos suficientes para evitar problemas como la eliminación no deseada de copias de redundancia.

Puede establecer la cantidad máxima de copias de redundancia en 500. Sin embargo, si tiene una gran cantidad de copias de redundancia o estas ocupan una gran cantidad de almacenamiento (a escala de TB) en un solo sistema de archivos, los procesos como la conmutación por error y la conmutación por recuperación pueden tardar más tiempo del esperado. Esto se debe a que Windows necesita que se ejecuten comprobaciones de coherencia en el almacenamiento de copias de redundancia. También es posible que experimente una mayor latencia en las operaciones de E/S debido a la necesidad de que Windows realice copy-on-write alguna actividad mientras mantiene las instantáneas.

Las recomendaciones del sistema de archivos para las copias de redundancia

A continuación, se presentan las recomendaciones del sistema de archivos para el uso de copias de redundancia.

- Asegúrese de proporcionar una capacidad de rendimiento suficiente para las necesidades de la carga de trabajo del sistema de archivos. Amazon FSx ofrece la función Shadow Copies proporcionada por Microsoft Windows Server. Por diseño, Microsoft Windows utiliza un copy-on-

write método para registrar los cambios desde el punto de instantánea más reciente, y esta copy-on-write actividad puede provocar hasta tres operaciones de E/S por cada operación de escritura de archivos. Si Windows no puede mantener la velocidad de entrada de operaciones de E/S por segundo, puede provocar que se eliminen todas las instantáneas, ya que ya no puede mantenerlas a través de ellas. copy-on-write Por lo tanto, es importante que proporcione una capacidad de rendimiento de E/S suficiente para las necesidades de la carga de trabajo del sistema de archivos. Esto es tanto para la dimensión de capacidad de rendimiento que determina el rendimiento de E/S del servidor de archivos, como para el tipo y la capacidad de almacenamiento que determinan el rendimiento de E/S del almacenamiento.

- Por lo general, recomendamos que utilice los sistemas de archivos configurados con almacenamiento en SSD en lugar de HDD cuando habilite las copias de redundancia. Esto se debe a que Windows consume un mayor rendimiento de E/S para mantener las copias de redundancia, y a que el almacenamiento en HDD proporciona una capacidad de rendimiento inferior para las operaciones de E/S.
- El sistema de archivos debe tener al menos 320 MB de espacio libre, además de la cantidad máxima de almacenamiento de copias de redundancia configurada (`MaxSpace`). Por ejemplo, si asignó 5 GB de `MaxSpace` a copias de redundancia, el sistema de archivos siempre debe tener al menos 320 MB de espacio libre además de los 5 GB de `MaxSpace`.

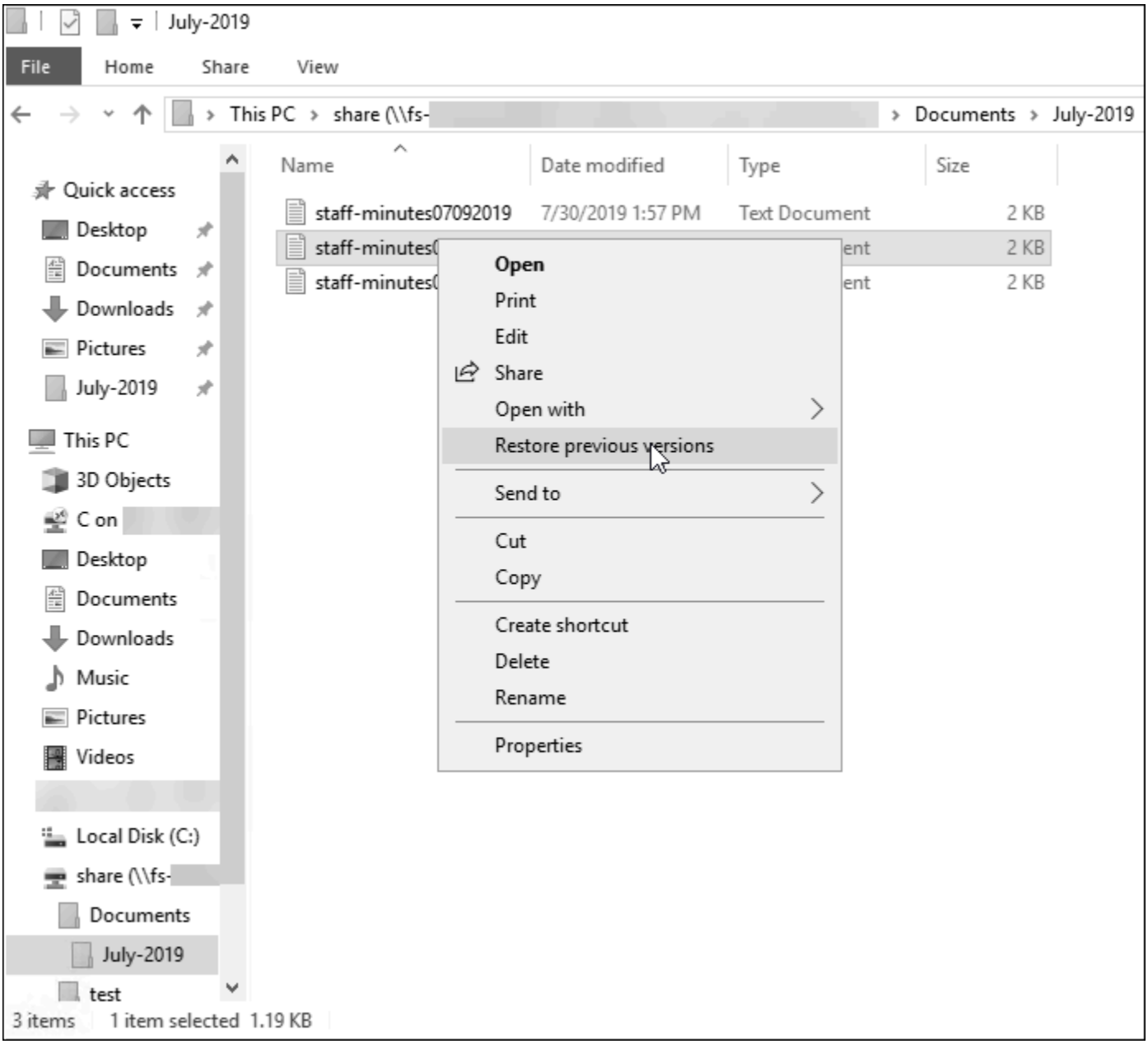
> **Warning**
>
> Al configurar el programa de copias de redundancia, asegúrese de no programarlas cuando migra datos o cuando esté programada la desduplicación de datos. Debe programar copias de redundancia cuando considere que el sistema de archivos esté inactivo. Para obtener información acerca de la configuración de un programa de copias de redundancia personalizado, consulte Creación de un programa de copias de redundancia personalizado.

Restauración de los archivos y las carpetas individuales

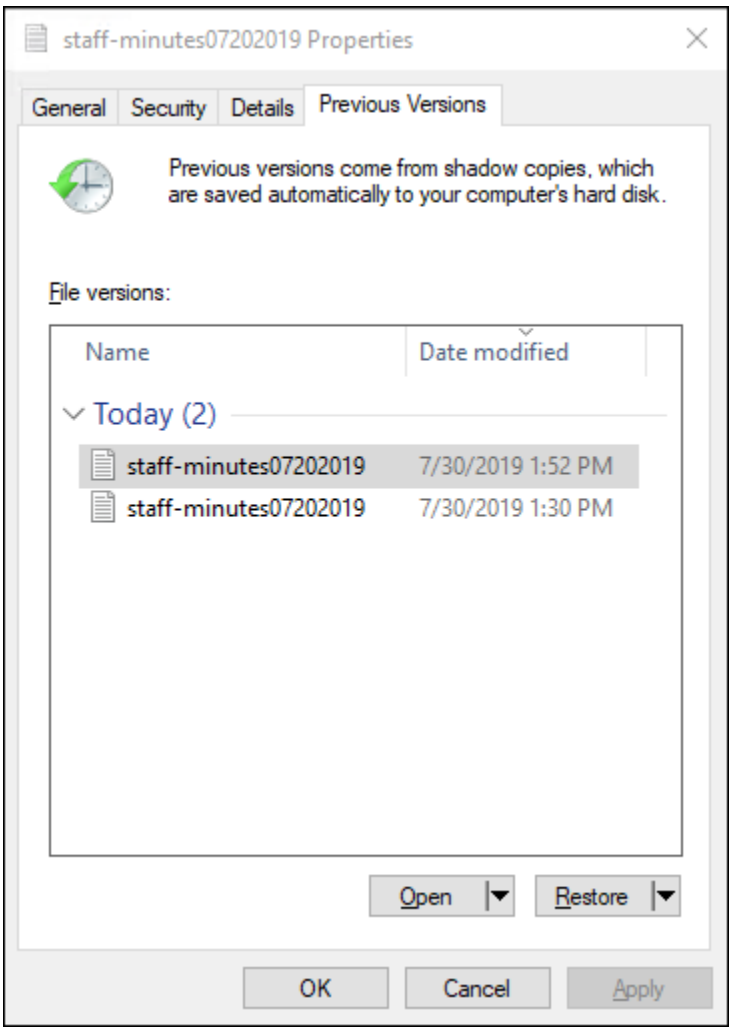
Tras configurar las instantáneas en el sistema de FSx archivos de Amazon, los usuarios pueden restaurar rápidamente las versiones anteriores de archivos o carpetas individuales y recuperar los archivos eliminados.

Los usuarios restauran los archivos a versiones anteriores con la interfaz conocida del Explorador de archivos de Windows. Para restaurar un archivo, elija el archivo que desea restaurar y, a

continuación, elija Restaurar versiones anteriores en el menú contextual (haga clic con el botón derecho).



A continuación, los usuarios pueden ver y restaurar una versión anterior desde la lista de Versiones anteriores.



Configuración de copias de redundancia para que usen el almacenamiento y la programación predeterminados

Puede configurar de forma rápida las copias de redundancia en el sistema de archivos mediante la configuración predeterminada para el almacenamiento y la programación de copias de redundancia. La configuración predeterminada de almacenamiento de copias de redundancia permite que estas consuman como máximo el 10 % de la capacidad de almacenamiento del sistema de archivos. Si aumenta la capacidad de almacenamiento del sistema de archivos, la cantidad de almacenamiento de copias de redundancia que está actualmente asignada no aumentará de manera similar.

La programación predeterminada hace copias de redundancia de manera automática todos los lunes, martes, miércoles, jueves y viernes, a las 7:00 a. m. y a las 12:00 p. m. UTC.

Cómo configurar el nivel predeterminado de almacenamiento de copias de redundancia

1. Conéctese a una instancia informática de Windows que tenga conectividad de red con el sistema de archivos.
2. Inicie sesión en la instancia informática de Windows como miembro del grupo de administradores del sistema de archivos. En AWS Managed Microsoft AD, ese grupo es FSx Administradores AWS delegados. En Microsoft AD autoadministrado, ese grupo figura como Administradores del dominio o el grupo personalizado que haya asignado como administrador cuando creó el sistema de archivos. Para obtener más información, consulte Conectarse a su instancia de Windows en la Guía del EC2 usuario de Amazon.
3. Configure la cantidad predeterminada de almacenamiento de redundancia con el comando siguiente. *FSxFileSystem-Remote-PowerShell-Endpoint*Sustitúyalo por el PowerShell punto final remoto de Windows del sistema de archivos que desee administrar. Puedes encontrar el PowerShell punto de conexión remoto de Windows en la FSx consola de Amazon, en la sección Red y seguridad de la pantalla de detalles del sistema de archivos o en la respuesta a la operación de la `DescribeFileSystem` API.

   ```
   PS C:\Users\delegateadmin> Invoke-Command -ComputerName FSxFileSystem-Remote-PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {Set-FsxShadowStorage -Default}
   ```

   La respuesta tiene este aspecto:

   ```
   FSx Shadow Storage Configuration

   AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
   -------------- ---------    -------- ------------------
                0         0 10737418240                 20
   ```

Cómo configurar la programación predeterminada de copias de redundancia

1. Conéctese a una instancia informática de Windows que tenga conectividad de red con el sistema de archivos.
2. Inicie sesión en la instancia informática de Windows como miembro del grupo de administradores del sistema de archivos. En AWS Managed Microsoft AD ese grupo se encuentran FSx los administradores AWS delegados. En Microsoft AD autoadministrado, ese grupo figura como Administradores del dominio o el grupo personalizado que haya asignado

como administrador cuando creó el sistema de archivos. Para obtener más información, consulte Conectarse a su instancia de Windows en la Guía del EC2 usuario de Amazon.

3. Configure la programación predeterminada de copias de redundancia mediante el siguiente comando.

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName FSxFileSystem-Remote-PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {Set-FsxShadowCopySchedule -Default}
```

La respuesta muestra la programación predeterminada que ahora está configurada.

```
FSx Shadow Copy Schedule

Start Time                Days of week                              WeeksInterval
----------                ------------                              -------------
2019-07-16T07:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
2019-07-16T12:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
```

Para obtener más información sobre las opciones adicionales y la creación de una programación de copias de redundancia personalizada, consulte Creación de un programa de copias de redundancia personalizado.

Configuración de la cantidad máxima de almacenamiento de copias de redundancia

La cantidad máxima de almacenamiento que pueden consumir las instantáneas en un sistema de archivos se define mediante el PowerShell comando `Set-FsxShadowStorage` custom. Puede especificar el tamaño máximo que pueden alcanzar las copias de redundancia mediante los parámetros `-Maxsize` o `-Default`. El uso de `Default` establece el 10 % como la capacidad máxima de almacenamiento del sistema de archivos. No puede especificar los parámetros `-Maxsize` y `-Default` en el mismo comando.

Con `-Maxsize`, puede definir el almacenamiento de copias de redundancia de la siguiente manera:

- En bytes: `Set-FsxShadowStorage -Maxsize 2500000000`
- En kilobytes, megabytes, gigabytes u otras unidades: `Set-FsxShadowStorage -Maxsize (2500MB)` o `Set-FsxShadowStorage -Maxsize (2.5GB)`

- Como porcentaje del almacenamiento general: `Set-FsxShadowStorage -Maxsize "20%"`
- Como ilimitado: `Set-FsxShadowStorage -Maxsize "UNBOUNDED"`

Use `-Default` para establecer que el almacenamiento de redundancia utilice hasta un 10 por ciento del sistema de archivos: `Set-FsxShadowStorage -Default`. Para obtener más información sobre cómo usar la opción predeterminada, consulte Configuración de copias de redundancia para que usen el almacenamiento y la programación predeterminados.

Para establecer la cantidad de almacenamiento de instantáneas en un sistema FSx de archivos del servidor de archivos de Windows

1. Conéctese a una instancia informática que tenga conectividad de red con el sistema de archivos como un usuario que sea miembro del grupo de administradores del sistema de archivos. En AWS Managed Microsoft AD, ese grupo está AWS Delegated FSx Administrators. En Microsoft AD autoadministrado, ese grupo figura como Administradores del dominio o el grupo personalizado que haya asignado como administrador cuando creó el sistema de archivos. Para obtener más información, consulte Conectarse a su instancia de Windows en la Guía del EC2 usuario de Amazon.
2. Abre una PowerShell ventana de Windows en la instancia de cómputo.
3. Usa el siguiente comando para abrir una PowerShell sesión remota en tu sistema de FSx archivos de Amazon. *`FSxFileSystem-Remote-PowerShell-Endpoint`*Sustitúyalo por el PowerShell punto final remoto de Windows del sistema de archivos que deseas administrar. Puedes encontrar el PowerShell punto de conexión remoto de Windows en la FSx consola de Amazon, en la sección Red y seguridad de la pantalla de detalles del sistema de archivos o en la respuesta a la operación de la `DescribeFileSystem` API.

   ```
   PS C:\Users\delegateadmin> enter-pssession -computername FSxFileSystem-Remote-
   PowerShell-Endpoint -configurationname fsxremoteadmin
   ```

4. Compruebe que el almacenamiento de copias de redundancia no esté ya configurado en el sistema de archivos con el siguiente comando.

   ```
   [fs-1234567890abcef12]: PS>Get-FsxShadowStorage
   No Fsx Shadow Storage Configured
   ```

5. Establezca la cantidad de almacenamiento de redundancia en el 10 % del volumen y la cantidad máxima de copias de redundancia en 20 mediante la opción `-Default`.

```
[fs-1234567890abcef12]: PS>Set-FsxShadowStorage -Default
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- ------------------
             0         0 32530536858                 20
```

Puede limitar la cantidad máxima de copias de redundancia permitidas en el sistema de archivos mediante el comando `Set-FSxShadowStorage` junto con el parámetro `-MaxShadowCopyNumber`, para lo que debe especificar un valor entre 1 y 500. De forma predeterminada, la cantidad máxima de copias de redundancia se establece en 20, como recomienda Microsoft para las cargas de trabajo activas.

Visualización del almacenamiento de copias de redundancia

Puede ver la cantidad de almacenamiento que actualmente consumen las instantáneas en su sistema de archivos mediante el `Get-FsxShadowStorage` comando en una PowerShell sesión remota en su sistema de archivos. Para obtener instrucciones sobre cómo iniciar una PowerShell sesión remota en el sistema de archivos, consulteUso de Amazon FSx CLI para PowerShell.

```
[fs-1234567890abcef12]: PS>PS>Get-fsxshadowstorage
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- ------------------
             0         0 10737418240                 20
```

El resultado muestra la configuración del almacenamiento paralelo, de la siguiente manera:

- `AllocatedSpace`: la cantidad de almacenamiento del sistema de archivos en bytes, que se asignó actualmente a las copias de redundancia. Inicialmente, este valor es 0.
- `UsedSpace`: la cantidad de almacenamiento, en bytes, que usan actualmente las copias de redundancia. Inicialmente, este valor es 0.
- `MaxSpace`: la cantidad máxima de almacenamiento, en bytes, hasta la que puede aumentar el almacenamiento de redundancia. Este es el valor que se establece para el almacenamiento de copias de redundancia con el comando `Set-FsxShadowStorage`.

- `MaxShadowCopyNumber`: la cantidad máxima de copias de redundancia que puede tener el sistema de archivos, entre 1 y 500.

Cuando la cantidad de `UsedSpace` alcance la cantidad máxima de almacenamiento de copias de redundancia configurada (`MaxSpace`) o la cantidad de copias de redundancia alcance la cantidad máxima de copias de redundancia configurada (`MaxShadowCopyNumber`), la siguiente copia de redundancia que realice sustituirá a la más antigua. Si no quiere perder las copias más antiguas, controle el almacenamiento de estas para asegurarse de que dispone de suficiente espacio para las nuevas. Si necesita más espacio, puede eliminar las copias de redundancia existentes o aumentar la cantidad máxima de almacenamiento de ellas.

> **Note**
>
> Cuando las copias de redundancia se crean automática o manualmente, usan como límite de almacenamiento la cantidad de almacenamiento de copias de redundancia que haya configurado. Las instantáneas aumentan de tamaño con el tiempo y utilizan el espacio de almacenamiento disponible que muestra la CloudWatch `FreeStorageCapacity` métrica hasta alcanzar la cantidad máxima de almacenamiento de instantáneas configurada (`MaxSpace`).

Creación de un programa de copias de redundancia personalizado

Las programaciones de copias de redundancia utilizan los activadores de tareas programadas en Microsoft Windows para especificar cuándo hacer las copias de manera automática. Una programación de copias de redundancia puede tener varios activadores, lo que le otorga una gran flexibilidad de programación. Solo puede existir un programa de copias de redundancia a la vez. Antes de poder crear un programa de copias de redundancia, primero debe establecer la cantidad de almacenamiento de copias de redundancia.

Al ejecutar el comando `Set-FsxShadowCopySchedule` en un sistema de archivos, se sobrescribe cualquier programa de copias de redundancia existente. Si el equipo del cliente se encuentra en la zona horaria UTC, también puede especificar la zona horaria de un activador con las zonas horarias de Windows y la opción `-TimezoneId`. Para obtener una lista de las zonas horarias de Windows, consulte la documentación de la Zona horaria predeterminada de Microsoft o ejecute lo siguiente en una línea de comandos de Windows: `tzutil /l`. Para obtener más información sobre los

activadores de tareas de Windows, consulte los Activadores de tareas en la documentación del Centro de desarrolladores de Microsoft Windows.

También, puede utilizar la opción `-Default` para configurar rápidamente un programa de copias de redundancia predeterminado. Para obtener más información, consulte Configuración de copias de redundancia para que usen el almacenamiento y la programación predeterminados.

Cómo crear un programa de copias de redundancia personalizado

1. Cree un conjunto de activadores de tareas programados de Windows para definir cuándo hacer las copias en la programación de copias de redundancia. Utilice el `new-scheduledTaskTrigger` comando PowerShell en una máquina local para configurar varios activadores.

   El siguiente ejemplo crea un programa de copias de redundancia personalizado que se ejecuta de lunes a viernes, a las 6:00 a. m. y a las 6:00 p. m. UTC. De forma predeterminada, las horas están en UTC, a menos que especifiques una zona horaria en los activadores de tareas programadas de Windows que cree.

   ```
   PS C:\Users\delegateadmin> $trigger1 = new-scheduledTaskTrigger -weekly -DaysOfWeek
    Monday,Tuesday,Wednesday,Thursday,Friday -at 06:00
   PS C:\Users\delegateadmin> $trigger2 = new-scheduledTaskTrigger -weekly -DaysOfWeek
    Monday,Tuesday,Wednesday,Thursday,Friday -at 18:00
   ```

2. Utilice el `invoke-command` para ejecutar el comando `scriptblock`. Al hacerlo, se escribe un script que establece la programación de copias de redundancia con el valor `new-scheduledTaskTrigger` que acaba de crear. *`FSxFileSystem-Remote-PowerShell-Endpoint`*Sustitúyalo por el PowerShell punto final remoto de Windows del sistema de archivos que desee administrar. Puedes encontrar el PowerShell punto de conexión remoto de Windows en la FSx consola de Amazon, en la sección Red y seguridad de la pantalla de detalles del sistema de archivos o en la respuesta a la operación de la `DescribeFileSystem` API.

   ```
   PS C:\Users\delegateadmin> invoke-command -ComputerName FSxFileSystem-Remote-
   PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {
   ```

3. Introduzca la siguiente línea en la indicación >> para establecer el programa de copias de redundancia con el comando `set-fsxshadowcopyschedule`.

```
>> set-fsxshadowcopyschedule -scheduledtasktriggers $Using:trigger1,$Using:trigger2
 -Confirm:$false }
```

La respuesta muestra el programa de copias de redundancia que configuró en el sistema de archivos.

```
FSx Shadow Copy Schedule


Start Time:    : 2019-07-16T06:00:00+00:00
Days of Week   : Monday,Tuesday,Wednesday,Thursday,Friday
WeeksInterval  : 1
PSComputerName : fs-0123456789abcdef1
RunspaceId     : 12345678-90ab-cdef-1234-567890abcde1

Start Time:    : 2019-07-16T18:00:00+00:00
Days of Week   : Monday,Tuesday,Wednesday,Thursday,Friday
WeeksInterval  : 1
PSComputerName : fs-0123456789abcdef1
RunspaceId     : 12345678-90ab-cdef-1234-567890abcdef
```

Visualización de la programación de copias de redundancia

Para ver la programación de instantáneas existente en su sistema de archivos, introduzca el siguiente comando en una PowerShell sesión remota en su sistema de archivos. Para obtener instrucciones sobre cómo iniciar una PowerShell sesión remota en su sistema de archivos, consulteUso de Amazon FSx CLI para PowerShell.

```
[fs-0123456789abcdef1]PS> Get-FsxShadowCopySchedule
FSx Shadow Copy Schedule

Start Time                Days of week                              WeeksInterval
----------                ------------                              -------------
2019-07-16T07:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
2019-07-16T12:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
```

Crear una copia de redundancia

Para crear manualmente una instantánea, introduzca el siguiente comando en una PowerShell sesión remota en su sistema de archivos. Para obtener instrucciones sobre cómo iniciar una PowerShell sesión remota en el sistema de archivos, consulteUso de Amazon FSx CLI para PowerShell.

```
[fs-0123456789abcdef1]PS>New-FsxShadowCopy

Shadow Copy {ABCDEF12-3456-7890-ABCD-EF1234567890} taken successfully
```

Visualización de copias de redundancia existentes

Para ver el conjunto de instantáneas existentes en su sistema de archivos, introduzca el siguiente comando en una PowerShell sesión remota en su sistema de archivos. Para obtener instrucciones sobre cómo iniciar una PowerShell sesión remota en su sistema de archivos, consulteUso de Amazon FSx CLI para PowerShell.

```
[fs-0123456789abcdef1]PS>Get-FsxShadowCopies
FSx Shadow Copies: 2 total

Shadow Copy ID                          Creation Time
--------------                          -----------------
{ABCDEF12-3456-7890-ABCD-EF1234567890} 6/17/2019 7:11:09 AM
{FEDCBA21-6543-0987-0987-EF3214567892} 6/19/2019 11:24:19 AM
```

Eliminar copias de redundancia

Puede eliminar una o más instantáneas existentes en su sistema de archivos mediante el `Remove-FsxShadowCopies` comando en una PowerShell sesión remota en su sistema de archivos. Para obtener instrucciones sobre cómo iniciar una PowerShell sesión remota en el sistema de archivos, consulteUso de Amazon FSx CLI para PowerShell.

Especifique qué copias de redundancia desea eliminar utilizando una de las siguientes opciones obligatorias:

- `-Oldest` elimina la copia de redundancia más antigua
- `-All` elimina todas las copias de redundancia existentes
- `-ShadowCopyId` elimina una copia de redundancia específica con el ID.

Solo puede usar una opción con el comando. Se produce un error si no se especifica qué instantáneas se van a eliminar, si se especifican varias instantáneas IDs o si se especifica un identificador de instantánea no válido.

Para eliminar la instantánea más antigua del sistema de archivos, introduzca el siguiente comando en una PowerShell sesión remota del sistema de archivos.

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopies -Oldest
Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-FSxShadowCopies" on target "Removing oldest shadow
 copy".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y": Y
Shadow Copy {ABCDEF12-3456-7890-ABCD-EF1234567890} deleted
```

Para eliminar una instantánea específica del sistema de archivos, introduzca el siguiente comando en una PowerShell sesión remota del sistema de archivos.

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopies -ShadowCopyId "{ABCDEF12-3456-7890-
ABCD-EF1234567890}"
Are you sure you want to perform this action?
Performing the operation "Remove-FSxShadowCopies" on target "Removing shadow copy
 {ABCDEF12-3456-7890-ABCD-EF1234567890}".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y":>Y
Shadow Copy \\AMZNFSXABCDE123\root\cimv2:Wind32_ShadowCopy.ID{ABCDEF12-3456-7890-ABCD-
EF1234567890}".ID deleted.
```

Para eliminar una cantidad determinada de las copias de redundancia más antiguas del sistema de archivos, actualice el parámetro `-MaxShadowCopyNumber` a la cantidad deseada de copias de redundancia que desee que queden. Sin embargo, este cambio solo tendrá efecto después de realizar la siguiente instantánea de copias de redundancia, cuando el sistema elimine automáticamente las copias de redundancia sobrantes. Use el siguiente comando en una PowerShell sesión remota en su sistema de archivos.

```
[fs-1234567890abcef12]: PS>Get-fsxshadowstorage
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace MaxSpace    MaxShadowCopyNumber
-------------- --------- ----------- -------------------
     556679168  21659648 10737418240                  50
```

```
[fs-1234567890abcef12]: PS>Set-FsxShadowStorage  -MaxShadowCopyNumber 5
Validation
You have 50 shadow copies. Older versions of shadow copies will be deleted, keeping 5
 latest shadow copies on your file system.
Do you want to continue?
[Y] Yes  [N] No  [?] Help (default is "N"): y
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- ------------------
     556679168  21659648 10737418240                  5
```

Eliminar una programación de copias de redundancia

Para eliminar la programación de instantáneas existente en su sistema de archivos, introduzca el siguiente comando en una PowerShell sesión remota en su sistema de archivos. Para obtener instrucciones sobre cómo iniciar una PowerShell sesión remota en su sistema de archivos, consulteUso de Amazon FSx CLI para PowerShell.

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopySchedule

Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-FsxShadowCopySchedule" on target "Removing FSx Shadow
 Copy Schedule".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y"): Y
[fs-0123456789abcdef1]PS>
```

Eliminar el almacenamiento de las copias de redundancia, la programación y todas las copias de redundancia

Puede eliminar la configuración de las copias de redundancia, incluidas todas las copias de redundancia existentes y su programación. Al mismo tiempo, puede liberar el almacenamiento de copias de redundancia del sistema de archivos.

Para ello, introduzca el `Remove-FsxShadowStorage` comando en una PowerShell sesión remota en su sistema de archivos. Para obtener instrucciones sobre cómo iniciar una PowerShell sesión remota en el sistema de archivos, consulteUso de Amazon FSx CLI para PowerShell.

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowStorage

Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-FsxShadowStorage" on target "Removing all Shadow
 Copies, Shadow Copy Schedule, and Shadow Storage".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y": Y
FSx Shadow Storage Configuration
Removing Shadow Copy Schedule
Removing Shadow Copies
All shadow copies removed.
Removing Shadow Storage
Shadow Storage removed successfully.
```

Solución de copias de redundancia

Existen varias causas posibles por las que falten dichas copias, o por las que no se pueda acceder a ellas, tal como se describe en la siguiente sección.

Temas

- Faltan las copias de redundancia más antiguas
- Faltan todas mis copias de redundancia
- No se pueden crear FSx copias de seguridad de Amazon ni acceder a instantáneas de un sistema de archivos recientemente restaurado o actualizado

Faltan las copias de redundancia más antiguas

Las copias de redundancia más antiguas se eliminan en una de estas situaciones:

- Si tiene 500 copias de redundancia, la siguiente copia sustituirá a la más antigua, independientemente del espacio de almacenamiento restante asignado a estas copias.
- Si se alcanza la cantidad máxima de almacenamiento de copias de redundancia configurada, la siguiente copia reemplaza a una o más de las más antiguas, incluso si tiene menos de 500.

Ambos resultados son comportamientos esperados. Si no tiene suficiente espacio de almacenamiento asignado para las copias de redundancia, considere la posibilidad de aumentar el almacenamiento que asignó.

Faltan todas mis copias de redundancia

Si el sistema de archivos tiene una capacidad de rendimiento de E/S insuficiente (ya sea, porque utiliza un disco duro, porque el almacenamiento en disco duro se quedó sin capacidad de ampliación, o porque la capacidad de rendimiento no es suficiente), es posible que Windows Server elimine todas las copias de redundancia, ya que no puede mantenerlas con la capacidad de rendimiento de E/S disponible. Tenga en cuenta las siguientes recomendaciones para evitar este problema:

- Si utilizas almacenamiento en disco duro, utiliza la FSx consola de Amazon o la FSx API de Amazon para cambiar a almacenamiento SSD. Para obtener más información, consulte Administrar el tipo de almacenamiento del sistema de archivos.
- Eleva la capacidad de rendimiento del sistema de archivos hasta un valor tres veces superior a la carga de trabajo prevista.
- Asegúrese de que el sistema de archivos tenga al menos 320 MB de espacio libre, además de la cantidad máxima de almacenamiento de copias de redundancia configurada.
- Programe la creación copias de redundancia para cuando se espera que el sistema de archivos esté inactivo.

Para obtener más información, consulte Las recomendaciones del sistema de archivos para las copias de redundancia.

No se pueden crear FSx copias de seguridad de Amazon ni acceder a instantáneas de un sistema de archivos recientemente restaurado o actualizado

Este es el comportamiento esperado. Amazon FSx reconstruye el estado de la copia oculta en un sistema de archivos restaurado recientemente y no permite el acceso a las instantáneas ni a las copias de seguridad mientras la reconstrucción esté en curso.

Replicación programada mediante AWS DataSync

Puede utilizarla AWS DataSync para programar la replicación periódica de su FSx sistema de archivos del servidor de archivos de Windows en un segundo sistema de archivos. Esta capacidad está disponible tanto para implementaciones dentro de la región como entre regiones. Para obtener más información, consulte Migración de archivos existentes a un servidor FSx de archivos de Windows mediante AWS DataSync esta guía y Transferencia de datos entre servicios AWS de almacenamiento en la Guía del AWS DataSync usuario.

Uso FSx para Windows File Server con Microsoft SQL Server

Normalmente, Microsoft SQL Server de alta disponibilidad (HA) se implementa en varios nodos de bases de datos de un clúster de conmutación por error de Windows Server (WSFC), y cada nodo tiene acceso al almacenamiento de los archivos compartido. Puede utilizar FSx Windows File Server como almacenamiento compartido para las implementaciones de Microsoft SQL Server de alta disponibilidad (HA) de dos maneras: como almacenamiento para archivos de datos activos y como testigo del uso compartido de archivos SMB.

> **Note**
>
> Actualmente, Amazon FSx no admite la función IFI (inicialización instantánea de archivos) de Microsoft SQL Server.

Se recomienda el almacenamiento en SSD para SQL Server. El almacenamiento en SSD está diseñado para las cargas de trabajo de mayor rendimiento y más sensibles a la latencia, incluidas las bases de datos.

Para obtener información sobre el uso de Amazon FSx para reducir la complejidad y los costes de las implementaciones de alta disponibilidad de SQL Server, consulte las siguientes publicaciones del blog sobre AWS almacenamiento:

- Simplifique las implementaciones de alta disponibilidad de Microsoft SQL Server con Amazon FSx for Windows File Server
- Optimice el coste de sus despliegues de SQL Server de alta disponibilidad en AWS
- Simplifique las implementaciones de SQL Server Always On con AWS Launch Wizard y Amazon FSx

Uso de Amazon FSx para archivos de datos de Active SQL Server

Microsoft SQL Server puede implementarse con un recurso compartido de archivos SMB como opción de almacenamiento para los archivos de datos activos. Amazon FSx está optimizado para proporcionar almacenamiento compartido para las bases de datos de SQL Server al admitir el uso

compartido de archivos de disponibilidad continua (CA). Dichos recursos están diseñados para aplicaciones como SQL Server, que requieren un acceso ininterrumpido a los datos de los archivos compartidos. Si bien puede crear recursos compartidos de CA en sistemas de archivos Single-AZ 2, es necesario que utilice recursos compartidos de CA en sistemas de archivos Multi-AZ para todas las implementaciones de SQL Server, ya sean de alta disponibilidad o no.

Cree un recurso compartido de disponibilidad continua

Puede crear recursos compartidos de CA mediante la Amazon FSx CLI para la administración remota en PowerShell. Para especificar que el recurso compartido es de disponibilidad continua, utilice la opción `New-FSxSmbShare` con la opción `-ContinuouslyAvailable` establecida en `$True`. Para obtener más información, consulte Cómo crear un recurso compartido de disponibilidad continua (CA).

Configure los ajustes de tiempo de espera de SMB

Como se describe en Proceso de conmutación por error, la conmutación por error y la conmutación por recuperación en zonas de disponibilidad múltiples pueden provocar pausas de E/S que, por lo general, se completan en menos de 30 segundos. La aplicación de SQL Server puede tener una sensibilidad diferente a los ajustes de tiempo de espera según cómo se la haya configurado.

Puede ajustar el tiempo de espera de la sesión de configuración del cliente SMB para asegurarse de que la aplicación resista las conmutaciones por error de los sistemas de archivos Multi-AZ. Para probar el comportamiento de la aplicación durante las conmutaciones por error, actualice la capacidad de rendimiento del sistema de archivos, lo que inicia una conmutación por error y una conmutación por recuperación.

Uso de Amazon FSx como testigo del intercambio de archivos para pequeñas y medianas empresas

Las implementaciones de clústeres de conmutación por error de Windows Server suelen implementar un testigo del recursos compartidos de archivos SMB para mantener el quórum de los recursos del clúster. Los testigos de recursos compartidos de archivos requieren solo una pequeña cantidad de almacenamiento para guardar la información sobre el quórum. Los sistemas de FSx archivos de Amazon se pueden utilizar como testigos del uso compartido de archivos SMB para las implementaciones de clústeres de conmutación por error de Windows Server.

Migración del almacenamiento de archivos existente a Amazon FSx

Amazon FSx for Windows File Server cuenta con las funciones, el rendimiento y la compatibilidad necesarios para ayudarle a llevar y trasladar fácilmente las aplicaciones empresariales a la nube de Amazon Web Services. El proceso para migrar el almacenamiento local de Microsoft Windows File Server a FSx Windows File Server consta de los cuatro pasos principales siguientes:

1. Migre sus archivos FSx a Windows File Server. Para obtener más información, consulte Migración del almacenamiento de archivos existente a un servidor FSx de archivos de Windows.
2. Migre la configuración de recursos compartidos FSx de archivos a Windows File Server. Para obtener más información, consulte Migración de las configuraciones de uso compartido de archivos locales a Amazon FSx.
3. Asocia tu nombre de DNS actual como un alias de DNS para tu sistema de FSx archivos de Amazon. Para obtener más información, consulta Cómo asociar un alias de DNS a Amazon FSx.
4. Cambie a FSx Windows File Server. Para obtener más información, consulte Traslado de las operaciones a Amazon FSx para Windows File Server.

Puede encontrar la información de cada paso del proceso en las siguientes secciones.

Temas

- Migración del almacenamiento de archivos existente a un servidor FSx de archivos de Windows
- Migración de las configuraciones de uso compartido de archivos locales a Amazon FSx
- Migración de la configuración de DNS local al servidor de FSx archivos de Windows
- Traslado de las operaciones a Amazon FSx para Windows File Server

Migración del almacenamiento de archivos existente a un servidor FSx de archivos de Windows

Para migrar los archivos existentes a FSx los sistemas de archivos de Windows File Server, le recomendamos que utilice AWS DataSync un servicio de transferencia de datos en línea diseñado para simplificar, automatizar y acelerar la copia de grandes cantidades de datos hacia y desde los servicios de AWS almacenamiento. DataSync copia datos a través de Internet o AWS Direct

Connect. Al ser un servicio totalmente gestionado, DataSync elimina gran parte de la necesidad de modificar aplicaciones, desarrollar scripts o gestionar la infraestructura. Para obtener más información, consulte Migración de archivos existentes a un servidor FSx de archivos de Windows mediante AWS DataSync.

Como solución alternativa, puede usar Robust File Copy, o Robocopy, que es un conjunto de comandos de replicación de archivos y directorios de línea de comandos para Microsoft Windows. Para obtener procedimientos detallados sobre cómo utilizar Robocopy para migrar el almacenamiento de archivos al FSx servidor de archivos de Windows, consulteMigración de archivos existentes al servidor de archivos FSx de Windows mediante Robocopy.

Prácticas recomendadas para migrar el almacenamiento de archivos existente a un servidor de archivos FSx de Windows

Para migrar grandes cantidades de datos al FSx servidor de archivos de Windows lo más rápido posible, utilice los sistemas de FSx archivos de Amazon configurados con almacenamiento en unidades de estado sólido (SSD). Una vez finalizada la migración, puede mover los datos a los sistemas de FSx archivos de Amazon mediante el almacenamiento en disco duro (HDD) si es la mejor solución para su aplicación.

Para mover datos de un sistema de FSx archivos de Amazon que utiliza un almacenamiento SSD a un almacenamiento en disco duro, puede seguir los siguientes pasos. (Tenga en cuenta que los sistemas de archivos de disco duro tienen una capacidad de almacenamiento mínima de 2 TB, y no se puede cambiar la capacidad de almacenamiento cuando se restaura a partir de una copia de seguridad).

1. Realice un backup del sistema de archivos de su SSD. Para obtener más información, consulte Crear copias de seguridad iniciadas por el usuario.
2. Restaure la copia de seguridad en un sistema de archivos mediante el almacenamiento en disco duro. Para obtener más información, consulte Restauración de copias de seguridad en un nuevo sistema de archivos.

Migración de archivos existentes a un servidor FSx de archivos de Windows mediante AWS DataSync

Te recomendamos que lo AWS DataSync utilices para transferir datos entre sistemas FSx de archivos del servidor de archivos de Windows. DataSync es un servicio de transferencia de

datos que simplifica, automatiza y acelera el traslado y la replicación de datos entre sistemas de almacenamiento locales y otros servicios de almacenamiento a través AWS de Internet 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.

DataSync permite copiar listas de control de acceso NTFS (ACLs) y también permite copiar información de control de auditoría de archivos, también conocidas como listas de control de acceso al sistema NTFS (SACLs), que los administradores utilizan para controlar el registro de auditoría de los intentos de los usuarios de acceder a los archivos.

Se puede utilizar DataSync para transferir archivos entre dos sistemas de archivos del servidor de archivos de Windows y también FSx para mover datos a un sistema de archivos de una cuenta Región de AWS o AWS sistema de archivos diferente. Se puede utilizar DataSync con FSx los sistemas de archivos del servidor de archivos de Windows 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 AWS DataSync, una ubicación FSx para un servidor de archivos de Windows es un punto final FSx para un servidor de archivos de Windows. Puede transferir archivos entre una ubicación FSx para el servidor de archivos de Windows y una ubicación para otros sistemas de archivos. Para obtener más información, consulte Trabajar con ubicaciones en la Guía del usuario de AWS DataSync .

DataSync accede a su servidor de archivos FSx para Windows mediante el protocolo Server Message Block (SMB). Se autentica con el nombre de usuario y la contraseña que configure en la AWS DataSync consola o. AWS CLI

Requisitos previos

Para migrar datos a la configuración del servidor de archivos de Amazon FSx para Windows, necesita un servidor y una red que cumplan los DataSync requisitos. Para obtener más información, consulte los requisitos DataSync de la Guía del AWS DataSync usuario.

Si va a realizar una migración de datos de gran tamaño o una migración que incluya muchos archivos pequeños, le recomendamos que utilice un sistema de FSx archivos Amazon con almacenamiento SSD. Esto se debe a que DataSync las tareas implican el escaneo de los metadatos de los archivos, lo que puede agotar los límites de IOPS de disco de los sistemas de archivos de disco duro, lo que provoca migraciones prolongadas y un impacto en el rendimiento del sistema de archivos. Para obtener más información, consulte: Prácticas recomendadas para migrar el almacenamiento de archivos existente a un servidor de archivos FSx de Windows.

Si su conjunto de datos se compone principalmente de archivos pequeños, con un número de archivos de millones o si tiene más ancho de banda de red disponible del que puede consumir una sola DataSync tarea, también puede acelerar las transferencias de datos con una arquitectura escalable. Para obtener más información, consulte: Cómo acelerar las transferencias de datos con arquitecturas AWS DataSync escalables.

Puede supervisar la utilización de E/S del disco de su sistema de archivos mediante métricas de FSx rendimiento.

Pasos básicos para migrar archivos mediante DataSync

Para transferir archivos desde una ubicación de origen a una ubicación de destino mediante DataSync, siga estos pasos básicos:

- Descargue e implemente un agente en su entorno y actívelo.
- Cree y configure una ubicación de origen y destino.
- Cree y configure una tarea.
- Ejecute la tarea para transferir archivos desde el origen al destino.

Para obtener información sobre cómo transferir archivos de un sistema de archivos local existente a su servidor de archivos FSx para Windows, consulte Transferencia de datos entre almacenamiento autogestionado y AWS, Creación de una ubicación para SMB y Creación de una ubicación para Amazon FSx para Windows File Server en la AWS DataSync Guía del usuario.

Para obtener información sobre cómo transferir archivos de un sistema de archivos en la nube existente a su servidor de archivos FSx para Windows, consulte Implementar su agente como una EC2 instancia de Amazon en la Guía del AWS DataSync usuario.

Migración entre dos sistemas de FSx archivos de Amazon

Se puede utilizar DataSync para migrar datos entre dos sistemas de FSx archivos de Amazon. Esto puede servirle si necesita trasladar su carga de trabajo de un sistema de archivos existente a un nuevo sistema de archivos con una configuración diferente, por ejemplo, de una configuración Single-AZ a una Multi-AZ. También se puede utilizar DataSync para dividir la carga de trabajo entre dos sistemas de archivos.

Este es un ejemplo de descripción general del proceso de migración:

1. Cree DataSync ubicaciones para los sistemas de archivos de origen y destino. Tenga en cuenta que el origen y el destino deben pertenecer al mismo dominio del Active Directory (AD) o tener una relación de confianza del AD entre ellos.
2. Cree y configure una DataSync tarea para transferir datos del origen al destino. Puede ejecutar la tarea como una instancia única, o puede la puede programar para que se ejecute de forma automática según lo configure.
3. Cuando la tarea finalice de forma correcta, los datos del sistema de archivos de destino serán una copia exacta de la fuente. Tenga en cuenta que, para completar esta tarea, tendrá que pausar cualquier actividad de escritura o actualización de archivos en el sistema de archivos de origen de manera momentánea. Luego, puede pasar al sistema de archivos de destino y eliminar el sistema de archivos de origen.

Antes de migrar desde el sistema de archivos de producción, puede probar el proceso de migración en un sistema de archivos que se haya restaurado a partir de una copia de seguridad reciente. Esto le permite estimar el tiempo que tarda el proceso de transferencia de datos y solucionar DataSync los errores con antelación.

Para minimizar el tiempo de transición, puede ejecutar DataSync las tareas con antelación y mover la mayoría de los datos del sistema de archivos de origen al sistema de archivos de destino. Tras detener el tráfico hacia el sistema de archivos de origen, puede ejecutar una última transferencia de tareas para sincronizar los datos que se hayan actualizado recientemente, desde que se detuvo el tráfico y, luego, pasarlos al sistema de archivos de destino.

Puede configurar DataSync las tareas para que solo se ejecuten en determinados directorios o para incluir o excluir determinadas rutas. Esto puede resultar útil si ejecuta varias tareas en paralelo o si desea migrar un subconjunto de datos.

Puede crear un alias del DNS en el sistema de archivos de destino que sea igual al nombre del DNS del de origen. Esto permite que los usuarios finales y las aplicaciones sigan accediendo a los datos de los archivos con el nombre del DNS del sistema de archivos de origen. Para obtener más información acerca de cómo configurar un alias del DNS, consulte Acceso a los datos mediante alias del DNS.

Cuando se realiza este tipo de migración, recomendamos lo siguiente:

- Programe la migración para evitar las copias de seguridad del sistema de archivos, el período de mantenimiento semanal y las tareas de `Data Deduplication`. En concreto, le recomendamos

deshabilitar la `Data Deduplication GarbageCollection` si coincide con la migración planificada.

- Utilice un tipo de almacenamiento en SSD para los sistemas de archivos de origen y destino. Puede cambiar entre los tipos de almacenamiento en HDD y SSD al hacer una restauración a partir de una copia de seguridad. Para obtener más información, consulte: Migración del almacenamiento de archivos existente a un servidor FSx de archivos de Windows.
- Configure los sistemas de archivos de origen y destino con una capacidad de rendimiento suficiente para la cantidad de datos que necesite transferir. Durante los procesos de DataSync tareas, supervise la utilización del rendimiento de los sistemas de archivos de origen y de destino. Para obtener más información, consulte: Monitorización con Amazon CloudWatch.
- Configure la DataSync supervisión para ayudarle a comprender el progreso de las tareas en curso. También puedes enviar DataSync registros al grupo Amazon CloudWatch Logs para ayudarte a depurar tus tareas si encuentras algún error.

Migración de archivos existentes al servidor de archivos FSx de Windows mediante Robocopy

Basado en Microsoft Windows Server, Amazon FSx for Windows File Server le permite migrar sus conjuntos de datos existentes por completo a sus sistemas de FSx archivos de Amazon. Puede migrar los datos de cada archivo. También puede migrar todos los metadatos de los archivos relevantes, incluidos los atributos, las marcas de tiempo, las listas de control de acceso (ACLs), la información del propietario y la información de auditoría. Con este soporte total de migración, Amazon FSx permite trasladar sus cargas de trabajo y aplicaciones basadas en Windows que dependen de estos conjuntos de datos de archivos a la nube de Amazon Web Services.

Utilice los siguientes temas como guía en el proceso de copia de los datos de archivos existentes. Al realizar esta copia, preserva todos los metadatos de los archivos de sus centros de datos locales o de sus servidores de archivos autogestionados en Amazon. EC2

Requisitos previos para la migración de archivos con Robocopy

Antes de comenzar, asegúrese de hacer lo siguiente:

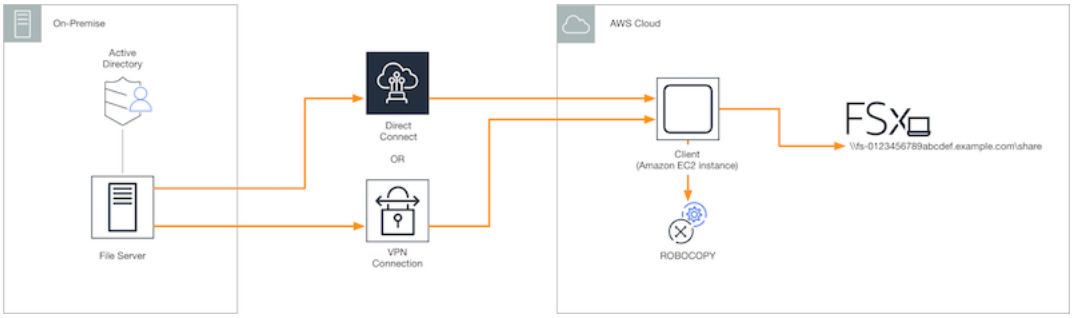
- Establezca la conectividad de red (mediante AWS Direct Connect una VPN) entre su Active Directory local y la VPC en la que desee crear el sistema de archivos de FSx Amazon.

- Crear una cuenta de servicio en el Active Directory con permisos delegados para unir equipos al dominio. Para obtener más información, consulte Delegar privilegios a su cuenta de servicio en la Guía de administración de AWS Directory Service .
- Cree un sistema de FSx archivos de Amazon, unido a su directorio autogestionado (local) de Microsoft AD.
- Anota la ubicación (por ejemplo`\\Source\Share`) del recurso compartido de archivos (local o interno AWS) que contiene los archivos existentes que deseas transferir a Amazon FSx.
- Anota la ubicación (por ejemplo`\\Target\Share`) del recurso compartido de archivos en tu sistema de FSx archivos de Amazon al que deseas transferir tus archivos existentes.

En la siguiente tabla se resumen los requisitos de accesibilidad de los sistemas de archivos de origen y destino para tres modelos de migración de acceso de los usuarios.

Modelo de acceso de los usuarios de migración	Requisitos de accesibilidad del sistema de archivos fuente	Requisitos de accesibilidad del servidor de FSx archivos de destino
Modelo de permisos de lectura/escritura directos	El usuario debe tener al menos permisos de lectura (NTFS ACLs) en los archivos y carpetas que se van a migrar.	El usuario debe tener al menos permisos de escritura (NTFS ACLs) en los archivos y carpetas que se van a migrar.
Modelo de privilegios de copia de seguridad/ restauración para anular los permisos de acceso	El usuario debe ser miembro del grupo de Operadores de Backup de Active Directory local y usar el indicador /b con. RoboCopy	El usuario debe ser miembro del grupo de administradores del sistema de FSx archivos de Amazon* y usar el indicador /b con. RoboCopy
Modelo de privilegios (completos) de administrador de dominios para anular los permisos de acceso	El usuario debe ser miembro del grupo de administradores de dominio del Active Directory en las instalaciones.	El usuario debe ser miembro del grupo de administradores del sistema de FSx archivos de Amazon* y usar el indicador /b con RoboCopy

> **Note**
>
> * Para los sistemas de archivos unidos a un Microsoft AD AWS gestionado, el grupo de administradores de sistemas de FSx archivos de Amazon es FSx Administradores AWS delegados. En tu Microsoft AD autogestionado, el grupo de administradores del sistema de FSx archivos de Amazon es Domain Admins o el grupo personalizado que especificaste para la administración cuando creaste tu sistema de archivos.



Migración de archivos con Robocopy

Puede migrar los archivos existentes de los sistemas de archivos locales a FSx los sistemas de archivos del servidor de archivos de Windows mediante el siguiente procedimiento.

Para migrar los archivos existentes a Amazon FSx mediante Robocopy

1. Lance una EC2 instancia de Amazon de Windows Server 2016 en la misma Amazon VPC que la de su sistema de FSx archivos de Amazon.
2. Conéctate a tu EC2 instancia de Amazon. Para obtener más información, consulte Conectarse a su instancia de Windows en la Guía del EC2 usuario de Amazon para instancias de Windows.
3. Abre la línea de comandos y asigna el archivo compartido de origen de tu servidor de archivos existente (local o interno AWS) a una letra de unidad (por ejemplo,*Y*:) de la siguiente manera. Para ello, debe proporcionar las credenciales de un miembro del grupo de Administradores de dominio de Active Directory en las instalaciones.

```
C:\>net use Y: \\fileserver1.mydata.com\localdata /user:mydata.com\Administrator
Enter the password for 'fileserver1.mydata.com': _

Drive Y: is now connected to \\fileserver1.mydata.com\localdata.
```

```
The command completed successfully.
```

4. Asigne el recurso compartido de archivos de destino en su sistema de FSx archivos de Amazon a una letra de unidad diferente (por ejemplo,*Z*:) en su EC2 instancia de Amazon de la siguiente manera. Como parte de esto, debe proporcionar las credenciales de una cuenta de usuario que es miembro del grupo de administradores de dominio de Active Directory local y del grupo de administradores del sistema de FSx archivos de Amazon. Para los sistemas de archivos unidos a un Microsoft AD AWS administrado, ese grupo es **`AWS Delegated FSx Administrators`**. En el Microsoft AD autoadministrado, ese grupo es **`Domain Admins`** o el grupo personalizado que haya asignado como administrador cuando creó el sistema de archivos.

   Para obtener más información, consulte la tabla de requisitos de accesibilidad del sistema de archivos de origen y destino en Requisitos previos para la migración de archivos con Robocopy.

   ```
   C:\>net use Z: \\amznfsxabcdef1.mydata.com\share /user:mydata.com\Administrator
   Enter the password for 'amznfsxabcdef1.mydata.com': _

   Drive Z: is now connected to \\amznfsxabcdef1.mydata.com\share.

   The command completed successfully.
   ```

5. Seleccione Ejecutar como administrador en el menú contextual. Abra Command Prompt o Windows PowerShell como administrador y ejecute el siguiente comando de Robocopy para copiar los archivos del recurso compartido de origen al recurso compartido de destino.

   El comando ROBOCOPY es una utilidad de transferencia de archivos flexible con múltiples opciones para controlar el proceso de transferencia de datos. Gracias a este proceso de ROBOCOPY comando, todos los archivos y directorios del recurso compartido de origen se copian al recurso compartido de FSx destino de Amazon. La copia conserva el NTFS del archivo y la carpeta ACLs, los atributos, las marcas de tiempo, la información del propietario y la información de auditoría.

   ```
   robocopy Y:\ Z:\ /copy:DATSOU /secfix /e /b /MT:8
   ```

   El comando de ejemplo anterior utiliza los siguientes elementos y opciones:

   - Y: hace referencia al recurso compartido de origen ubicado en el bosque del Active Directory en las instalaciones, mydata.com.

- Z: se refiere a la acción objetivo\\ amznfsxabcdef1.mydata.com\ share en Amazon. FSx
- /copy: especifica las siguientes propiedades del archivo que se van a copiar:
  - D: datos
  - A: atributos
  - T: marcas de tiempo
  - S: NTFS ACLs
  - O: información del propietario
  - U: información de auditoría.
- /secfix: corrige la seguridad de todos los archivos, incluso los omitidos.
- /e: copia los subdirectorios, incluso los vacíos.
- /b: utiliza los privilegios de copia de seguridad y restauración de Windows para copiar archivos aunque su NTFS ACLs deniegue los permisos al usuario actual.
- /MT:8: especifica cuántos subprocesos se van a utilizar para realizar copias con varios subprocesos.

> **Note**
>
> Si va a copiar archivos de gran tamaño a través de una conexión lenta o poco fiable, puede activar el modo reiniciable utilizando la opción de /zb con robocopy en lugar de la opción /b. Con el modo reiniciable, si se interrumpe la transferencia de un archivo de gran tamaño, la siguiente operación de Robocopy puede reanudarse en mitad de la transferencia, en lugar de tener que volver a copiar todo el archivo desde el principio. Habilitar el modo reiniciable puede reducir la velocidad de transferencia de datos.

Migración de las configuraciones de uso compartido de archivos locales a Amazon FSx

Puedes migrar una configuración de uso compartido de archivos existente a Amazon FSx mediante el siguiente procedimiento. En este procedimiento, el servidor de archivos de origen es el servidor de archivos cuya configuración de recursos compartidos de archivos quieres migrar a Amazon FSx.

> **Note**
>
> Primero, migre sus archivos a Amazon FSx antes de migrar su configuración de compartición de archivos. Para obtener más información, consulte Migración del almacenamiento de archivos existente a un servidor FSx de archivos de Windows.

Para migrar los recursos compartidos de archivos existentes FSx a Windows File Server

1. En el servidor de archivos de origen, seleccione Ejecutar como administrador en el menú contextual. Abra Windows PowerShell como administrador.
2. Exporte los archivos compartidos del servidor de archivos de origen a un archivo denominado `SmbShares.xml` ejecutando los siguientes comandos en PowerShell. En este ejemplo, sustituya F: por la letra de unidad del servidor de archivos desde el que exporta los recursos compartidos de archivos.

   ```
   $shareFolder = Get-SmbShare -Special $false | ? { $_.Path -like “F:\*” }
   $shareFolder | Export-Clixml -Path F:\SmbShares.xml
   ```

3. Edita el `SmbShares.xml` archivo y sustituye todas las referencias a F: (la letra de tu unidad) por D:\share, ya que los sistemas de FSx archivos de Amazon se encuentran en D:\share.
4. Importe la configuración de compartición de archivos existente FSx para Windows File Server. En un cliente que tenga acceso a tu sistema de FSx archivos Amazon de destino y al servidor de archivos de origen, copia la configuración de compartición de archivos guardada. A continuación, impórtela en una variable con el siguiente comando.

   ```
   $shares = Import-Clixml -Path F:\SmbShares.xml
   ```

5. Prepare el objeto de credenciales necesario para crear los recursos compartidos de archivos en su servidor de archivos FSx para Windows File Server mediante una de las siguientes opciones.

   Para generar el objeto de credenciales de forma interactiva, utilice el siguiente comando.

   ```
   $credential = Get-Credential
   ```

   Para generar el objeto de credenciales mediante un AWS Secrets Manager recurso, utilice el siguiente comando.

```
$credential = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
 $AdminSecret).SecretString
$FSxAdminUserCredential = (New-Object PSCredential($credential.UserName,(ConvertTo-
SecureString $credential.Password -AsPlainText -Force)))
```

6. Migre la configuración del recurso compartido de archivos a su servidor de FSx archivos de Amazon mediante el siguiente script.

```
$FSxAcceptedParameters = ("ContinuouslyAvailable", "Description",
 "ConcurrentUserLimit", "CATimeout", "FolderEnumerationMode", "CachingMode",
 "FullAccess", "ChangeAccess", "ReadAccess", "NoAccess", "SecurityDescriptor",
 "Path", "Name", "EncryptData")
ForEach ($item in $shares) {
    $param = @{};
    Foreach ($property in $item.psObject.properties) {
        if ($property.Name -In $FSxAcceptedParameters) {
            $param[$property.Name] = $property.Value
        }
    }
    Invoke-Command -ConfigurationName FSxRemoteAdmin -ComputerName
 amznfsxxxxxxxxx.corp.com -ErrorVariable errmsg -ScriptBlock { New-FSxSmbShare -
Credential $Using:credential @Using:param }
}
```

Migración de la configuración de DNS local al servidor de FSx archivos de Windows

FSx para Windows, el servidor de archivos proporciona un nombre de sistema de nombres de dominio (DNS) predeterminado para cada sistema de archivos que puede utilizar para acceder a los datos de su sistema de archivos. También puedes acceder a tus sistemas de archivos con cualquier nombre DNS que elijas configurando el nombre DNS alternativo como un alias de DNS para tu sistema de FSx archivos de Amazon.

Con los alias de DNS, puedes seguir utilizando tus nombres de DNS actuales para acceder a los datos almacenados en Amazon FSx al migrar el almacenamiento del sistema de archivos de un entorno local a Amazon. FSx Esto ayuda a eliminar la necesidad de actualizar cualquier herramienta o aplicación que utilice tus nombres de DNS al migrar a Amazon FSx. Puede asociar los alias de DNS a los sistemas de archivos del servidor de archivos de Windows existentes FSx al crear nuevos

sistemas de archivos y al crear un nuevo sistema de archivos a partir de una copia de seguridad. Puede asociar hasta 50 alias del DNS con un sistema de archivos en cualquier momento. Para obtener más información, consulte La administración de los alias del DNS.

Un alias del DNS debe cumplir los siguientes requisitos:

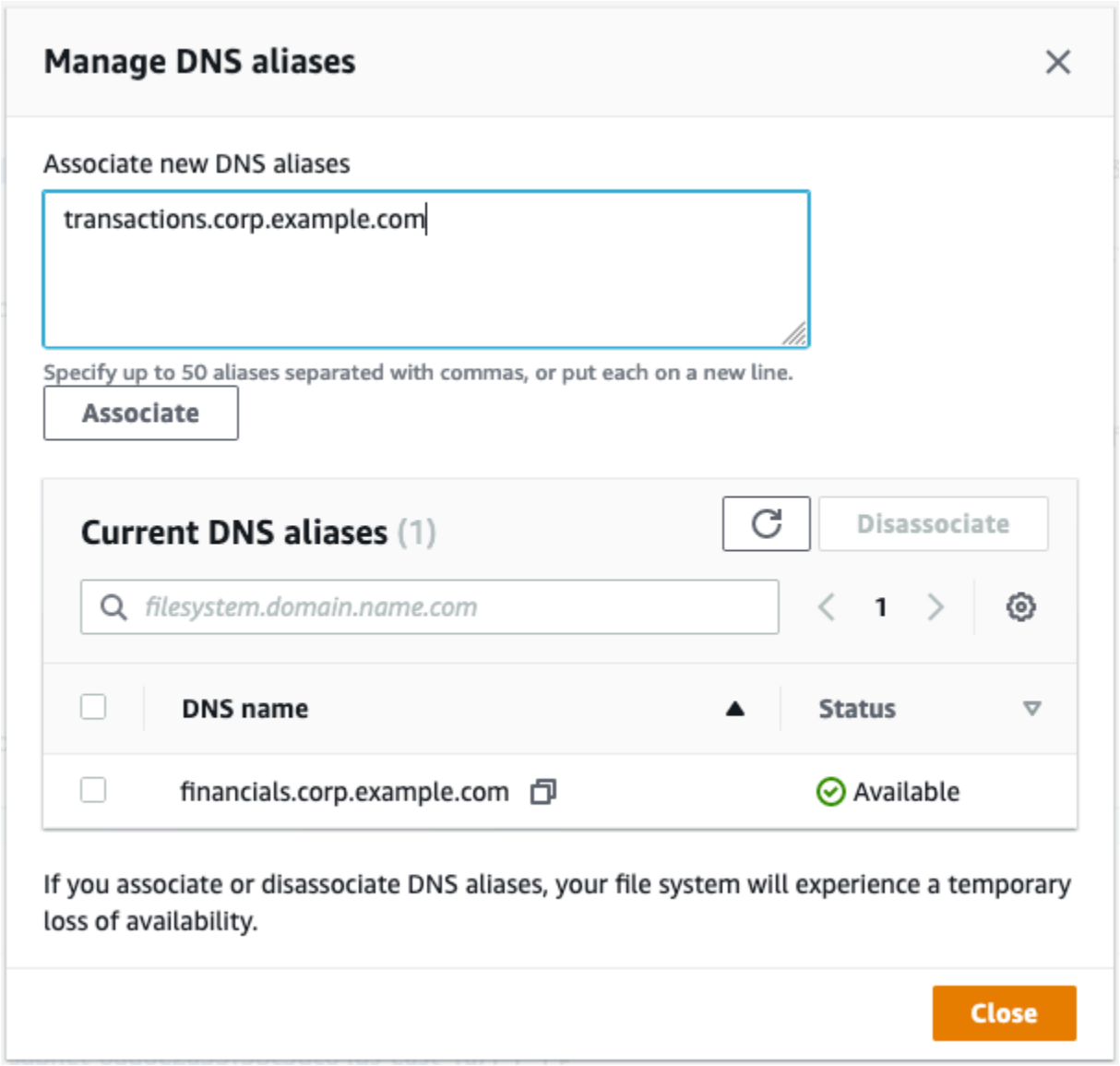
- Debe tener el formato del nombre de dominio completo (FQDN), por ejemplo, `accounting.example.com`.
- Puede contener caracteres alfanuméricos y guión (-).
- No puede empezar ni terminar con un guion.
- Puede comenzar con un número.

Para los nombres de alias de DNS, Amazon FSx almacena los caracteres alfabéticos como letras minúsculas (a-z), independientemente de cómo los especifiques: mayúsculas, minúsculas o las letras correspondientes en los códigos de escape.

Los siguientes procedimientos describen cómo asociar los alias de DNS con los sistemas de archivos FSx de Windows File Server existentes mediante la FSx consola, la CLI y la API de Amazon. Para obtener más información sobre la asociación de alias del DNS al crear nuevos sistemas de archivos, que incluye los nuevos sistemas de archivos a partir de una copia de seguridad, consulte Asociación de alias del DNS a los sistemas de archivos.

Para asociar alias del DNS con un sistema de archivos existente (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 de Windows al que desee asociar los alias del DNS.
3. En la pestaña Red y seguridad, seleccione Administrar en los Alias del DNS para abrir el cuadro de diálogo Administrar alias del DNS.



4. En el cuadro Asociar nuevos alias, introduzca los alias del DNS que desee asociar.
5. Seleccione Asociar para añadir los alias al sistema de archivos.

   Puede controlar el estado de los alias que acaba de asociar en la lista de Alias actuales. Cuando el estado es Disponible, el alias se asocia al sistema de archivos (un proceso que puede tardar hasta 2,5 minutos).

Para asociar los alias del DNS a un sistema de archivos (CLI) existente

- Utilice el comando `associate-file-system-aliases` CLI o la operación AssociateFileSystemAliasesAPI para asociar los alias DNS a un sistema de archivos existente.

La siguiente solicitud de CLI asocia dos alias con el sistema de archivos especificado.

```
aws fsx associate-file-system-aliases \
    --file-system-id fs-0123456789abcdef0 \
    --aliases financials.corp.example.com transfers.corp.example.com
```

La respuesta muestra el estado de los alias que Amazon FSx está asociando al sistema de archivos.

```
{
      "Aliases": [
          {
              "Name": "financials.corp.example.com",
              "Lifecycle": CREATING
          },
          {
              "Name": "transfers.corp.example.com",
              "Lifecycle": CREATING
          }
      ]
  }
```

Para supervisar el estado de los alias que está asociando, utilice el comando `describe-file-system-aliases` CLI (DescribeFileSystemAliases es la operación API equivalente). Cuando el `Lifecycle` de un alias tiene el valor DISPONIBLE, puede usarlo para acceder al sistema de archivos (un proceso que puede tardar hasta 2,5 minutos).

Traslado de las operaciones a Amazon FSx para Windows File Server

Tras migrar el almacenamiento de archivos local, la configuración de los recursos compartidos de archivos y la configuración de DNS, el siguiente paso es pasar las operaciones a los sistemas de archivos del servidor FSx de archivos de Windows. Para pasar al sistema de archivos del servidor de archivos de Windows, lleve a cabo los siguientes pasos: FSx

- Prepararse para la migración total.

  - Desconecte temporalmente los clientes SMB del sistema de archivos original.
  - Realice una sincronización final de la configuración del archivo y del recurso compartido de archivos.
- Configura los nombres principales de servicio (SPNs) para tu sistema de FSx archivos de Amazon.
- Actualiza los registros CNAME de DNS para que apunten a tu sistema de FSx archivos de Amazon.

Los procedimientos para realizar cada uno de estos pasos se encuentran en las siguientes secciones.

Temas

- Preparándose para la transición a Amazon FSx
- Configure SPNs para la autenticación Kerberos
- Actualiza los registros CNAME de DNS para el sistema de FSx archivos de Amazon

Preparándose para la transición a Amazon FSx

Para preparar la transición a tu sistema de FSx archivos de Amazon, debes hacer lo siguiente:

- Desconecte todos los clientes que escriban en el sistema de archivos original.
- Realice una sincronización final de archivos mediante Robocopy AWS DataSync . Para obtener más información, consulte Migración del almacenamiento de archivos existente a un servidor FSx de archivos de Windows.
- Realice una sincronización final de la configuración del recurso compartido de archivos. Para obtener más información, consulte Migración de las configuraciones de uso compartido de archivos locales a Amazon FSx.

Configure SPNs para la autenticación Kerberos

Te recomendamos que utilices la autenticación y el cifrado basados en Kerberos en tránsito con Amazon. FSx Kerberos brinda la autenticación más segura para los clientes que acceden a su sistema de archivos. Para habilitar la autenticación Kerberos para los clientes que acceden a Amazon FSx mediante un alias de DNS, debe añadir los nombres principales de servicio (SPNs) que correspondan al alias de DNS del objeto informático de Active Directory del sistema de FSx archivos de Amazon.

Se requieren dos SPNs para la autenticación de Kerberos.

```
HOST/alias
HOST/alias.domain
```

Por ejemplo, si el alias es`finance.domain.com`, los dos necesarios SPNs son los siguientes.

```
HOST/finance
HOST/finance.domain.com
```

Un SPN sólo puede asociarse a un único objeto informático de Active Directory a la vez. Si existen nombres DNS configurados SPNs para el objeto informático de Active Directory de su sistema de archivos original, debe eliminarlos antes de crearlos SPNs para su sistema de FSx archivos de Amazon.

Los siguientes procedimientos describen cómo encontrar los objetos existentes SPNs, eliminarlos y crear nuevos SPNs para el objeto informático de Active Directory del sistema de FSx archivos de Amazon.

Para instalar el módulo de PowerShell Active Directory necesario

1. Inicie sesión en una instancia de Windows unida al Active Directory al que está unido su sistema de FSx archivos de Amazon.
2. PowerShell Ábrela como administrador.
3. Instale el módulo PowerShell Active Directory mediante el siguiente comando.

   ```
   Install-WindowsFeature RSAT-AD-PowerShell
   ```

Para buscar y eliminar el alias de DNS existente SPNs en el objeto informático de Active Directory del sistema de archivos original

1. Busque cualquier existente SPNs mediante los siguientes comandos. Sustituya *alias_fqdn* por el alias del DNS que asoció al sistema de archivos en Migración de la configuración de DNS local al servidor de FSx archivos de Windows.

   ```
   ## Find SPNs for original file system's AD computer object
   $ALIAS = "alias_fqdn"
   SetSPN /Q ("HOST/" + $ALIAS)
   ```

```
SetSPN /Q ("HOST/" + $ALIAS.Split(".")[0])
```

2. Elimine el HOST existente SPNs devuelto en el paso anterior mediante el siguiente script de ejemplo.

   - Sustituya *alias_fqdn* por el alias del DNS completo que asoció al sistema de archivos en Migración de la configuración de DNS local al servidor de FSx archivos de Windows.
   - Sustituya *file_system_DNS_name* por el nombre del DNS del sistema de archivos original.

```
## Delete SPNs for original file system's AD computer object
$Alias = "alias_fqdn"
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})

SetSPN /D ("HOST/" + ${Alias}) ${FSxAdComputer}.Name
SetSPN /D ("HOST/" + ${Alias}.Split(".")[0]) ${FSxAdComputer}.Name
```

3. Repita estos pasos para cada alias del DNS que haya asociado al sistema de archivos en Migración de la configuración de DNS local al servidor de FSx archivos de Windows.

Para configurar SPNs en el objeto informático de Active Directory del sistema de FSx archivos de Amazon

1. Configura un nuevo FSx archivo SPNs para tu sistema de archivos de Amazon ejecutando los siguientes comandos.

   - *file_system_DNS_name*Sustitúyalo por el nombre DNS que Amazon FSx asignó al sistema de archivos.

     Para encontrar el nombre DNS de tu sistema de archivos en la FSx consola de Amazon, selecciona Sistemas de archivos y elige tu sistema de archivos. Seleccione el panel Red y seguridad de la página de información del sistema de archivos. También puedes obtener el nombre DNS en la respuesta a la operación de la DescribeFileSystemsAPI.
   - Sustituya *alias_fqdn* por el alias del DNS completo que asoció al sistema de archivos en Migración de la configuración de DNS local al servidor de FSx archivos de Windows.

```
## Set SPNs for FSx file system AD computer object
$FSxDnsName = "file_system_DNS_name"
$Alias = "alias_fqdn"
$FileSystemHost = (Resolve-DnsName $FSxDnsName | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity $FileSystemHost)

Set-AdComputer -Identity $FSxAdComputer -Add @{"msDS-
AdditionalDnsHostname"="$Alias"}
SetSpn /S ("HOST/" + $Alias.Split('.')[0]) $FSxAdComputer.Name
SetSpn /S ("HOST/" + $Alias) $FSxAdComputer.Name
```

> **Note**
>
> Se producirá un error al configurar un SPN para tu sistema de FSx archivos de Amazon si existe un SPN para el alias DNS en el AD del objeto informático del sistema de archivos original. Para obtener información sobre cómo buscar y eliminar los existentes SPNs, consulta. Para buscar y eliminar el alias de DNS existente SPNs en el objeto informático de Active Directory del sistema de archivos original

2. Compruebe que los nuevos SPNs están configurados para el alias DNS mediante el siguiente script de ejemplo. Asegúrese de que la respuesta incluya dos HOST SPNs `HOST/alias` y`HOST/alias_fqdn`.

   *file_system_DNS_name*Sustitúyelo por el nombre DNS que Amazon FSx asignó a su sistema de archivos. Para encontrar el nombre DNS de tu sistema de archivos en la FSx consola de Amazon, selecciona Sistemas de archivos, elige tu sistema de archivos y, a continuación, selecciona el panel Red y seguridad en la página de detalles del sistema de archivos.

   También puedes obtener el nombre DNS en la respuesta a la operación de la DescribeFileSystemsAPI.

```
## Verify SPNs on FSx file system AD computer object
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})
SetSpn /L ${FSxAdComputer}.Name
```

3. Repita los pasos anteriores para cada alias del DNS que tenga asociado al sistema de archivos Migración de la configuración de DNS local al servidor de FSx archivos de Windows.

> **Note**
>
> Puede aplicar la autenticación y el cifrado de Kerberos en tránsito con los clientes que se conectan a su sistema de archivos mediante alias de DNS configurando los siguientes objetos de política de grupo (GPOs) en su Active Directory:
>
> - Restrinja el NTLM: el tráfico NTLM saliente a servidores remotos
> - Restrinja el NTLM: agregue excepciones de servidor remoto para la autenticación del NTLM
>
> Para obtener más información, consulte Aplicar la autenticación de Kerberos mediante objetos de política de grupo () GPOs en la Explicación 5: eso de alias del DNS para acceder al sistema de archivos.

Actualiza los registros CNAME de DNS para el sistema de FSx archivos de Amazon

Tras configurar correctamente el sistema SPNs de archivos, puede pasar a Amazon FSx sustituyendo cada registro DNS que se resolvió en el sistema de archivos original por un registro DNS que se resolviera en el nombre DNS predeterminado del sistema de FSx archivos de Amazon.

Para instalar los PowerShell cmdlets necesarios

1. Inicie sesión en una instancia de Windows unida a Active Directory a la que esté unido su sistema de FSx archivos de Amazon como usuario que sea miembro de un grupo que tenga permisos de administración de DNS (administradores del sistema de nombres de dominio AWS delegados en Microsoft Active Directory AWS administrado y administradores de dominio u otro grupo al que haya delegado permisos de administración de DNS en su Active Directory autogestionado)

   Para obtener más información, consulta Cómo conectarse a tu instancia de Windows en la Guía del EC2 usuario de Amazon.
2. Abre PowerShell como administrador.

3. El módulo del servidor PowerShell DNS es necesario para realizar las instrucciones de este procedimiento. Instálelo con el siguiente comando.

```
Install-WindowsFeature RSAT-DNS-Server
```

Para actualizar un registro CNAME del DNS existente

1. El siguiente script actualiza todos los registros CNAME de DNS existentes *alias_fqdn* para el objeto informático de tu sistema de FSx archivos de Amazon. Si no se encuentra ninguno, se crea un nuevo registro CNAME de DNS para el alias de DNS *alias_fqdn* que se convierte en el nombre de DNS predeterminado de tu sistema de FSx archivos de Amazon.

   Para ejecutar el script:

   - Sustituya *alias_fqdn* por el alias del DNS que asoció al sistema de archivos.
   - *file_system_DNS_name*Sustitúyalo por el nombre DNS predeterminado FSx que Amazon ha asignado al sistema de archivos.

```
$Alias="alias_fqdn"
$FSxDnsName="file_system_dns_name"
$AliasHost=$Alias.Split('.')[0]
$ZoneName=((Get-WmiObject Win32_ComputerSystem).Domain)
$DnsServerComputerName = (Resolve-DnsName $ZoneName -Type NS | Where Type -eq 'A' |
 Select -ExpandProperty Name)[0]

Add-DnsServerResourceRecordCName -Name $AliasHost -ComputerName
 $DnsServerComputerName -HostNameAlias $FSxDnsName -ZoneName $ZoneName
```

2. Repita el paso anterior para cada alias del DNS que tenga asociado al sistema de archivos en Migración de la configuración de DNS local al servidor de FSx archivos de Windows.

Supervisión FSx de sistemas de archivos de Windows File Server

La supervisión es una parte importante para mantener la confiabilidad, la disponibilidad y el rendimiento FSx de Windows File Server y sus AWS soluciones. Debe recopilar los datos de supervisión de todas las partes de la AWS solución para poder depurar más fácilmente los errores en caso de que se produzcan. Sin embargo, antes de empezar a supervisar FSx el servidor de archivos de Windows, debe crear un plan de supervisión que incluya las respuestas a las siguientes preguntas:

- ¿Cuáles son los objetivos de la supervisión?
- ¿Qué recursos va a supervisar?
- ¿Con qué frecuencia va a supervisar estos recursos?
- ¿Qué herramientas de supervisión va a utilizar?
- ¿Quién se encargará de realizar las tareas de supervisión?
- ¿Quién debería recibir una notificación cuando surjan problemas?

Para obtener más información sobre el inicio de sesión y FSx la supervisión de Windows File Server, consulte los temas siguientes.

Temas

- Supervisión automatizada y manual
- Monitorización con Amazon CloudWatch
- Registro de llamadas a la API de Amazon FSx para Windows File Server mediante AWS CloudTrail

Supervisión automatizada y manual

AWS proporciona varias herramientas que puede utilizar FSx para supervisar el servidor de archivos de Windows. Puede configurar algunas de estas herramientas para que supervisen por usted, mientras que otras requieren una intervención manual. Le recomendamos que automatice las tareas de supervisión en la medida de lo posible.

Herramientas de monitoreo automatizadas

Puede utilizar las siguientes herramientas de supervisión automática FSx para detectar el servidor de archivos de Windows e informar cuando algo vaya mal:

- Amazon CloudWatch Alarms: observe una sola métrica durante un período de tiempo que especifique y realice una o más acciones en función del valor de la métrica en relación con un umbral determinado durante varios períodos de tiempo. La acción es una notificación enviada a un tema del Servicio de Notificación Simple (Amazon SNS) o a una política de Amazon EC2 Auto Scaling. CloudWatch las alarmas no invocan acciones simplemente porque se encuentran en un estado determinado; el estado debe haber cambiado y se ha mantenido durante un número específico de períodos. Para obtener más información, consulte Monitorización con Amazon CloudWatch.
- Amazon CloudWatch Logs: supervise, almacene y acceda a sus archivos de registro desde AWS CloudTrail u otras fuentes. Para obtener más información, consulta ¿Qué es Amazon CloudWatch Logs? en la Guía del usuario CloudWatch de Amazon Logs.
- AWS CloudTrail Supervisión de registros: comparta archivos de registro entre cuentas, supervise los archivos de CloudTrail registro en tiempo real enviándolos a CloudWatch Logs, escriba aplicaciones de procesamiento de registros en Java y valide que sus archivos de registro no hayan cambiado después de su entrega CloudTrail. Para obtener más información, consulte Trabajar con archivos de CloudTrail registro en la Guía del AWS CloudTrail usuario.

Herramientas de supervisión manuales

Otra parte importante de la supervisión FSx de Windows File Server implica la supervisión manual de los elementos que las CloudWatch alarmas de Amazon no cubren. Los paneles de control de la AWS consola FSx para Windows CloudWatch, el servidor de archivos y otros paneles proporcionan una at-a-glance vista del estado de su AWS entorno.

El panel FSx de monitoreo y rendimiento de Amazon muestra:

- Advertencias y CloudWatch alarmas actuales
- Un resumen de la actividad del sistema de archivos
- La capacidad de almacenamiento y la utilización del sistema de archivos
- El rendimiento del volumen de almacenamiento y del servidor de archivos
- CloudWatch alarmas

Amazon CloudWatch Dashboard muestra:

- Alarmas y estado actual
- Gráficos de alarmas y recursos
- Estado de los servicios

Además, puedes CloudWatch hacer lo siguiente:

- Crear paneles personalizados para supervisar los servicios que utiliza.
- Realizar un gráfico con los datos de las métricas para resolver problemas y descubrir tendencias.
- Busca y examina todas las métricas AWS de tus recursos.
- Crear y editar las alarmas de notificación de problemas.

Para obtener más información sobre el panel FSx de monitoreo y rendimiento de Amazon, consulteUso de métricas del sistema de archivos.

Monitorización con Amazon CloudWatch

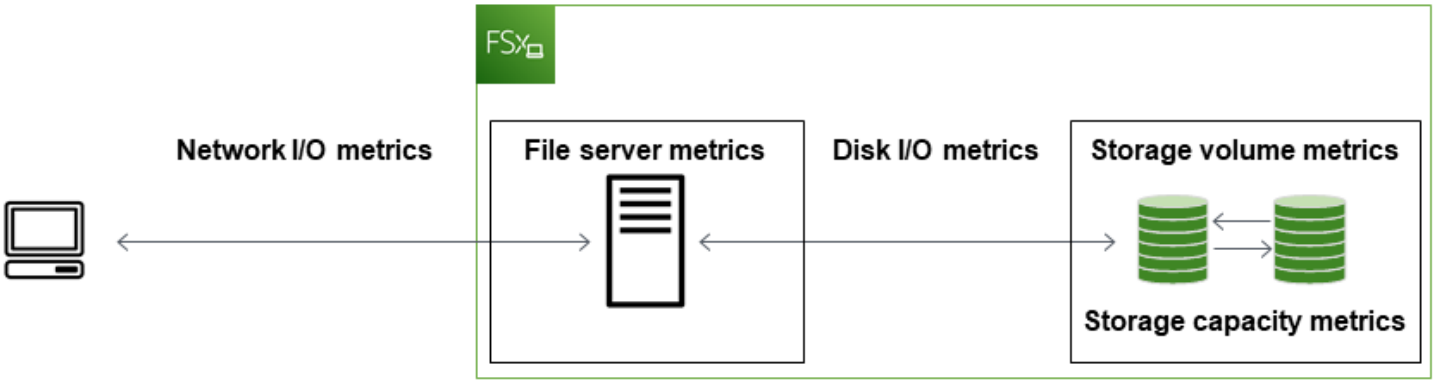
Amazon CloudWatch recopila y procesa datos sin procesar de su sistema de archivos FSx para Windows File Server para convertirlos en métricas legibles y prácticamente en tiempo real. Estas estadísticas se retienen por un periodo de 15 meses, lo que le proporciona acceso a la información del historial y lo ayuda a tener una perspectiva del desempeño del flujo de trabajo o del sistema de archivos.

FSx para Windows File Server publica CloudWatch métricas en los siguientes dominios:

- Las métricas de E/S de la red miden la actividad entre los clientes que acceden al sistema de archivos y al servidor de archivos.
- Las métricas del servidor de archivos miden el uso del rendimiento de la red, la CPU y la memoria del servidor de archivos y el rendimiento del disco del servidor de archivos y la utilización de IOPS.
- Las métricas de E/S del disco miden la actividad que hay entre el servidor de archivos y los volúmenes de almacenamiento.
- Las métricas de volumen de almacenamiento miden el rendimiento del disco, la utilización de los volúmenes de almacenamiento en HDD y la utilización de IOPS en los volúmenes de almacenamiento en SSD.

- Las métricas de capacidad de almacenamiento miden el uso del almacenamiento, incluidos los ahorros de almacenamiento derivados de la desduplicación de datos.

El siguiente diagrama ilustra un sistema FSx de archivos del servidor de archivos de Windows, sus componentes y los dominios métricos.



De forma predeterminada, Amazon FSx for Windows File Server envía los datos de las métricas CloudWatch en períodos de 1 minuto, con las siguientes excepciones, que se emiten en intervalos de 5 minutos:

- `FileServerDiskThroughputBalance`
- `FileServerDiskIopsBalance`

Para obtener más información CloudWatch, consulta ¿Qué es Amazon CloudWatch? en la Guía del CloudWatch usuario de Amazon.

Es posible que no se publiquen las métricas de los sistemas de archivos Single-AZ durante el mantenimiento del sistema o la sustitución de componentes de la infraestructura. De la misma manera, es posible que no se publiquen las métricas de los sistemas de archivos Multi-AZ durante la conmutación por error y la conmutación por recuperación entre los servidores de archivos principal y secundario.

Algunas FSx CloudWatch métricas de Amazon se presentan como bytes sin procesar. Los bytes no se redondean a un decimal o múltiple binario de la unidad.

Temas

- CloudWatch métricas y dimensiones
- Uso de métricas del sistema de archivos
- Advertencias y recomendaciones de rendimiento

- Acceso a métricas del sistema de archivos
- Creación de CloudWatch alarmas

CloudWatch métricas y dimensiones

FSx para Windows File Server publica las siguientes métricas en el espacio de `AWS/FSx` nombres de Amazon CloudWatch para todos los sistemas de archivos:

- `DataReadBytes`
- `DataWriteBytes`
- `DataReadOperations`
- `DataWriteOperations`
- `MetadataOperations`
- `FreeStorageCapacity`

FSx para Windows File Server publica las métricas descritas en las siguientes secciones en el espacio de `AWS/FSx` nombres de Amazon CloudWatch para sistemas de archivos configurados con una capacidad de rendimiento de al menos 32. MBps

Métricas de E/S de red

El espacio de nombres `AWS/FSx` incluye las siguientes métricas de E/S de red.

Métrica	Descripción
`DataReadBytes`	El número de bytes de las operaciones de lectura de los clientes que acceden al sistema de archivos. Unidades: bytes Estadísticas válidas: `Sum`
`DataWriteBytes`	El número de bytes de las operaciones de escritura de los clientes que acceden al sistema de archivos. Unidades: bytes

Métrica	Descripción
	Estadísticas válidas: `Sum`
`DataReadOperations`	El número de operaciones de lectura de los clientes que acceden al sistema de archivos. Unidades: recuento Estadísticas válidas: `Sum`
`DataWriteOperations`	El número de operaciones de escritura de los clientes que acceden al sistema de archivos. Unidades: recuento Estadísticas válidas: `Sum`
`MetadataOperations`	El número de operaciones de metadatos de los clientes que acceden al sistema de archivos. Unidades: recuento Estadísticas válidas: `Sum`
`ClientConnections`	El número de conexiones activas entre los clientes y el servidor de archivos. Unidades: recuento

Métricas del servidor de archivos

El espacio de nombres `AWS/FSx` incluye las siguientes métricas del sistema de archivos.

Métrica	Descripción
`NetworkThroughputUtilization`	El rendimiento de la red de los clientes que acceden al sistema de archivos, expresado como porcentaje del límite aprovisionado.

Métrica	Descripción
	Unidad: porcentaje
`CPUUtilization`	El porcentaje de utilización de los recursos del CPU del servidor de archivos. Unidad: porcentaje
`MemoryUtilization`	El porcentaje de utilización de los recursos de la memoria del servidor de archivos. Unidad: porcentaje
`FileServerDiskThroughputUtilization`	El rendimiento del disco entre el servidor de archivos y sus volúmenes de almacenamiento, expresado en el porcentaje del límite aprovisionado que lo determina la capacidad de rendimiento. Unidad: porcentaje
`FileServerDiskThroughputBalance`	El porcentaje de créditos de ráfaga que están disponibles para el rendimiento del disco entre el servidor de archivos y sus volúmenes de almacenamiento. Válido para sistemas de archivos aprovisionados con una capacidad de rendimiento de 256 o menos. MBps Unidad: porcentaje
`FileServerDiskIopsUtilization`	Las IOPS de disco entre el servidor de archivos y los volúmenes de almacenamiento, como el porcentaje del límite aprovisionado que lo determina la capacidad de rendimiento. Unidad: porcentaje

Métrica	Descripción
`FileServerDiskIopsBalance`	El porcentaje de créditos de ráfaga disponibles para las IOPS de disco entre el servidor de archivos y sus volúmenes de almacenamiento. Válido para sistemas de archivos aprovisionados con una capacidad de rendimien to de 256 o menos. MBps Unidad: porcentaje

Métricas de E/S de disco

El espacio de nombres de `AWS/FSx` incluye las siguientes métricas de E/S de disco.

Métrica	Descripción
`DiskReadBytes`	El número de bytes de las operaciones de lectura que acceden a los volúmenes de almacenamiento. Unidades: bytes Estadísticas válidas: Sum
`DiskWriteBytes`	El número de bytes de las operaciones de escritura que acceden a los volúmenes de almacenamiento. Unidades: bytes Estadísticas válidas: Sum
`DiskRead0 perations`	El número de operaciones de lectura del servidor de archivos que accede a los volúmenes de almacenamiento. Unidades: recuento Estadísticas válidas: `Sum`
`DiskWrite Operations`	El número de operaciones de escritura del servidor de archivos que accede a los volúmenes de almacenamiento.

Métrica	Descripción
	Unidades: recuento Estadísticas válidas: `Sum`

FSx para métricas de volumen de almacenamiento de Windows

El espacio de nombres `AWS/FSx` incluye las siguientes métricas de los volúmenes de almacenamiento.

Métrica	Descripción
`DiskThroughputUtilization`	(Solo en HDD) El rendimiento del disco entre el servidor de archivos y sus volúmenes de almacenamiento, expresado en un porcentaje del límite aprovisionado que determinan los volúmenes de almacenamiento. Unidad: porcentaje
`DiskThroughputBalance`	(Solo en HDD) El porcentaje de créditos de expansión disponibles para el rendimiento y las IOPS del disco según los volúmenes de almacenamiento. Unidad: porcentaje
`DiskIopsUtilization`	(Solo en SSD) Las IOPS del disco entre el servidor de archivos y los volúmenes de almacenamiento, expresado en un porcentaje del límite de IOPS aprovisionadas que determinan los volúmenes de almacenamiento. Unidad: porcentaje

Métricas de capacidad de almacenamiento

El espacio de nombres `AWS/FSx` incluye las siguientes métricas de la capacidad de almacenamiento.

Métrica	Descripción
`FreeStorageCapacity`	La cantidad de capacidad de almacenamiento disponible. Unidades: bytes Estadísticas válidas: `Average`, `Minimum`
`StorageCapacityUtilization`	La capacidad de almacenamiento físico utilizado expresado en un porcentaje de la capacidad total de almacenamiento. Unidad: porcentaje
`DeduplicationSavedStorage`	La cantidad de espacio de almacenamiento que ahorra la desduplicación de datos, si está habilitada. Unidades: bytes

Espacio de nombres y dimensiones FSx para las métricas del servidor de archivos de Windows

FSx para las métricas del servidor de archivos de Windows, utilice el espacio de `FSx` nombres y proporcione métricas para una sola dimensión,. `FileSystemId` Puede encontrar el ID de un sistema de archivos mediante el describe-file-systems AWS CLI comando o el comando DescribeFileSystemsAPI. El ID de un sistema de archivos adopta la forma de*`fs-0123456789abcdef0`*.

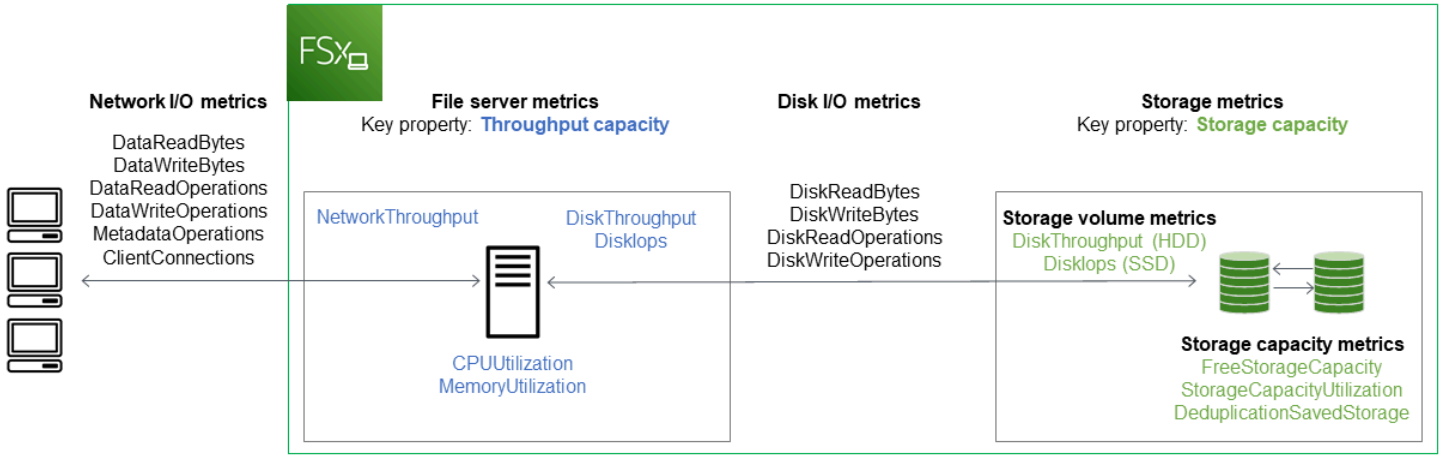
Uso de métricas del sistema de archivos

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

- El servidor de archivos que proporciona los datos a los clientes que acceden al sistema de archivos.
- Los volúmenes de almacenamiento que alojan los datos en el sistema de archivos.

FSx en el caso de Windows, File Server publica métricas CloudWatch que permiten realizar un seguimiento del rendimiento y el uso de los recursos del servidor de archivos y los volúmenes de

almacenamiento de su sistema de archivos. El siguiente diagrama ilustra un sistema de FSx archivos de Amazon con sus componentes arquitectónicos y las CloudWatch métricas de rendimiento y recursos disponibles para la supervisión. La propiedad clave que se muestra para un conjunto de métricas es la del sistema de archivos que determina la capacidad de esas métricas. Al ajustar esa propiedad, se modifica el rendimiento del sistema de archivos de ese conjunto de métricas.



Usa el panel Supervisión y rendimiento de la FSx consola de Amazon FSx para ver las CloudWatch métricas del servidor de archivos de Windows que se describen en la siguiente tabla.

Panel de Supervisión y rendimiento	¿Cómo...?	Gráfico	Métricas relevantes
Resumen	... determino las IOPS totales de mi sistema de archivos?	Total de IOPS	SUMA(`DataReadOperations + DataWriteOperations +MetadataOperations`)/Período (en segundos)
	... determino el rendimiento total de mi sistema de archivos?	Rendimiento total	SUMA(`DataReadBytes +DataWriteBytes`)/Período (en segundos)

Panel de Supervisión y rendimiento	¿Cómo...?	Gráfico	Métricas relevantes
Almacenamiento	... determino la cantidad de capacidad de almacenamiento disponible en mi sistema de archivos?	Capacidad de almacenamiento disponible	`FreeStorageCapacity`
	... determino el número de conexiones que se establecen entre los clientes y el servidor de archivos?	Conexiones de clientes	`ClientConnections`
	... determino la cantidad de espacio físico en disco utilizado expresado en un porcentaje de la capacidad total de almacenamiento del sistema de archivos?	Utilización de la capacidad de almacenamiento	`StorageCapacityUtilization`
	... determino la cantidad de espacio físico en disco que ahorra la desduplicación de datos?	Almacenamiento ahorrado por la desduplicación de datos	`DeduplicationSavedStorage`

Panel de Supervisión y rendimiento	¿Cómo...?	Gráfico	Métricas relevantes
	... determino el rendimiento de la red de los clientes que acceden al sistema de archivos, expresado en un porcentaje del rendimiento aprovisionado del sistema de archivos?	Utilización del rendimiento de la red	`NetworkThroughputUtilization` [1]
	... determino el rendimiento del disco entre el servidor de archivos y sus volúmenes de almacenamiento, expresado en un porcentaje del límite aprovisionado que determina la capacidad de rendimiento?	Utilización de rendimiento de disco	`FileServerDiskThroughputUtilization` [1]
Rendimiento: servidor de archivos	... determino el porcentaje de créditos de ráfaga disponibles para el rendimiento del disco entre el servidor de archivos y sus volúmenes de almacenamiento?	Rendimiento de disco y saldo de ráfaga	`FileServerDiskThroughputBalance`
	... determino la cantidad de IOPS de disco que hay entre el servidor de archivos y los volúmenes de almacenamiento, expresado en un porcentaje del límite aprovisionado que determina la capacidad de rendimiento?	Utilización de IOPS de disco	`FileServerDiskIopsUtilization`
	... determino el porcentaje de créditos de ráfaga disponibles para las IOPS de disco entre el servidor de archivos y los volúmenes de almacenamiento?	Saldo de ráfaga de IOPS de disco	`FileServerDiskIopsBalance`

Panel de Supervisión y rendimiento	¿Cómo...?	Gráfico	Métricas relevantes
	... determino el porcentaje de utilización del CPU del servidor de archivos?	Utilización de la CPU	`CPUUtilization`
	... determino el porcentaje de utilización de la memoria del servidor de archivos?	Utilización de la memoria	`MemoryUtilization`
Rendimiento: volúmenes de almacenamiento	... determino el rendimiento de las operaciones que acceden a los volúmenes de almacenamiento, expresado en un porcentaje del límite aprovisionado que determina la capacidad de almacenamiento en HDD?	Utilización del rendimiento de disco (HDD)	`DiskThroughputUtilization`
	…determina el porcentaje de créditos de expansión disponibles para el rendimiento y las IOPS de las operaciones que acceden a los volúmenes de almacenamiento en HDD?	Saldo de ráfagas del rendimiento del disco (HDD)	`DiskThroughputBalance` [2]

Panel de Supervisión y rendimiento	¿Cómo...?	Gráfico	Métricas relevantes
	…determina las IOPS para las operaciones que acceden a los volúmenes de almacenamiento, expresado en un porcentaje del límite aprovisionado que determina la capacidad de almacenamiento en HSD?	Utilización de IOPS en disco (HSD)	SUM (`DiskReadOperations` + `DiskWriteOperations`)/`Period` (en segundos)/ (12 * capacidad de almacenamiento en HDD aprovisionada en TiB)
	... determino las IOPS para las operaciones que acceden a los volúmenes de almacenamiento, expresado en un porcentaje del límite aprovisionado que determinar la capacidad de almacenamiento en SSD?	Utilización de IOPS de disco (SSD)	`DiskIopsUtilization`

Note

[1]Le recomendamos que mantenga una utilización media de la capacidad de rendimiento inferior al 50 % para asegurarse de tener suficiente capacidad de rendimiento sobrante para los picos inesperados de la carga de trabajo, así como para cualquier operación de almacenamiento de Windows en segundo plano (como la sincronización del almacenamiento, la desduplicación o las copias de redundancia).

[2]Los volúmenes de almacenamiento en HDD pueden tener variaciones de rendimiento significativas en función de la carga de trabajo. Los picos repentinos de IOPS o del rendimiento pueden provocar una degradación del rendimiento del disco. Para obtener más información, consulte Rendimiento por ráfagas de HDD.

Advertencias y recomendaciones de rendimiento

FSx para Windows proporciona advertencias de rendimiento para los sistemas de archivos configurados con una capacidad de rendimiento de al menos 32 MBps. Amazon FSx muestra una advertencia para un conjunto de CloudWatch 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 se encuentre en estado de ALARMA aparecen en el panel Supervisión y rendimiento de la sección Resumen. La advertencia también aparece en la sección del panel en la que figura el gráfico métrico.

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

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.

Si hay una advertencia para esta métrica	Haga lo siguiente
Rendimiento de la red: utilización	Aumente la capacidad de rendimiento
Servidor de archivos > IOPS de disco: utilización	
Servidor de archivos > Rendimiento del disco: utilización	
Servidor de archivos > IOPS de disco: saldo de ráfagas	

Si hay una advertencia para esta métrica	Haga lo siguiente
Servidor de archivos > Rendimiento del disco: saldo de ráfagas	
Utilización de la capacidad de almacenamiento	Aumente la capacidad de almacenamiento
Volumen de almacenamiento > Rendimiento del disco: utilización (HDD)	Aumente la capacidad de almacenamiento o pase al tipo de almacenamiento en SDD
Volumen de almacenamiento > Rendimiento del disco: saldo de ráfaga (HDD)	
Volumen de almacenamiento > IOPS de disco: utilización (SSD)	Aumente las IOPS de SSD

> **Note**
>
> Algunos eventos del sistema de archivos pueden consumir los recursos de rendimiento de E/S del disco y, es posible que activen advertencias de rendimiento. Por ejemplo:
>
> - La fase de optimización del escalado de la capacidad de almacenamiento puede generar un aumento del rendimiento del disco, como se describe en Los aumentos de capacidad de almacenamiento y el rendimiento del sistema de archivos
> - En el caso de los sistemas de archivos Multi-AZ, los eventos como el escalado de la capacidad de rendimiento, la sustitución del hardware o la interrupción de la zona de disponibilidad provocan eventos de conmutación por error y de conmutación por recuperación. Cualquier cambio de datos que se produzca durante este tiempo se debe sincronizar entre los servidores de archivos principal y secundario, y Windows Server ejecuta una tarea de sincronización de datos que puede consumir recursos de E/S del disco. Para obtener más información, consulte Administración de la capacidad de rendimiento.

Para obtener más información del rendimiento del sistema de archivos, consulte FSx para el rendimiento del servidor de archivos de Windows.

Acceso a métricas del sistema de archivos

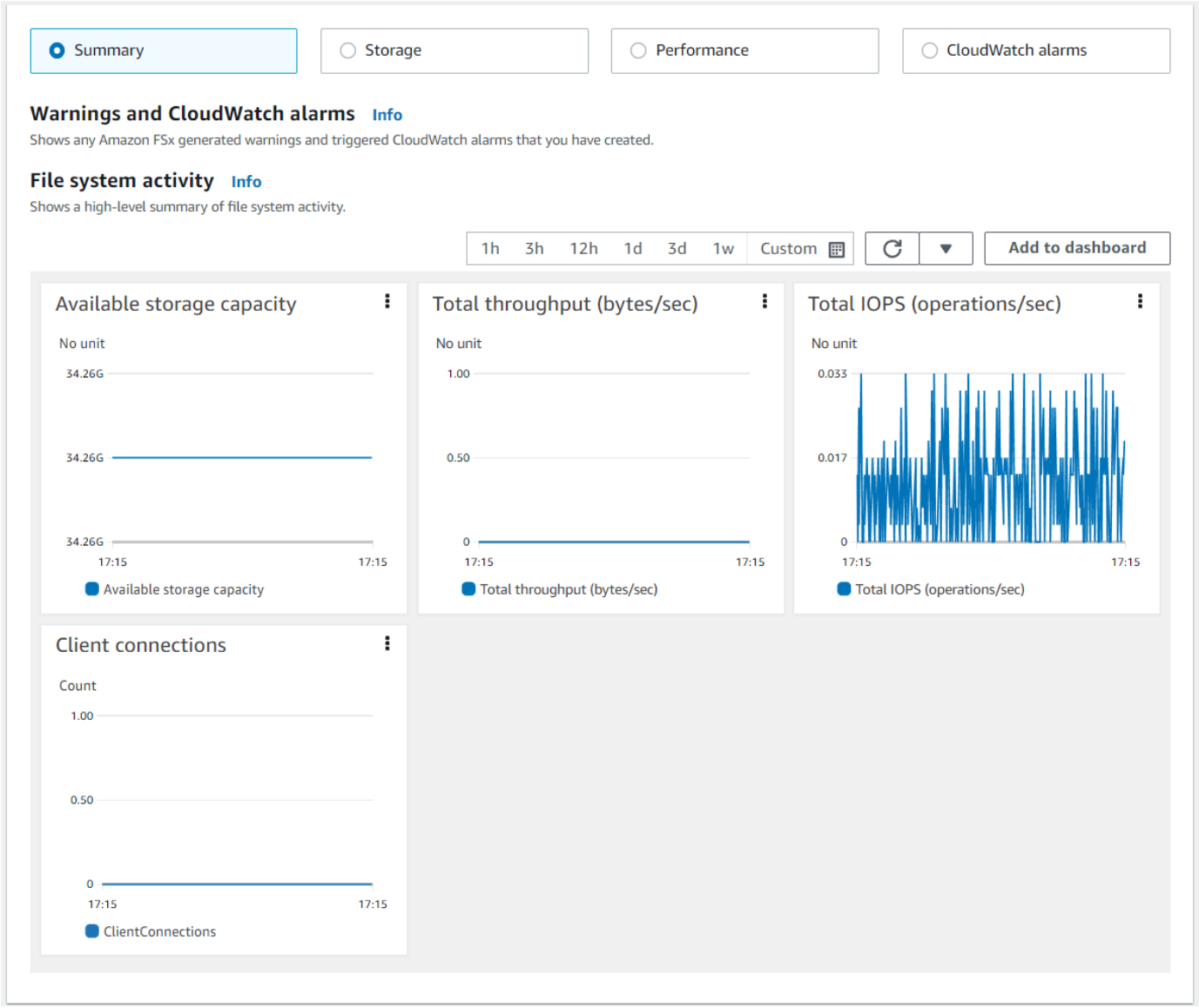
Puedes ver FSx las métricas de Amazon CloudWatch de las siguientes maneras.

- La FSx consola Amazon
- ¿La CloudWatch consola
- La CloudWatch CLI
- La CloudWatch API

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

Para ver las métricas del sistema de archivos mediante la FSx consola de Amazon

1. Abre la FSx consola de Amazon en https://console.aws.amazon.com/fsx/.
2. Para mostrar la página de Información del sistema de archivos, seleccione Sistemas de archivos en el panel de navegación.
3. Elija el sistema de archivos cuyas métricas desea ver.
4. Para ver los gráficos de las métricas del sistema de archivos, seleccione Supervisión y rendimiento en el segundo panel.

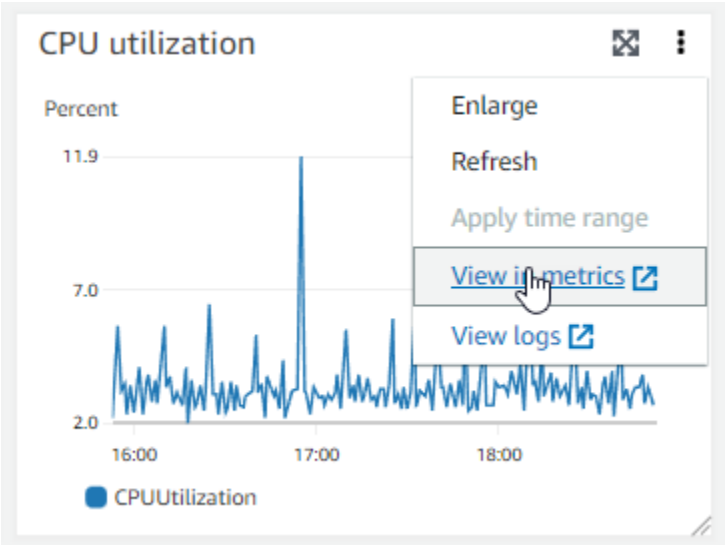


- Las métricas resumidas se muestran de forma predeterminada y muestran las advertencias y CloudWatch alarmas activas junto con las métricas de actividad del sistema de archivos.
- Elija Almacenamiento para ver las métricas de capacidad y utilización de almacenamiento.
- Elija Rendimiento para ver las métricas de rendimiento del almacenamiento y de los servidores de archivos
- Seleccione CloudWatch las alarmas para ver los gráficos de cualquier alarma configurada para el sistema de archivos.

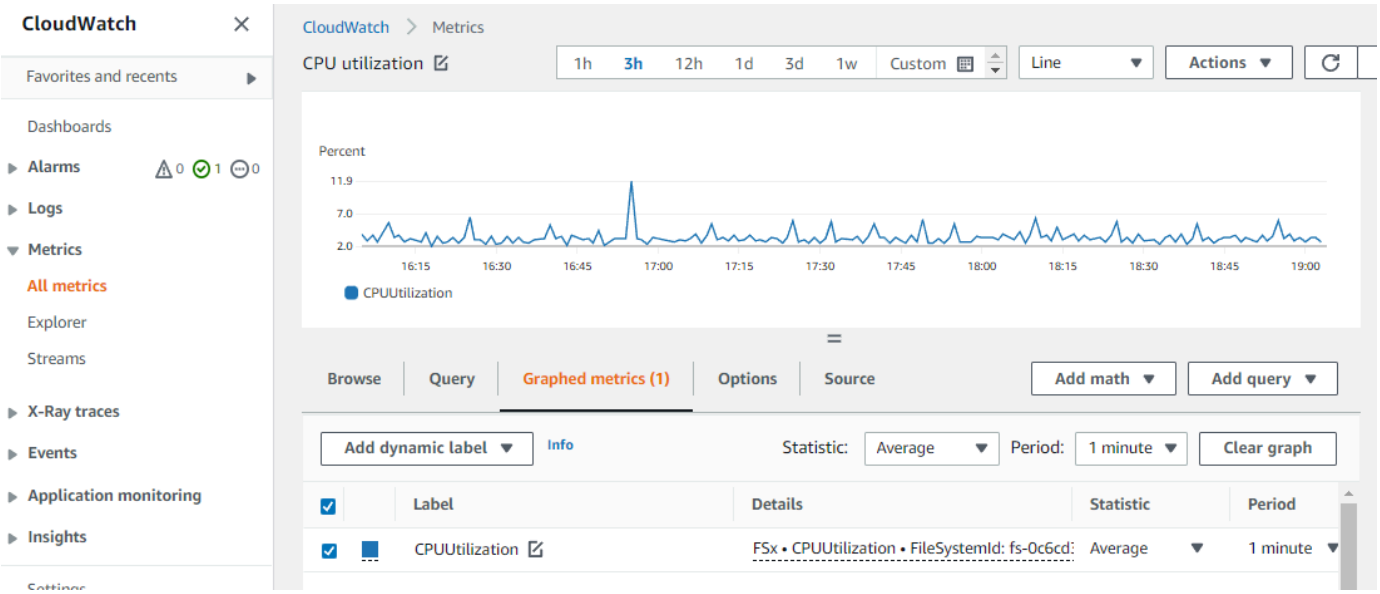
Para obtener más información, consulte Uso de métricas del sistema de archivos

Para ver las métricas en la CloudWatch consola

1. Para ver una métrica del sistema de archivos en la página de métricas de la CloudWatch consola de Amazon, navega hasta la métrica en el panel Supervisión y rendimiento de la FSx consola de Amazon.
2. Seleccione Ver en métricas en el menú de acciones de la parte superior derecha del gráfico de métricas, como se muestra en la siguiente imagen.



Se abre la página de métricas de la CloudWatch consola, que muestra el gráfico de métricas, tal y como se muestra en la siguiente imagen.



Para añadir métricas a un panel CloudWatch

1. Para añadir un conjunto de FSx métricas del sistema de archivos de Windows a un panel de control de la CloudWatch consola, elige el conjunto de métricas (resumen, almacenamiento o rendimiento) en el panel Supervisión y rendimiento de la FSx consola de Amazon.
2. Selecciona Añadir al panel de control en la parte superior derecha del panel y se abrirá la CloudWatch consola.
3. Seleccione un CloudWatch panel existente de la lista o cree uno nuevo. Para obtener más información, consulta Uso de los CloudWatch paneles de Amazon en la Guía del CloudWatch usuario de Amazon.

Para acceder a las métricas desde AWS CLI

- Utilice el comando `list-metrics` con el espacio de nombres de `--namespace "AWS/FSx"`. Para obtener más información, consulte Referencia de comandos de la AWS CLI.

```
$ aws cloudwatch list-metrics --namespace "AWS/FSx"
aws cloudwatch list-metrics --namespace "AWS/FSx"
{
    "Metrics": [
        {
            "Namespace": "AWS/FSx",
            "MetricName": "DataWriteOperationTime",
            "Dimensions": [
                {
                    "Name": "FileSystemId",
                    "Value": "fs-09a106ebc3a0bb087"
                }
            ]
        },
        {
            "Namespace": "AWS/FSx",
            "MetricName": "CapacityPoolWriteBytes",
            "Dimensions": [
                {
                    "Name": "VolumeId",
                    "Value": "fsvol-0cb2281509f5db3c2"
                },
                {
                    "Name": "FileSystemId",
                    "Value": "fs-09a106ebc3a0bb087"
```

```
                }
            ]
        },
        {
            "Namespace": "AWS/FSx",
            "MetricName": "DiskReadBytes",
            "Dimensions": [
                {
                    "Name": "FileSystemId",
                    "Value": "fs-09a106ebc3a0bb087"
                }
            ]
        },
        {
            "Namespace": "AWS/FSx",
            "MetricName": "CompressionRatio",
            "Dimensions": [
                {
                    "Name": "FileSystemId",
                    "Value": "fs-0f84c9a176a4d7c92"
                }
            ]
        },
.
.
.
}
```

Uso de la CloudWatch API

Para acceder a las métricas desde la CloudWatch API

- Llamar a `GetMetricStatistics`. Para obtener más información, consulta Amazon CloudWatch API Reference.

Creación de CloudWatch alarmas

Puede crear una CloudWatch alarma que envíe un mensaje de Amazon SNS cuando la alarma cambie de estado. Una alarma vigila una única métrica durante el período especificado y realiza una o varias acciones en función del valor de la métrica relativo a un determinado umbral durante una

serie de períodos de tiempo. La acción es una notificación que se envía a un tema de Amazon SNS o a una política de escalado automático.

Las alarmas invocan acciones únicamente en caso de cambios de estado sostenidos. CloudWatch las alarmas no invocan acciones simplemente porque se encuentran en un estado determinado; el estado debe haber cambiado y se ha mantenido durante un número específico de períodos. Puedes crear una alarma desde la FSx consola de Amazon o desde la CloudWatch consola.

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

Para configurar una CloudWatch alarma (consola)

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

> **Note**
>
> Es posible que las métricas no se publiquen durante el mantenimiento del sistema de archivos en los sistemas de archivos Single-AZ, ni durante la conmutación por error y la conmutación por recuperación hacia o desde los servidores principales o secundarios en los sistemas de archivos Multi-AZ. 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 quieres enviarte una notificación por correo electrónico o CloudWatch a una red social cuando el estado de alarma active la acción, selecciona un estado de alarma para «Siempre que esté este estado de alarma».

    En Seleccionar un tema de SNS, elija un tema de SNS existente. Si selecciona Crear tema, puede definir el nombre y las direcciones de correo electrónico de una nueva lista de suscripción de correo electrónico. Esta lista se guarda y aparece en el campo para futuras alarmas. Elija Siguiente.

    > **Note**
    >
    > Si utiliza Crear tema para crear un nuevo tema de Amazon SNS, debe verificar las direcciones de correo electrónico para que reciban notificaciones. Los correos electrónicos solo se envían cuando la alarma entra en estado de alarma. Si este cambio en el estado de la alarma se produce antes de que se verifiquen las direcciones de correo electrónico, no reciben una notificación.

12. Rellene los valores de Nombre, Descripción, y Siempre que de la métrica, y luego seleccione Siguiente.
13. Previsualice la alarma que va a crear en la página Previsualizar y crear y, a continuación, elija Crear alarma .

Para configurar las alarmas mediante la consola CloudWatch

1. Inicie sesión en AWS Management Console y abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. Elija Crear alarma para iniciar el Asistente de creación de alarmas.
3. Elige FSx Métricas y desplázate por las FSx métricas de Amazon para localizar la métrica en la que quieres colocar una alarma. Para mostrar solo las FSx métricas de Amazon en este cuadro de diálogo, busque el ID del sistema de archivos de su sistema de archivos. Seleccione la métrica en la cual crear una alarma y elija Siguiente.
4. Rellene los valores de Nombre, Descripción y En cualquier momento para la métrica.
5. Si CloudWatch quieres enviarte un correo electrónico cuando se alcance el estado de alarma, en Cuando esta alarma, selecciona State is ALARM. En Enviar notificación a, elija un tema de SNS existente. Si selecciona Crear tema, puede definir el nombre y las direcciones de correo

electrónico de una nueva lista de suscripción de correo electrónico. Esta lista se guarda y aparece en el campo para futuras alarmas.

> **Note**
>
> Si utiliza Crear tema para crear un nuevo tema de Amazon SNS, debe verificar las direcciones de correo electrónico para que reciban notificaciones. Los correos electrónicos solo se envían cuando la alarma entra en estado de alarma. Si este cambio en el estado de la alarma se produce antes de que se verifiquen las direcciones de correo electrónico, no reciben una notificación.

6. En este momento, el área Vista previa de la alarma le ofrece la oportunidad de previsualizar la que está a punto de crear. Elija Crear alarma.

Para configurar una CloudWatch alarma (CLI)

- Llame a `put-metric-alarm`. Para obtener más información, consulte la referencia de comandos de la AWS CLI.

Cómo definir una alarma (API)

- Llamar a `PutMetricAlarm`. Para obtener más información, consulta Amazon CloudWatch API Reference.

Registro de llamadas a la API de Amazon FSx para Windows File Server mediante AWS CloudTrail

Amazon FSx para Windows File Server 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 API de Amazon FSx como eventos. Las llamadas capturadas incluyen llamadas desde la FSx consola de Amazon y llamadas en código a las 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, la dirección IP desde la que se realizó la solicitud, quién la hizo, 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 tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad 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 eventos recientes en tu Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para tener un registro continuo de tus eventos Cuenta de AWS, incluidos los de Amazon FSx, crea una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. La ruta registra los eventos de todas 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 más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas FSx las acciones de Amazon se registran CloudTrail y se documentan en la referencia de la FSx API de Amazon. Por ejemplo, las llamadas a `CreateBackup` y `TagResource` las acciones generan entradas en los archivos de CloudTrail registro. `CreateFileSystem`

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 userIdentity de 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 usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

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"
}
```

Seguridad en Amazon FSx

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la nube de Amazon Web Services. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores independientes prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de conformidad que se aplican a Amazon FSx for Windows File Server, consulte AWS Servicios incluidos en el ámbito de aplicación por programa de conformidad.
- 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 le ayuda a entender cómo aplicar el modelo de responsabilidad compartida al utilizar Amazon FSx for Windows File Server. En los temas siguientes se muestra cómo configurar Amazon FSx for Windows File Server para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger los recursos del servidor de archivos de Amazon FSx para Windows.

Temas

- Protección de datos en Amazon FSx para Windows File Server
- Control de acceso a nivel de archivos y carpetas mediante Windows ACLs
- Control de acceso al sistema de archivos con Amazon VPC
- Registro del acceso de usuarios finales con auditoría de acceso a archivos
- Administración de identidades y accesos para Amazon FSx para Windows File Server
- Validación de conformidad de Amazon FSx para Windows File Server
- Servidor de archivos FSx de Amazon para Windows y puntos finales de VPC de interfaz

Protección de datos en Amazon FSx para Windows File Server

El modelo de se aplica a protección de datos en Amazon FSx for Windows File Server. 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.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail 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 trabaja con un servidor de archivos FSx de Windows u otro tipo Servicios de AWS mediante la consola, la API o. AWS CLI AWS SDKs 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.

Cifrado de datos FSx para Windows File Server

Amazon FSx para Windows File Server 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. El cifrado de los datos en tránsito se admite en los recursos compartidos de archivos que están mapeados en una instancia informática compatible con el protocolo SMB 3.0 o posterior. Amazon cifra FSx automáticamente los datos en tránsito mediante el cifrado SMB a medida que accedes a tu sistema de archivos sin necesidad de modificar tus aplicaciones.

Cuando utilizar el cifrado

Si su organización está sujeta a políticas reglamentarias o corporativas que requieren el cifrado de datos y metadatos en reposo, recomendamos crear un sistema de archivos cifrados montando el sistema de archivos con el cifrado de datos en tránsito.

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.

Cifrado de datos en reposo

Todos los sistemas de FSx archivos de Amazon están cifrados en reposo con claves administradas mediante AWS Key Management Service (AWS KMS). Los datos se cifran de manera automática antes de escribirse en el sistema de archivos y se descifran de la misma manera a medida que se leen. 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 un AWS KMS key para cifrar tu sistema de archivos. Usted elige la clave de KMS que se utiliza para cifrar y descifrar los sistemas de archivos (tanto de datos como de metadatos). Puede habilitar, deshabilitar o revocar concesiones en esta clave de KMS. Esta clave del KMS puede ser de uno de los dos siguientes tipos:

- Clave administrada de AWS: esta es la clave del KMS predeterminada, y su uso es gratuito.
- Clave administrada por el cliente: se trata de la clave del KMS más flexible, ya que puede configurar las políticas de claves y concesiones para varios usuarios o servicios. Para obtener más información sobre la creación de claves administradas por el cliente, consulte Creación de claves en la Guía para AWS Key Management Service desarrolladores.

Si utiliza una clave administrada por el cliente como clave de KMS para el cifrado y descifrado de datos de archivo, puede activar la rotación de claves. Cuando 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 del KMS. Para obtener más información, consulte Rotación AWS KMS keys en la Guía para AWS Key Management Service desarrolladores.

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 los sistemas de archivos cifrados en reposo:

- kms:Encrypt - (opcional): cifra texto plano en texto cifrado. Este permiso está incluido en la política de claves predeterminada.
- kms: Decrypt: (obligatorio) descifra texto cifrado. El texto cifrado es texto no cifrado que se ha cifrado previamente. Este permiso está incluido en la política de claves predeterminada.
- kms: ReEncrypt — (opcional) Cifra los datos del lado del servidor con una nueva clave de KMS, sin exponer el texto sin formato de los datos del lado del cliente. Los datos se descifran en primer lugar y luego se vuelven a cifrar. Este permiso está incluido en la política de claves predeterminada.
- kms: GenerateDataKeyWithoutPlaintext — (Obligatorio) Devuelve una clave de cifrado de datos cifrada con una clave KMS. Este permiso está incluido en la política de claves predeterminada en kms: GenerateDataKey *.
- kms: CreateGrant — (Obligatorio) Añade una concesión a una clave para especificar quién puede utilizarla y en qué condiciones. Las concesiones son mecanismos de permiso alternativo para las políticas de claves. Para obtener más información sobre las subvenciones, consulta Cómo usar las subvenciones en la Guía para AWS Key Management Service desarrolladores. Este permiso está incluido en la política de claves predeterminada.
- kms: DescribeKey — (Obligatorio) Proporciona información detallada sobre la clave de 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

El cifrado de los datos en tránsito se admite en los recursos compartidos de archivos que están mapeados en una instancia informática compatible con el protocolo SMB 3.0 o posterior. Esto incluye todas las versiones de Windows a partir de Windows Server 2012 y Windows 8, y todos los clientes Linux con el cliente Samba versión 4.2 o posterior. Amazon FSx para Windows File Server cifra automáticamente los datos en tránsito mediante el cifrado SMB a medida que accede a su sistema de archivos sin necesidad de modificar las aplicaciones.

El cifrado SMB utiliza AES-128-GCM o AES-128-CCM como algoritmo de cifrado (se elige la variante GCM si el cliente es compatible con SMB 3.1.1) y, además, garantiza la integridad de los datos de la firma mediante claves de sesión SMB Kerberos. El uso de AES-128-GCM mejora el rendimiento,

por ejemplo, duplica el rendimiento al copiar archivos de gran tamaño a través de conexiones SMB cifradas.

Para cumplir con los requisitos de conformidad que obligan a cifrar siempre data-in-transit, puede limitar el acceso al sistema de archivos para permitir el acceso únicamente a los clientes que admiten el cifrado SMB. También, puede activar o desactivar el cifrado en tránsito para cada recurso compartido de archivos o para todo el sistema de archivos. Esto le permite tener una combinación de recursos compartidos de archivos cifrados y no cifrados en el mismo sistema de archivos.

Administración del cifrado en tránsito

Puede usar un conjunto de PowerShell comandos personalizados para controlar el cifrado de los datos en tránsito entre el sistema de archivos del servidor FSx de archivos de Windows y los clientes. Puede limitar el acceso al sistema de archivos únicamente a los clientes que admitan el cifrado SMB para que siempre data-in-transit esté cifrado. Si el cifrado está activado data-in-transit, los usuarios que accedan al sistema de archivos desde clientes que no admiten el cifrado SMB 3.0 no podrán acceder a los archivos compartidos en los que el cifrado esté activado.

También puede controlar el cifrado a nivel de recurso compartido data-in-transit en lugar de a nivel de servidor de archivos. Puede utilizar los controles de cifrado a nivel de recursos compartidos de archivos para tener una combinación de recursos compartidos de archivos cifrados y no cifrados en el mismo sistema de archivos si desea aplicar el cifrado en tránsito para algunos recursos compartidos de archivos que contienen datos confidenciales y permitir que todos los usuarios accedan a otros recursos compartidos de archivos. El cifrado de todo el servidor tiene prioridad sobre el cifrado a nivel de recursos compartidos. Si el cifrado global está activado, no se puede deshabilitar de forma selectiva el cifrado para determinados recursos compartidos.

Puede administrar el cifrado en tránsito en su sistema de archivos mediante la Amazon FSx CLI para la administración remota en PowerShell. Para obtener información sobre cómo utilizar esta CLI, consulte Uso de Amazon FSx CLI para PowerShell.

A continuación, se muestran los comandos que puede utilizar para administrar el cifrado en tránsito de los usuarios en su sistema de archivos.

Cifrado en comando de tránsito	Descripción
Get-FSxSmbServerConfiguration	Recupera la configuración de bloque de mensajes del servidor (SMB). En la respuesta del sistema, puede determinar la

Cifrado en comando de tránsito	Descripción
	configuración del cifrado en tránsito del sistema de archivos en función de los valores de las propiedades `EncryptData` y `RejectUnencryptedAccess` .
Set-FSxSmbServerConfiguration	Este comando tiene dos opciones para configurar el cifrado en tránsito de forma global en el sistema de archivos: • `-EncryptData $True\|$False` : defina este parámetro como `True` para activar el cifrado de datos en tránsito. Defina este parámetro como `False` para desactivar el cifrado de datos en tránsito. • `-RejectUnencryptedAccess $True\|$False` : defina este parámetro como `True` para impedir que los clientes que no admiten el cifrado accedan al sistema de archivos. Defina este parámetro como `False` para permitir que los clientes que no admiten el cifrado accedan al sistema de archivos.
Set-FSxSmbShare -name ***name*** -EncryptData $True	Establezca este parámetro en `True` para activar el cifrado de datos en tránsito para el recurso compartido. Establezca este parámetro `False` para desactivar el cifrado de datos en tránsito del recurso compartido.

La ayuda en línea de cada comando brinda una referencia de todas las opciones de comando. Para acceder a esta ayuda, ejecute el comando con -?, por ejemplo, Get-FSxSmbServerConfiguration -?.

Control de acceso a nivel de archivos y carpetas mediante Windows ACLs

Amazon FSx para Windows File Server admite la autenticación basada en la identidad a través del protocolo Server Message Block (SMB) a través de Microsoft Active Directory. 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 los servidores de archivos, y las cuentas de usuario y

equipo de la red. Para obtener más información sobre la compatibilidad con Active Directory en Amazon FSx, consulteTrabajar con Microsoft Active Directory.

Sus instancias informáticas unidas a un dominio pueden acceder a los recursos compartidos de FSx archivos de Amazon mediante las credenciales de Active Directory. Utiliza las listas de control de acceso estándar de Windows (ACLs) para un control de acceso detallado a nivel de archivos y carpetas. Los sistemas de FSx archivos de Amazon verifican automáticamente las credenciales de los usuarios que acceden a los datos del sistema de archivos para aplicar estos Windows ACLs.

Todos los sistemas de FSx archivos de Amazon vienen con un recurso compartido de archivos de Windows predeterminado llamado`share`. Las ventanas de esta carpeta compartida están configuradas ACLs para permitir el acceso de lectura y escritura a los usuarios del dominio. También, las ACL permiten que el grupo de administradores delegados de Active Directory, al que se le delegó la tarea de realizar acciones administrativas en los sistemas de archivos, tenga el control total. Si va a integrar su sistema de archivos con Microsoft AD AWS administrado, este grupo se denomina FSx Administradores AWS delegados. Si va a integrar el sistema de archivos a la configuración del Microsoft AD autoadministrado, este grupo puede ser Administradores de dominio. O puede ser algún grupo de administradores delegados personalizado que haya especificado cuando creó el sistema de archivos. Para cambiarlo ACLs, puede asignar el recurso compartido como un usuario que sea miembro del grupo de administradores delegados.

> **Warning**
>
> Amazon FSx requiere que el usuario del SISTEMA tenga permisos de ACL de NTFS de control total en todas las carpetas del sistema de archivos. No cambie los permisos de las ACL de NTFS de este usuario en sus carpetas. Si lo hace, el recurso compartido de archivos se puede volver inaccesible e impedir que se puedan utilizar las copias de seguridad del sistema de archivos.

Vínculos relacionados

- ¿Qué es AWS Directory Service? en la Guía AWS Directory Service de administración.
- Cree su directorio AWS administrado de Microsoft AD en la Guía de AWS Directory Service administración.
- Cuándo crear una relación de confianza en la Guía de administración de AWS Directory Service .

- Paso 1. Configuración de un Active Directory.

Control de acceso al sistema de archivos con Amazon VPC

El acceso al sistema de FSx archivos de Amazon se realiza a través de una interfaz de red elástica. Esta interfaz de red reside en la nube privada virtual (VPC) basada en el servicio Amazon Virtual Private Cloud (Amazon VPC) que asocia al sistema de archivo. Te conectas a tu sistema de FSx archivos de Amazon a través de su nombre de Domain Name Service (DNS). El nombre del DNS se asigna a la dirección IP privada de la interface de red elástica del sistema de archivos en la VPC. Solo los recursos de la VPC asociada, los recursos conectados a la VPC asociada mediante una VPN AWS Direct Connect o los recursos de la VPC interconectada VPCs pueden acceder a la interfaz de red del sistema de archivos. Para obtener más información, consulte ¿Qué es Amazon VPC? en la Guía del usuario de Amazon VPC.

> **Warning**
>
> No debe modificar ni eliminar 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.

FSx para Windows File Server admite el uso compartido de VPC, lo que le permite ver, crear, modificar y eliminar recursos de una subred compartida en una VPC propiedad de otra cuenta. AWS Para obtener más información, consulte Trabajar con contenido compartido VPCs en la Guía del usuario de Amazon VPC.

Grupos de seguridad de Amazon VPC

Utilice los grupos de seguridad para limitar el acceso a los sistemas de archivos. De esta manera, podrá ejercer un control más estricto del tráfico de la red que pasa por las interfaces de red elásticas del sistema de archivos dentro de la VPC. Un grupo de seguridad es un firewall con estado que controla el tráfico hacia y desde las interfaces de red asociadas. En este caso, el recurso asociado son las interfaces de red del sistema de archivos.

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

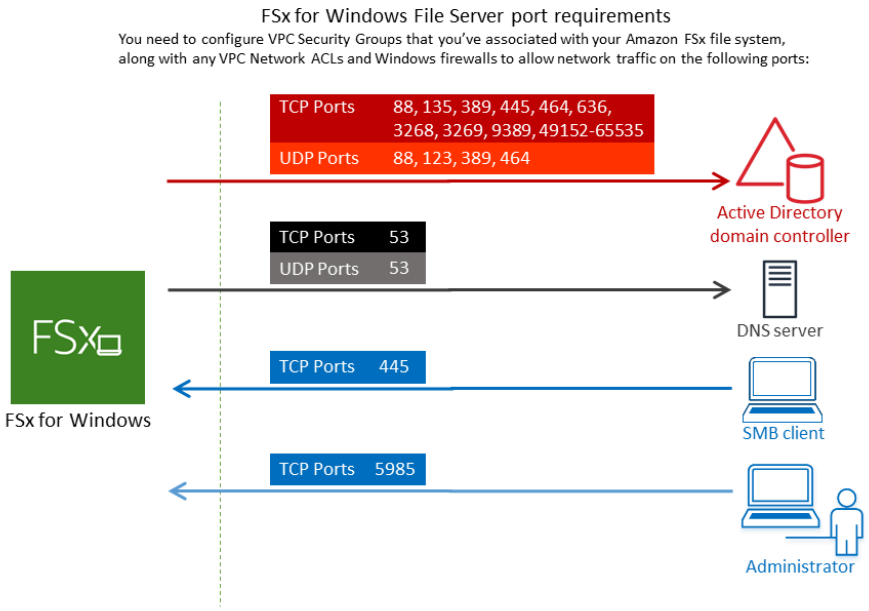
grupo de seguridad para asignar el recurso compartido de FSx archivos de su sistema de archivos de Amazon a una carpeta de la instancia de procesamiento compatible.

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.

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. Agregue las siguientes reglas para permitir el tráfico de red saliente en los siguientes puertos:

   a. En el caso de los grupos de seguridad de VPC, el grupo de seguridad predeterminado de la Amazon VPC predeterminada ya está agregado al sistema de archivos en la consola. Asegúrese de que el grupo de seguridad y la red ACLs de VPC de las subredes en las que va a crear el sistema de FSx archivos permitan el tráfico en los puertos y en las direcciones que se muestran en el siguiente diagrama.



En la siguiente tabla se identifica la función de cada puerto.

Protocolo	Puertos	Rol
TCP/UDP	53	Sistema de nombres de dominio (DNS)
TCP/UDP	88	Autenticación de Kerberos
TCP/UDP	464	Cambiar/establecer contraseña
TCP/UDP	389	Protocolo ligero de acceso a directorios (LDAP)
UDP	123	Protocolo de tiempo de red (NTP)
TCP	135	Entorno de computación distribuido/asignador de puntos de conexión (DCE/EPMAP)
TCP	445	Uso compartido de archivos SMB de Directory Services
TCP	636	Protocolo ligero de acceso a directorios sobre TLS/SSL (LDAP)

Protocolo	Puertos	Rol
TCP	3268	Catálogo global de Microsoft
TCP	3269	Catálogo global de Microsoft mediante SSL
TCP	5985	WinRM 2.0 (Administración remota de Microsoft Windows)
TCP	9389	Servicios web de Microsoft AD DS, PowerShell
TCP	49152 - 65535	Puertos efímeros para RPC

> **Important**
>
> Es necesario permitir el tráfico saliente del puerto TCP 9389 para las implementaciones de sistemas de archivos Single-AZ 2 y Multi-AZ.

b. Asegúrese de que estas reglas de tráfico también se reflejen en los firewalls que se aplican a cada uno de los controladores de dominio, servidores DNS, FSx clientes y administradores de AD. 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.

> **Note**
>
> Si tiene sitios de Active Directory definidos, debe asegurarse de que las subredes de la VPC asociadas a su sistema de archivos de FSx Amazon estén definidas en un sitio de Active Directory y de que no existan conflictos entre las subredes de su VPC y las subredes de sus otros sitios. Puede ver y cambiar esta configuración con el complemento MMC de sitios y servicios de Active Directory.

> **Note**
>
> En algunos casos, es posible que haya modificado las reglas de su grupo de seguridad de AWS Managed Microsoft AD con respecto a la configuración predeterminada. Si es así, asegúrate de que este grupo de seguridad tenga las reglas de entrada necesarias para permitir el tráfico desde tu sistema de FSx archivos de Amazon. Para obtener más información sobre las reglas de entrada necesarias, consulte los requisitos previos de AWS Managed Microsoft AD en la Guía de administración de AWS Directory Service .

Ahora que ha creado su grupo de seguridad, puede asociarlo a las interfaces de red elásticas de su sistema de FSx archivos de Amazon.

Para asociar un grupo de seguridad a tu sistema de FSx archivos de Amazon

1. Abre la FSx consola de Amazon en https://console.aws.amazon.com/fsx/.
2. En el panel de control, elija el sistema de archivo para ver la información.
3. Seleccione la pestaña Red y seguridad, y elija las interfaces de red del sistema de archivos; por ejemplo, ENI-01234567890123456. En el caso de los sistemas de archivos Single-AZ, verá una interfaz de red única. En el caso de los sistemas de archivos Multi-AZ, verá una interfaz de red en la subred preferida y otra, en la subred en espera.
4. Para cada interfaz de red, elíjala y, en Acciones, seleccione Cambiar grupos de seguridad.
5. En el cuadro de diálogo Cambiar grupos de seguridad, elija los grupos de seguridad que desee utilizar y seleccione Guardar.

Denegar el acceso a un sistema de archivos

Para impedir temporalmente que los clientes tengan acceso de red al sistema de archivos, puede eliminar los grupos de seguridad asociados a las interfaces de red elásticas del sistema de archivos y sustituirlos por un grupo que no tenga reglas de entrada y salida.

Red Amazon VPC ACLs

Otra opción para proteger el acceso al sistema de archivos de la VPC es establecer listas de control de acceso a la red (red ACLs). ACLs Las redes son independientes de los grupos de seguridad, pero

tienen una funcionalidad similar para añadir una capa de seguridad adicional a los recursos de la VPC. Para obtener más información sobre la red ACLs, consulte Red ACLs en la Guía del usuario de Amazon VPC.

Registro del acceso de usuarios finales con auditoría de acceso a archivos

Amazon FSx para Windows File Server admite la auditoría del acceso de los usuarios finales a los archivos, carpetas y recursos compartidos de archivos. Puede optar por enviar los registros de eventos de auditoría de un sistema de archivos a otros servicios de AWS que ofrecen un amplio conjunto de características. Estas incluyen la posibilidad de consultar, procesar, almacenar y archivar los registros, emitir notificaciones y activar acciones para mejorar aún más los objetivos de seguridad y cumplimiento.

Para obtener más información sobre el uso de la auditoría de acceso a los archivos para obtener información sobre los patrones de acceso e implementar notificaciones de seguridad para la actividad de los usuarios finales, consulte Información sobre los patrones de acceso al almacenamiento de archivos e Implementación de notificaciones de seguridad para la actividad de los usuarios finales.

> **Note**
>
> La auditoría del acceso a los archivos solo se admite en FSx los sistemas de archivos de Windows con una capacidad de procesamiento de 32 MBps o más. Ahora puede modificar la capacidad de rendimiento para sistemas de archivos actuales. Para obtener más información, consulte Administración de la capacidad de rendimiento.

La auditoría de acceso a archivos le permite registrar los accesos de los usuarios finales a archivos, carpetas y recursos compartidos de archivos individuales en función de los controles de auditoría definidos. Los controles de auditoría también se conocen como listas de control de acceso al sistema NTFS ()SACLs. Si ya tiene controles de auditoría configurados en los datos de sus archivos existentes, puede aprovechar la auditoría de acceso a los archivos creando un nuevo sistema de archivos Amazon FSx for Windows File Server y migrando sus datos.

Amazon FSx admite los siguientes eventos de auditoría de Windows para el acceso a archivos, carpetas y archivos compartidos:

- Para el acceso a los archivos, es compatible con: Todos, Recorrer carpeta/Ejecutar archivo, Enumerar carpeta/Leer datos, Leer atributos, Crear archivos/Escribir datos, Crear carpetas/Agregar datos, Escribir atributos, Eliminar subcarpetas y archivos, Eliminar, Leer permisos, Cambiar permisos y Asumir la propiedad.
- Para los accesos a archivos compartidos, admite: Conectarse a un recurso compartido de archivos.

En todos los accesos a archivos, carpetas y archivos compartidos, Amazon FSx admite el registro de los intentos exitosos (por ejemplo, un usuario con permisos suficientes para acceder correctamente a un archivo o recurso compartido de archivos), los intentos fallidos o ambos.

Puede configurar si desea acceder a la auditoría únicamente a los archivos y carpetas, solo a los archivos compartidos o a ambos. También puede configurar qué tipos de accesos deben registrarse (solo los intentos exitosos, solo los intentos fallidos o ambos). También puede desactivar la auditoría de acceso a archivos en cualquier momento.

> **Note**
>
> La auditoría de acceso a los archivos registra los datos de acceso de los usuarios finales solo desde el momento en que se habilitó. Es decir, la auditoría de acceso a los archivos no genera registros de eventos de auditoría de la actividad de acceso a archivos, carpetas y archivos compartidos de los usuarios finales que se produjo antes de que se habilitara la auditoría de acceso a los archivos.

La tasa máxima de eventos de auditoría de acceso admitidos es de 5000 eventos por segundo. Los eventos de auditoría de acceso no se generan para cada operación de lectura y escritura de archivos, sino que se generan una vez por cada operación de metadatos de archivo, por ejemplo, cuando un usuario crea, abre o elimina un archivo.

Temas

- Audite los destinos del registro de eventos
- Migración de los controles de auditoría
- Visualización de registros de eventos
- Configuración de controles de auditoría de archivos y carpetas
- Administrar la auditoría de acceso a los archivos

Audite los destinos del registro de eventos

Cuando habilitas la auditoría de acceso a archivos, debes configurar un AWS servicio al que Amazon FSx envíe los registros de eventos de auditoría. Puede enviar los registros de eventos de auditoría a una secuencia de CloudWatch registros de Amazon Logs de un grupo de CloudWatch registros de Logs o a una transmisión de entrega de Amazon Data Firehose. Usted elige el destino de los registros de eventos de auditoría al crear su sistema de archivos de Amazon FSx for Windows File Server o en cualquier momento posterior al actualizar un sistema de archivos existente. Para obtener más información, consulte Administrar la auditoría de acceso a los archivos.

A continuación, se incluyen algunas recomendaciones que pueden ayudarle a decidir qué destino de los registros de eventos de auditoría elegir:

- Elija CloudWatch Logs si desea almacenar, ver y buscar registros de eventos de auditoría en la CloudWatch consola de Amazon, ejecutar consultas en los CloudWatch registros mediante Logs Insights y activar CloudWatch alarmas o funciones Lambda.
- Elija Amazon Data Firehose si desea transmitir eventos de forma continua al almacenamiento en Amazon S3, a una base de datos en Amazon Redshift, a OpenSearch Amazon Service o a soluciones de socios como Splunk o Datadog AWS para un análisis más detallado.

De forma predeterminada, Amazon FSx creará y utilizará un grupo de CloudWatch registros predeterminado en tu cuenta como destino del registro de eventos de auditoría. Si quieres usar un grupo de CloudWatch registros personalizado o usar Firehose como destino del registro de eventos de auditoría, estos son los requisitos para los nombres y ubicaciones del destino del registro de eventos de auditoría:

- El nombre del grupo de CloudWatch registros debe empezar por el `/aws/fsx/` prefijo. Si no tienes un grupo de CloudWatch registros existente al crear o actualizar un sistema de archivos en la consola, Amazon FSx puede crear y usar un flujo de registros predeterminado en el grupo de CloudWatch `/aws/fsx/windows` registros. Si no quieres usar el grupo de registros predeterminado, la interfaz de usuario de configuración te permite crear un grupo de CloudWatch registros al crear o actualizar tu sistema de archivos en la consola.
- El nombre del flujo de entrega de Firehose debe empezar por el prefijo `aws-fsx-`. Si no tiene un flujo de entrega de Data Firehose existente, puede hacer uno al crear o actualizar el sistema de archivos en la consola.

- El flujo de entrega de Firehose debe estar configurado para que se use `Direct PUT` como origen. No puede utilizar un flujo de datos de Kinesis existente como origen de datos para la transmisión de entrega.
- El destino (grupo de CloudWatch registros de Logs o flujo de entrega de Firehose) debe estar en la misma AWS partición y Cuenta de AWS que tu sistema de FSx archivos de Amazon. Región de AWS

Puede cambiar el destino del registro de eventos de auditoría en cualquier momento (por ejemplo, de CloudWatch Logs a Firehose). Al hacerlo, los nuevos registros de eventos de auditoría se envían solo al nuevo destino.

Entrega de registros de eventos de auditoría de la mejor forma

Por lo general, los registros de eventos de auditoría se entregan al destino en cuestión de minutos, pero a veces pueden tardar más. En muy raras ocasiones, es posible que no se registren los registros de eventos de auditoría. Si su caso de uso requiere una semántica específica (por ejemplo, asegurarse de que no se omita ningún evento de auditoría), le recomendamos que tenga en cuenta los eventos omitidos al diseñar sus flujos de trabajo. Puede realizar una auditoría para detectar eventos omitidos escaneando la estructura de archivos y carpetas de su sistema de archivos.

Migración de los controles de auditoría

Si ya tienes los controles de auditoría (SACLs) configurados en los datos de tus archivos existentes, puedes crear un sistema de FSx archivos de Amazon y migrar tus datos a tu nuevo sistema de archivos. Te recomendamos que lo AWS DataSync utilices para transferir los datos y los archivos asociados SACLs a tu sistema de FSx archivos de Amazon. Como solución alternativa, puede utilizar Robocopy (Robust File Copy). Para obtener más información, consulte Migración del almacenamiento de archivos existente a Amazon FSx.

Visualización de registros de eventos

Puedes ver los registros de eventos de auditoría una vez que Amazon FSx haya empezado a emitirlos. El lugar y la forma de ver los registros dependen del destino del registro de eventos de auditoría:

- Para ver CloudWatch los registros, vaya a la CloudWatch consola y elija el grupo de registros y el flujo de registros a los que se enviarán los registros de los eventos de auditoría. Para obtener más

información, consulta Ver los datos de registro enviados a CloudWatch Logs en la Guía del usuario de Amazon CloudWatch Logs.

Puede utilizar CloudWatch Logs Insights para buscar y analizar sus datos de registro de forma interactiva. Para obtener más información, consulte Análisis de datos de registro con CloudWatch Logs Insights, en la Guía del usuario de Amazon CloudWatch Logs.

También puede exportar registros de eventos de auditoría a Amazon S3. Para obtener más información, consulte Exportación de datos de registro a Amazon S3, también en la Guía del usuario de Amazon CloudWatch Logs.

- No puede ver los registros de eventos de auditoría en Firehose. Sin embargo, puede configurar Firehose para que reenvíe los registros a un destino desde el que pueda leer. Los destinos incluyen Amazon S3, Amazon Redshift, Amazon OpenSearch Service y soluciones de socios como Splunk y Datadog. Para obtener más información, consulte Choose destination en la Guía para desarrolladores de Amazon Data Firehose.

Campos de eventos de auditoría

Esta sección proporciona descripciones de la información de los registros de eventos de auditoría y ejemplos de eventos de auditoría.

A continuación, se describen los campos más destacados de un evento de auditoría de Windows.

- EventID hace referencia al ID de evento de registro de eventos de Windows definido por Microsoft. Consulte la documentación de Microsoft para obtener información sobre los eventos del sistema de archivos y los eventos de archivos compartidos.
- SubjectUserNamese refiere al usuario que realiza el acceso.
- ObjectNamehace referencia al archivo, carpeta o recurso compartido de archivos de destino al que se ha accedido.
- ShareNameestá disponible para los eventos que se generan para el acceso a los archivos compartidos. Por ejemplo, `EventID 5140` se genera cuando se accede a un objeto compartido de red.
- IpAddressse refiere al cliente que inició el evento para los eventos de uso compartido de archivos.
- Keywords, cuando están disponibles, se refieren a si el acceso al archivo se ha realizado correctamente o no. Para que los accesos se realicen correctamente, el valor es `0x8020000000000000`. Para los accesos fallidos, el valor es `0x8010000000000000`.

- TimeCreated SystemTimehace referencia a la hora en que el evento se generó en el sistema y se mostró en formato <AAAA-MM-:MM:SS.S>z. DDThh
- Computadora hace referencia al nombre DNS del sistema de archivos Windows Remote Endpoint y se puede usar para identificar el sistema de archivos. PowerShell
- AccessMask, cuando está disponible, se refiere al tipo de acceso a los archivos realizado (por ejemplo, ReadData, WriteData).
- AccessListse refiere al acceso solicitado o concedido a un objeto. Para obtener más información, consulte la tabla siguiente y la documentación de Microsoft (por ejemplo, en el Evento 4556).

Tipo de acceso	Máscara de acceso	Valor
Leer datos o directorio de la lista	0x1	%%4416
Escribir datos o añadir un archivo	0x2	%%4417
Añadir datos o añadir un subdirectorio	0x4	%%4418
Atributos de lectura extendidos	0x8	%%4419
Atributos de escritura extendidos	0x10	%%4420
Ejecutar/recorrer	0x20	%%4421
Eliminar elemento secundario	0x40	%%4422
Atributos de lectura	0x80	%%4423
Atributos de escritura	0x100	%%4424
Eliminar	0x10000	%%1537
ACL de lectura	0x20000	%%1538

Tipo de acceso	Máscara de acceso	Valor
ACL de escritura	0x40000	%%1539
Propietario de escritura	0x80000	%%1540
Sincronizar	0x100000	%%1541
ACL de seguridad de acceso	0x1000000	%%1542

A continuación, se presentan algunos eventos clave con algunos ejemplos. Tenga en cuenta que el XML tiene un formato que se puede leer.

El ID de evento 4660 se registra cuando se elimina un objeto.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4660</EventID><Version>0</Version><Level>0</Level>
<Task>12800</Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-05-18T04:51:56.916563800Z'/>
<EventRecordID>315452</EventRecordID><Correlation/>
<Execution ProcessID='4' ThreadID='5636'/><Channel>Security</Channel>
<Computer>amznfsxgyzohmw8.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x50932f71</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='HandleId'>0x12e0</Data><Data Name='ProcessId'>0x4</Data><Data
 Name='ProcessName'></Data>
<Data Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data></EventData></
Event>
```

El ID de evento 4659 se registra en una solicitud de eliminación de un archivo.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4659</EventID><Version>0</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
```

```
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-0603T19:18:09.951551200Z'/>
<EventRecordID>308888</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='5540'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device\HarddiskVolume8\shar
\event.txt</Data>
<Data Name='HandleId'>0x0</Data><Data
 Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data>
<Data Name='AccessList'>%%1537
    %%4423
    </Data><Data Name='AccessMask'>0x10080</Data><Data Name='PrivilegeList'>-</Data>
<Data Name='ProcessId'>0x4</Data></EventData></Event>
```

El ID de evento 4663 se registra cuando se realiza una operación específica en el objeto. El siguiente ejemplo muestra la lectura de datos de un archivo, que se puede interpretar a partir de `AccessList %%4416`.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4663< /EventID><Version>1</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:10:13.887145400Z'/>
<EventRecordID>308831</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='6916'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData>< Data
 Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113< /Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\event.txt</Data>
<Data Name='HandleId'>0x101c</Data><Data Name='AccessList'>%%4416
    </Data>
<Data Name='AccessMask'>0x1</Data><Data Name='ProcessId'>0x4</Data>
```

```
<Data Name='ProcessName'></Data><Data Name='ResourceAttributes'>S:AI</Data>
</EventData></Event>
```

El siguiente ejemplo muestra la escritura/adición de datos de un archivo, que se puede interpretar a partir de `AccessList %%4417`.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4663</EventID><Version>1</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:12:16.813827100Z'/>
<EventRecordID>308838</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='5828'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\event.txt</Data>
<Data Name='HandleId'>0xa38</Data><Data Name='AccessList'>%%4417
    </Data><Data Name='AccessMask'>0x2</Data><Data Name='ProcessId'>0x4</Data>
<Data Name='ProcessName'></Data><Data Name='ResourceAttributes'>S:AI</Data></
EventData></Event>
```

El ID de evento 4656 indica que se ha solicitado un acceso específico para un objeto. En el siguiente ejemplo, la solicitud de lectura se inició como ObjectName «prueba de permiso» y fue un intento fallido, como se ve en el valor de palabras clave de. `0x8010000000000000`

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4656</EventID><Version>1</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8010000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:22:55.113783500Z'/>
<EventRecordID>308919</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='4924'/>
```

```
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\permtest</Data>
<Data Name='HandleId'>0x0</Data><Data
 Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data>
<Data Name='AccessList'>%%1541
    %%4416
    %%4423
    </Data><Data Name='AccessReason'>%%1541: %%1805
    %%4416: %%1805
    %%4423: %%1811 D:(A;OICI;0x1301bf;;;AU)
    </Data><Data Name='AccessMask'>0x100081</Data><Data Name='PrivilegeList'>-</Data>
<Data Name='RestrictedSidCount'>0</Data><Data Name='ProcessId'>0x4</Data><Data
 Name='ProcessName'></Data>
<Data Name='ResourceAttributes'>-</Data></EventData></Event>
```

El ID de evento 4670 se registra cuando se cambian los permisos de un objeto. En el siguiente ejemplo, se muestra que el usuario «admin» modificó el permiso de «permtest» para añadir permisos al SID ObjectName «S-1-5-21-658495921-4185342820-3824891517-1113". Consulte la documentación de Microsoft para obtener más información sobre cómo interpretar los permisos.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4670</EventID><Version>0</Version><Level>0</Level>
<Task>13570</Task><Opcode>0</Opcode><Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime='2021-06-03T19:39:47.537129500Z'/><EventRecordID>308992</
EventRecordID>
<Correlation/><Execution ProcessID='4' ThreadID='2776'/><Channel>Security</Channel>
<Computer>amznfsxgyzohmw8.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\permtest</Data>
<Data Name='HandleId'>0xcc8</Data>
<Data Name='OldSd'>D:PAI(A;OICI;FA;;;SY)
(A;OICI;FA;;;S-1-5-21-658495921-4185342820-3824891517-2622)</Data>
```

```
<Data Name='NewSd'>D:PARAI(A;OICI;FA;;;S-1-5-21-658495921-4185342820-3824891517-1113)
(A;OICI;FA;;;SY)(A;OICI;FA;;;
S-1-5-21-658495921-4185342820-3824891517-2622)</Data><Data Name='ProcessId'>0x4</Data>
<Data Name='ProcessName'></Data></EventData></Event>
```

El ID de evento 5140 se registra cada vez que se accede a un archivo compartido.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>5140</EventID><Version>1</Version><Level>0</Level><Task>12808</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:32:07.535208200Z'/>
<EventRecordID>308947</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='3120'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-2620</
Data>
<Data Name='SubjectUserName'>EC2AMAZ-1GP4HMN$</Data><Data
 Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2d4ca529</Data><Data Name='ObjectType'>File</Data><Data
 Name='IpAddress'>172.45.6.789</Data>
<Data Name='IpPort'>49730</Data><Data Name='ShareName'>\\AMZNFSXCYDKLDZZ\share</Data>
<Data Name='ShareLocalPath'>\??\D:\share</Data><Data Name='AccessMask'>0x1</Data><Data
 Name='AccessList'>%%4416
    </Data></EventData></Event>
```

El ID de evento 5145 se registra cuando se deniega el acceso en el nivel de archivos compartidos. En el siguiente ejemplo, se muestra que se denegó el acceso a «demoshare01". ShareName

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>5145</EventID><Version>0</Version><Level>0</Level>
<Task>12811</Task><Opcode>0</Opcode><Keywords>0x8010000000000000</Keywords>
<TimeCreated SystemTime='2021-05-19T22:30:40.485188700Z'/><EventRecordID>282939</
EventRecordID>
<Correlation/><Execution ProcessID='4' ThreadID='344'/><Channel>Security</Channel>
<Computer>amznfsxtmn9autz.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-
```

```
1113</Data><Data Name='SubjectUserName'>Admin</Data><Data
 Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x95b3fb7</Data><Data Name='ObjectType'>File</Data>
<Data Name='IpAddress'>172.31.7.112</Data><Data Name='IpPort'>59979</Data>
<Data Name='ShareName'>\\AMZNFSXDPNTE0DC\demoshare01</Data><Data Name='ShareLocalPath'>
\??\D:\demoshare01</Data>
<Data Name='RelativeTargetName'>Desktop.ini</Data><Data Name='AccessMask'>0x120089</
Data>
<Data Name='AccessList'>%%1538 %%1541 %%4416 %%4419 %%4423 </Data><Data
 Name='AccessReason'>%%1538:
%%1804 %%1541: %%1805 %%4416: %%1805 %%4419: %%1805 %%4423: %%1805 </Data></
EventData></Event>
```

Si utilizas CloudWatch Logs Insights para buscar tus datos de registro, puedes ejecutar consultas en los campos de eventos, como se muestra en los siguientes ejemplos:

- Para consultar un ID de evento específico:

```
fields @message
   | filter @message like /4660/
```

- Para consultar todos los eventos que coincidan con un nombre de archivo concreto:

```
fields @message
   | filter @message like /event.txt/
```

Para obtener más información sobre el lenguaje de consulta de CloudWatch Logs Insights, consulte Análisis de datos de registro con CloudWatch Logs Insights, en la Guía del usuario de Amazon CloudWatch Logs.

Configuración de controles de auditoría de archivos y carpetas

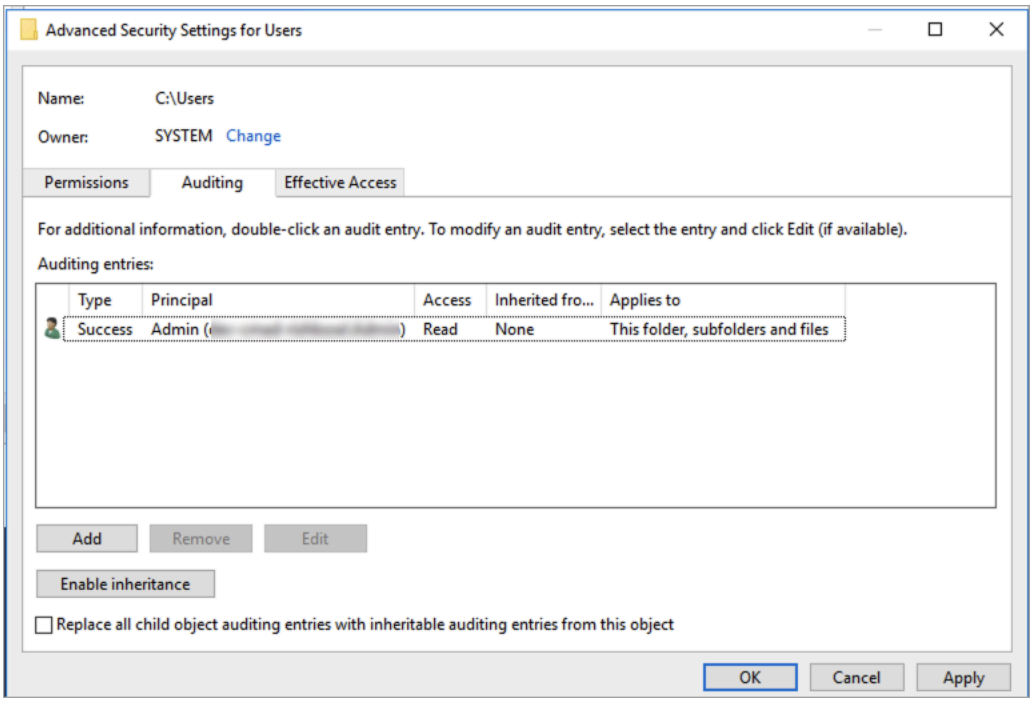
Debe establecer controles de auditoría en los archivos y carpetas que desee auditar para los intentos de acceso de los usuarios. Los controles de auditoría también se conocen como listas de control de acceso al sistema NTFS (SACLs).

Los controles de auditoría se configuran mediante la interfaz gráfica de usuario nativa de Windows o mediante programación mediante comandos de Windows. PowerShell Si la herencia está habilitada, normalmente tendrá que configurar los controles de auditoría únicamente en las carpetas de nivel superior en las que desee registrar los accesos.

Uso de la interfaz gráfica de usuario de Windows para configurar el acceso de auditoría

Si desea utilizar una interfaz gráfica de usuario para configurar los controles de auditoría en sus archivos y carpetas, utilice el Explorador de archivos de Windows. En un archivo o carpeta determinados, abra el Explorador de archivos de Windows y seleccione la pestaña Propiedades > Seguridad > Avanzada > Auditoría.

En el siguiente ejemplo de control de auditoría, se auditan los eventos correctos de una carpeta. Se emitirá una entrada en el registro de eventos de Windows cada vez que el usuario administrador abra ese identificador para que lo lea correctamente.



El campo Tipo indica qué acciones desea auditar. Defina este campo en Éxito para auditar los intentos correctos, Error para auditar los intentos fallidos o Todos para auditar tanto los intentos exitosos como los fallidos.

Para obtener más información sobre los campos de entrada de auditoría, consulte Aplicar una política de auditoría básica a un archivo o carpeta en la documentación de Microsoft.

Uso de PowerShell comandos para configurar el acceso de auditoría

Puede usar el comando `Set-Acl` de Microsoft Windows para configurar la SACL de auditoría en cualquier archivo o carpeta. Para obtener información acerca de este comando, consulte la documentación de Microsoft Set-Acl.

A continuación, se muestra un ejemplo del uso de una serie de PowerShell comandos y variables para configurar el acceso de auditoría para que los intentos se realicen correctamente. Puede adaptar estos comandos de ejemplo para que se ajusten a las necesidades de su sistema de archivos.

```
$path = "C:\Users\TestUser\Desktop\DemoTest\"

$ACL = Get-Acl $path

$ACL | Format-List

$AuditUser = "TESTDOMAIN\TestUser"

$AuditRules = "FullControl"

$InheritType = "ContainerInherit,ObjectInherit"

$AuditType = "Success"

$AccessRule = New-Object System.Security.AccessControl.FileSystemAuditRule($AuditUser,
$AuditRules,$InheritType,"None",$AuditType)

$ACL.SetAuditRule($AccessRule)

$ACL | Set-Acl $path

Get-Acl $path -Audit | Format-List
```

Administrar la auditoría de acceso a los archivos

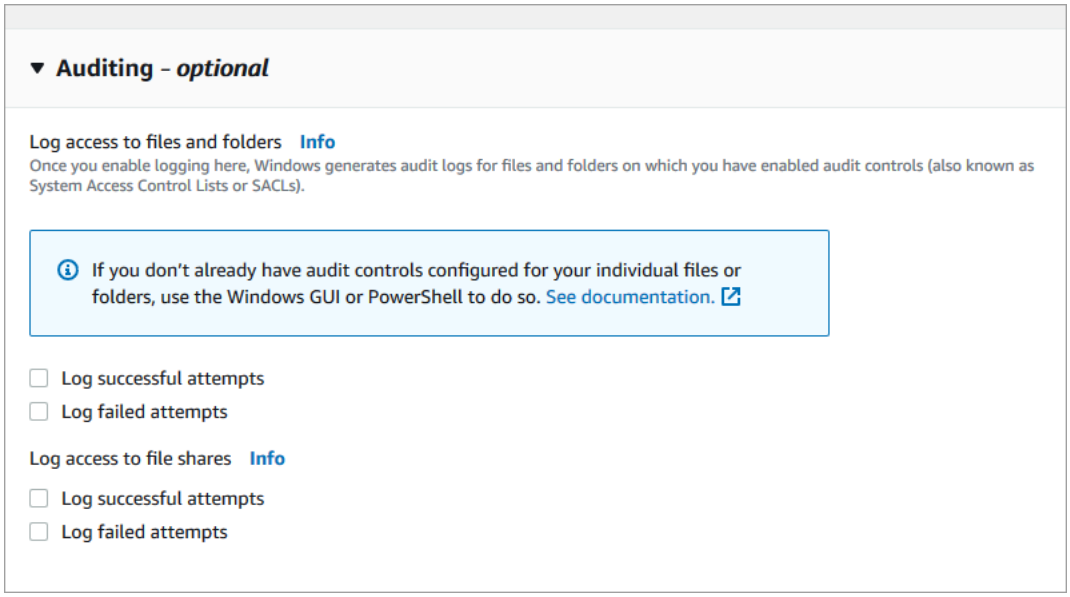
Puede habilitar la auditoría de acceso a los archivos al crear un nuevo sistema de archivos de Amazon FSx para Windows File Server. La auditoría de acceso a los archivos está desactivada de forma predeterminada al crear un sistema de archivos desde la FSx consola de Amazon.

En los sistemas de archivos existentes que tienen habilitada la auditoría de acceso a los archivos, puede cambiar la configuración de la auditoría de acceso a los archivos, incluidos los tipos de intentos de acceso para los accesos a archivos y recursos compartidos, y el destino del registro de eventos de auditoría. Puedes realizar estas tareas mediante la FSx consola o la AWS CLI API de Amazon.

> **Note**
>
> La auditoría de acceso a los archivos solo se admite en los sistemas de archivos Amazon FSx para Windows File Server con una capacidad de procesamiento de 32 MBps o más. No puede crear ni actualizar un sistema de archivos con una capacidad de rendimiento inferior a 32 MBps si la auditoría de acceso a los archivos está habilitada. Puede modificar la capacidad de rendimiento en cualquier momento después de crear el sistema de archivos. Para obtener más información, consulte Administración de la capacidad de rendimiento.

Cómo habilitar la auditoría de acceso a archivos al crear un sistema de archivos (consola)

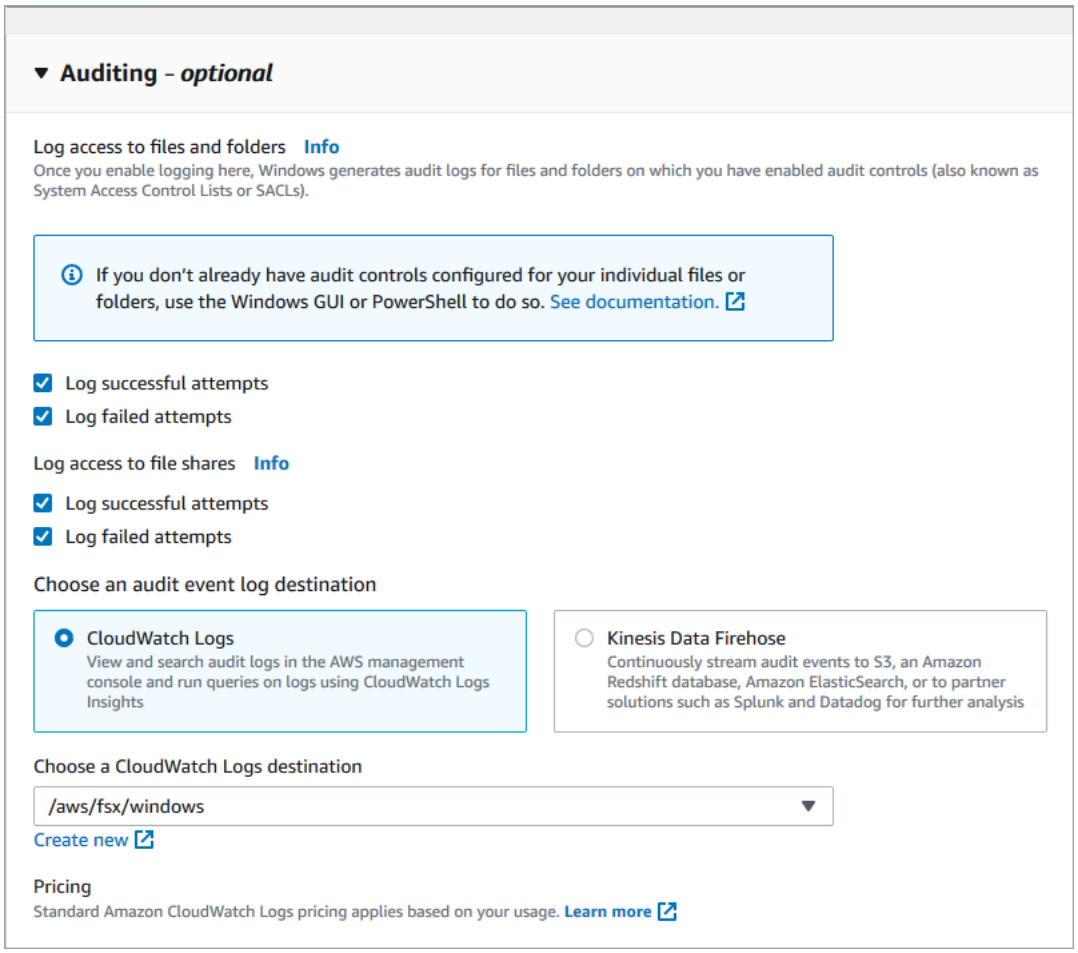
1. Abre la FSx consola de Amazon en https://console.aws.amazon.com/fsx/.
2. Siga el procedimiento para crear un nuevo sistema de archivos que se describe en Paso 5. Crear el sistema de archivos en la sección Primeros pasos.
3. Abra la sección Auditoría (opcional). La auditoría de acceso a archivos está deshabilitada de forma predeterminada.



4. Para habilitar y configurar la auditoría de acceso a los archivos, haga lo siguiente.
   - En Registrar el acceso a archivos y carpetas, seleccione el registro de los intentos correctos o fallidos. El registro estará desactivado para los archivos y carpetas si no selecciona nada.
   - En Registrar el acceso a archivos compartidos, seleccione el registro de los intentos correctos o fallidos. El registro estará desactivado para los archivos compartidos si no selecciona nada.

- En Elija un destino de registro de eventos de auditoría, elija CloudWatch Logs o Firehose. A continuación, seleccione un registro o flujo de entrega existente o cree uno nuevo. En el CloudWatch caso de Logs, Amazon FSx puede crear y usar un flujo de registros predeterminado en el grupo de CloudWatch `/aws/fsx/windows` registros Logs.

A continuación, se muestra un ejemplo de una configuración de auditoría de acceso a archivos que auditará los intentos de acceso correctos y fallidos de los usuarios finales a los archivos, las carpetas y los archivos compartidos. Los registros de eventos de auditoría se enviarán al destino predeterminado del grupo de CloudWatch `/aws/fsx/windows` registros.



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

Cuando el sistema de archivos está Disponible, la característica de auditoría de acceso a los archivos está habilitada.

Cómo habilitar la auditoría de acceso a archivos al crear un sistema de archivos (CLI)

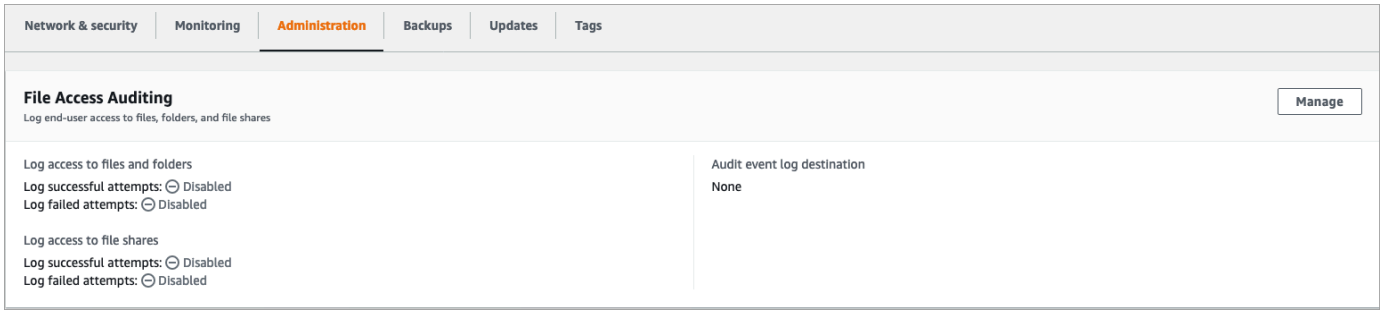
1. Al crear un nuevo sistema de archivos, utilice la `AuditLogConfiguration` propiedad con la operación de CreateFileSystemAPI para habilitar la auditoría del acceso a los archivos del nuevo sistema de archivos.

```
aws fsx create-file-system \
  --file-system-type WINDOWS \
  --storage-capacity 300 \
  --subnet-ids subnet-123456 \
  --windows-configuration
 AuditLogConfiguration='{FileAccessAuditLogLevel="SUCCESS_AND_FAILURE", \
    FileShareAccessAuditLogLevel="SUCCESS_AND_FAILURE", \
    AuditLogDestination="arn:aws:logs:us-east-1:123456789012:log-group:/aws/fsx/my-
customer-log-group"}'
```

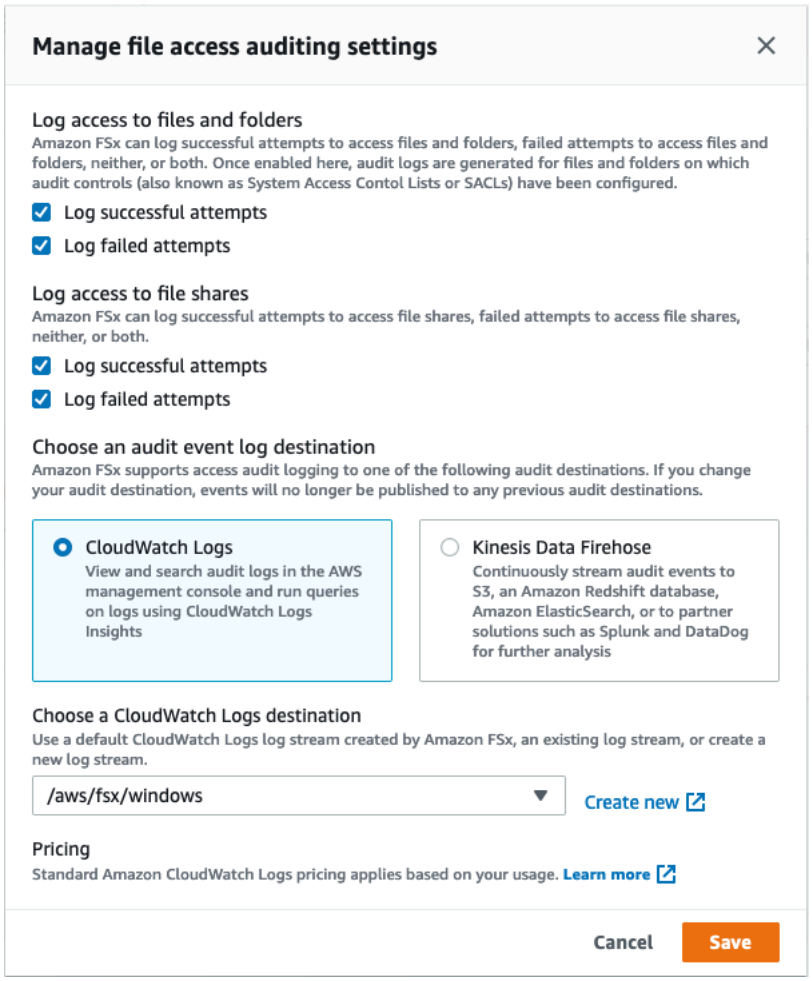
2. Cuando el sistema de archivos está Disponible, la característica de auditoría de acceso a los archivos está habilitada.

Cómo cambiar la configuración de auditoría de acceso a los archivos (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 de Windows para el que desee administrar la auditoría de acceso a archivos.
3. Elija la pestaña Administración.
4. En el panel de Auditoría de acceso a archivos, seleccione Administrar.



5. En el cuadro de diálogo Administrar la configuración de auditoría del acceso a los archivos, cambie la configuración deseada.



- En Registrar el acceso a archivos y carpetas, seleccione el registro de los intentos correctos o fallidos. El registro estará desactivado para los archivos y carpetas si no selecciona nada.
- En Registrar el acceso a archivos compartidos, seleccione el registro de los intentos correctos o fallidos. El registro estará desactivado para los archivos compartidos si no selecciona nada.
- En Elija un destino de registro de eventos de auditoría, elija CloudWatch Logs o Firehose. A continuación, seleccione un registro o flujo de entrega existente o cree uno nuevo.

6. Seleccione Save.

Cómo cambiar la configuración de auditoría de acceso a archivos (CLI)

- Utilice el comando de CLI `update-file-system` o la operación de la API `UpdateFileSystem` equivalente.

```
aws fsx update-file-system \
  --file-system-id fs-0123456789abcdef0 \
```

```
  --windows-configuration
 AuditLogConfiguration='{FileAccessAuditLogLevel="SUCCESS_ONLY", \
    FileShareAccessAuditLogLevel="FAILURE_ONLY", \
    AuditLogDestination="arn:aws:logs:us-east-1:123456789012:log-group:/aws/fsx/my-
customer-log-group"}'
```

Administración de identidades y accesos para Amazon FSx para Windows File Server

AWS Identity and Access Management (IAM) es una 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) FSx para usar los recursos del servidor de archivos de Windows. Puede utilizar IAM sin coste adicional. Servicio de AWS

Temas

- Público
- Autenticación con identidades
- Administración de acceso mediante políticas
- Cómo funciona Amazon FSx para Windows File Server con IAM
- Ejemplos de políticas basadas en identidad FSx para Amazon para Windows File Server
- AWS políticas gestionadas de Amazon FSx para OpenZFS
- Solución de problemas de identidad y acceso al servidor de archivos de Amazon FSx para Windows
- Uso de etiquetas con Amazon FSx
- Uso de roles vinculados a servicios FSx para Windows File Server

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que se realice con Windows File Server. FSx

Usuario del servicio: si utiliza el servicio de servidor de archivos de Windows FSx para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que

vaya utilizando más funciones del servidor de archivos de Windows FSx para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarle a solicitar los permisos correctos al administrador. Si no puede acceder a una función del servidor FSx de archivos de Windows, consulteSolución de problemas de identidad y acceso al servidor de archivos de Amazon FSx para Windows.

Administrador de servicios: si está a cargo de FSx los recursos del servidor de archivos de Windows en su empresa, probablemente tenga acceso completo al servidor FSx de archivos de Windows. Es su responsabilidad determinar a qué FSx características y recursos del servidor de archivos de Windows deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su gestionador 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 FSx Windows File Server, consulteCómo funciona Amazon FSx para Windows File Server con IAM.

Administrador de IAM: si es administrador de IAM, puede que le interese obtener más información sobre cómo redactar políticas FSx para administrar el acceso a Windows File Server. Para ver un FSx ejemplo de políticas basadas en la identidad del servidor de archivos de Windows que puede usar en IAM, consulte. Ejemplos de políticas basadas en identidad FSx para Amazon para Windows File Server

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su gestionador 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 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 para Windows File Server con IAM

Antes de utilizar IAM para gestionar el acceso al FSx servidor de archivos de Windows, infórmese sobre las funciones de IAM disponibles FSx para su uso en el servidor de archivos de Windows.

Funciones de IAM que puede utilizar con Amazon FSx for Windows File Server

Característica de IAM	FSx soporte
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
ACLs	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Sesiones de acceso directo	Sí
Roles de servicio	No
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo FSx funcionan otros AWS servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en la identidad para 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 la identidad para FSx

Para ver ejemplos de políticas basadas en FSx la identidad del servidor de archivos de Windows, consulte. Ejemplos de políticas basadas en identidad FSx para Amazon para Windows File Server

Políticas basadas en recursos dentro de FSx

Admite políticas basadas en recursos: no

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

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política

en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política basada en recursos concede acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Cross account resource access in IAM en la Guía del usuario de IAM.

Acciones políticas para 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 acciones, consulte Acciones definidas por Amazon FSx para Windows File Server en la Referencia de autorización de servicios.

Las acciones políticas FSx utilizan el siguiente prefijo antes de la acción:

```
fsx
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "fsx:action1",
      "fsx:action2"
         ]
```

Para ver ejemplos de FSx políticas basadas en la identidad del servidor de archivos de Windows, consulte. Ejemplos de políticas basadas en identidad FSx para Amazon para Windows File Server

Recursos de políticas para 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 y sus ARNs correspondientes, consulte Recursos definidos por Amazon FSx para Windows File Server en la Referencia de autorización de servicios. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte Acciones definidas FSx por Amazon para Windows File Server.

Para ver ejemplos de FSx políticas basadas en la identidad del servidor de archivos de Windows, consulte. Ejemplos de políticas basadas en identidad FSx para Amazon para Windows File Server

Claves de condición de la política para 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 condición, consulta Claves de condición de Amazon FSx para Windows File Server 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 Windows File Server.

Para ver ejemplos de FSx políticas basadas en la identidad del servidor de archivos de Windows, consulte. Ejemplos de políticas basadas en identidad FSx para Amazon para Windows File Server

ACLs in FSx

Soporta ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (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.

ABAC con 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.

Utilizar credenciales temporales con FSx

Compatibilidad con credenciales temporales: sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluidas las que Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para 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 FSx

Admite sesiones de acceso directo (FAS): sí

Cuando utiliza un usuario o un rol de IAM para realizar acciones en AWSél, se le considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Roles de servicio para FSx

Compatible con roles de servicio: No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio puede interrumpir FSx la funcionalidad. Edite las funciones de servicio solo cuando se FSx proporcionen instrucciones para hacerlo.

Funciones vinculadas al servicio para 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 administración de funciones FSx vinculadas a un servicio de Windows File Server, consulte. Uso de roles vinculados a servicios FSx para Windows File Server

Ejemplos de políticas basadas en identidad FSx para Amazon para Windows File Server

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar FSx los recursos del servidor de archivos de Windows. 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 FSx, incluido el ARNs formato de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de Amazon FSx para Windows File Server en la Referencia de autorización de servicios.

Temas

- Prácticas recomendadas sobre las políticas
- Mediante la consola de FSx
- 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 recursos del servidor de archivos de Windows de su FSx cuenta, acceder a ellos o eliminarlos. 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 conceden 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.

Mediante la consola de FSx

Para acceder a la consola de Amazon FSx for Windows File Server, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos del servidor FSx de archivos de Windows en su 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 realizan llamadas a la API AWS CLI o a la AWS API. 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, adjunte también la política FSx `AmazonFSxConsoleReadOnlyAccess` AWS administrada a las entidades. Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas 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": "*"
        }
    ]
}
```

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 FSx para Windows File Server 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 FSx para Windows File Server.

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, exceptoBypassSnaplockEnterpriseRetention.
- `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, exceptoBypassSnaplockEnterpriseRetention.
- `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 del documento página de Amazon.

Cambio	Descripción	Fecha
Amazon FSx ConsoleFullAccess: actualización de una política existente	Amazon FSx agregó un nuevo permiso `fsx:CreateAndAttachS3AccessPoint` que permite a los directores crear un S3 y adjuntarlo a un FSx volumen.	14 de abril de 2025

Cambio	Descripción	Fecha
Amazon FSx ConsoleFullAccess: actualización de una política existente	Amazon FSx agregó un nuevo permiso `fsx:DescribeS3AccessPointAttachments` 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 ConsoleFullAccess: actualización de una política existente	Amazon FSx agregó un nuevo permiso `fsx:UpdateS3AccessPointAttachments` 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 `fsx:DetachAndDeleteS3AccessPoint` 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 `fsx:CreateAndAttachS3AccessPoint` 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 `fsx:DescribeS3AccessPointAttachments` 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 FullAccess: actualización de una política existente	Amazon FSx agregó un nuevo permiso `fsx:UpdateS3AccessPointAttachments` que permite a los directores modificar un S3 existente.	14 de abril de 2025
Amazon FSx FullAccess: actualización de una política existente	Amazon FSx agregó un nuevo permiso `fsx:DetachAndDeleteS3AccessPoint` 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 `ec2:DescribeNetworkInterfaces` 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 `ec2:DescribeNetworkInterfaces` que permite a los directores ver las interfaces de red elásticas asociadas a su sistema de archivos.	7 de febrero de 2025

Cambio	Descripción	Fecha
Amazon FSx ServiceRolePolicy: actualización de una política existente	Amazon FSx agregó un nuevo permiso `ec2:GetSecurityGroupsForVpc` que permite a los directores proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una VPC.	9 de enero de 2024
Amazon FSx ReadOnlyAccess: actualización de una política existente	Amazon FSx agregó un nuevo permiso `ec2:GetSecurityGroupsForVpc` que permite a los directores proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una VPC.	9 de enero de 2024
Amazon FSx ConsoleReadOnlyAccess: actualización de una política existente	Amazon FSx agregó un nuevo permiso `ec2:GetSecurityGroupsForVpc` que permite a los directores proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una VPC.	9 de enero de 2024

Cambio	Descripción	Fecha
Amazon FSx FullAccess: actualización de una política existente	Amazon FSx agregó un nuevo permiso `ec2:GetSecurityGroupsForVpc` que permite a los directores proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una VPC.	9 de enero de 2024
Amazon FSx ConsoleFullAccess: actualización de una política existente	Amazon FSx agregó un nuevo permiso `ec2:GetSecurityGroupsForVpc` que permite a los directores proporcionar una validación mejorada de los grupos de seguridad de todos los grupos de seguridad que se pueden usar con una VPC.	9 de enero de 2024
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

Cambio	Descripción	Fecha
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
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

Cambio	Descripción	Fecha
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
AWS política gestionada: Amazon FSxServiceRolePolicy: actualización a una política existente	Amazon FSx modificó el `cloudwatch:PutMetricData` 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 `fsx:*` permiso y añadir `fsx` acciones específicas.	13 de julio de 2023
Amazon FSx ConsoleFullAccess: actualización de una política existente	Amazon FSx actualizó la política para eliminar el `fsx:*` permiso y añadir `fsx` 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

Cambio	Descripción	Fecha
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
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 llamadas restringidas.	2 de septiembre de 2021

Cambio	Descripción	Fecha
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
Amazon FSx ConsoleFullAccess: 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 llamadas restringidas.	2 de septiembre de 2021
Amazon FSx ServiceRolePolicy: 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 CloudWatch 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 ConsoleFullAccess: 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 ConsoleReadOnlyAccess: 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

Solución de problemas de identidad y acceso al servidor de archivos de Amazon FSx para Windows

Utilice la siguiente información para ayudarle a diagnosticar y solucionar los problemas más comunes que pueden surgir al trabajar con FSx Windows File Server e IAM.

Temas

- No estoy autorizado a realizar ninguna acción en FSx
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis FSx recursos

No estoy autorizado a realizar ninguna acción en FSx

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `fsx:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fsx:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `fsx:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su AWS administrador. El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibe un mensaje de error que indica que no está autorizado a realizar la `iam:PassRole` acción, debe actualizar sus políticas para que pueda transferir una función al FSx servidor de archivos de Windows.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

El siguiente ejemplo de error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en FSx el servidor de archivos de Windows. 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 necesita ayuda, póngase en contacto con el AWS administrador. El gestionador 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

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 respaldan 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 FSx Windows File Server admite estas funciones, consulte. Cómo funciona Amazon FSx para Windows File Server 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 de su propiedad Cuenta de AWS en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulta 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 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). Los usuarios deben tener permiso para aplicar etiquetas a FSx los recursos de Amazon durante la creación.

Conceder permisos para etiquetar recursos durante la creación

Algunas acciones de la API de creación de recursos FSx para Windows File Server permiten especificar etiquetas al crear el recurso. Puede utilizar etiquetas de recursos para implementar el

control de acceso basado en atributos (ABAC). Para obtener más información, consulte ¿Qué es ABAC para AWS? en la Guía del usuario de IAM.

Para permitir que los usuarios etiqueten los recursos durante su creación, es preciso que tengan permisos para utilizar la acción que crea el recurso (por ejemplo, `fsx:CreateFileSystem` o `fsx:CreateBackup`). Si se especifican etiquetas en la acción de creación de recursos, Amazon 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 muestra una política que permite a los usuarios crear sistemas de archivos y aplicar etiquetas a los sistemas de archivos durante la creación de un sistema específico. Cuenta de AWS

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateFileSystem",
         "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/*"
    }
  ]
}
```

De la misma manera, la siguiente política permite que los usuarios creen copias de seguridad en un sistema de archivos específico, y apliquen cualquier etiqueta a la copia de seguridad durante la creación de la copia de seguridad.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateBackup"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/file-system-id*"
    },
    {
```

```
      "Effect": "Allow",
      "Action": [
         "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:backup/*"
    }
  ]
}
```

La acción `fsx:TagResource` solo se evalúa si se aplican etiquetas durante la acción de creación de recursos. Por lo tanto, un usuario que tenga permisos para crear un recurso (suponiendo que no existan condiciones de etiquetado) no necesita permisos 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, consulteEtiquetar tus recursos de Amazon FSx . Para obtener más información sobre el uso de etiquetas para controlar el acceso a FSx los recursos, consulteUso de etiquetas para controlar el acceso a tus FSx recursos de Amazon.

Uso de etiquetas para controlar el acceso a tus FSx recursos de Amazon

Para controlar el acceso a FSx los recursos y acciones de Amazon, puedes usar políticas AWS Identity and Access Management (IAM) basadas en etiquetas. Puede proporcionar el control de dos maneras:

1. Controle el acceso a FSx los recursos de Amazon en función de las etiquetas de esos recursos.
2. Controlar las etiquetas que se pueden pasar en una condición de solicitud de IAM.

Para obtener información sobre cómo utilizar las etiquetas para controlar el acceso a AWS los recursos, consulte Controlar el acceso mediante etiquetas en la Guía del usuario de IAM. Para obtener más información sobre cómo etiquetar FSx los recursos de Amazon en el momento de la creación, consulteConceder permisos para etiquetar recursos durante la creación. Para obtener más información acerca del etiquetado de recursos, consulte Etiquetar tus 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 política: crear un sistema de archivos al proporcionar una etiqueta específica

Esta política permite que el usuario cree un sistema de archivos solo cuando lo etiqueta con un par clave-valor específico, en este ejemplo, `key=Department, value=Finance`.

```
{
    "Effect": "Allow",
    "Action": [
        "fsx:CreateFileSystem",
        "fsx:TagResource"
    ],
    "Resource": "arn:aws:fsx:region:account-id:file-system/*",
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/Department": "Finance"
        }
    }
}
```

Example política: cree copias de seguridad solo de los sistemas de FSx archivos de Amazon con una etiqueta específica

Esta política permite que los usuarios creen copias de seguridad únicamente de los sistemas de archivos que estén etiquetados con el par clave-valor `key=Department, value=Finance`, y la copia de seguridad se creará con la etiqueta `Deparment=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
```

```
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }

    ]
}
```

Example política: crear un sistema de archivos con una etiqueta específica a partir de copias de seguridad que tengan una etiqueta específica

Esta política permite que los usuarios creen sistemas de archivos que tengan la etiqueta `Department=Finance` únicamente a partir de copias de seguridad etiquetadas con `Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateFileSystemFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
```

```
            "Effect": "Allow",
            "Action": [
                "fsx:CreateFileSystemFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example política: 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"
                }
            }
        }
    ]
}
```

Uso de roles vinculados a servicios FSx para Windows File Server

Amazon FSx for Windows File Server utiliza funciones vinculadas a servicios AWS Identity and Access Management (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM al que se vincula directamente para Windows File Server. FSx Las funciones vinculadas a un servicio están predefinidas FSx para Windows File Server e incluyen todos los permisos que el servicio necesita para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio facilita la configuración del servidor FSx de archivos de Windows, ya que no es necesario añadir manualmente los permisos necesarios. FSx para Windows File Server define los permisos de sus funciones vinculadas a servicios y, a menos que se defina lo contrario, solo FSx para Windows File Server 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 sus recursos del servidor FSx de archivos de Windows porque no puede 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 rol vinculados a un servicio para Windows File Server FSx

FSx para Windows, el servidor de archivos utiliza el rol vinculado al servicio denominado `AWSServiceRoleForAmazonFSx` — que realiza determinadas acciones en la cuenta, como la creación de interfaces de red elásticas para los sistemas de archivos de la VPC.

La política de permisos de roles permite que FSx Windows File Server complete las siguientes acciones en todos los recursos aplicables: AWS

No puedes adjuntar Amazon FSx ServiceRolePolicy a tus entidades de IAM. Esta política está asociada a una función vinculada al servicio que permite FSx gestionar AWS los recursos en tu nombre. Para obtener más información, consulte Uso de roles vinculados a servicios FSx para Windows File Server.

Para obtener actualizaciones de esta política, consulte Amazon FSx ServiceRolePolicy

Esta política otorga permisos administrativos que permiten FSx administrar AWS los recursos en nombre del usuario.

Detalles de los permisos

Los permisos de los FSx ServiceRolePolicy roles de Amazon se definen en la política FSx ServiceRolePolicy AWS gestionada de Amazon. Amazon FSx ServiceRolePolicy tiene los siguientes permisos:

> **Note**
>
> Amazon FSx ServiceRolePolicy lo utilizan todos los tipos de sistemas de FSx archivos de Amazon; es posible que algunos de los permisos enumerados no se apliquen a FSx Windows.

- `ds`— Permite FSx ver, autorizar y desautorizar las aplicaciones de su AWS Directory Service directorio.
- `ec2`— Permite FSx 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 publicar puntos de datos métricos CloudWatch en el espacio de FSx nombres AWS/.
- `route53`— Permite FSx asociar una Amazon VPC a una zona alojada privada.

- `logs`— Permite FSx describir y escribir en los CloudWatch registros los flujos de registro. Esto permite a los usuarios enviar los registros de auditoría de acceso a los archivos de un sistema FSx de archivos del servidor de archivos de Windows a un flujo de CloudWatch registros.
- `firehose`— Permite FSx describir y escribir en los flujos de entrega de Amazon Data Firehose. Esto permite a los usuarios publicar los registros de auditoría de acceso a los archivos de un sistema de archivos FSx para Windows File Server en una transmisión de entrega de Amazon Data Firehose.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateFileSystem",
            "Effect": "Allow",
            "Action": [
                "ds:AuthorizeApplication",
                "ds:GetAuthorizedApplicationDetails",
                "ds:UnauthorizeApplication",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAddresses",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVPCs",
                "ec2:DisassociateAddress",
                "ec2:GetSecurityGroupsForVpc",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PutMetrics",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": [
```

```
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/FSx"
                }
            }
        },

        {
            "Sid": "TagResourceNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "AmazonFSx.FileSystemId"
                }
            }
        },
        {
            "Sid": "ManageNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
                }
            }
        },
```

```
        {
            "Sid": "ManageRouteTable",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
                }
            }
        },
        {
            "Sid": "PutCloudWatchLogs",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/fsx/*"
        },
        {
            "Sid": "ManageAuditLogs",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
        }
    ]
}
```

Todas las actualizaciones de esta política están detalladas en Amazon FSx actualiza las políticas 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 el servidor de archivos de FSx Windows

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 FSx para Windows, el servidor de archivos crea automáticamente el rol vinculado al servicio.

> **Important**
>
> Este rol vinculado a servicios puede aparecer en su cuenta si se ha completado una acción en otro servicio que utilice las características compatibles con este rol. Para obtener más información, consulte Un nuevo rol ha aparecido en mi cuenta de IAM.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al crear un sistema de archivos, en el caso de Windows, FSx File Server vuelve a crear el rol vinculado al servicio.

Edición de un rol vinculado a un servicio para FSx el servidor de archivos de Windows

FSx para Windows File Server no permite editar el rol 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 Windows File Server FSx

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Sin embargo, debe eliminar todos los sistemas de archivo y copias de seguridad para poder eliminar el rol vinculado al servicio de forma manual.

> **Note**
>
> Si el servicio FSx de servidor de archivos de Windows utiliza el rol al intentar 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 . Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones compatibles FSx para las funciones vinculadas al servicio del servidor de archivos de Windows

FSx para Windows File Server, admite el uso de roles vinculados a un servicio en todas las regiones en las que el servicio está disponible. Para obtener más información, consulte Regiones y puntos de conexión de AWS.

Validación de conformidad de Amazon FSx para Windows File Server

Para saber si un programa de cumplimiento Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- 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 de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulta la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Servidor de archivos FSx de Amazon para Windows y puntos finales de VPC de interfaz

Puede mejorar la 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 Windows File Server 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 aún más el acceso a la FSx API de Amazon, si lo desea, puede adjuntar una política AWS Identity and Access Management (IAM) a su punto de conexión de VPC. La política especifica lo siguiente:

- La entidad principal que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos en los que se pueden llevar a cabo las acciones.

Para obtener más información, consulte Control del acceso a los servicios con puntos de conexión de VPC en la Guía del usuario de Amazon VPC.

Trabajar con otros servicios de

Además de Amazon CloudWatch, AWS Identity and Access Management, y AWS CloudTrail, FSx para Windows AWS DataSync, File Server también se integra con lo siguiente Servicios de AWS:

- Amazon AppStream 2.0 — AppStream 2.0 es un servicio de streaming de aplicaciones totalmente gestionado que proporciona a los usuarios acceso instantáneo a sus aplicaciones de escritorio desde cualquier lugar. AppStream La versión 2.0 administra AWS los recursos necesarios para alojar y ejecutar sus aplicaciones, se amplía automáticamente y proporciona acceso a los usuarios cuando lo soliciten. Aprenda a crear almacenamiento persistente para usuarios individuales y a compartir el almacenamiento entre muchos usuarios en sus sistemas FSx de archivos Windows File Server mediante la AppStream versión 2.0. Para obtener más información, consulte Uso de Amazon FSx con Amazon AppStream 2.0.
- Amazon Kendra: se trata de un servicio de búsqueda inteligente que usa el procesamiento del lenguaje natural y algoritmos avanzados de machine learning para devolver respuestas específicas a las preguntas de búsqueda a partir de sus datos. Con Amazon Kendra, puede crear una experiencia de búsqueda unificada conectando varios repositorios de datos a un índice e incorporando y rastreando documentos. Para obtener más información sobre el uso de Amazon Kendra con FSx Windows File Server, consulte. Uso del servidor FSx de archivos de Windows con Amazon Kendra

Temas

- Uso de Amazon FSx con Amazon AppStream 2.0
- Uso del servidor FSx de archivos de Windows con Amazon Kendra

Uso de Amazon FSx con Amazon AppStream 2.0

Al ser compatible con el protocolo Server Message Block (SMB), Amazon FSx for Windows File Server permite acceder al sistema de archivos desde instancias de Amazon EC2 AWS, VMware Cloud on WorkSpaces, Amazon y Amazon AppStream 2.0. AppStream 2.0 es un servicio de streaming de aplicaciones totalmente gestionado. Puede gestionar de forma centralizada sus aplicaciones de escritorio en la AppStream versión 2.0 y entregarlas de forma segura a un navegador de cualquier ordenador. Para obtener más información sobre la AppStream versión 2.0, consulte la Guía de administración de Amazon AppStream 2.0. Para obtener instrucciones sobre cómo puedes

agilizar la administración de tus imágenes y flotas de Amazon AppStream 2.0, consulta la entrada del AWS blog Crea automáticamente imágenes personalizadas de Windows AppStream 2.0.

Los siguientes procedimientos le muestran cómo usar Amazon FSx con AppStream 2.0 para proporcionar almacenamiento persistente personal a cada usuario y proporcionar una carpeta compartida para que varios usuarios puedan acceder a archivos comunes.

Brindar almacenamiento persistente y personal a cada usuario

Puedes usar Amazon FSx para proporcionar a cada usuario de tu organización una unidad de almacenamiento única en las sesiones de streaming AppStream 2.0. El usuario tendrá permisos para acceder únicamente a la carpeta de dicho usuario. La unidad se monta de manera automática al inicio de una sesión de streaming, y los archivos actualizados o añadidos a la unidad se conservan automáticamente entre las sesiones de streaming.

Hay tres procedimientos que deberá realizar para completar esta tarea.

Para crear carpetas de inicio para los usuarios de dominios que utilizan Amazon FSx

1. Crea un sistema de FSx archivos de Amazon. Para obtener más información, consulte Primeros pasos con Amazon FSx para Windows File Server.
2. Cuando el sistema de archivos esté disponible, crea una carpeta para cada usuario del dominio AppStream 2.0 en tu sistema de FSx archivos de Amazon. En el siguiente ejemplo, se utiliza el nombre de usuario del dominio del usuario para nombrar la carpeta correspondiente. Esto significa que puede crear el nombre de UNC del recurso compartido de archivos para mapearlo con facilidad con la variable `%username%` de entorno de Windows.
3. Comparta cada una de estas carpetas como una carpeta compartida. Para obtener más información, consulte Crear, actualizar y eliminar recursos compartidos de archivos.

Para lanzar un generador de imágenes AppStream 2.0 unido a un dominio

1. Inicie sesión en la consola AppStream 2.0: /appstream2 https://console.aws.amazon.com
2. Elija Directory Configs en el menú de navegación y cree un objeto Directory Config. Para obtener más información, consulte Uso de Active Directory con AppStream 2.0 en la Guía de administración de Amazon AppStream 2.0.
3. Seleccione Imágenes, Generador de imágenes e inicie un nuevo constructor de imágenes.
4. Elija el objeto de configuración de directorios creado anteriormente en el asistente de inicio del generador de imágenes para unirlo al dominio del Active Directory.

5. Lanza el generador de imágenes en la misma VPC que la de tu sistema de FSx archivos de Amazon. Asegúrate de asociar el generador de imágenes al mismo AWS Managed Microsoft AD directorio al que está unido tu sistema de FSx archivos de Amazon. Los grupos de seguridad de VPC que asocie al generador de imágenes deben permitir el acceso a su sistema de FSx archivos de Amazon.
6. Cuando el generador de imágenes esté disponible, conéctese a él e inicie sesión con la cuenta de administrador de dominio.
7. Instale las aplicaciones.

Para vincular los FSx archivos compartidos de Amazon con AppStream 2.0

1. En el generador de imágenes, cree un script por lotes con el siguiente comando y guárdelo en una ubicación de archivo conocida (por ejemplo: C:\Scripts\map -fs.bat). En el siguiente ejemplo, se utiliza S: como letra de unidad para mapear la carpeta compartida del sistema de FSx archivos de Amazon. En este script, utilizas el nombre DNS de tu sistema de FSx archivos de Amazon o un alias de DNS asociado al sistema de archivos, que puedes obtener en la vista de detalles del sistema de archivos de la FSx consola de Amazon.

   Si utiliza el nombre del DNS del sistema de archivos:

   ```
   @echo off
   net use S: /delete
   net use S: \\file-system-DNS-name\users\%username%
   ```

   Si utiliza un alias del DNS asociado al sistema de archivos:

   ```
   @echo off
   net use S: /delete
   net use S: \\fqdn-DNS-alias\users\%username%
   ```

2. Abre un PowerShell mensaje y ejecútalo`gpedit.msc`.
3. En Configuración de usuario, elija Configuración de Windows y, a continuación, Iniciar sesión.
4. Halle el script por lotes que creó en el primer paso de este procedimiento y selecciónelo.
5. En Configuración del equipo, elija Plantillas administrativas, Sistema y, a continuación, elija Política de grupo.

6. Elija la política Configurar el retraso del script de inicio de sesión. Habilite la política y reduzca el retraso a `0`. Esta configuración ayuda a garantizar que el script de inicio de sesión del usuario se ejecute de forma inmediata cuando el usuario inicie una sesión de streaming.
7. Crea tu imagen y asígnala a una flota AppStream 2.0. Asegúrese de unir también la flota AppStream 2.0 al mismo dominio de Active Directory que utilizó para el creador de imágenes. Lanza la flota en la misma VPC que utiliza tu sistema de FSx archivos de Amazon. Los grupos de seguridad de VPC que asocie a la flota deben proporcionar acceso a su sistema de FSx archivos de Amazon.
8. Inicie una sesión de streaming con el SSO de SAML. Para conectarse a una flota que esté unida al Active Directory, configure la federación de inicio de sesión único mediante un proveedor de SAML. Para obtener más información, consulte Acceso mediante inicio de sesión único a AppStream 2.0 mediante SAML 2.0 en la Guía de administración de Amazon AppStream 2.0.
9. Tu recurso compartido de FSx archivos de Amazon está asignado a la letra S: drive dentro de la sesión de streaming.

Proporcionar una carpeta compartida entre los usuarios

Puedes usar Amazon FSx para proporcionar una carpeta compartida a los usuarios de tu organización. Una carpeta compartida se puede utilizar para mantener los archivos comunes (por ejemplo, archivos de demostración, ejemplos de código, manuales de instrucciones, etc.) que necesitan todos los usuarios.

Hay tres procedimientos que deberá realizar para completar esta tarea.

Para crear una carpeta compartida con Amazon FSx

1. Crea un sistema de FSx archivos de Amazon. Para obtener más información, consulte Primeros pasos con Amazon FSx para Windows File Server.
2. Todos los sistemas de FSx archivos de Amazon incluyen una carpeta compartida de forma predeterminada a la que puedes acceder mediante la dirección*`file-system-DNS-name`*\\ \ share o*`fqdn-DNS-alias`*\\\ share si utilizas alias DNS. Puede usar el recurso compartido predeterminado o crear otra carpeta compartida. Para obtener más información, consulte Crear, actualizar y eliminar recursos compartidos de archivos.

Para lanzar un generador de imágenes AppStream 2.0

1. Desde la consola AppStream 2.0, inicie un nuevo generador de imágenes o conéctese a un generador de imágenes existente. Lanza el generador de imágenes en la misma VPC que utiliza tu sistema de FSx archivos de Amazon. Los grupos de seguridad de VPC que asocie al generador de imágenes deben permitir el acceso a su sistema de FSx archivos de Amazon.
2. Cuando el generador de imágenes esté disponible, conéctese a él como usuario administrador.
3. Instale o actualice las aplicaciones como administrador.

Para vincular la carpeta compartida con 2.0 AppStream

1. Cree un script por lotes, como se describe en el procedimiento anterior, para montar la carpeta compartida de forma automática cada vez que un usuario inicie una sesión de streaming. Para completar el script, necesita el nombre DNS del sistema de archivos o un alias DNS asociado al sistema de archivos (que puede obtener en la vista de detalles del sistema de archivos de Amazon FSx Console) y las credenciales para acceder a la carpeta compartida.

   Si utiliza el nombre del DNS del sistema de archivos:

   ```
   @echo off
   net use S: /delete
   net use S: \\file-system-DNS-name\share /user:username password
   ```

   Si utiliza un alias del DNS asociado al sistema de archivos:

   ```
   @echo off
   net use S: /delete
   net use S: \\fqdn-DNS-alias\share /user:username password
   ```

2. Cree una política de grupo para ejecutar este script por lotes cada vez que un usuario inicie sesión. Puede seguir las mismas instrucciones de la sección anterior.
3. Cree la imagen y asígnela a la flota.
4. Inicie una sesión de streaming. Ahora debería ver la carpeta compartida asignada de manera automática a la letra de la unidad.

Uso del servidor FSx de archivos de Windows con Amazon Kendra

Amazon Kendra es un servicio de búsqueda inteligente y de alta precisión. FSx para Windows File Server, los sistemas de archivos se pueden utilizar como fuentes de datos para Amazon Kendra, lo que le permite indexar y buscar de forma inteligente la información contenida en los documentos almacenados en su sistema de archivos.

- Para obtener más información acerca de Amazon Kendra, consulte Qué es Amazon Kendra en la Guía para desarrolladores de Amazon Kendra.
- Para obtener más información sobre cómo añadir su sistema de archivos como fuente de datos de Amazon Kendra, consulte Introducción a una fuente de FSx datos de Amazon (consola) en la Guía del desarrollador de Amazon Kendra.
- Para obtener información general sobre Amazon Kendra, consulte el sitio web de Amazon Kendra.
- Para obtener información detallada sobre cómo buscar en su sistema de archivos con Amazon Kendra, consulte Búsqueda segura de datos no estructurados en sistemas de archivos Windows con el conector Amazon Kendra para FSx Amazon File Server en el blog Machine Learning.AWS

El rendimiento del sistema de archivos

Al añadir un sistema de archivos FSx para Windows File Server como fuente de datos, Amazon Kendra rastrea los archivos y carpetas del sistema de archivos con una frecuencia de sincronización normal para crear y mantener su índice de búsqueda. (Puede seleccionar la frecuencia de sincronización cuando establece la integración). Esta actividad de acceso a archivos de Amazon Kendra consumirá recursos del sistema de archivos, de forma similar a la actividad de sus propias cargas de trabajo que acceden al sistema de archivos.

Asegúrese de que el sistema de archivos esté configurado con los recursos suficientes para que el rendimiento de la carga de trabajo no se vea afectado. En concreto, si planea indexar una gran cantidad de archivos, le recomendamos que utilice un sistema de archivos con almacenamiento en SSD. Esto le proporciona un rendimiento máximo y le otorga los niveles de IOPS más altos para las solicitudes que necesitan acceder a los volúmenes de almacenamiento. Para obtener más información sobre el modelo de FSx rendimiento de Amazon, consulteFSx para el rendimiento del servidor de archivos de Windows.

Cuotas

A continuación, puede obtener información sobre las cuotas al trabajar con Amazon FSx for Windows File Server.

Temas

- Cuotas que puede aumentar
- Cuotas de recursos para cada sistema de archivos
- Consideraciones adicionales
- Las cuotas específicas de Microsoft Windows

Cuotas que puede aumentar

A continuación se muestran las cuotas de Amazon FSx for Windows File Server para cada una Cuenta de AWS de ellas que puede aumentar. Región de AWS

Recurso	Predeterminado/a	Descripción
Los sistemas de archivos de Windows	100	El número máximo de sistemas de archivos de Amazon FSx para Windows Server que puedes crear en esta cuenta.
La capacidad de rendimiento de Windows	10240	La cantidad total de capacidad de procesamiento (in MBps) permitida para todos los sistemas de archivos de Amazon FSx para Windows de esta cuenta.
La capacidad de almacenam iento de Windows en HDD	524288	La cantidad máxima de capacidad de almacenam iento en disco duro (en GiB) permitida para todos los

Recurso	Predeterminado/a	Descripción
		sistemas de archivos de Amazon FSx para Windows File Server de esta cuenta.
La capacidad de almacenamiento de Windows en SSD	524288	La cantidad máxima de capacidad de almacenamiento SSD (en GiB) permitida para todos los sistemas de archivos de Amazon FSx para Windows File Server de esta cuenta.
Las IOPS totales de SSD de Windows	500.000	La cantidad total de IOPS de SSD permitida para todos los sistemas de archivos de Amazon FSx for Windows File Server de esta cuenta.
Las copias de seguridad de Windows	500	El número máximo de copias de seguridad iniciadas por el usuario FSx para todos los sistemas de archivos de Amazon for Windows File Server que puede tener en esta cuenta.

Cómo solicitar un aumento de cuota

1. Abra la consola de Service Quotas.
2. En el panel de navegación, elija Servicios de AWS .
3. Elija Amazon FSx.
4. Elija una cuota.
5. Seleccione Solicitar aumento de cuota y siga las instrucciones para solicitar un aumento de cuota.

6. Para ver el estado de la solicitud de cuota, seleccione Historial de solicitudes de cuota en el panel de navegación de la consola.

Para obtener más información, consulte Solicitud de un aumento de cuota en la Guía del usuario de Service Quotas.

Cuotas de recursos para cada sistema de archivos

A continuación se muestran las cuotas de recursos de Amazon FSx para Windows File Server para cada sistema de archivos de un Región de AWS.

Recurso	Límite por sistema de archivos
Número máximo de etiquetas	50
Período máximo de retención para las copias de seguridad automatizadas	90 días
Número máximo de solicitudes de copia de seguridad en curso a una única Región de destino por cuenta.	5
La capacidad mínima de almacenamiento, sistemas de archivos SSD	32 GiB
La capacidad mínima de almacenamiento, sistemas de archivos HDD	2000 GiB
La capacidad máxima de almacenamiento, SSD y HDD	64 TiB
El mínimo de IOPS de SSD	96
El máximo de IOPS de SSD	400.000
La capacidad de rendimiento mínima	8 MBps
La capacidad de rendimiento máxima	12.288 MBps
El número máximo de recursos compartidos de archivos	100 000

Consideraciones adicionales

Además, tenga en cuenta lo siguiente:

- Puedes usar cada clave AWS Key Management Service (AWS KMS) en un máximo de 125 sistemas de FSx archivos de Amazon.
- Para obtener una lista de Regiones de AWS dónde puede crear sistemas de archivos, consulte Amazon FSx Endpoints and Quotas en. Referencia general de AWS
- Usted mapea los archivos compartidos de las EC2 instancias de Amazon en su nube privada virtual (VPC) con sus nombres de servicio de nombres de dominio (DNS).

Las cuotas específicas de Microsoft Windows

Para obtener más información, consulte los límites de NTFS en el Centro de desarrollo de Microsoft Windows.

Solución de problemas de Amazon FSx

Utiliza las siguientes secciones para ayudarte a solucionar los problemas que tengas con Amazon FSx.

Si te encuentras con problemas que no aparecen en la lista de seguidores mientras utilizas Amazon FSx, prueba a hacer una pregunta en el FSx foro de Amazon.

Temas

- No puede acceder al sistema de archivos
- Se produce un error al crear un nuevo sistema de FSx archivos de Amazon
- El sistema de archivos está mal configurado
- No puede configurar el DFS-R en un sistema de archivos Multi-AZ o Single-AZ 2
- Las actualizaciones del almacenamiento o la capacidad de rendimiento fallan

No puede acceder al sistema de archivos

Existen varias causas posibles por las que no pueda acceder al sistema de archivos, cada una tiene su propia resolución, como se indica a continuación.

Temas

- Se modificó o eliminó la interface 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 del sistema de archivos carece de las reglas de entrada o salida requeridas.
- El grupo de seguridad de la instancia informática carece de las reglas de salida requeridas
- La instancia informática no está unida a un Active Directory
- El recurso compartido de archivos no existe
- El usuario de Active Directory carece de los permisos necesarios
- Permita que se eliminen los permisos de control total de las ACL de NTFS
- No puede acceder a un sistema de archivos mediante un cliente en las instalaciones
- El nuevo sistema de archivos no está registrado en el DNS
- No se puede acceder al sistema de archivos con un alias del DNS

- No se puede acceder al sistema de archivos con una dirección IP

Se modificó o eliminó la interface de red elástica del sistema de archivos

No debe modificar ni eliminar la interfaz de red elástica del sistema de archivos. Si se modifica o elimina la interfaz de red, se puede provocar una pérdida permanente de la conexión entre la VPC y el sistema de archivos. Cree un nuevo sistema de archivos y no modifique ni elimine la interfaz de red FSx elástica 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, que se adjunta a la interfaz de red elástica de un sistema de archivos. Para obtener más información, consulte Acceso a sus datos.

El grupo de seguridad del sistema de archivos carece de las reglas de entrada o salida 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 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 instancia informática no está unida a un Active Directory

Es posible que las instancias informáticas no estén unidas correctamente a uno de los dos tipos de Active Directory:

- El AWS Managed Microsoft AD directorio al que está unido su sistema de archivos.

- Un directorio de Microsoft Active Directory que tiene una relación de confianza en el bosque unidireccional establecida con el directorio AWS Managed Microsoft AD .

Asegúrese de que las instancias informáticas estén unidas a uno de los dos tipos de directorio. Un tipo es el AWS Managed Microsoft AD directorio al que está unido el sistema de archivos. El otro tipo es un directorio de Microsoft Active Directory que tiene una relación de confianza en el bosque unidireccional establecida con el AWS Managed Microsoft AD directorio. Para obtener más información, consulte Uso de Amazon FSx con AWS Directory Service for Microsoft Active Directory.

El recurso compartido de archivos no existe

El recurso compartido de archivos de Microsoft Windows al que intenta acceder no existe.

Si utiliza un recurso compartido de archivos existente, asegúrese de que el nombre del DNS del sistema de archivos y el nombre del recurso compartido estén especificados de manera correcta. Para administrar los recursos compartidos de archivos, consulte Crear, actualizar y eliminar recursos compartidos de archivos.

El usuario de Active Directory carece de los permisos necesarios

El usuario de Active Directory con el que está accediendo al recurso compartido de archivos no cuenta con los permisos de acceso necesarios.

Asegúrese de que los permisos de acceso al recurso compartido de archivos y las listas de control de acceso de Windows (ACLs) a la carpeta compartida permitan el acceso a los usuarios de Active Directory que lo necesiten.

Permita que se eliminen los permisos de control total de las ACL de NTFS

Si elimina los permisos de las ACL NTFS llamados Permitir el control total para el usuario del SISTEMA de una carpeta que compartió, es posible que ese recurso compartido quede inaccesible y que las copias de seguridad del sistema de archivos realizadas a partir de ese momento no se puedan utilizar.

Deberá volver a crear el recurso compartido de archivos afectado. Para obtener más información, consulte Crear, actualizar y eliminar recursos compartidos de archivos. Tras volver a crear la carpeta o el recurso compartido, puede mapear y usar los recursos compartidos de archivos de Windows de las instancias informáticas.

No puede acceder a un sistema de archivos mediante un cliente en las instalaciones

Utiliza su sistema de FSx archivos de Amazon desde un entorno local mediante AWS Direct Connect una VPN y utiliza un intervalo de direcciones IP no privadas para el cliente local.

Amazon FSx solo admite el acceso desde clientes locales con direcciones IP no privadas en sistemas de archivos creados después del 17 de diciembre de 2020.

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

El nuevo sistema de archivos no está registrado en el DNS

En el caso de los sistemas de archivos unidos a un Active Directory autogestionado, Amazon FSx no registró el DNS del sistema de archivos al crearlo porque la red del cliente no utiliza el DNS de Microsoft.

Amazon FSx no registra los sistemas de archivos en el DNS si la red utiliza un servicio de DNS de terceros en lugar del DNS de Microsoft. Debes configurar manualmente las entradas A de DNS para tus sistemas de FSx archivos de Amazon. Para los sistemas de archivos Single-AZ 1, necesitará añadir una entrada A del DNS; para los sistemas de archivos Single-AZ 2 y Multi-AZ, tendrá que añadir dos entradas A del DNS. Utilice el siguiente procedimiento para obtener la o las direcciones IP del sistema de archivos que se van a utilizar al añadir las entradas A del DNS de forma manual.

1. En el https://console.aws.amazon.com/fsx/, elige el sistema de archivos del que deseas obtener la dirección IP para que aparezca la página de detalles del sistema de archivos.
2. En la pestaña Red y seguridad, realice una de las siguientes acciones:

   - En el caso de un sistema de archivos Single-AZ 1:
     - En el panel de subred, elija la interfaz de red elástica que se muestra en Interfaz de red para abrir la página Interfaces de red en Amazon EC2 .
     - La dirección IP que debe utilizar el sistema de archivos Single-AZ 1 se muestra en la columna IPv4 IP privada principal.
   - Para un sistema de archivos Single-AZ 2 o Multi-AZ:

- En el panel de subred preferida, elija la interfaz de red elástica que se muestra en Interfaz de red para abrir la página Interfaces de red en Amazon EC2 .
- La dirección IP de la subred preferida a utilizar se muestra en la columna IPv4 IP privada secundaria.
- En el panel de subred Amazon FSx Standby, elija la interfaz de red elástica que se muestra en Interfaz de red para abrir la página Interfaces de red en la EC2 consola de Amazon.
- La dirección IP que debe utilizar la subred en espera se muestra en la columna IPv4 IP privada secundaria.

No se puede acceder al sistema de archivos con un alias del DNS

Si no puede acceder a un sistema de archivos con un alias del DNS, utilice el siguiente procedimiento para solucionar el problema.

1. Compruebe que el alias esté asociado al sistema de archivos mediante uno de los siguientes pasos:

   a. Uso de la FSx consola de Amazon: elige el sistema de archivos al que intentas acceder. En la página de Información del sistema de archivos, los alias del DNS se muestran en la pestaña Red y seguridad.

   b. Uso de la CLI o la API: utilice el comando `describe-file-system-aliases`CLI o la operación de DescribeFileSystemAliasesAPI para recuperar los alias actualmente asociados al sistema de archivos.

2. Si el alias del DNS no aparece en la lista, debe asociarlo al sistema de archivos. Para obtener más información, consulte La administración de los alias del DNS en los sistemas de archivos existentes.
3. Si el alias del DNS está asociado al sistema de archivos, compruebe que también haya configurado los siguientes elementos obligatorios:

   - Creó los nombres principales de servicio (SPNs) correspondientes al alias DNS del objeto informático de Active Directory del sistema de FSx archivos de Amazon.

     Para obtener más información, consulte Configure los nombres principales de servicio () para Kerberos SPNs.
   - Creó un registro CNAME de DNS para el alias de DNS que se convierte en el nombre de DNS predeterminado del sistema de FSx archivos de Amazon.

Para obtener más información, consulte Actualizar o crear un registro CNAME del DNS.

4. Si ha creado un registro CNAME de DNS válido SPNs , compruebe que el DNS del cliente tiene el registro CNAME de DNS que se resuelve en el sistema de archivos correcto.

   a. Ejecute `nslookup` para confirmar que el registro existe y que se resuelve con el nombre del DNS predeterminado del sistema de archivos.

   b. Si el CNAME de DNS se resuelve en otro sistema de archivos, espere a que se actualice la caché del DNS del cliente y, luego, vuelva a comprobar el registro CNAME. Puede acelerar el proceso vaciando la caché del DNS del cliente con el siguiente comando.

   ```
   ipconfig /flushdns
   ```

5. Si el registro CNAME de DNS se convierte en el DNS predeterminado del sistema de FSx archivos de Amazon y el cliente sigue sin poder acceder al sistema de archivos, consulta los pasos adicionales No puede acceder al sistema de archivos de solución de problemas.

No se puede acceder al sistema de archivos con una dirección IP

Si no puede acceder al sistema de archivos con una dirección IP, pruebe utilizar el nombre o el alias del DNS asociado.

Puedes encontrar el nombre DNS del sistema de archivos y cualquier alias DNS asociado en la FSx consola de Amazon si eliges Servidor de archivos, red y seguridad de Windows. O bien, puede encontrarlos en la respuesta de la operación de CreateFileSystem o de las API de DescribeFileSystems. Para obtener más información acerca de alias del DNS, consulte La administración de los alias del DNS.

- En el caso de un sistema de archivos Single-AZ unido a un Microsoft Active Directory AWS administrado, el nombre DNS tiene el siguiente aspecto.

  ```
  fs-0123456789abcdef0.ad-domain.com
  ```

- En todos los sistemas de archivos Multi-AZ y en los sistemas de archivos Single-AZ unidos a un Active Directory autoadministrado, el nombre del DNS tiene el siguiente aspecto.

  ```
  amznfsxaa11bb22.ad-domain.com
  ```

Se produce un error al crear un nuevo sistema de FSx archivos de Amazon

Existen varias causas posibles por las que se produce un error en una solicitud de creación de un sistema de archivos, tal como se describe en la siguiente sección.

Temas

- Red y grupo de seguridad de VPC mal configurados ACLs
- Nombres de grupos de administradores de sistemas de archivos duplicados
- No se puede acceder a los servidores del DNS ni a los controladores de dominio
- Credenciales de cuenta de servicio inválidas
- Permisos de cuenta de servicio insuficientes
- Se superó la capacidad de la cuenta de servicio
- Amazon no FSx puede acceder a la unidad organizativa (OU)
- La cuenta de servicio no puede acceder al grupo de administradores
- Amazon FSx perdió la conectividad en el dominio
- La cuenta de servicio no tiene los permisos correctos
- Se usan caracteres Unicode en los parámetros de creación
- Se produce un error al pasar el tipo de almacenamiento a disco duro durante la restauración de una copia de seguridad

Red y grupo de seguridad de VPC mal configurados ACLs

Asegúrese de que los grupos de seguridad y la red de VPC ACLs estén configurados con la configuración de grupos de seguridad recomendada. Para obtener más información, consulte Creación de grupos de seguridad.

Nombres de grupos de administradores de sistemas de archivos duplicados

La creación de un sistema de archivos unido a su Active Directory autoadministrado falla con el siguiente mensaje de error:

```
File system creation failed. Amazon FSx is unable to apply your Microsoft Active
 Directory configuration with the
```

```
specified file system administrators group. Please ensure that your Active Directory
 does not contain multiple domain
groups with the name: domain_group.
```

Amazon FSx no creó el sistema de archivos porque hay varios grupos de administradores en el dominio con el mismo nombre.

Si no especificas un nombre de grupo, Amazon FSx intentará usar el valor predeterminado «Domain Admins» como grupo de administradores. La solicitud dará error si hay más de un grupo que use el nombre predeterminado “Administradores de dominio”.

Siga los pasos a continuación para resolver el problema.

1. Revise los requisitos previos para unir el sistema de archivos al Active Directory autoadministrado.
2. Utilice la herramienta de validación de Amazon FSx Active Directory para validar la configuración autogestionada de Active Directory antes de crear un sistema de archivos FSx para Windows File Server unido a un Active Directory autogestionado.
3. Cree un nuevo sistema de archivos con o. AWS Management Console AWS CLI Para obtener más información, consulte Unir un sistema de FSx archivos de Amazon a un dominio autogestionado de Microsoft Active Directory.
4. Proporcione un nombre para el grupo de administradores del sistema de archivos que sea único en el dominio del Active Directory autoadministrado.

No se puede acceder a los servidores del DNS ni a los controladores de dominio

La creación de un sistema de archivos unido a su Active Directory autoadministrado falla con el siguiente mensaje de error:

```
Amazon FSx can't reach the DNS servers provided or the domain controllers for your
 self-managed directory in Microsoft Active Directory.
File system creation failed. Amazon FSx is unable to communicate with your Microsoft
 Active Directory domain controllers.
This is because Amazon FSx can't reach the DNS servers provided or domain controllers
 for your domain.
To fix this problem, delete your file system and create a new one with valid DNS
 servers and networking configuration that allows
```

```
traffic from the file system to the domain controller.
```

Siga los pasos a continuación para solucionar el problema.

1. Compruebe que ha cumplido los requisitos previos para establecer la conectividad de red y el enrutamiento entre la subred en la que va a crear un sistema de FSx archivos de Amazon y su Active Directory autogestionado. Para obtener más información, consulte Requisitos previos.

   Utilice la herramienta de validación de Amazon FSx Active Directory para probar y verificar esta configuración de red.

   > **Note**
   >
   > Si ha definido varios sitios de Active Directory, asegúrese de que las subredes de la VPC asociadas a su sistema de archivos de FSx Amazon estén definidas en un sitio de Active Directory y de que no existan conflictos de IP entre las subredes de su VPC y las subredes de sus otros sitios. Puede ver y cambiar esta configuración con el complemento MMC de sitios y servicios de Active Directory.

2. Compruebe que ha configurado los grupos de seguridad de VPC que ha asociado a su sistema de FSx archivos de Amazon, junto con cualquier red de VPC ACLs, para permitir el tráfico de red saliente en todos los puertos.

   > **Note**
   >
   > Si desea implementar el privilegio mínimo, puede permitir el tráfico saliente solo a los puertos específicos que se necesiten para que haya comunicación con los controladores de dominio del Active Directory. Para obtener más información, consulte la documentación de Microsoft Active Directory.

3. Compruebe que los valores de las propiedades administrativas del servidor de archivos o de la red de Microsoft Windows no contengan caracteres que no sean latin-1. Por ejemplo, se produce un error en la creación del sistema de archivos si se utiliza `Domänen-Admins` como nombre del grupo de administradores del sistema de archivos.
4. Compruebe que los controladores de dominio y los servidores del DNS del dominio del Active Directory estén activos y puedan responder a las solicitudes del dominio proporcionado.
5. Asegúrese de que el nivel funcional del dominio del Active Directory sea Windows Server 2008 R2 o superior.

6. Asegúrese de que las reglas de firewall de los controladores de dominio de su dominio de Active Directory permitan el tráfico desde su sistema de FSx archivos de Amazon. Para obtener más información, consulte la documentación de Microsoft Active Directory.

Credenciales de cuenta de servicio inválidas

Se produce un error al crear un sistema de archivos unido al Active Directory autoadministrado y aparece el siguiente mensaje de error:

```
Amazon FSx is unable to establish a connection with your Microsoft Active Directory
 domain controllers
because the service account credentials provided are invalid. To fix this problem,
 delete your file
system and create a new one using a valid service account.
```

Siga los pasos a continuación para solucionar el problema.

1. Compruebe que esté escribiendo únicamente el nombre de usuario como entrada en el nombre de usuario de la cuenta de servicio, por ejemplo `ServiceAcct`, en la configuración del Active Directory autoadministrado.

   > **Important**
   >
   > NO incluya un prefijo de dominio (`corp.com\ServiceAcct`) o un sufijo de dominio (`ServiceAcct@corp.com`) al escribir el nombre de usuario de la cuenta de servicio. NO utilice el nombre distintivo (DN) al introducir el nombre de usuario de la cuenta de servicio (CN=ServiceAcct, OU=example, DC=corp, DC=com).

2. Compruebe que la cuenta de servicio que proporcionó existe en el dominio de Active Directory.
3. 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

Para obtener más información acerca de la creación de una cuenta de servicio con los permisos correctos, consulte Cuenta de FSx servicio de Amazon.

Permisos de cuenta de servicio insuficientes

La creación de un sistema de archivos unido a su Active Directory autoadministrado falla con el siguiente mensaje de error:

```
Amazon FSx is unable to establish a connection with your
Microsoft Active Directory domain controllers. This is because the service account
 provided does not
have permission to join the file system to the domain with the specified organizational
 unit.
To fix this problem, delete your file system and create a new one using a service
 account with
permission to join the file system to the domain with the specified organizational
 unit.
```

Siga el siguiente procedimiento para solucionar el 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

  Para obtener más información acerca de la creación de una cuenta de servicio con los permisos correctos, consulte Cuenta de FSx servicio de Amazon.

Se superó la capacidad de la cuenta de servicio

La creación de un sistema de archivos unido a su Active Directory autoadministrado falla con el siguiente mensaje de error:

```
Amazon FSx can't establish a connection with your Microsoft Active Directory
domain controllers. This is because the service account provided has reached the
maximum number of computers that it can join to the domain. To fix this problem,
delete your file system and create a new one, supplying a service account that
is able to join new computers to the domain.
```

Para resolver el problema, compruebe que la cuenta de servicio que proporcionó no haya alcanzado el número máximo de equipos que puede unir al dominio. Si ha alcanzado el límite máximo, cree una cuenta de servicio nueva con los permisos correctos. Utilice la cuenta de servicio nueva y cree un sistema de archivos nuevo. Para obtener más información, consulte Cuenta de FSx servicio de Amazon.

Amazon no FSx puede acceder a la unidad organizativa (OU)

La creación de un sistema de archivos unido a su Active Directory autoadministrado falla con el siguiente mensaje de error:

```
Amazon FSx can't establish a connection with your Microsoft Active Directory domain
 controller(s).
This is because the organizational unit you specified either doesn't exist or isn't
 accessible
to the service account provided. To fix this problem, delete your file system and
 create a new one specifying an
organizational unit to which the service account can join the file system.
```

Siga los pasos a continuación para solucionar el problema.

1. Compruebe que la unidad organizativa que proporcionó se encuentre dentro del dominio del Active Directory.
2. Asegúrese de haber delegado los permisos necesarios en la cuenta de servicio que proporcionó. La cuenta de servicio debe poder crear y eliminar objetos informático en la unidad organizativa del dominio al que se va a unir el sistema de archivos. La cuenta de servicio también debe tener, como mínimo, 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
- Tener delegado el control para crear y eliminar objetos informáticos
- 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 Cuenta de FSx servicio de Amazon.

La cuenta de servicio no puede acceder al grupo de administradores

La creación de un sistema de archivos unido a su Active Directory autoadministrado falla con el siguiente mensaje de error:

```
Amazon FSx is unable to apply your Microsoft Active Directory configuration. This is
 because the file system
administrators group you provided either doesn't exist or isn't accessible to the
 service account you
provided. To fix this problem, delete your file system and create a new one specifying
 a file
system administrators group in the domain that is accessible to the service account
provided.
```

Siga los pasos a continuación para solucionar el problema.

1. Asegúrese de proporcionar solo el nombre del grupo como cadena para el parámetro del grupo de administradores.

   > **Important**
   >
   > NO incluya un prefijo de dominio (`corp.com\FSxAdmins`) o un sufijo de dominio (`FSxAdmins@corp.com`) al proporcionar el parámetro de nombre de grupo.
   > NO utilice el nombre distintivo (DN) para el grupo. Un ejemplo de nombre distintivo es CN= FSx Admins, OU=Example, DC=Corp, DC=com.

2. Asegúrese de que el grupo de administradores ingresado exista en el mismo dominio de Active Directory al que desea unir el sistema de archivos.

3. Si no has proporcionado un parámetro de grupo de administradores, Amazon FSx intentará usar el `Builtin Domain Admins` grupo en tu dominio de Active Directory. Si se cambió el nombre de dicho grupo o si utiliza un grupo diferente para la administración del dominio, debe establecer ese nombre para el grupo.

Amazon FSx perdió la conectividad en el dominio

La creación de un sistema de archivos unido a su Active Directory autoadministrado falla con el siguiente mensaje de error:

```
Amazon FSx is unable to apply your Microsoft Active Directory configuration. To fix
 this problem, delete your file system and create a new one
meeting the pre-requisites described in the Amazon FSx user guide.
```

Al crear su sistema de archivos, Amazon FSx pudo acceder a los servidores DNS y controladores de dominio de su dominio de Active Directory y unir el sistema de archivos correctamente a su dominio de Active Directory. Sin embargo, al completar la creación del sistema de archivos, Amazon FSx perdió la conectividad o la membresía en tu dominio. Siga los pasos a continuación para solucionar el problema.

1. Asegúrese de que siga existiendo conectividad de red entre su sistema de FSx archivos de Amazon y su Active Directory. Además, asegúrese de que se siga permitiendo el tráfico de red entre ellos mediante reglas de enrutamiento, reglas de grupos de seguridad de VPC ACLs, redes de VPC y reglas de firewall de controladores de dominio.
2. Asegúrese de que los objetos informáticos creados por Amazon FSx para sus sistemas de archivos en su dominio de Active Directory siguen activos y no se han eliminado ni manipulado de ningún otro modo.

La cuenta de servicio no tiene los permisos correctos

La creación de un sistema de archivos unido a su Active Directory autoadministrado falla con el siguiente mensaje de error:

```
File system creation failed. Amazon FSx is unable to establish a connection with your
 Microsoft Active Directory domain controller(s).
This is because the service account provided does not have permission to join the file
 system to the domain with the specified
```

```
organizational unit (OU). To fix this problem, delete your file system and create a new
 one using a service account with permission
to create computer objects and reset passwords within the specified organizational
 unit.
```

Asegúrese de haber delegado los permisos necesarios en la cuenta de servicio que proporcionó. Siga los pasos a continuación para solucionar el problema.

La cuenta de servicio debe tener, como mínimo, los siguientes permisos:

- Tener delegado el control para crear y eliminar objetos informáticos en la unidad organizativa a la que va a unir el sistema de archivos
- Tener los siguientes permisos en la unidad organizativa a la que se va a unir al sistema de archivos:
  - Posibilidad de restablecer las contraseñas
  - Capacidad de restringir la lectura y escritura de datos en las cuentas
  - Capacidad validada para escribir en el nombre de host del DNS
  - Capacidad validada para escribir en el nombre de entidad principal del servicio
  - La capacidad de crear y eliminar objetos informáticos (se puede delegar)
  - Capacidad validada para leer y escribir las restricciones de la cuenta
  - La capacidad de modificar los permisos

  Para obtener más información acerca de la creación de una cuenta de servicio con los permisos correctos, consulte Cuenta de FSx servicio de Amazon.

Se usan caracteres Unicode en los parámetros de creación

La creación de un sistema de archivos unido a su Active Directory autoadministrado falla con el siguiente mensaje de error:

```
File system creation failed. Amazon FSx is unable to create a file system within the
 specified
Microsoft Active Directory. To fix this problem, please delete your file system and
 create a new one
meeting the pre-requisites described in the FSx for ONTAP User Guide.
```

Amazon FSx no admite caracteres Unicode. Compruebe que ninguno de los parámetros de creación tenga caracteres Unicode, como acentos. Esto incluye los parámetros que se pueden dejar en blanco, donde el valor predeterminado se rellena de forma automática. Asegúrese de que los valores predeterminados correspondientes del Active Directory tampoco contengan caracteres Unicode.

Se produce un error al pasar el tipo de almacenamiento a disco duro durante la restauración de una copia de seguridad

La creación de un sistema de archivos a partir de una copia de seguridad falla, y recibe el siguiente mensaje de error:

```
Switching storage type to HDD while creating a file system from backup
backup_id is not supported because a storage scaling activity was still
under way on the source file system to increase storage capacity from less
than 2000 GiB when the backup backup_id was taken, and the minimum storage
capacity for HDD storage is 2000 GiB.
```

Este problema se produce cuando se quiere restaurar una copia de seguridad, y previamente se pasó el tipo de almacenamiento de SSD a HDD. La restauración a partir de una copia de seguridad falla, porque la copia que está restaurando se realizó cuando aún se estaba produciendo un aumento de la capacidad de almacenamiento en el sistema de archivos original. La capacidad de almacenamiento en SSD del sistema de archivos antes de la solicitud de aumento era inferior a 2000 GiB. Esta es la capacidad de almacenamiento mínima requerida para crear un sistema de archivos en HDD.

Utilice el siguiente proceso para resolver este problema.

1. Espere a que se complete la solicitud de aumento de la capacidad de almacenamiento, y que el sistema de archivos tenga al menos 2000 GiB de capacidad de almacenamiento en SSD. Para obtener más información, consulte Supervisión de los aumentos de capacidad de almacenamiento.
2. Realice una copia de seguridad del sistema de archivos iniciada por el usuario. Para obtener más información, consulte Trabajo con copias de seguridad iniciadas por el usuario.
3. Restaure dicha copia en un sistema de archivos nuevo y use el almacenamiento en disco duro. Para obtener más información, consulte Restauración de copias de seguridad en un nuevo sistema de archivos.

El sistema de archivos está mal configurado

Un sistema FSx de archivos del servidor de archivos de Windows puede pasar a un estado mal configurado debido a un cambio en el entorno de Active Directory. En este estado, el sistema de archivos deja de estar disponible o corre el riesgo de perder la disponibilidad. Y, es posible que las copias de seguridad no se realicen correctamente.

El estado de configuración incorrecta incluye un mensaje de error y una acción correctiva recomendada a la que puedes acceder mediante la FSx consola de Amazon, la API o AWS CLI. Tras tomar las medidas correctivas, compruebe que el estado del sistema de archivos cambie finalmente a `Available` (Disponible): tenga en cuenta que este cambio puede tardar varios minutos en completarse.

El sistema de archivos puede entrar en un estado desconfigurado por varios motivos, como los siguientes:

- Las direcciones IP del servidor DNS ya no son válidas.
- Las credenciales de la cuenta de servicio ya no son válidas o no tienen los permisos necesarios.
- No se puede acceder al controlador de dominio del Active Directory debido a problemas de conectividad de red, como grupos de seguridad de la VPC no válidos, la configuración de las ACL de la red de la VPC o la configuración de la tabla de enrutamiento o del firewall del controlador de dominio.

> **Important**
>
> No muevas los objetos de ordenador que Amazon FSx cree en la unidad organizativa una vez creado el sistema de archivos. Si lo hace, el sistema de archivos no se configurará de manera correcta.

(Para ver la lista completa de requisitos de Active Directory, consulteRequisitos previos. También puede validar que su entorno de Active Directory esté configurado correctamente para cumplir estos requisitos mediante la herramienta de validación de Amazon FSx Active Directory.)

Para resolver algunos de estos problemas, es necesario que actualice directamente uno o más parámetros de la configuración del Active Directory del sistema de archivos, como cambiar las direcciones IP del servidor del DNS o cambiar el nombre de usuario o la contraseña de la cuenta de

servicio. En estos casos, la acción correctiva implicará necesariamente el uso de la FSx consola o la API de Amazon o AWS CLI la actualización de los parámetros de configuración necesarios.

Es posible que para solucionar otros problemas no haga falta cambiar ningún parámetro de la configuración del Active Directory, como la configuración del firewall del controlador de dominio o los grupos de seguridad de VPC. Sin embargo, en estos casos, tendrá que tomar medidas adicionales para que el sistema de archivos pase a estar `Available` (Disponible). Tras comprobar que su entorno de Active Directory está configurado correctamente, seleccione el botón Intentar recuperación situado junto al estado Configuración incorrecta en la FSx consola de Amazon o utilice el `StartMisconfiguredStateRecovery` comando en la FSx consola de Amazon, la API o AWS CLI.

Temas

- Sistema de archivos mal configurado: Amazon no FSx puede acceder a los servidores DNS ni a los controladores de dominio de tu dominio.
- Sistema de archivos desconfigurado: las credenciales de la cuenta de servicio no son válidas
- Sistema de archivos desconfigurado: la cuenta de servicio proporcionada no tiene permiso para unir el sistema de archivos al dominio
- Sistema de archivos desconfigurado: la cuenta de servicio no puede unir más equipos al dominio
- Sistema de archivos desconfigurado: la cuenta de servicio no tiene acceso a la OU

Sistema de archivos mal configurado: Amazon no FSx puede acceder a los servidores DNS ni a los controladores de dominio de tu dominio.

Un sistema de archivos pasará a un `Misconfigured` estado en el que Amazon no FSx pueda comunicarse con el controlador o los controladores de dominio de Microsoft Active Directory.

Para resolverlo, haga lo siguiente:

1. Asegúrese de que la configuración de red permita el tráfico del sistema de archivos al controlador de dominio.
2. Utilice la herramienta de validación de Amazon FSx Active Directory para probar y verificar la configuración de red de su Active Directory autogestionado. Para obtener más información, consulte Uso de un Active Directory de Microsoft autoadministrado.
3. Revise la configuración de Active Directory autogestionada del sistema de archivos en la FSx consola de Amazon.

4. Para actualizar la configuración autogestionada de Active Directory del sistema de archivos, puede utilizar la FSx consola de Amazon.

   a. En el panel de navegación, elija Sistemas de archivos y elija el que desee actualizar; aparecerá la página de Información del sistema de archivos.

   b. En la página de Información del sistema de archivos, seleccione Actualizar en la pestaña Redes y seguridad.

   También puede utilizar el `update-file-system` comando Amazon FSx CLI o la operación de API UpdateFileSystem.

Sistema de archivos desconfigurado: las credenciales de la cuenta de servicio no son válidas

Amazon no FSx puede establecer una conexión con el controlador o controladores de dominio de Microsoft Active Directory. Esto se debe a que las credenciales de la cuenta de servicio que se ingresaron no son válidas. Para obtener más información, consulte Uso de un Active Directory de Microsoft autoadministrado.

Para solucionar el error de configuración, haga lo siguiente:

1. Compruebe que esté utilizando la cuenta de servicio y las credenciales correctas para dicha cuenta.
2. A continuación, actualiza la configuración del sistema de archivos con la cuenta de servicio o las credenciales de la cuenta correctas mediante la FSx consola de Amazon.

   a. En el panel de navegación, seleccione Sistemas de archivos y elija el sistema de archivos desconfigurado que desee actualizar.

   b. En la página de Información del sistema de archivos, seleccione Actualizar en la pestaña Redes y seguridad.

   También puedes usar la operación de la FSx API de Amazon`update-file-system`. Para obtener más información, consulta la referencia UpdateFileSystemde la FSx API de Amazon.

Sistema de archivos desconfigurado: la cuenta de servicio proporcionada no tiene permiso para unir el sistema de archivos al dominio

Amazon no FSx puede establecer una conexión con los controladores de dominio de Microsoft Active Directory. Esto se debe a que la cuenta de servicio que se ingresó no tiene permiso para unir el sistema de archivos al dominio con la OU especificada.

Para solucionar el error de configuración, haga lo siguiente:

1. Añade los permisos necesarios a la cuenta de FSx servicio de Amazon o crea una nueva cuenta de servicio con los permisos necesarios. Para obtener más información sobre este procedimiento, consulte Cuenta de FSx servicio de Amazon.
2. A continuación, actualice la configuración del Active Directory autoadministrado del sistema de archivos con las credenciales nuevas de la cuenta de servicio. Para actualizar la configuración, puedes usar la FSx consola de Amazon.

   a. En el panel de navegación, elija Sistemas de archivos y elija el que desee actualizar; aparecerá la página de Información del sistema de archivos.
   b. En la página de Información del sistema de archivos, seleccione Actualizar en la pestaña Redes y seguridad.

   También puedes usar la operación de la FSx API de Amazon`update-file-system`. Para obtener más información, consulta la referencia UpdateFileSystemde la FSx API de Amazon.

Sistema de archivos desconfigurado: la cuenta de servicio no puede unir más equipos al dominio

Amazon no FSx puede establecer una conexión con los controladores de dominio de Microsoft Active Directory. En este caso, esto se debe a que la cuenta de servicio que se ingresó alcanzó el número máximo de equipos que puede unir al dominio.

Para solucionar el error de configuración, haga lo siguiente:

1. Identifique otra cuenta de servicio o cree una nueva que pueda unir más equipos al dominio.
2. A continuación, actualice la configuración autogestionada de Active Directory del sistema de archivos con las nuevas credenciales de la cuenta de servicio mediante la FSx consola de Amazon.

a. En el panel de navegación, elija Sistemas de archivos y elija el que desee actualizar; aparecerá la página de Información del sistema de archivos.

b. En la página de Información del sistema de archivos, seleccione Actualizar en la pestaña Redes y seguridad.

También puedes usar la operación de la FSx API de Amazon`update-file-system`. Para obtener más información, consulta la referencia UpdateFileSystemde la FSx API de Amazon.

Sistema de archivos desconfigurado: la cuenta de servicio no tiene acceso a la OU

Amazon no FSx puede establecer una conexión con los controladores de dominio de Microsoft Active Directory porque la cuenta de servicio proporcionada no tiene acceso a la OU especificada.

Para solucionar el error de configuración, haga lo siguiente:

1. Identifique otra cuenta de servicio o cree una nueva que tenga acceso a la OU.
2. A continuación, actualice la configuración del Active Directory autoadministrado del sistema de archivos con las credenciales nuevas de la cuenta de servicio.

   a. En el panel de navegación, elija Sistemas de archivos y elija el que desee actualizar; aparecerá la página de Información del sistema de archivos.

   b. En la página de Información del sistema de archivos, seleccione Actualizar en la pestaña Redes y seguridad.

   También puedes usar la operación de la FSx API de Amazon`update-file-system`. Para obtener más información, consulta la referencia UpdateFileSystemde la FSx API de Amazon.

No puede configurar el DFS-R en un sistema de archivos Multi-AZ o Single-AZ 2

La replicación del sistema de archivos distribuido (DFS-R) de Microsoft no es compatible con los sistemas de archivos Multi-AZ y Single-AZ 2.

Los sistemas de archivos Multi-AZ están configurados de forma nativa para ofrecer redundancia en varias zonas de acceso. Utilice el tipo de implementación Multi-AZ para obtener una alta disponibilidad en varias zonas de disponibilidad. Para obtener más información, consulte Disponibilidad y durabilidad: sistemas de archivos Single-AZ y Multi-AZ..

Las actualizaciones del almacenamiento o la capacidad de rendimiento fallan

Existen varias causas posibles por las que se produce un error en las solicitudes de actualización de la capacidad de rendimiento y almacenamiento del sistema de archivos. Y cada una tiene su propia resolución.

El aumento de la capacidad de almacenamiento fracasa porque Amazon no FSx puede acceder al sistema de archivos AWS KMS key

Se produjo un error en una solicitud de aumento de la capacidad de almacenamiento porque Amazon no FSx pudo acceder a la clave de KMS utilizada para cifrar el sistema de archivos.

Debe asegurarse de que Amazon FSx tiene acceso a la clave KMS utilizada para cifrar el sistema de archivos para poder ejecutar la acción administrativa. Utilice la siguiente información para resolver el problema de acceso a la clave.

- Si se eliminó la clave KMS, el sistema de archivos y cualquiera de sus copias de seguridad con dicha clave KMS no se pueden recuperar. Para obtener más información, consulte Eliminar AWS KMS key s en la Guía para AWS Key Management Service desarrolladores.
- Si la clave KMS está deshabilitada y es una clave administrada por el cliente, vuelva a habilitarla y, a continuación, vuelva a intentar la solicitud de aumento de la capacidad de almacenamiento. Para obtener más información, consulte Habilitar y deshabilitar claves en la Guía para AWS Key Management Service desarrolladores.
- Si la clave no es válida porque su eliminación está pendiente, debe cancelar la eliminación de la clave mientras tenga un estado `PendingDeletion`. Puede reintentar la solicitud una vez que la clave KMS esté `Enabled`.
- Si la clave no es válida porque su importación está pendiente, debe esperar a que se complete dicha importación y, luego, volver a intentar la solicitud de aumento de almacenamiento.
- Si se superó el límite de concesión de la clave, debe solicitar un aumento en el número de concesiones de la clave. Para obtener más información, consulte Cuotas de recursos en la Guía

para AWS Key Management Service desarrolladores. Cuando se conceda el aumento de cuota, vuelva a intentar la solicitud de aumento de almacenamiento.

Se produce un error en la actualización del almacenamiento o la capacidad de rendimiento, porque el Active Directory autoadministrado está mal configurado

Se produjo un error en la solicitud de actualización de la capacidad de rendimiento o almacenamiento, porque el Active Directory autoadministrado del sistema de archivos está en estado de desconfigurado.

Para resolver el estado desconfigurado en específico, consulte El sistema de archivos está mal configurado.

El aumento de la capacidad de almacenamiento falla debido a una capacidad de rendimiento insuficiente

La solicitud de aumento de la capacidad de almacenamiento falló porque la capacidad de rendimiento del sistema de archivos está establecida en 8 MBps.

Aumente la capacidad de rendimiento del sistema de archivos a un mínimo de 16 y, a continuación MBps, vuelva a intentar la solicitud. Para obtener más información, consulte Administración de la capacidad de rendimiento.

Se produce un error al actualizar la capacidad de rendimiento a 8 MBps

Falló una solicitud para modificar la capacidad de rendimiento de un sistema de archivos a 8 MBps .

Esto puede ocurrir cuando una solicitud de aumento de la capacidad de almacenamiento está pendiente o en curso. Los aumentos de capacidad de almacenamiento requieren un rendimiento mínimo de 16. MBps Espere hasta que se complete la solicitud de aumento de la capacidad de almacenamiento y, luego, vuelva a intentar la solicitud de modificación de la capacidad de rendimiento.

Historial del documento

- Versión de la API: 01-03-2018
- Última actualización de la documentación: 28 de mayo de 2025

En la siguiente tabla se describen los cambios importantes en la Guía del usuario de Amazon FSx Windows. Para obtener notificaciones sobre las actualizaciones de la documentación, puede suscribirse a la fuente RSS.

Cambio	Descripción	Fecha
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:Descr`	28 de mayo de 2025

	`ibeS3AccessPointAttachments`	
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
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 FSx para los puntos finales de VPC de interfaz y servidor de archivos de Windows.	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
Versión actualizada de la herramienta FSx de validación de Active Directory del servidor de archivos de Windows	Hay disponible una versión actualizada FSx de la herramienta de validación de Active Directory del servidor de archivos de Windows. Para obtener más información, consulte Validar la configuración de Active Directory	6 de noviembre de 2024

Support agregado para niveles más altos de IOPS en sistemas de archivos con capacidades de rendimiento de 4 GBps o más	FSx para Windows File Server está aumentando las IOPS máximas de 130 000 a 150 000 para los sistemas de archivos con una capacidad GBps de rendimiento del 4% o superior, de 175 000 a 200 000 para los sistemas de archivos con una capacidad GBps de rendimiento del 6% o superior, de 260 000 a 300 000 para los sistemas de archivos con un 9% GBps de capacidad de rendimien to o superior y de 350 000 a 400 000 para los sistemas de archivos con una capacidad GBps de rendimiento del 12% o superior. Para obtener más información, consulte el rendimiento del servidor de archivos de Windows. FSx	17 de enero de 2024
Amazon FSx actualizó las políticas FSx ServiceRo lePolicy AWS gestionadas de Amazon FSx FullAccess FSx ConsoleFullAccess FSx ReadOnlyAccess FSxConsol eReadOnlyAccess, Amazon, Amazon y Amazon	Amazon FSx actualizó las FSx ServiceRolePolicy políticas de Amazon FSx FullAcces s FSx ConsoleFullAccess FSxReadOnlyAccess, Amazon FSxConsoleReadOnlyAccess, Amazon y Amazon para añadir el `ec2:GetSecurityGro upsForVpc` permiso. Para obtener más informaci ón, 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
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

Se agregó compatibilidad para actualizar el tipo de almacenamiento del sistema de archivos	FSx para Windows File Server, los sistemas de archivos ahora admiten la actualización del tipo de almacenamiento HDD al tipo de almacenamiento SSD. Para obtener más información, consulte Administración del tipo de almacenamiento.	9 de agosto de 2023
Se agregó compatibilidad para una mayor capacidad de rendimiento máximo	FSx para Windows File Server, los sistemas de archivos ahora admiten una capacidad de GBps procesamiento de hasta el 12%. Para obtener más información, consulte el apartado sobre FSx el rendimiento del servidor de archivos de Windows.	9 de agosto de 2023
Se agregó compatibilidad para el aprovisionamiento de IOPS de SSD	FSx para Windows File Server, los sistemas de archivos ahora admiten el aprovisionamiento de IOPS en SSD independientemente de la capacidad de almacenamiento, hasta un máximo de 350 000 IOPS. Para obtener más información, consulte Administración de IOPS de SSD.	9 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 ServiceRolePolicy.	24 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
Support agregado para nuevas CloudWatch métricas de Amazon FSx para Windows File Server	FSx para Windows File Server ahora proporciona CloudWatch métricas adicionales que monitorizan el rendimiento del servidor de archivos y el volumen de almacenamiento y el uso de la capacidad. Para obtener más información, consulte Métricas y dimensiones.	22 de septiembre de 2022

Se agregó compatibilidad para las advertencias de rendimiento del sistema de archivos	Amazon FSx ahora proporciona advertencias en la ventana Rendimiento y supervisión cuando alguna de un conjunto de CloudWatch métricas se acerca o cruza los umbrales predeterminados para estas métricas. Cada advertencia también proporciona una recomendación práctica para mejorar el rendimiento del sistema de archivos. Para obtener más información, consulte Advertencias y recomendaciones de rendimiento.	22 de septiembre de 2022
Se agregó compatibilidad para un monitoreo mejorado del rendimiento del sistema de archivos	El panel de supervisión del sistema de archivos de Amazon FSx console FSx para los sistemas de archivos de Windows File Server incluye nuevas secciones de resumen, almacenamiento y rendimiento. Estas secciones muestran gráficos de nuevas CloudWatch métricas que le proporcionan una supervisión mejorada del rendimiento. Para obtener más información, consulte Supervisar las métricas con CloudWatch.	22 de septiembre de 2022

Support agregado para los puntos AWS PrivateLink finales 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
Se agregó compatibilidad para Amazon Kendra	Ahora puede usar su FSx sistema de archivos del servidor de archivos de Windows como fuente de datos para Amazon Kendra, lo que le permite indexar y buscar la información contenida en los documento s almacenados en su sistema de archivos. Para obtener más información, consulte Uso FSx de Windows File Server con Amazon Kendra.	26 de marzo de 2022
Se agregó compatibilidad para la auditoría de acceso a archivos	Ahora puede habilitar la auditoría de los accesos de los usuarios finales a los archivos, carpetas y recursos compartid os de archivos. Puede optar por enviar los registros de eventos de auditoría a los servicios Amazon CloudWatc h Logs o Amazon Data Firehose. Para obtener más información, consulte Auditoría de acceso de archivos.	8 de junio de 2021

Se agregó compatibilidad para copiar copias de seguridad	Ahora puedes usar Amazon FSx para copiar copias de seguridad de la misma AWS cuenta a otra Región de AWS (copias entre regiones) o dentro de la misma Región de AWS (copias dentro de la región). Para obtener más información, consulte Copiar copias de seguridad.	12 de abril de 2021
Aumente automáticamente la capacidad de almacenamiento de un sistema de archivos	Usa una AWS CloudForm ation plantilla personalizable AWS desarrollada por ti para aumentar automáticamente la capacidad de almacenamiento de tu sistema de archivos cuando su capacidad alcance el umbral que especifiques. Para obtener más información, consulte Aumento dinámico de la capacidad de almacenam iento.	17 de febrero de 2021

Se agregó compatibilidad para el acceso de clientes mediante direcciones IP no privadas	Puede acceder a FSx los sistemas de archivos del servidor de archivos de Windows con clientes locales que utilizan direcciones IP no privadas. Para obtener más información, consulte Entornos compatibles. Puede unir el sistema FSx de archivos del servidor de archivos de Windows a un Microsoft Active Directory autoadmin istrado con servidores DNS y controladores de dominio de AD que utilizan direcciones IP no privadas. Para obtener más información, consulte Uso de Amazon FSx con su Microsoft Active Directory autogesti onado.	17 de diciembre de 2020
Se agregó compatibilidad para el uso de alias de DNS	Ahora puede asociar alias DNS a sus FSx sistemas de archivos del servidor de archivos de Windows, que puede utilizar para acceder a los datos de su sistema de archivos. Para obtener más información, consulte Administrar alias de DNS y Tutorial 5: uso de alias de DNS para acceder a su sistema de archivos.	9 de noviembre de 2020

Se agregó compatibilidad para Amazon Elastic Container Service	Ahora puede usarlo FSx para Windows File Server con Amazon ECS. Para obtener más información, consulte Clientes compatibles.	9 de noviembre de 2020
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 FSx copias de seguridad nativas de Amazon. Para obtener más información, consulta Uso AWS Backup con Amazon FSx.	9 de noviembre de 2020
Se agregó compatibilidad para el escalado de la capacidad de rendimiento	Ahora puede modificar la capacidad de rendimiento de los sistemas de archivos existentes FSx para Windows File Server a medida que evolucionen sus requisito s de rendimiento. Para obtener más información, consulte Administración de la capacidad de rendimiento.	1 de junio de 2020

Se agregó compatibilidad para el escalado de la capacidad de almacenamiento	Ahora puede aumentar la capacidad de almacenamiento de los sistemas de archivos existentes FSx para Windows File Server a medida que evolucionen sus requisitos de almacenamiento. Para obtener más información, consulte Administración de la capacidad de almacenamiento.	1 de junio de 2020
Se agregó compatibilidad para opciones de almacenamiento en unidad de disco duro (HDD)	El almacenamiento en disco duro le ofrece flexibilidad en FSx cuanto a precio y rendimiento si lo utiliza con Windows File Server. Para obtener más información, consulta Cómo optimizar los costes con Amazon FSx.	26 de marzo de 2020
Support agregado para la transferencia de archivos mediante AWS DataSync	Ahora puede usarlo AWS DataSync para transferir archivos desde y hacia su servidor FSx de archivos de Windows. Para obtener más información, consulte Migración de archivos a Amazon FSx para Windows File Server mediante AWS DataSync.	4 de febrero de 2020

FSx para las versiones de Windows File Server, soporte para tareas adicionales de administración del sistema de archivos de Windows	Ahora puede gestionar y administrar los recursos compartidos de archivos, la deduplicación de datos, las cuotas de almacenamiento y el cifrado en tránsito de sus recursos compartidos de archivos mediante Amazon FSx CLI para la administración remota activada PowerShell. Para obtener más informaci ón, consulte Administración de sistemas de archivos.	20 de noviembre de 2019
FSx para las versiones de Windows File Server, compatibilidad nativa con múltiples zonas de disponibi lidad	Puede utilizar la implement ación Multi-AZ FSx para Windows File Server para crear más fácilmente sistemas de archivos con alta disponibi lidad que abarquen varias zonas de disponibilidad ()AZs. Para obtener más informaci ón, consulte Disponibilidad y durabilidad: sistemas de archivos Single-AZ y Multi-AZ.	20 de noviembre de 2019

FSx para las versiones de Windows File Server, compatibilidad con la administración de sesiones de usuario y archivos abiertos	Ahora puede usar la herramienta de carpetas compartidas nativa de Microsoft Windows para administrar las sesiones de usuario y abrir archivos en sus FSx sistemas de archivos de Windows File Server. Para obtener más información, consulte Administración de sesiones de usuario y archivos abiertos.	17 de octubre de 2019
Amazon FSx lanza soporte para copias instantáneas de Microsoft Windows	Ahora puede configurar instantáneas de Windows en sus sistemas FSx de archivos del servidor de archivos de Windows. Las copias de redundancia permiten a los usuarios deshacer fácilmente los cambios en los archivos y comparar las versiones de los archivos mediante la restauración de los archivos a versiones anteriores. Para obtener más información, consulte Trabajar con copias de redundancia.	31 de julio de 2019

Amazon FSx lanza el soporte compartido para Microsoft Active Directory	Ahora puede unir los sistemas FSx de archivos del servidor de archivos de Windows a AWS Managed Microsoft AD directorios que se encuentra n en una VPC diferente o en un sistema de archivos Cuenta de AWS diferente del sistema de archivos. Para obtener más información, consulte Compatibilidad con Active Directory.	25 de junio de 2019
Amazon FSx lanza soporte mejorado para Microsoft Active Directory	Ahora puede unir los sistemas FSx de archivos de Windows File Server a sus dominios autogestionados de Microsoft Active Directory, ya sea de forma local o en la nube. Para obtener más información, consulte Compatibilidad con Active Directory.	24 de junio de 2019
Amazon FSx cumple con la certificación SOC	Se FSx ha evaluado que Amazon cumple con la certificación SOC. Para obtener más información, consulte Seguridad y protección de los datos.	16 de mayo de 2019

Se agregó una nota aclaratoria sobre el AWS Direct Connect soporte de conexiones de VPN y VPC interregionales	Se puede acceder a los sistemas de FSx archivos de Amazon creados después del 22 de febrero de 2019 mediante AWS Direct Connect VPN e interconexión de VPC entre regiones. Para obtener más información, consulte Métodos de acceso compatibles.	25 de febrero de 2019
Se agregó compatibilidad con AWS Direct Connect, VPN, y la conexión de emparejamiento de VPC entre regiones	Ahora puede acceder a los sistemas de archivos de Amazon FSx for Windows File Server desde recursos locales y desde recursos de una Amazon Cuenta de AWS VPC diferente o. Para obtener más información, consulte Métodos de acceso compatibles.	22 de febrero de 2019
Amazon ya FSx está disponible de forma general	Amazon FSx for Windows File Server proporciona servidores de archivos de Microsoft Windows totalmente gestionados y respaldados por un sistema de archivos Windows totalmente nativo. Amazon FSx para Windows File Server proporciona las funciones, el rendimiento y la compatibilidad para impulsar y cambiar fácilmente las aplicaciones empresariales AWS.	28 de noviembre de 2018

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.