Guía del usuario de Amazon FSx File Gateway

AWS Storage Gateway

Versión de API 2021-03-31

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Storage Gateway: Guía del usuario de Amazon FSx File Gateway

Copyright © 2026 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

..... xi
Qué es la puerta de enlace de archivo de Amazon FSx 1
Cómo funciona la puerta de enlace de archivo de FSx 1
Cómo empezar con AWS Storage Gateway 4
Inscribirse en Amazon Web Services 4
Creación de un usuario de IAM con privilegios de administrador 5
Accediendo AWS Storage Gateway 7
Regiones de AWS compatibles con Storage Gateway 7
Requisitos de configuración de la puerta de enlace de archivo 9
Requisitos previos 9
Requisitos de hardware y almacenamiento 10
Requisitos de hardware para instalaciones locales VMs 10
Requisitos para los tipos de instancia de Amazon EC2 10
Requisitos de almacenamiento 11
Requisitos de red y firewall 12
Requisitos de los puertos 13
Requisitos de red y firewall para el dispositivo de hardware 29
Permisos de acceso de gateway a través de firewalls y routers 32
Configuración de grupos de seguridad 34
Hipervisores compatibles y requisitos de host 35
Clientes de SMB compatibles con la puerta de enlace de archivo 36
Operaciones del sistema de archivos compatibles 37
Administración de discos locales 37
Cálculo de la cantidad de almacenamiento en disco local 38
Agregar almacenamiento en caché 39
Uso del almacenamiento efímero con puertas de enlace de EC2 40
Uso del dispositivo de hardware 41
Configuración del dispositivo de hardware 42
Instalación física del dispositivo de hardware 44
Acceso a la consola del dispositivo de hardware 46
Configuración de los parámetros de red del dispositivo de hardware 47
Activación del dispositivo de hardware 48
Creación de una puerta de enlace en el dispositivo de hardware 50
Configuración de una dirección IP de puerta de enlace en el dispositivo de hardware 51

Eliminación del software de puerta de enlace del dispositivo de hardware 54
Eliminación del dispositivo de hardware 55
Creación de la puerta de enlace 57
Descripción general: activación de una puerta de enlace 57
Configuración de una puerta de enlace 57
Connect to AWS 58
Revisión y activación 58
Descripción general: configuración de la puerta de enlace 58
Descripción general: recursos de almacenamiento 58
Creación de un sistema de archivos de Amazon FSx para Windows File Server 59
Crear y activar un Amazon FSx File Gateway 60
Configurar un Amazon FSx File Gateway 60
Conecta tu Amazon FSx File Gateway a AWS 62
Revisa la configuración y activa tu Amazon FSx File Gateway 63
Configure su Amazon FSx File Gateway 64
Activación de una puerta de enlace en una VPC 67
Crear un punto de conexión de VPC para Storage Gateway 67
Configurar ajustes de acceso de dominio de Microsoft Active Directory 69
Adjunta un sistema de FSx archivos de Amazon 71
Monta y usa tu recurso compartido de FSx archivos de Amazon 74
Montar el recurso compartido de archivos SMB en el cliente 74
Pruebe su puerta de enlace FSx de archivos 76
Administración de los recursos de Amazon FSx File Gateway 77
Estado de la puerta de enlace 77
Descripción de los estados del sistema de archivos 78
Editar la información básica de la puerta de enlace 79
Establecer el nivel de seguridad de la puerta de enlace 80
Edición de la configuración de Active Directory para n FSx File Gateway 82
Edición de la configuración de un sistema de FSx archivos de Amazon 83
Separar un sistema de FSx archivos de Amazon 84
Supervisión de Storage Gateway 86
Comprensión de CloudWatch las alarmas 87
Cree CloudWatch las alarmas recomendadas 88
Crea una CloudWatch alarma personalizada 89
Supervisión de su puerta de enlace de 91
Obtener los registros de estado de 92

Uso de CloudWatch las métricas de Amazon 93
Información acerca de las métricas de gateway 94
Descripción de las métricas de sistemas de archivos 101
Descripción de los registros de auditoría de FSx 105
Mantenimiento de la puerta de enlace 109
Administración de actualizaciones de puertas de enlace 109
Frecuencia de actualización y comportamiento esperado 110
Activación o desactivación de las actualizaciones de mantenimiento 111
Modificación del programa de periodos de mantenimiento de la puerta de enlace 112
Aplicación de una actualización manualmente 114
Realización de tareas de mantenimiento con la consola local 115
Acceso a la consola local de la puerta de enlace 115
Realización de tareas en la consola local de la máquina virtual 118
Realización de tareas en la consola local de EC2 135
Apagado de la máquina virtual de puerta de enlace 143
Sustituir la puerta de enlace de archivos de existente por una nueva instancia 144
Eliminación de la puerta de enlace y eliminación de los recursos 146
Eliminación de la puerta de enlace mediante la consola de Storage Gateway 147
Rendimiento y optimización 149
Guía básica de rendimiento para File Gateway 149
FSx Rendimiento de File Gateway en clientes Windows 150
Optimizing Gateway Performance 150
Añada recursos a la gateway 151
Añada recursos al entorno de aplicaciones 153
Maximización del rendimiento de la puerta de enlace de archivo de S3 154
Implementar la puerta de enlace en la misma ubicación que los clientes 154
Reducir los cuellos de botella causados por la lentitud de los discos 155
Ajustar la asignación de recursos de la máquina virtual para los discos de CPU, RAM y caché 155
Ajustar el nivel de seguridad de SMB 157
Utilizar varios subprocesos y clientes para paralelizar las operaciones de escritura 158
Desactivar la actualización automática de la caché 160
Aumentar el número de subprocesos del cargador de Amazon S3 161
Aumentar la configuración de tiempo de espera de SMB 162
Activar el bloqueo oportunista para las aplicaciones compatibles 162

Ajustar la capacidad de la puerta de enlace en función del tamaño del conjunto de archivos de trabajo ... 163
Implementar varias puertas de enlace para cargas de trabajo más grandes ... 164
Optimización de la puerta de enlace de archivo de S3 para copias de seguridad de bases de datos de SQL Server ... 165
Implementar la puerta de enlace en la misma ubicación que los servidores SQL ... 166
Reducir los cuellos de botella causados por la lentitud de los discos ... 166
Ajustar la asignación de recursos de la máquina virtual de puerta de enlace de archivo de S3 para los discos de CPU, RAM y caché ... 167
Mejorar el rendimiento de los clientes de SMB mediante el ajuste del nivel de seguridad de la puerta de enlace de archivo de S3 ... 169
Mejorar el rendimiento de los de clientes SMB mediante la división de las copias de seguridad de SQL en varios archivos ... 170
Evitar errores al copiar archivos de gran tamaño mediante el aumento la configuración de tiempo de espera de SMB ... 171
Aumentar el número de subprocesos del cargador de Amazon S3 ... 171
Desactivar la actualización automática de la caché ... 172
Implementar varias puertas de enlace para soportar la carga de trabajo ... 173
Recursos adicionales para cargas de trabajo de copia de seguridad de bases de datos ... 173
Seguridad ... 174
Protección de datos ... 174
Cifrado de datos ... 175
Identity and Access Management ... 176
Público ... 177
Autenticación con identidades ... 177
Administración del acceso con políticas ... 179
Cómo funciona AWS Storage Gateway con IAM ... 180
Ejemplos de políticas basadas en identidades ... 186
Resolución de problemas ... 189
Uso de etiquetas para controlar el acceso a los recursos de ... 191
Validación de conformidad ... 194
Resiliencia ... 195
Seguridad de la infraestructura ... 196
AWS Prácticas recomendadas de seguridad ... 196
Registro y supervisión ... 197
Información sobre Storage Gateway en CloudTrail ... 197

Descripción de las entradas de archivos de registro de Storage Gateway 198
Resolución de problemas 201
Solución de problemas: problemas sin conexión de puerta de enlace 202
Comprobación del firewall o el proxy asociados 202
Comprobación para una inspección continua de SSL o de paquetes exhaustiva del tráfico de la puerta de enlace 202
Compruebe la métrica IOWait porcentual tras un reinicio o una actualización de software ... 203
Comprobación de si hay un corte de energía o un error de hardware en el host del hipervisor 203
Comprobación de si hay problemas con un disco de caché asociado 203
Solución de problemas: problemas relacionados con Active Directory 204
Confirme que la puerta de enlace puede llegar al controlador de dominio mediante la ejecución de una prueba de ping 204
Compruebe las opciones de DHCP configuradas para la VPC de la instancia de puerta de enlace de Amazon EC2 205
Confirme que la puerta de enlace puede resolver el dominio ejecutando una consulta de búsqueda 205
Compruebe la configuración y los roles del controlador de dominio 207
Compruebe que la puerta de enlace esté unida al controlador de dominio más cercano 207
Confirmar que Active Directory crea nuevos objetos de equipo en la unidad organizativa (UO) predeterminada 207
Comprobar los registros de eventos del controlador de dominio 208
Solución de problemas: problemas de activación de la puerta de enlace 208
Resolución de errores al activar la puerta de enlace mediante un punto de conexión público 209
Resolución de errores al activar la puerta de enlace mediante un punto de conexión de VPC de Amazon 212
Resuelva los errores al activar la puerta de enlace mediante un punto de conexión público y hay un punto de conexión de VPC de Storage Gateway en la misma VPC 216
Solución de problemas: problemas relacionados con la puerta de enlace en las instalaciones . 217
Activa el Soporte acceso para ayudar a solucionar los problemas de tu puerta de enlace 222
Solución de problemas: problemas con la configuración de Microsoft Hyper-V 223
Solución de problemas: problemas con la puerta de enlace de Amazon EC2 227
La puerta de enlace no se ha activado poco tiempo después 227
No encuentra la instancia de la puerta de enlace de EC2 en la lista de instancias 228
Conexión a la puerta de enlace de Amazon EC2 con la consola serie 228

Activar el Soporte acceso para ayudar a solucionar los problemas de la puerta de enlace ... 228
Solución de problemas: problemas con el dispositivo de hardware ... 231
Cómo determinar la dirección IP del servicio ... 231
Cómo restablecer la configuración de fábrica ... 231
Cómo realizar un reinicio remoto ... 232
Cómo obtener soporte para iDRAC de Dell ... 232
Cómo encontrar el número de serie del dispositivo hardware ... 232
Cómo obtener soporte para el dispositivo de hardware ... 232
Solución de problemas: problemas con la puerta de enlace de archivo ... 233
Error: FileMissing ... 234
Error: FsxFileSystemAuthenticationFailure ... 234
Error: FsxFileSystemConnectionFailure ... 235
Error: FsxFileSystemFull ... 235
Error: GatewayClockOutOfSync ... 235
Error: InvalidFileState ... 236
Error: ObjectMissing ... 236
Error: DroppedNotifications ... 236
Notificación: HardReboot ... 237
Notificación: reinicio ... 237
Solución de problemas relacionados con el dominio de Active Directory ... 238
Solución de problemas con CloudWatch las métricas ... 240
Notificaciones de estado de alta disponibilidad ... 243
Solución de problemas: problemas de alta disponibilidad ... 243
Notificaciones de estado ... 243
Métricas ... 245
Prácticas recomendadas ... 246
Recuperación de datos ... 246
Recuperación de un cierre inesperado de una VM ... 246
Recuperación de datos a partir de un disco de la caché que no funciona correctamente ... 247
Recuperación de datos de un centro de datos inaccesible ... 247
Restaurar datos en Amazon FSx ... 248
limpieza de recursos innecesarios ... 248
Recursos adicionales ... 250
Configuración del host ... 251
Implementar un host de Amazon EC2 predeterminado para la puerta de enlace de archivo ... 251

Implementar un host de Amazon EC2 personalizado para la puerta de enlace de archivo ... 254
Modificación de las opciones de metadatos de la instancia de Amazon EC2 ... 258
Sincronización de la hora de la máquina virtual con la hora del host KVM de Hyper-V o Linux ... 259
Sincronice la hora de la máquina virtual con la hora del host VMware ... 259
Configuración de adaptadores de red para la puerta de enlace ... 261
Uso de Storage Gateway con VMware HA ... 264
Obtención de la clave de activación ... 269
Linux (curl) ... 270
Linux (bash/zsh) ... 271
Microsoft Windows PowerShell ... 272
Mediante la consola local ... 272
Usando Direct Connect ... 273
Permisos de Active Directory ... 273
Obtención de la dirección IP de la puerta de enlace ... 274
Obtención de una dirección IP de un host Amazon EC2 ... 275
Comprensión de los recursos y los recursos IDs ... 276
Trabajando con un recurso IDs ... 276
Etiquetado de recursos ... 277
Trabajo con etiquetas ... 278
Componentes de código abierto ... 279
Componentes de código abierto para Storage Gateway ... 280
Componentes de código abierto para Amazon FSx File Gateway ... 280
Cuotas ... 281
Cuotas para los sistemas de FSx archivos de Amazon ... 281
Tamaños de disco local recomendados para la puerta de enlace ... 281
referencia de la API ... 283
Encabezados de solicitud obligatorios ... 283
Firmar solicitudes ... 286
Ejemplo de cálculo de firma ... 287
Respuestas de error ... 288
Excepciones ... 289
Códigos de error de operación ... 291
Respuestas de error ... 312
Acciones ... 314
Historial de revisión ... 315

Actualizaciones anteriores 329

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.

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.

Qué es la puerta de enlace de archivo de Amazon FSx

La puerta de enlace de archivo de Amazon FSx (puerta de enlace de archivo de FSx) es un nuevo tipo de puerta de enlace de archivo que proporciona baja latencia y acceso eficiente a los recursos compartidos de archivos de FSx para Windows File Server en la nube en las instalaciones. Si mantiene el almacenamiento de archivos en las instalaciones debido a los requisitos de latencia o ancho de banda, puede usar la puerta de enlace de archivo de FSx para un acceso sin problemas a los recursos compartidos de archivos de Windows completamente administrados, altamente fiables y prácticamente ilimitados proporcionados en la nube de AWS por FSx para Windows File Server.

Ventajas de usar la puerta de enlace de archivo de Amazon FSx

La puerta de enlace de archivo de FSx ofrece las siguientes ventajas:

- Ayuda a eliminar los servidores de archivos en las instalaciones y consolida todos los datos en AWS para aprovechar la escala y la economía del almacenamiento en la nube.
- Ofrece opciones que puede usar para todas las cargas de trabajo de archivos, incluidas las que requieren acceso en las instalaciones a los datos en la nube.
- Las aplicaciones que deben permanecer en las instalaciones ahora pueden disfrutar de la misma baja latencia y alto rendimiento que tienen en AWS, sin sobrecargar sus redes ni afectar a las latencias que experimentan las aplicaciones más exigentes.

Cómo funciona la puerta de enlace de archivo de Amazon FSx

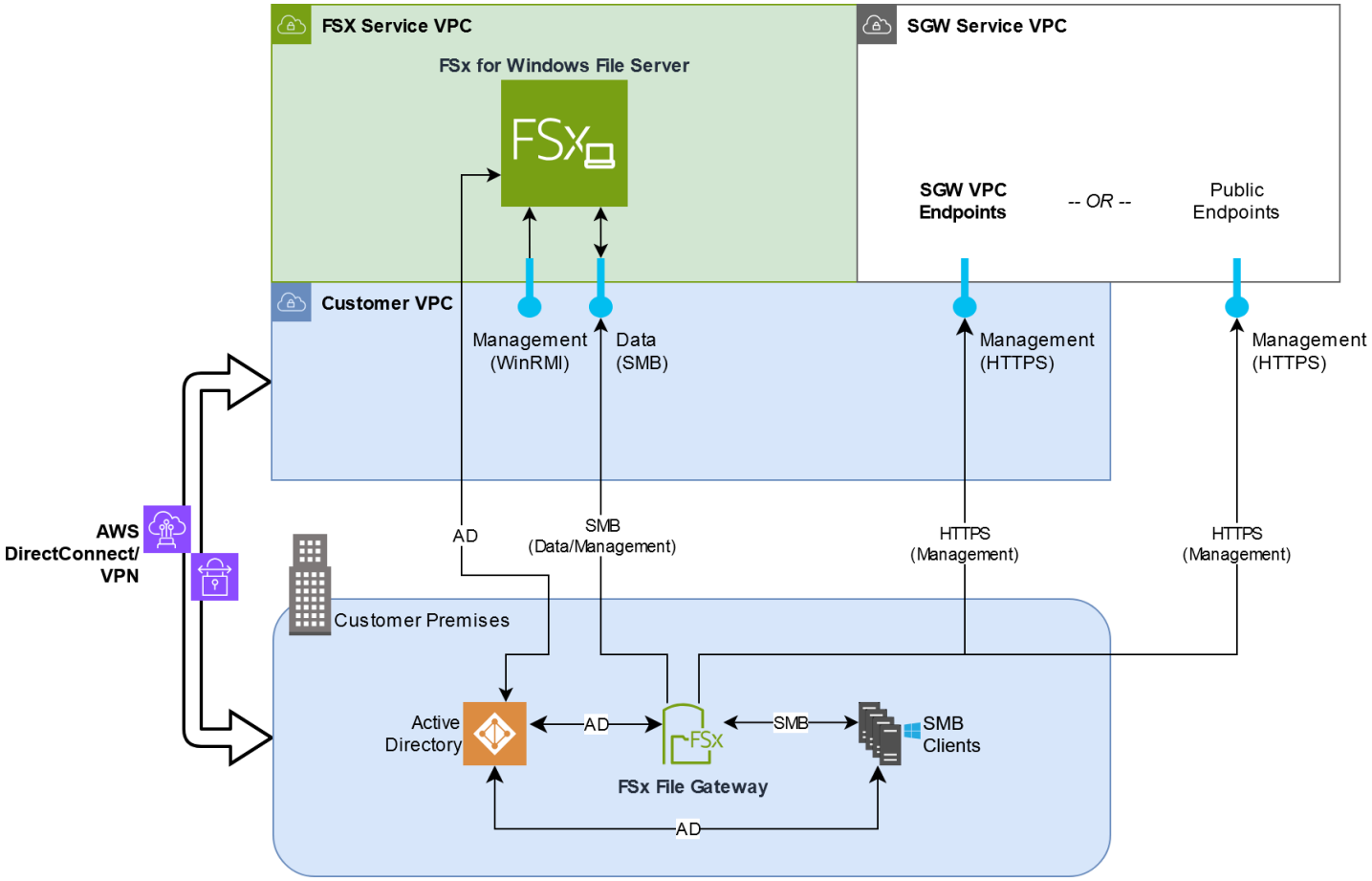
Para utilizar la puerta de enlace de archivo de Amazon FSx (puerta de enlace de archivo de FSx), debe tener al menos un sistema de archivos Amazon FSx para Windows File Server. También debe tener acceso en las instalaciones a FSx para Windows File Server, ya sea a través de una VPN o a través de una conexión de Direct Connect. Para obtener más información sobre el uso de los sistemas de archivos de Amazon FSx, consulte ¿Qué es Amazon FSx para Windows File Server?

La puerta de enlace del entorno en las instalaciones se implementa como máquina virtual (VM) que se ejecuta en un VMware ESXi, Microsoft Hyper-V o una máquina virtual basada en el kernel (KVM) de Linux, o como un dispositivo de hardware adquirido al distribuidor de su elección. También puede implementar la máquina virtual de Storage Gateway en VMware Cloud en AWS o como AMI en Amazon EC2. Tras implementar el dispositivo, debe activar la puerta de enlace de archivo de FSx desde la consola de Storage Gateway o mediante la API de Storage Gateway.

Una vez que la puerta de enlace de archivo de Amazon FSx esté activada y pueda acceder a FSx para Windows File Server, utilice la consola de Storage Gateway para unirla al dominio de Microsoft Active Directory. Una vez que la puerta de enlace se une correctamente a un dominio, se utiliza la consola de Storage Gateway para conectar la puerta de enlace a un FSx para Windows File Server existente. La puerta de enlace de archivo de FSx para Windows File Server hace que todos los recursos compartidos del servidor estén disponibles como recursos compartidos en la puerta de enlace de archivo de Amazon FSx. A continuación, puede utilizar un cliente para buscar y conectarse a los recursos compartidos de archivos de la puerta de enlace de archivo de FSx que correspondan a la puerta de enlace de archivo de FSx seleccionada.

Cuando los recursos compartidos de archivos están conectados, puede leer y escribir los archivos localmente y, al mismo tiempo, beneficiarse de todas las características disponibles en FSx para Windows File Server. La puerta de enlace de archivo de FSx asigna los recursos compartidos de archivos locales y su contenido a los recursos compartidos de archivos almacenados remotamente en FSx para Windows File Server. Existe una correspondencia 1:1 entre los archivos remotos y los visibles localmente y sus recursos compartidos.

En el diagrama siguiente se proporciona información general de la implementación del almacenamiento de archivos para Storage Gateway.



Observe el siguiente diagrama:

- Se necesita Direct Connecto una VPN para permitir que la puerta de enlace de archivo de FSx acceda al recurso compartido de archivos de Amazon FSx mediante SMB y para permitir que FSx para Windows File Server se una a su dominio de Active Directory en las instalaciones.
- Se necesita Amazon Virtual Private Cloud (Amazon VPC) para conectarse a la VPC del servicio de FSx para Windows File Server y a la VPC del servicio de Storage Gateway mediante puntos de conexión privados. La puerta de enlace de archivo de FSx también se puede conectar a los puntos de conexión públicos.

Puede utilizar la puerta de enlace de archivo de Amazon FSx en todas las regiones de AWS en las que esté disponible FSx para Windows File Server.

Cómo empezar con AWS Storage Gateway

En esta sección se proporcionan instrucciones para empezar AWS. Necesita una AWS cuenta antes de poder empezar a usarla AWS Storage Gateway. Puede utilizar una cuenta de AWS existente o registrarse en una nueva. También necesita un usuario de IAM en su AWS cuenta que pertenezca a un grupo con los permisos administrativos necesarios para realizar las tareas de Storage Gateway. Los usuarios con los privilegios adecuados pueden acceder a la consola de Storage Gateway y a la API de Storage Gateway para realizar tareas de implementación, configuración y mantenimiento de la puerta de enlace. Si es la primera vez que lo utiliza, le recomendamos que consulte las secciones AWS Regiones compatibles y Requisitos de configuración de File Gateway antes de empezar a trabajar con Storage Gateway.

Esta sección contiene los temas siguientes, que ofrecen información adicional acerca de cómo empezar a utilizar AWS Storage Gateway:

Temas

- Inscribirse en Amazon Web Services- Obtenga información sobre cómo registrarse AWS y crear una AWS cuenta.
- Creación de un usuario de IAM con privilegios de administrador: obtenga información sobre cómo crear un usuario de IAM con privilegios administrativos para la cuenta de AWS .
- Accediendo AWS Storage Gateway- Aprenda a acceder a AWS Storage Gateway través de la consola Storage Gateway o mediante programación mediante. AWS SDKs
- Regiones de AWS compatibles con Storage Gateway- Descubra qué AWS regiones puede usar para almacenar sus datos al activar su puerta de enlace en Storage Gateway.

Inscribirse en Amazon Web Services

Un Cuenta de AWS es un requisito fundamental para acceder a AWS los servicios. El suyo Cuenta de AWS es el contenedor básico para todos los AWS recursos que cree como AWS usuario. También Cuenta de AWS es el límite de seguridad básico para sus AWS recursos. Los recursos que crea en la cuenta están disponibles para los usuarios que tienen credenciales para la cuenta. Antes de que puedas empezar a usarlos AWS Storage Gateway, necesitas registrarte en un Cuenta de AWS.

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

Para inscribirte en 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.

Recomendamos también exigir a los usuarios que utilicen credenciales temporales cuando accedan a AWS. Para proporcionar credenciales temporales, puede utilizar una federación y un proveedor de identidad, como el AWS IAM Identity Center. Si su empresa ya utiliza un proveedor de identidad, puede utilizarlo junto con la federación para simplificar el acceso a los recursos de su AWS cuenta.

Creación de un usuario de IAM con privilegios de administrador

Tras crear su AWS cuenta, siga los siguientes pasos para crear un usuario AWS Identity and Access Management (de IAM) para usted y, a continuación, agréguelo a un grupo que tenga permisos administrativos. Para obtener más información sobre el uso del AWS Identity and Access Management servicio para controlar el acceso a los recursos de Storage Gateway, consulteAdministración de identidades y accesos para AWS Storage Gateway.

Para crear un usuario administrador, elija una de las siguientes opciones.

Elegir una forma de administrar el administrador	Para	Haga esto	También puede
En IAM Identity Center (recomendado)	Usar credenciales a corto plazo para acceder a AWS. Esto se ajusta a las prácticas recomendadas de seguridad. Para obtener información sobre las prácticas recomendadas, consulta Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.	Siga las instrucciones en Introducción en la Guía del usuario de AWS IAM Identity Center .	Configure el acceso mediante programación configurando el AWS CLI que se utilizará AWS IAM Identity Center en la Guía del AWS Command Line Interface usuario.
En IAM (no recomendado)	Usar credenciales a largo plazo para acceder a AWS.	Siguiendo las instrucciones de Crear un usuario de IAM para acceso de emergencia de la Guía del usuario de IAM.	Configure el acceso programático mediante Administrar las claves de acceso de los usuarios de IAM en la Guía del usuario de IAM.

Warning

Los usuarios de IAM tienen credenciales de larga duración, lo que supone un riesgo de seguridad. Para ayudar a mitigar este riesgo, le recomendamos que brinde a estos usuarios

únicamente los permisos que necesitan para realizar la tarea y que los elimine cuando ya no los necesiten.

Accediendo AWS Storage Gateway

Puede usar la consola de AWS Storage Gateway para realizar diversas tareas de configuración y mantenimiento de puertas de enlace, como activar o eliminar los dispositivos de hardware de Storage Gateway de la implementación, crear, administrar y eliminar los distintos tipos de puertas de enlace, asociar, administrar y desasociar sistemas de archivos, y supervisar el estado de varios elementos del servicio de Storage Gateway. Para simplificar y facilitar su uso, esta guía se centra en realizar tareas mediante la interfaz web de la consola de Storage Gateway. Puede acceder a la consola de Storage Gateway a través del navegador web en: https://console.aws.amazon.com/storagegateway/home/.

Si prefiere un enfoque programático, puede usar la interfaz de programación de AWS Storage Gateway aplicaciones (API) o la interfaz de línea de comandos (CLI) para configurar y administrar los recursos de la implementación de Storage Gateway. Para obtener más información sobre las acciones, los tipos de datos y la sintaxis requerida para la API de Storage Gateway, consulte la Referencia de la API de Storage Gateway. Para obtener más información sobre la CLI de Storage Gateway, consulte la Referencia de comandos de la CLI de AWS.

También puede utilizarla AWS SDKs para desarrollar aplicaciones que interactúen con Storage Gateway. La AWS SDKs versión para Java, .NET y PHP incluye la API Storage Gateway subyacente para simplificar las tareas de programación. Para obtener información sobre la descarga de las bibliotecas de SDK, consulte el Centro para desarrolladores de AWS.

Para obtener información sobre precios, consulte Precios de AWS Storage Gateway.

Regiones de AWS compatibles con Storage Gateway

An Región de AWS es una ubicación física en el mundo donde AWS hay varias zonas de disponibilidad. Las zonas de disponibilidad constan de uno o más centros de AWS datos discretos, cada uno con alimentación, redes y conectividad redundantes, alojados en instalaciones independientes. Esto significa que cada una de ellas Región de AWS está aislada físicamente y es independiente de las demás regiones. Las regiones proporcionar tolerancia a errores, estabilidad y resistencia, y también pueden reducir la latencia. Los recursos que cree en una región no existen en ninguna otra, a menos que utilice explícitamente una función de replicación ofrecida por un AWS

servicio. Por ejemplo, Amazon S3 y Amazon EC2 admiten la replicación entre regiones. Algunos servicios, por ejemplo AWS Identity and Access Management, no tienen recursos regionales. Puede lanzar AWS recursos en ubicaciones que cumplan con los requisitos de su empresa. Por ejemplo, es posible que desee lanzar instancias de Amazon EC2 para alojar sus AWS Storage Gateway dispositivos en o Región de AWS en Europa para estar más cerca de sus usuarios europeos o para cumplir con los requisitos legales. Usted Cuenta de AWS determina cuáles de las regiones compatibles con un servicio específico están disponibles para su uso.

Amazon FSx File Gateway almacena los datos de los archivos en la AWS región en la que se encuentra FSx el sistema de archivos de Amazon. Antes de empezar a implementar la puerta de enlace, elija una región en la esquina superior derecha de la consola de Storage Gateway.

- Amazon FSx File Gateway: para ver AWS las regiones compatibles y una lista de los puntos de enlace de AWS servicio que puede utilizar con Amazon FSx File Gateway, consulte los puntos de enlace y las cuotas de Amazon FSx File Gateway en. Referencia general de AWS
- Storage Gateway: para ver AWS las regiones compatibles y una lista de los puntos de enlace de AWS servicio que puede usar con Storage Gateway, consulte los AWS Storage Gateway puntos de enlace y las cuotas en. Referencia general de AWS
- Dispositivo de hardware de Storage Gateway: para conocer las regiones compatibles que puede utilizar con el dispositivo de hardware, consulte Regiones del dispositivo de hardware de AWS Storage Gateway en la Referencia general de AWS.

Requisitos de configuración de la puerta de enlace de archivo

A menos que se especifique lo contrario, los siguientes requisitos son comunes a todos los tipos de puerta de enlace de archivo en AWS Storage Gateway. La configuración debe cumplir los requisitos descritos en esta sección. Revise los requisitos que se aplican a la configuración de la puerta de enlace antes de implementarla.

Temas

- Requisitos previos
- Requisitos de hardware y almacenamiento
- Requisitos de red y firewall
- Hipervisores compatibles y requisitos de host
- Clientes de SMB compatibles con la puerta de enlace de archivo
- Operaciones del sistema de archivos compatibles con la puerta de enlace de archivo
- Administración de discos locales para la puerta de enlace

Requisitos previos

Antes de configurar Amazon FSx File Gateway (FSx File Gateway) , debe cumplir los siguientes requisitos previos:

- Cree y configure un sistema de archivos FSx para Windows File Server. Para obtener instrucciones, consulta el paso 1: Crea tu sistema de archivos en la Guía del usuario del servidor de archivos de Amazon FSx para Windows.
- Configure Microsoft Active Directory (AD) y cree una cuenta de servicio de Active Directory con los permisos necesarios. Para obtener más información, consulte Requisitos de permiso de la cuenta de servicio de Active Directory.
- Asegúrese de que haya suficiente ancho de banda de la red entre la puerta de enlace y AWS. Se requiere un mínimo de 100 Mbps para descargar, activar y actualizar correctamente la puerta de enlace.
- Configure la conexión que desee utilizar para el tráfico de red entre el entorno local en el que va a implementar la puerta de enlace AWS y el entorno local en el que vaya a implementar. Puede

conectarse mediante una red pública de Internet, una red privada, una VPN o Direct Connect. Si desea que su puerta de enlace se comunique a AWS través de una conexión privada a una Amazon Virtual Private Cloud, configure Amazon VPC antes de configurar la puerta de enlace.

- Asegúrese de que la puerta de enlace pueda resolver el nombre del controlador de dominio de Active Directory. Puede usar DHCP en su dominio de Active Directory para gestionar la resolución o especificar un servidor DNS manualmente desde el menú de ajustes de configuración de red de la consola local de la puerta de enlace.

Requisitos de hardware y almacenamiento

En las siguientes secciones se proporciona información sobre las configuraciones mínimas de hardware y almacenamiento necesarias para la puerta de enlace y la cantidad mínima de espacio en disco que se debe asignar para el almacenamiento necesario.

Requisitos de hardware para instalaciones locales VMs

Cuando implemente la puerta de enlace de archivo en las instalaciones, debe asegurarse de que el hardware subyacente en el que esté implementando la máquina virtual (VM) de puerta de enlace de archivo pueda dedicar los siguientes recursos mínimos:

- Cuatro procesadores virtuales asignados a la VM
- 16 GiB de RAM reservada para puertas de enlace de archivo
- 80 GiB de espacio de disco para la instalación de los datos del sistema y la imagen de la máquina virtual

Requisitos para los tipos de instancia de Amazon EC2

Cuando implemente la puerta de enlace en Amazon Elastic Compute Cloud (Amazon EC2), el tamaño de la instancia debe ser al menos **`xlarge`** para que la puerta de enlace funcione. Sin embargo, para la familia de instancias optimizadas para la computación el tamaño debe ser, como mínimo, **`2xlarge`**.

> **Note**
>
> La AMI de Storage Gateway solo es compatible con instancias basadas en x86 que utilizan procesadores Intel o AMD. No se admiten las instancias basadas en ARM que utilizan procesadores Graviton.

Utilice uno de los siguientes tipos de instancias recomendadas para su tipo de gateway.

Recomendadas para los tipos de puerta de enlace de archivo

- Familia de instancias de uso general: tipo de instancia m5, m6 o m7. Elija el tamaño de instancia xlarge o superior para cumplir con los requisitos de procesador Storage Gateway y RAM.
- Familia de instancias optimizadas para la computación: tipos de instancia c5, c6 o c7. Elija el tamaño de instancia 2xlarge o superior para cumplir con los requisitos de procesador Storage Gateway y RAM.
- Familia de instancias optimizadas para memoria: tipos de instancia r5, r6 o r7. Elija el tamaño de instancia xlarge o superior para cumplir con los requisitos de procesador Storage Gateway y RAM.
- Familia de instancias optimizadas para el almacenamiento: tipos de instancia i3, i4 o i7. Elija el tamaño de instancia xlarge o superior para cumplir con los requisitos de procesador Storage Gateway y RAM.

> **Note**
>
> Cuando se lanza la puerta de enlace en Amazon EC2 y el tipo de instancia elegida es compatible con almacenamiento efímero, los discos se muestran de forma automática. Para obtener más información sobre el almacenamiento de la instancia de Amazon EC2, consulte Almacenamiento de instancias en la Guía del usuario de Amazon EC2.

Requisitos de almacenamiento

Además de 80 GiB de espacio en disco para la máquina virtual, también necesitará discos adicionales para la puerta de enlace.

Tipo de puerta de enlace	Caché (mínimo)	Caché (máximo)			
Puerta de enlace de archivo	150 GiB	64 TiB			

> **Note**
>
> Puede configurar una o más unidades locales para la memoria caché hasta la capacidad máxima.
> Cuando se agrega caché a una puerta de enlace existente, es importante crear nuevos discos en el host (hipervisor o instancia de Amazon EC2). No cambie el tamaño de los discos si se han asignado previamente como caché.

Requisitos de red y firewall

La gateway necesita obtener acceso a Internet, las redes locales, los servidores de nombres de dominio (DNS), firewalls, routers, etc.

Los requisitos de ancho de banda de la red varían en función de la cantidad de datos que carga y descarga la puerta de enlace. Se requiere un mínimo de 100 Mbps para descargar, activar y actualizar correctamente la puerta de enlace. Sus patrones de transferencia de datos determinarán el ancho de banda necesario para soportar su carga de trabajo.

A continuación, puede encontrar información sobre los puertos necesarios y cómo permitir el acceso a través de firewalls y routers.

> **Note**
>
> En algunos casos, podría implementar la puerta de enlace en Amazon EC2 o utilizar otros tipos de implementación (incluyendo en las instalaciones) con las políticas de seguridad de red que restringen los rangos de direcciones IP de AWS . En estos casos, es posible que la puerta de enlace experimente problemas de conectividad del servicio cuando cambien los

valores del rango de AWS IP. Los valores del rango de direcciones AWS IP que debes usar se encuentran en el subconjunto de servicios de Amazon de la AWS región en la que activas tu puerta de enlace. Para obtener los valores actuales de rango de IP, consulte AWS Rangos de direcciones IP de en la Referencia general de AWS.

Temas

- Requisitos de los puertos
- Requisitos de red y firewall para el dispositivo de hardware de Storage Gateway
- Permitir el AWS Storage Gateway acceso a través de firewalls y enrutadores
- Configuración de grupos de seguridad para la instancia de puerta de enlace de Amazon EC2

Requisitos de los puertos

FSx File Gateway requiere que puertos específicos pasen a través de la seguridad de la red para una implementación y un funcionamiento satisfactorios. Algunos puertos son necesarios para todas las puertas de enlace, mientras que otros solo son necesarios para configuraciones específicas, como cuando se conecta a puntos de conexión de VPC.

En el caso de FSx File Gateway, debe usar Microsoft Active Directory para permitir que los usuarios del dominio accedan a un recurso compartido de archivos del bloque de mensajes del servidor (SMB). Puede unir la puerta de enlace de archivo a cualquier dominio válido de Microsoft Windows (que se pueda resolver por DNS).

También puede utilizarla Directory Service para crear una AWS Managed Microsoft ADen la nube de Amazon Web Services. Para la mayoría de AWS Managed Microsoft AD las implementaciones, debe configurar el servicio de Protocolo de configuración dinámica de host (DHCP) para su VPC. Para obtener información sobre cómo crear un conjunto de opciones de DHCP, consulte Crear un conjunto de opciones de DHCP en la Guía de administración de AWS Directory Service .

En la siguiente tabla se enumeran los puertos necesarios y se describen los requisitos condicionales en la columna Notas.

FSx

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
Navegadc web	El navegado web	VM de Storage Gateway	TCP HTTP	80	✓	✓	✓	Lo utilizan los sistemas locales para obtener la clave de activación de Storage Gateway. El puerto 80 solo se utiliza durante la activación de un dispositivo de Storage Gateway. La máquina virtual de Storage Gateway no

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
								requiere que el puerto 80 sea accesible públicamente. El nivel de acceso exigido al puerto 80 depende de la configuración de la red. Si activa la puerta de enlace desde la consola de administración de Storage Gateway, el host desde

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
								el que se conecta a la consola debe tener acceso al puerto 80 de la puerta de enlace.
Navegadc web	VM de Storage Gateway	AWS	TCP HTTPS	443	✓	✓	✓	AWS Consola de administración (todas las demás operaciones)

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
DNS	VM de Storage Gateway	Servidor DNS (Domain Name Service)	DNS TCP y UDP	53	✓	✓	✓	Se utiliza para la comunicación entre una VM de Storage Gateway y el servidor DNS para la resolución de nombres de IP.

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
NTP	VM de Storage Gateway	Servidor de Network Time Protocol (NTP)	NTP TCP y UDP	123	✓	✓	✓	Lo utilizan los sistemas en las instalaciones para sincronizar la hora de la VM con la hora del host. Una VM de Storage Gateway está configurada para utilizar los siguientes servidores NTP: • 0.amazon.pool.ntp.org

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
								• 1.amazon.pool.ntp.org • 2.amazon.pool.ntp.org • 3.amazon.pool.ntp.org **Note** No es necesario para las puertas de enlace alojadas en Amazon EC2.

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
Storage Gateway	VM de Storage Gateway	Soporte Punto final	TCP SSH	22	✓	✓	✓	Permite acceder Soporte a su puerta de enlace para ayudarle a solucionar los problemas de la puerta de enlace. No necesita este puerto abierto para el funcionamiento normal de la gateway, pero se exige para la solución de

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
								problemas. Para obtener una lista de los puntos de conexión admitidos, consulte puntos de conexión de Soporte.
Storage Gateway	VM de Storage Gateway	AWS	TCP HTTPS	443	✓	✓	✓	Control de administración
Amazon CloudFront	VM de Storage Gateway	AWS	TCP HTTPS	443	✓	✓	✓	Para la activación

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
VPC	VM de Storage Gateway	AWS	TCP HTTPS	443	✓	✓	✓*	Control de administración *Requerido solo cuando se utilizan puntos de conexión de VPC
VPC	VM de Storage Gateway	AWS	TCP HTTPS	1026		✓	✓*	Punto de conexión del plano de control *Requerido solo cuando se utilizan puntos de conexión de VPC

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
VPC	VM de Storage Gateway	AWS	TCP HTTPS	1027		✓	✓*	Plano de control anónimo (para activación) *Requerido solo cuando se utilizan puntos de conexión de VPC
VPC	VM de Storage Gateway	AWS	TCP HTTPS	1028		✓	✓*	Punto de conexión de proxy *Requerido solo cuando se utilizan puntos de conexión de VPC

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
VPC	VM de Storage Gateway	AWS	TCP HTTPS	1031		✓	✓*	Plano de datos *Requerido solo cuando se utilizan puntos de conexión de VPC

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
VPC	VM de Storage Gateway	AWS	TCP HTTPS	2222		✓	✓*	Canal de soporte SSH para VPCe *Requerido solo para abrir un canal de soporte cuando se utilizan puntos de conexión de VPC

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
VPC	VM de Storage Gateway	AWS	TCP HTTPS	443	✓	✓	✓*	Control de administración *Requerido solo cuando se utilizan puntos de conexión de VPC

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
Cliente de recurso compartido de archivos	Cliente de SMB	VM de Storage Gateway	TCP o UDP SMBv3	445	✓	✓	✓	Servicio de sesión de transferencia de datos de uso compartido de archivos. Sustituye a los puertos 137-139 de Microsoft Windows NT y versiones posteriores.
Microsoft Active Directory	VM de Storage Gateway	Servidor de Active Directory	UDP NetBIOS	137	✓	✓	✓	Nombre de servicio
Microsoft Active Directory	VM de Storage Gateway	Servidor de Active Directory	UDP NetBIOS	138	✓	✓	✓	Servicio de datagramas

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
Microsoft Active Directory	VM de Storage Gateway	Servidor de Active Directory	LDAP TCP y UDP	389	✓	✓	✓	Conexión de cliente de Directory System Agent (DSA)
Microsoft Active Directory	VM de Storage Gateway	Servidor de Active Directory	Kerberos TCP y UDP	88	✓	✓	✓	Kerberos
Microsoft Active Directory	VM de Storage Gateway	Servidor de Active Directory	Mapeador de Environment/Endpuntos de computación distribuida TCP (DCE/EMAP)	135	✓	✓	✓	RPC

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
FSx Conexión a Amazon	VM de Storage Gateway	FSx para Windows File Server	TCP o UDP SMBv3	445	✓	✓	✓	Servicio de sesión de transferencia de datos de uso compartido de archivos

Requisitos de red y firewall para el dispositivo de hardware de Storage Gateway

Cada dispositivo de hardware de Storage Gateway requiere los siguientes servicios de red:

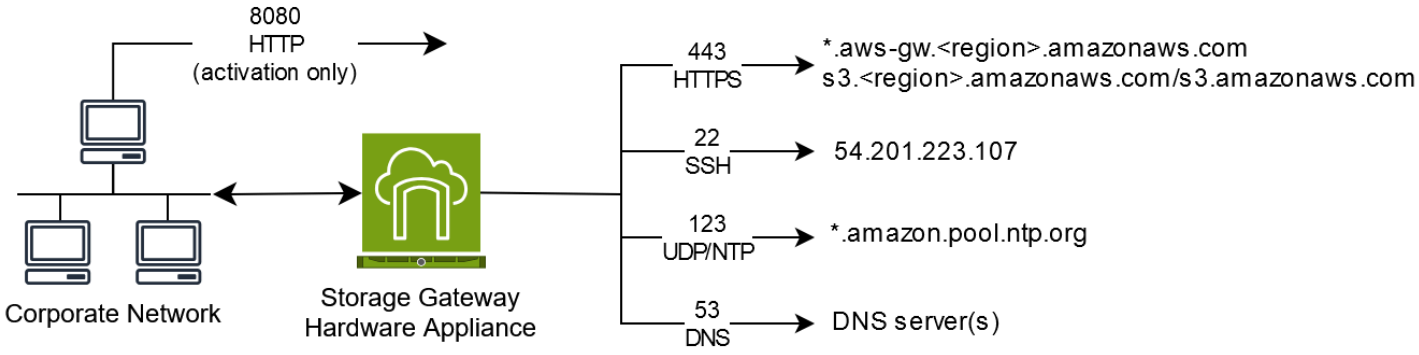
- Acceso a Internet: una conexión de red permanente a Internet a través de cualquier interfaz de red del servidor.
- Servicios DNS: servicios DNS para la comunicación entre el dispositivo de hardware y el servidor DNS.
- Sincronización horaria: se debe poder acceder a un servicio horario de Amazon NTP configurado automáticamente.
- Dirección IP: una dirección DHCP o estática asignada IPv4. No puede asignar una IPv6 dirección.

Hay cinco puertos de red físicos en la parte posterior del servidor Dell PowerEdge R640. De izquierda a derecha (mirando a la parte posterior del servidor) estos puertos son los siguientes:

1. iDRAC
2. `em1`
3. `em2`
4. `em3`

5. em4

Puede utilizar el puerto iDRAC para la administración remota del servidor.



Un dispositivo de hardware requiere los siguientes puertos para funcionar.

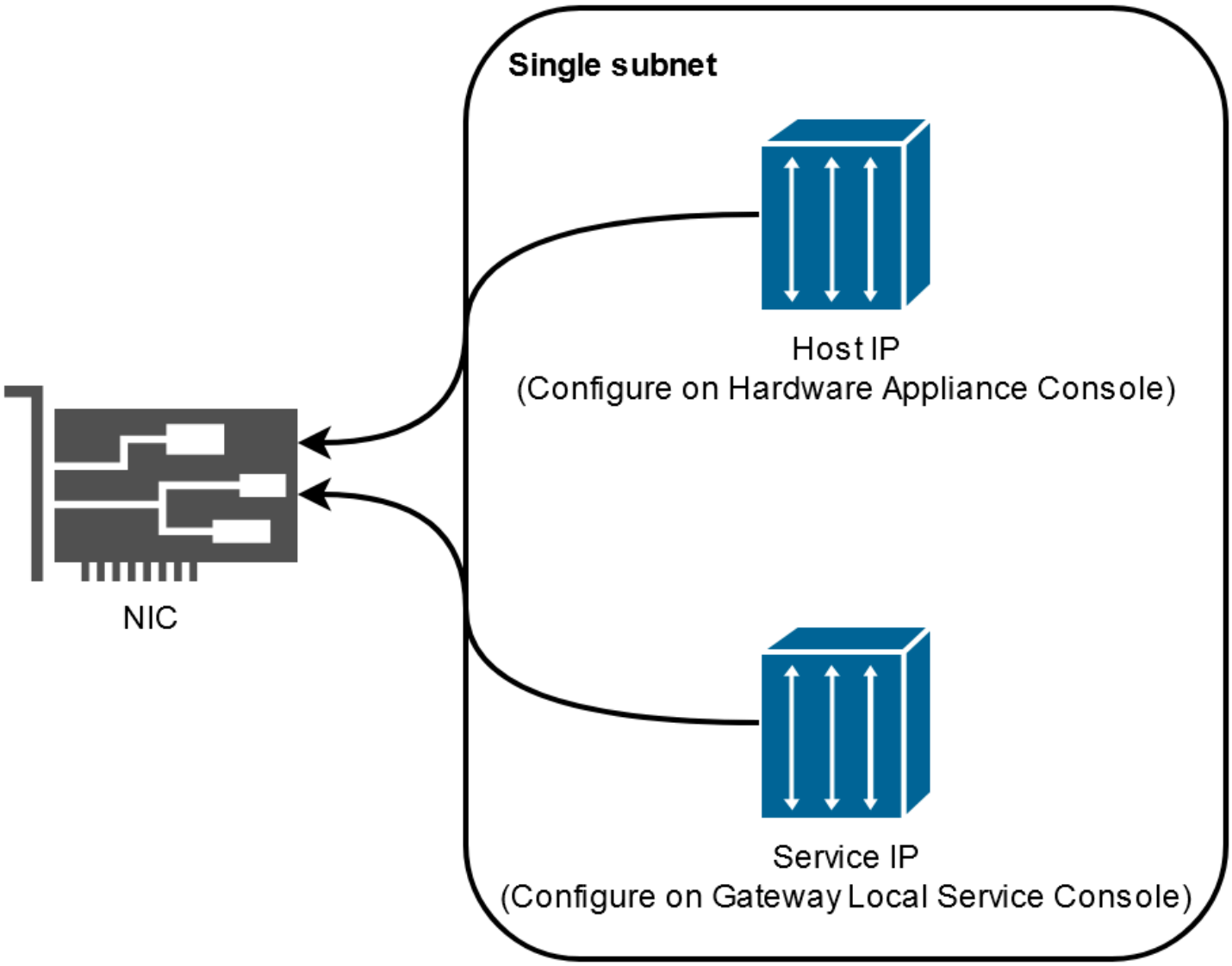
Protocolo	Puerto	Dirección	Origen	Destino	De uso
SSH	22	Salida	Dispositivo de hardware	`54.201.223.107`	canal de soporte
DNS	53	Salida	Dispositivo de hardware	Servidores DNS	Resolución de nombres
UDP/NTP	123	Salida	Dispositivo de hardware	`*.amazon.pool.ntp.org`	Sincronización horaria
HTTPS	443	Salida	Dispositivo de hardware	`*.amazonaws.com`	Transferencia de datos
HTTP	8080	Entrada	AWS	Dispositivo de hardware	Activación (solo brevemente)

Para rendir de acuerdo con el diseño, un dispositivo de hardware requiere que la configuración de red y de firewall sea como se indica a continuación:

- Configure todas las interfaces de red conectadas en la consola del hardware.
- Asegúrese de que cada interfaz de red se encuentre en su propia subred.
- Proporcione todas las interfaces de red conectadas con acceso de salida a los puntos de enlace que se enumeran en el diagrama anterior.
- Configure al menos una interfaz de red para admitir el dispositivo de hardware. Para obtener más información, consulte Configuración de los parámetros de red del dispositivo de hardware.

> **Note**
>
> Para ver una ilustración que muestra la parte posterior del servidor con sus puertos, consulteInstalación física del dispositivo de hardware.

Todas las direcciones IP de la misma interfaz de red (NIC), ya sea para una gateway o un host, deben estar en la misma subred. La siguiente ilustración muestra el esquema de direccionamiento.



Para obtener más información acerca de la activación y la configuración de un dispositivo de hardware, consulte Uso del dispositivo de hardware AWS Storage Gateway.

Permitir el AWS Storage Gateway acceso a través de firewalls y enrutadores

Su puerta de enlace requiere acceso a los siguientes puntos finales del servicio Storage Gateway para poder comunicarse con AWS ellos. Durante la configuración de la puerta de enlace, seleccione el tipo de punto de conexión de la puerta de enlace en función del entorno de red. Si utiliza un firewall o un router para filtrar o limitar el tráfico de red, debe configurar el firewall y el router para dar permiso a los puntos de conexión de servicio para mantener comunicaciones de salida con AWS.

> **Note**
>
> Si configura puntos de enlace de VPC privados para que Storage Gateway los utilice para la conexión y la transferencia de datos desde y hacia AWS, su puerta de enlace no requiere acceso a la Internet pública. Para obtener más información, consulte Activación de una puerta de enlace en una nube virtual privada.

> **Important**
>
> *region*En los siguientes ejemplos de puntos de conexión, sustituya por la Región de AWS cadena correcta para su puerta de enlace, por ejemplo. `us-west-2` *amzn-s3-demo-bucket*Sustitúyalo por el nombre real del bucket de Amazon S3 de la implementación. También puede usar un asterisco (`*`) en lugar de *amzn-s3-demo-bucket* para crear una entrada comodín en las reglas de su firewall, lo que le permitirá incluir el punto final del servicio para todos los nombres de los buckets.
> Si sus puertas de enlace están implementadas Regiones de AWS en los Estados Unidos o Canadá y requieren conexiones de punto final que cumplan con la Norma Federal de Procesamiento de la Información (FIPS), sustitúyalas por. *s3* `s3-fips`

Tipo de punto de conexión

Puntos de conexión estándar

Estos puntos finales admiten el IPv4 tráfico entre su dispositivo de puerta de enlace y. AWS

Todas las puertas de enlace requieren el siguiente punto de conexión de servicio para las operaciones Head Bucket.

```
bucket-name.s3.region.amazonaws.com:443
```

Los siguientes puntos de conexión de servicio son necesarios para todas las puertas de enlace para operaciones de ruta de control (`anon-cp`, `client-cp` y `proxy-app`) y de ruta de datos (`dp-1`).

```
anon-cp.storagegateway.region.amazonaws.com:443
client-cp.storagegateway.region.amazonaws.com:443
proxy-app.storagegateway.region.amazonaws.com:443
```

```
dp-1.storagegateway.region.amazonaws.com:443
```

El siguiente punto de enlace de servicio de la gateway es necesario para realizar llamadas a la API.

```
storagegateway.region.amazonaws.com:443
```

El siguiente ejemplo es un punto de conexión de servicio de la puerta de enlace en la región Oeste de EE. UU. (Oregón) (`us-west-2`).

```
storagegateway.us-west-2.amazonaws.com:443
```

Además de los puntos finales del servicio Storage Gateway y Amazon S3, Storage Gateway VMs también requiere acceso de red a los siguientes servidores NTP:

```
time.aws.com
0.amazon.pool.ntp.org
1.amazon.pool.ntp.org
2.amazon.pool.ntp.org
3.amazon.pool.ntp.org
```

Para obtener más información sobre los puntos finales compatibles Regiones de AWS y de servicio, consulte Storage Gateway en. Referencia general de AWS

Configuración de grupos de seguridad para la instancia de puerta de enlace de Amazon EC2

En AWS Storage Gateway, un grupo de seguridad controla el tráfico a su instancia de puerta de enlace Amazon EC2. A la hora de configurar un grupo de seguridad, recomendamos las siguientes acciones:

- El grupo de seguridad no debe permitir conexiones entrantes procedentes de Internet. Solamente debe permitir que se comuniquen con la gateway las instancias que se encuentren dentro del grupo de seguridad de la gateway.

  Si necesita permitir la conexión de instancias con la puerta de enlace desde el exterior de su grupo de seguridad, se recomienda permitir solamente conexiones en el puerto 80 (para la activación).
- Si desea activar la puerta de enlace desde un host de Amazon EC2 fuera del grupo de seguridad de la puerta de enlace, permita las conexiones entrantes en el puerto 80 desde la dirección IP de

ese host. Si no puede determinar la dirección IP del host de activación, puede abrir el puerto 80, activar la gateway y, a continuación, cerrar el acceso en el puerto 80 tras completar la activación.

- Permita el acceso al puerto 22 solo si lo utiliza Soporte para solucionar problemas. Para obtener más información, consulte Quiere ayudar Soporte a solucionar los problemas de su puerta de enlace Amazon EC2.

Hipervisores compatibles y requisitos de host

Puede ejecutar Storage Gateway localmente como un dispositivo de máquina virtual (VM) o un dispositivo de hardware físico, o AWS como una instancia de Amazon EC2.

> **Note**
>
> Se requiere el modo de arranque UEFI con el arranque seguro desactivado (loader_secure=no) para File Gateway 2.x, Volume Gateway 3.x y Tape Gateway 3.x. Se proporciona un archivo xml con cada descarga de qcow como configuración de configuración rápida.

Storage Gateway es compatible con las siguientes versiones de hipervisores y hosts:

- VMware ESXi Hipervisor (versión 7.0 u 8.0): para esta configuración, también necesita un cliente VMware vSphere para conectarse al host.
- Hipervisor Microsoft Hyper-V (2019, 2022 o 2025): para esta configuración, necesitará Microsoft Hyper-V Manager en un equipo cliente Microsoft Windows para conectarse al host.
- Máquina virtual basada en el kernel (KVM) de Linux: tecnología de virtualización gratuita y de código abierto. KVM está incluida en todas las versiones de Linux 2.6.20 y posteriores. Storage Gateway se ha probado y es compatible con las CentOS/RHEL distribuciones 7.7, RHEL 8.6 Ubuntu 16.04 LTS y Ubuntu 18.04 LTS. Cualquier otra distribución moderna de Linux puede funcionar, pero la funcionalidad o el rendimiento no están garantizados. Recomendamos esta opción si ya tiene un entorno KVM en funcionamiento y ya está familiarizado con el funcionamiento de KVM. Consulte el aws-storage-gateway archivo.xml proporcionado para ver las configuraciones de arranque sugeridas. Se requiere el modo de arranque UEFI con el arranque seguro desactivado (loader_secure=no) para File Gateway 2.x, Volume Gateway 3.x y Tape Gateway 3.x.

- Nutanix AHV (hipervisor Acropolis) a partir de la versión 10.0.1.1, una plataforma de virtualización basada en KVM que está integrada en la solución de infraestructura hiperconvergente (HCI) de Nutanix.
- Instancia de Amazon EC2: proporciona una imagen de máquina de Amazon (AMI) que contiene la imagen de la VM de la puerta de enlace. Para obtener información sobre cómo implementar una puerta de enlace en Amazon EC2, consulte Implemente un host Amazon EC2 predeterminado para File Gateway FSx.
- Dispositivo de hardware de Storage Gateway: Storage Gateway proporciona un dispositivo de hardware físico como opción de implementación en las instalaciones para ubicaciones con una infraestructura de máquina virtual limitada.

> **Note**
>
> Storage Gateway no permite recuperar una puerta de enlace desde una máquina virtual que se creó a partir de una instantánea o un clon de otra máquina virtual de puerta de enlace o desde la AMI de Amazon EC2. Si la MV de la gateway no funciona correctamente, active una nueva gateway y recupere los datos para esa gateway. Para obtener más información, consulte Recuperación de un cierre inesperado de una máquina virtual.
> Storage Gateway no es compatible con la memoria dinámica ni con la asignación dinámica (ballooning) de memoria virtual.

Clientes de SMB compatibles con la puerta de enlace de archivo

La puerta de enlace de archivo admite los siguientes clientes de Service Message Block (SMB):

- Microsoft Windows Server 2008 R2 y posteriores
- Versiones de escritorio de Windows: 10, 8 y 7.
- Windows Terminal Server que se ejecuta en Windows Server 2008 y versiones posteriores

> **Note**
>
> El cifrado de Server Message Block requiere clientes que admitan los dialectos de SMB v3.

Operaciones del sistema de archivos compatibles con la puerta de enlace de archivo

El cliente de SMB puede escribir, leer, eliminar y truncar archivos. Cuando los clientes envían escrituras a Storage Gateway, este escribe en la caché local de forma síncrona. Luego escribe en Amazon de forma FSx asíncrona a través de transferencias optimizadas. Las lecturas se sirven primero a través de la caché local. Si los datos no están disponibles, se obtienen a través de Amazon FSx como caché de lectura.

Las escrituras y las lecturas se optimizan de tal forma que solamente se transfieren a través de la gateway las partes modificadas o solicitadas. Elimina o elimina archivos de Amazon FSx.

Administración de discos locales para la puerta de enlace

La máquina virtual (VM) de la puerta de enlace utiliza los discos locales que se le asignan en las instalaciones para almacenamiento en búfer y permanente. Una puerta de enlace de archivo creada en una instancia de Amazon EC2 utilizará volúmenes de Amazon EBS como discos locales. Puede elegir el número y el tamaño de los discos que va a asignar a la gateway. La puerta de enlace utiliza el almacenamiento en caché asignado para proporcionar acceso de baja latencia a los datos a los que se ha tenido acceso recientemente. El almacenamiento en caché actúa como un almacén duradero local para los datos pendientes de carga en Amazon FSx. Las puertas de enlace de archivo requieren al menos un disco de 150 GiB para utilizar como caché. Tras la configuración y la implementación iniciales de la puerta de enlace, puede añadir más discos para el almacenamiento en caché a medida que aumente la carga de trabajo. Esta sección contiene los temas siguientes, que describen los conceptos y procedimientos relacionados con la administración de discos locales.

Temas

- Cálculo de la cantidad de almacenamiento en disco local: obtenga información sobre cómo determinar el número y el tamaño de discos de caché locales para asignar a la puerta de enlace de archivo.
- Configuración de almacenamiento en caché adicional: obtenga información sobre cómo aumentar la capacidad de almacenamiento en caché de la puerta de enlace de archivo a medida que cambian las necesidades de la aplicación.
- Uso del almacenamiento efímero con puertas de enlace de EC2: obtenga información sobre cómo evitar la pérdida de datos al usar almacenamiento en disco efímero con la puerta de enlace de archivo.

Cálculo de la cantidad de almacenamiento en disco local

Al implementar una puerta de enlace de , tenga en cuenta la cantidad de memoria caché que desea asignar. File Gateway utiliza el algoritmo utilizado menos recientemente para desalojar automáticamente los datos de la memoria caché. La memoria caché de una puerta de enlace de archivos de se comparte entre todos los recursos compartidos de archivos de esa puerta de enlace. Si tiene varios recursos compartidos activos, es importante tener en cuenta que el uso intensivo de un recurso compartido podría afectar a la cantidad de recursos de caché a los que otro recurso compartido tiene acceso, lo que podría afectar al rendimiento.

Al determinar la cantidad de disco caché que necesita para una carga de trabajo determinada, es importante tener en cuenta que siempre puede añadir un disco caché a la puerta de enlace (hasta las cuotas actuales de File Gateway), pero no puede reducir la caché de una puerta de enlace determinada. Puede realizar un análisis básico del conjunto de datos para determinar la cantidad correcta de disco de caché, pero no hay forma de determinar exactamente cuántos son datos recientes y deben almacenarse localmente, y cuántos son datos fríos y se pueden agrupar en la nube. Las cargas de trabajo cambian con el tiempo, y File Gateway proporciona flexibilidad y elasticidad en función de la cantidad de recursos que se pueden consumir. La cantidad de caché siempre se puede aumentar, por lo que el enfoque más rentable es empezar con poca y aumentarla según sea necesario.

Puede utilizar una aproximación inicial de 150 GiB para aprovisionar discos para el almacenamiento en caché durante la configuración de la puerta de enlace. A continuación, puede utilizar las métricas CloudWatch operativas de Amazon para supervisar el uso del almacenamiento en caché y aprovisionar más almacenamiento según sea necesario mediante la consola. Para obtener información sobre cómo usar las métricas y configurar las alarmas, consulte Rendimiento y optimización.

> **Note**
>
> Los recursos de almacenamiento físico subyacentes se representan como un almacén de datos en VMware. Al implementar la máquina virtual de gateway, debe elegir el almacén de datos en el que se almacenarán los archivos de la máquina virtual. Al aprovisionar un disco local (por ejemplo, para utilizarlo como almacenamiento en caché), tiene la opción de almacenar el disco virtual en el mismo almacén de datos que la máquina virtual o en otro distinto.
>
> Si hay más de un almacén de datos, se recomienda encarecidamente elegir un almacén de datos para el almacenamiento en caché. Un almacén de datos respaldado por un único disco

físico subyacente puede hacer que disminuya el rendimiento en algunas situaciones si se utiliza para el almacenamiento en caché. Esto también es cierto si la copia de seguridad es una configuración RAID de menor rendimiento, por ejemplo. RAID1

Configuración de almacenamiento en caché adicional

A medida que cambian las necesidades de la aplicación, puede aumentar la capacidad de almacenamiento en caché de la puerta de enlace. Puede agregar capacidad de almacenamiento a la puerta de enlace sin interrumpir la funcionalidad ni provocar tiempos de inactividad. Cuando agregue más almacenamiento, hágalo con la máquina virtual de la puerta de enlace encendida.

Important

Cuando se agrega caché a una puerta de enlace existente, se deben crear nuevos discos en el hipervisor del host de la puerta de enlace o la instancia de Amazon EC2. No elimine ni cambie el tamaño de los discos existentes que ya se hayan asignado como caché.

Cómo configurar almacenamiento en caché adicional para la puerta de enlace

1. Aprovisione uno o más discos nuevos en el hipervisor del host de la puerta de enlace o en la instancia de Amazon EC2. Para obtener información sobre cómo aprovisionar un disco en un hipervisor, consulte el manual de usuario del hipervisor. Para obtener información acerca del aprovisionamiento de volúmenes de Amazon EBS para una instancia de Amazon EC2, consulte Volúmenes de Amazon EBS en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux. En los siguientes pasos, configurará este disco como almacenamiento en caché.
2. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
3. En el panel de navegación, seleccione Puertas de enlace.
4. Busque la puerta de enlace y selecciónela de la lista.
5. En el menú Acciones, seleccione Configurar almacenamiento en caché.
6. En la sección Configurar almacenamiento en caché, identifique los discos que aprovisionó. Si no ve los discos, seleccione el icono de actualización para actualizar la lista. Para cada disco, elija Caché en el menú desplegable Asignado a.

> **Note**
>
> La opción Caché es la única disponible para asignar discos en una puerta de enlace de archivo.

7. Elija Guardar cambios para guardar los ajustes de configuración.

Uso del almacenamiento efímero con puertas de enlace de EC2

No recomendamos el uso de discos efímeros para el almacenamiento en caché en FSx File Gateways.

Los discos efímeros proporcionan un almacenamiento por bloques temporal para la instancia de Amazon EC2. Cuando se lanza la puerta de enlace con la imagen de máquina de Amazon en Amazon EC2 y el tipo de instancia que se ha seleccionado es compatible con almacenamiento efímero, los discos efímeros se muestran de forma automática. Puede seleccionar uno de los discos para almacenar los datos de caché de la puerta de enlace. Para obtener más información, consulte Almacén de instancias de Amazon EC2 en la Guía del usuario de Amazon EC2.

Los datos que las aplicaciones escriben en la puerta de enlace se almacenan de forma sincrónica en la memoria caché de los discos efímeros y, a continuación, se cargan de forma asíncrona en un almacenamiento duradero en S3 para Windows File Server. FSx Si la instancia de Amazon EC2 se detiene después de escribir los datos en un almacenamiento efímero, pero antes de que se produzca una carga asíncrona, se pueden perder todos los datos que aún no se hayan cargado en el servidor de archivos de .

> **Important**
>
> Si detiene e inicia una puerta de enlace de Amazon EC2 que utiliza almacenamiento efímero, esta se desconectará permanentemente. Esto sucede porque se ha reemplazado el disco de almacenamiento físico. No hay una solución para este problema. La única solución es eliminar la puerta de enlace y activar una nueva en una nueva instancia de EC2.

Uso del dispositivo de hardware AWS Storage Gateway

> **Note**
>
> Aviso de fin de disponibilidad: a partir del 12 de mayo de 2025, el dispositivo de AWS Storage Gateway hardware dejará de estar disponible. Los clientes actuales que dispongan del dispositivo de AWS Storage Gateway hardware pueden seguir utilizándolo y recibiendo asistencia hasta mayo de 2028. Como alternativa, puede utilizar el AWS Storage Gateway servicio para ofrecer a sus aplicaciones un acceso local y en la nube a un almacenamiento en la nube prácticamente ilimitado.

El AWS Storage Gateway Hardware Appliance es un dispositivo de hardware físico con el software Storage Gateway preinstalado en una configuración de servidor validada. Puede administrar los dispositivos de hardware de su implementación desde la página de información general del dispositivo de hardware de la AWS Storage Gateway consola.

El dispositivo de hardware es un servidor 1U de alto rendimiento que puede implementar en su centro de datos o en las instalaciones, dentro de su firewall corporativo. Cuando compre y active el dispositivo de hardware, el proceso de activación asocia el dispositivo de hardware con la Cuenta de AWS. Después de la activación, el dispositivo de hardware aparece en la consola en la página Información general sobre el dispositivo de hardware. Puede configurar el dispositivo de hardware como un tipo S3 File Gateway, FSx File Gateway, Tape Gateway o Volume Gateway. El procedimiento que se utiliza para implementar estos tipos de puertas de enlace en un dispositivo de hardware es el mismo que en una plataforma virtual.

Para obtener una lista de los dispositivos de hardware compatibles Regiones de AWS en los que el dispositivo de hardware AWS Storage Gateway está disponible para su activación y uso, consulte las regiones del dispositivo de hardware AWS Storage Gateway en el Referencia general de AWS.

En las secciones siguientes, encontrará instrucciones sobre cómo configurar, montar en rack, alimentar, configurar, activar, lanzar, usar y eliminar un dispositivo de hardware AWS Storage Gateway.

Temas

- Configuración del dispositivo de hardware AWS Storage Gateway
- Instalación física del dispositivo de hardware

- Acceso a la consola del dispositivo de hardware
- Configuración de los parámetros de red del dispositivo de hardware
- Activación del dispositivo de hardware AWS Storage Gateway
- Creación de una puerta de enlace en el dispositivo de hardware
- Configuración de una dirección IP de puerta de enlace en el dispositivo de hardware
- Eliminación del software de puerta de enlace del dispositivo de hardware
- Eliminar el dispositivo de hardware AWS Storage Gateway

Configuración del dispositivo de hardware AWS Storage Gateway

> **Note**
>
> Aviso de fin de disponibilidad: a partir del 12 de mayo de 2025, el dispositivo de AWS Storage Gateway hardware dejará de estar disponible. Los clientes actuales que dispongan del dispositivo de AWS Storage Gateway hardware pueden seguir utilizándolo y recibiendo asistencia hasta mayo de 2028. Como alternativa, puede utilizar el AWS Storage Gateway servicio para ofrecer a sus aplicaciones un acceso local y en la nube a un almacenamiento en la nube prácticamente ilimitado.

Tras recibir el dispositivo de hardware Storage Gateway, utiliza la consola local del dispositivo de hardware para configurar las redes a fin de proporcionar una conexión permanente AWS y activar el dispositivo. La activación asocia el dispositivo a la AWS cuenta que se utiliza durante el proceso de activación. Una vez activado el dispositivo, puede iniciar S3 File Gateway, FSx File Gateway, Tape Gateway o Volume Gateway desde la consola Storage Gateway.

Cómo instalar y configurar su dispositivo de hardware

1. Monte el bastidor del dispositivo y conecte la alimentación y las conexiones de red. Para obtener más información, consulte Instalación física del dispositivo de hardware.
2. Establezca las direcciones del Protocolo de Internet versión 4 (IPv4) para el dispositivo de hardware (el host). Para obtener más información, consulte Configuración de los parámetros de red del dispositivo de hardware.

3. Active el dispositivo de hardware en la página de información general del dispositivo de hardware de la consola, en la AWS región que elija. Para obtener más información, consulte Activación del dispositivo de hardware AWS Storage Gateway.
4. Cree una puerta de enlace en el dispositivo de hardware. Para obtener más información, consulte Creación de la puerta de enlace.

   Las puertas de enlace de su dispositivo de hardware se configuran de la misma manera que las puertas de enlace en VMware ESXi, Microsoft Hyper-V, la máquina virtual basada en el kernel (KVM) de Linux o Amazon EC2.

Cómo aumentar el almacenamiento en caché utilizable

Puede aumentar el almacenamiento utilizable en el dispositivo de hardware de 5 TB a 12 TB. De este modo, se obtiene una memoria caché más grande para acceder a los datos con baja latencia AWS. Si ha pedido el modelo de 5 TB, puede aumentar el almacenamiento utilizable a 12 TB si compra cinco unidades de estado sólido de 1,92 TB SSDs .

A continuación, puede agregarlas al dispositivo de hardware antes de activarlo. Si ya ha activado el dispositivo de hardware y desea aumentar el almacenamiento utilizable en el dispositivo hasta 12 TB, haga lo siguiente:

1. Restablezca el dispositivo de hardware a su configuración de fábrica. Póngase en contacto con AWS Support para obtener instrucciones sobre cómo hacerlo.
2. Añada cinco unidades de 1,92 TB SSDs al dispositivo.

Opciones de tarjeta interfaz de red

Según el modelo de dispositivo que haya pedido, puede venir con una tarjeta de red 10G-Base-T de RJ45 cobre o una tarjeta de red DA/SFP+ de 10G.

- Configuración de 10 NIC: G-Base-T
  - Utilice CAT6 cables para 10 G o CAT5 (e) para 1 G
- Configuración de NIC DA/SFP+ de 10 G:
  - Utilice cables de conexión directa de cobre Twinax de hasta 5 metros
  - Módulos ópticos SFP+ compatibles con Dell/Intel (SR o LR)
  - Transceptor de cobre SFP/SFP+ para 1 o 10G-Base-T G-Base-T

Instalación física del dispositivo de hardware

> **Note**
>
> Aviso de fin de disponibilidad: a partir del 12 de mayo de 2025, el dispositivo de AWS Storage Gateway hardware dejará de estar disponible. Los clientes actuales que dispongan del dispositivo de AWS Storage Gateway hardware pueden seguir utilizándolo y recibiendo asistencia hasta mayo de 2028. Como alternativa, puede utilizar el AWS Storage Gateway servicio para ofrecer a sus aplicaciones un acceso local y en la nube a un almacenamiento en la nube prácticamente ilimitado.

Su dispositivo tiene un factor de forma de 1U y cabe en un bastidor estándar de 19 pulgadas que cumple con las normas de la Comisión Electrotécnica Internacional (CEI).

Requisitos previos

Para instalar su dispositivo de hardware, necesita los siguientes componentes:

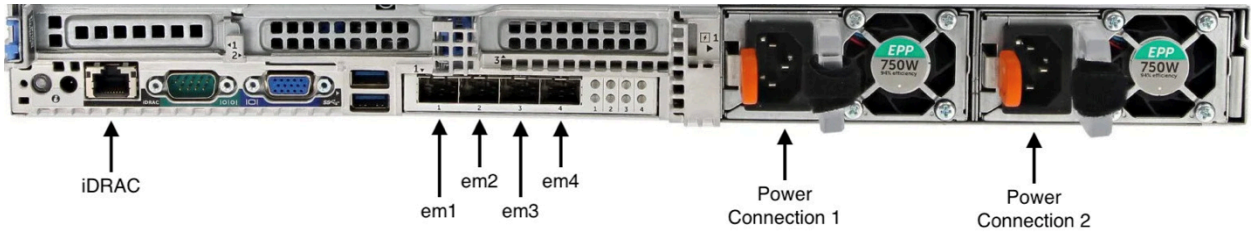
- Cables de alimentación: se necesita uno pero se recomienda tener dos.
- Cableado de red compatible (según la tarjeta de interfaz de red [NIC] que se incluya en el dispositivo de hardware). DAC de cobre Twinax, módulo óptico SFP+ (compatible con Intel) o transceptor de cobre SFP a Base-T.
- Un teclado y un monitor o una solución de conmutador con teclado, vídeo y ratón (KVM).

> **Note**
>
> Antes de realizar el siguiente procedimiento, asegúrese de que cumple todos los requisitos del dispositivo de hardware de Storage Gateway como se describe en Requisitos de red y firewall para el dispositivo de hardware de Storage Gateway.

Instalación física del dispositivo de hardware

1. Desembale el dispositivo de hardware y siga las instrucciones que se encuentran en la caja para montar el servidor en un bastidor.

La siguiente imagen muestra la parte posterior del dispositivo de hardware con puertos para conectar la alimentación, Ethernet, el monitor, el teclado USB e iDRAC.
una parte trasera del dispositivo de hardware con etiquetas de conectores de red y alimentación.



una parte trasera del dispositivo de hardware con etiquetas de conectores de red y alimentación.

2. Conecte una conexión de alimentación a cada una de las fuentes de alimentación. Es posible conectar solo una conexión de alimentación, pero recomendamos conectar ambas fuentes de alimentación por motivos de redundancia.
3. Conecte un cable Ethernet al puerto `em1` para proporcionar una conexión a Internet permanente. El puerto `em1` es el primero de los cuatro puertos de red físicos de la parte trasera, de izquierda a derecha.

> **Note**
>
> El dispositivo de hardware no admite el enlace troncal de VLAN. Configure el puerto del conmutador al que va a conectar el dispositivo de hardware como puerto de red VLAN no troncal.

4. Conecte el teclado y el monitor.
5. Encienda el servidor presionando el botón Power del panel delantero, como se muestra en la siguiente imagen.
parte delantera del dispositivo de hardware con etiqueta de botón de encendido.

parte delantera del dispositivo de hardware con etiqueta de botón de encendido.

Paso siguiente

Acceso a la consola del dispositivo de hardware

Acceso a la consola del dispositivo de hardware

> **Note**
>
> Aviso de fin de disponibilidad: a partir del 12 de mayo de 2025, el dispositivo de AWS Storage Gateway hardware dejará de estar disponible. Los clientes actuales que dispongan del dispositivo de AWS Storage Gateway hardware pueden seguir utilizándolo y recibiendo asistencia hasta mayo de 2028. Como alternativa, puede utilizar el AWS Storage Gateway servicio para ofrecer a sus aplicaciones un acceso local y en la nube a un almacenamiento en la nube prácticamente ilimitado.

Al encender el dispositivo de hardware, la consola del dispositivo de hardware aparece en el monitor. La consola del dispositivo de hardware presenta una interfaz de usuario específica AWS que puede utilizar para establecer una contraseña de administrador, configurar los parámetros iniciales de la red y abrir un canal de soporte. AWS

Para trabajar con la consola del dispositivo de hardware, ingrese texto con el teclado y utilice las teclas `Up`, `Down`, `Right` y `Left Arrow` para desplazarse por la pantalla en la dirección indicada. Utilice la tecla `Tab` para avanzar en orden a través de los elementos en pantalla. En algunas configuraciones, puede utilizar la combinación de teclas `Shift+Tab` para retroceder de forma secuencial. Utilice la tecla `Enter` para guardar las selecciones o para elegir un botón de la pantalla.

La primera vez que aparezca la consola del dispositivo de hardware, aparecerá la página de bienvenida y se le solicitará que establezca una contraseña para la cuenta de usuario de administrador antes de poder acceder a la consola.

Establecimiento de una contraseña de administrador

- En la petición Establezca su contraseña de inicio de sesión, haga lo siguiente:
  a. En Set Password, introduzca una contraseña y, a continuación, presione `Down arrow`.
  b. En Confirm, vuelva a introducir la contraseña y, a continuación, seleccione Save Password.

Tras configurar la contraseña, aparece la página de inicio de la consola de hardware. La página de inicio muestra la información de red de las interfaces de red em1, em2, em3 y em4 y tiene las siguientes opciones de menú:

- Configurar la red
- Abrir la consola de servicio
- Cambio de contraseña
- Cerrar sesión
- Abrir la consola de soporte

Paso siguiente

Configuración de los parámetros de red del dispositivo de hardware

Configuración de los parámetros de red del dispositivo de hardware

> **Note**
>
> Aviso de fin de disponibilidad: a partir del 12 de mayo de 2025, el dispositivo de AWS Storage Gateway hardware dejará de estar disponible. Los clientes actuales que dispongan del dispositivo de AWS Storage Gateway hardware pueden seguir utilizándolo y recibiendo asistencia hasta mayo de 2028. Como alternativa, puede utilizar el AWS Storage Gateway servicio para ofrecer a sus aplicaciones un acceso local y en la nube a un almacenamiento en la nube prácticamente ilimitado.

Tras arrancar el dispositivo de hardware y configurar la contraseña de usuario de administrador en la consola de hardware tal y como se describe en Acceso a la consola del dispositivo de hardware, utilice el siguiente procedimiento para configurar los parámetros de red para que el dispositivo de hardware se pueda conectar a AWS.

Establecimiento de una dirección de red

1. En la página de inicio, elija Configurar red y, a continuación, presione `Enter`. Aparece la página Configurar red. La página Configurar red muestra la información de IP y DNS de cada una de las cuatro interfaces de red del dispositivo de hardware e incluye opciones de menú para configurar las direcciones DHCP o estáticas para cada una de ellas.
2. Para la interfaz em1, realice una de las acciones siguientes:

   - Elija DHCP y pulse `Enter` para usar la IPv4 dirección asignada por el servidor del Protocolo de configuración dinámica de host (DHCP) a su puerto de red físico.

Anote esta dirección para utilizarla más adelante en el paso de activación.

- Elija Estático y pulse `Enter` para configurar una dirección estática IPv4 .

  Introduzca una dirección IP, una máscara de subred, una puerta de enlace y una dirección de servidor DNS válidas para la interfaz de red em1.

  Cuando haya terminado, elija Guardar y, a continuación, presione `Enter` para guardar la configuración.

> **Note**
>
> Puede usar este procedimiento para configurar otras interfaces de red además de em1. Si configura otras interfaces, deben proporcionar la misma conexión permanente a los AWS puntos finales enumerados en los requisitos.
> La vinculación de redes y el protocolo de control de agregación de enlaces (LACP) no son compatibles con el dispositivo de hardware o Storage Gateway.
> No recomendamos configurar varias interfaces de red en la misma subred, ya que esto a veces puede provocar problemas de enrutamiento.

Cómo cerrar sesión en la consola de hardware

1. Elija Atrás y presione `Enter` para volver a la página de inicio.
2. Elija Cerrar sesión y presione `Enter` para volver a la página de bienvenida.

Paso siguiente

Activación del dispositivo de hardware AWS Storage Gateway

Activación del dispositivo de hardware AWS Storage Gateway

> **Note**
>
> Aviso de fin de disponibilidad: a partir del 12 de mayo de 2025, el dispositivo de AWS Storage Gateway hardware dejará de estar disponible. Los clientes actuales que dispongan del dispositivo de AWS Storage Gateway hardware pueden seguir utilizándolo y recibiendo

asistencia hasta mayo de 2028. Como alternativa, puede utilizar el AWS Storage Gateway servicio para ofrecer a sus aplicaciones un acceso local y en la nube a un almacenamiento en la nube prácticamente ilimitado.

Tras configurar la dirección IP, introduzca esta dirección IP en la página Hardware de la AWS Storage Gateway consola para activar el dispositivo de hardware. El proceso de activación registra el dispositivo en la cuenta de AWS .

Puede optar por activar su dispositivo de hardware en cualquiera de los dispositivos compatibles Regiones de AWS. Para obtener una lista de los dispositivos de hardware compatibles Regiones de AWS, consulte las regiones de los dispositivos de hardware de Storage Gateway en Referencia general de AWS.

Para activar su dispositivo de hardware AWS Storage Gateway

1. Inicie sesión en la consola de administración de AWS Storage Gateway e inicie sesión con las credenciales de la cuenta que desea utilizar para activar su hardware.

   > **Note**
   >
   > Únicamente para la activación, deben cumplirse las siguientes condiciones:
   >
   > - Su navegador debe estar en la misma red que su dispositivo de hardware.
   > - Su firewall debe permitir el acceso HTTP al puerto 8080 del dispositivo para el tráfico de entrada.

2. Elija Hardware en el menú de navegación del lado izquierdo de la página.
3. Seleccione Activar dispositivo.
4. En Dirección IP, introduzca la dirección IP que configuró para el dispositivo de hardware y, a continuación, seleccione Conectar.

   Para obtener más información sobre la configuración de la dirección IP, consulte Configuración de parámetros de red.
5. En Nombre, escriba un nombre para su dispositivo de hardware. Los nombres pueden tener una longitud máxima de 225 caracteres y no pueden incluir barras inclinadas.

6. En Zona horaria del dispositivo de hardware, introduzca la zona horaria local desde la que se generará la mayor parte de la carga de trabajo de la puerta de enlace y, a continuación, seleccione Siguiente.

   La zona horaria controla cuándo se realizan las actualizaciones de hardware y se utilizan las 2:00 h como hora programada predeterminada para realizar las actualizaciones. Lo ideal es que, si la zona horaria está configurada correctamente, las actualizaciones se realicen de forma predeterminada fuera del horario laboral local.
7. Revise los parámetros de activación en la sección de detalles del dispositivo de hardware. Puede seleccionar Anterior para volver atrás y realizar los cambios necesarios. De lo contrario, seleccione Activar para finalizar la activación.

Aparecerá un banner en la página Resumen del dispositivo de hardware que indica que el dispositivo de hardware se ha activado correctamente.

En este momento, el dispositivo está asociado a su cuenta. El siguiente paso es configurar e iniciar una puerta de enlace de archivos S3, una puerta de enlace de FSx archivos, una puerta de enlace de cinta o una puerta de enlace de volumen S3 en el nuevo dispositivo.

Paso siguiente

Creación de una puerta de enlace en el dispositivo de hardware

Creación de una puerta de enlace en el dispositivo de hardware

> **Note**
>
> Aviso de fin de disponibilidad: a partir del 12 de mayo de 2025, el dispositivo de AWS Storage Gateway hardware dejará de estar disponible. Los clientes actuales que dispongan del dispositivo de AWS Storage Gateway hardware pueden seguir utilizándolo y recibiendo asistencia hasta mayo de 2028. Como alternativa, puede utilizar el AWS Storage Gateway servicio para ofrecer a sus aplicaciones un acceso local y en la nube a un almacenamiento en la nube prácticamente ilimitado.

Puede crear una puerta de enlace de archivos S3, una puerta de enlace de FSx archivos, una puerta de enlace de cinta o una puerta de enlace de volumen en cualquier dispositivo de hardware AWS Storage Gateway de su implementación.

Cómo crear una puerta de enlace en su dispositivo de hardware

1. Inicie sesión en la consola Storage Gateway de su https://console.aws.amazon.com/storagegateway/casa Consola de administración de AWS y ábrala.
2. Siga los procedimientos que se describen en Creación de la puerta de enlace para instalar, conectar y configurar el tipo de Storage Gateway que desea implementar.

Cuando termine de crear la puerta de enlace en la consola de Storage Gateway, el software Storage Gateway comenzará a instalarse automáticamente en el dispositivo de hardware. Si usa el protocolo de configuración dinámica de host (DHCP), una puerta de enlace puede tardar entre 5 y 10 minutos en mostrarse como si estuviera en línea en la consola. Para asignar una dirección IP estática a la puerta de enlace instalada, consulte Configuración de una dirección IP para la puerta de enlace.

Para asignar una dirección IP estática a la gateway instalada, configure las interfaces de red de la gateway para que las aplicaciones puedan utilizarlas.

Paso siguiente

Configuración de una dirección IP de puerta de enlace en el dispositivo de hardware

Configuración de una dirección IP de puerta de enlace en el dispositivo de hardware

> **Note**
>
> Aviso de fin de disponibilidad: a partir del 12 de mayo de 2025, el dispositivo de AWS Storage Gateway hardware dejará de estar disponible. Los clientes actuales que dispongan del dispositivo de AWS Storage Gateway hardware pueden seguir utilizándolo y recibiendo asistencia hasta mayo de 2028. Como alternativa, puede utilizar el AWS Storage Gateway servicio para ofrecer a sus aplicaciones un acceso local y en la nube a un almacenamiento en la nube prácticamente ilimitado.

Antes de activar el dispositivo de hardware, asignó una dirección IP a su interfaz de red física. Ahora que ha activado el dispositivo e iniciado el Storage Gateway en él, debe asignar otra dirección IP a la máquina virtual de Storage Gateway que se ejecuta en el dispositivo de hardware. Para asignar una dirección IP estática a una puerta de enlace instalada en el dispositivo de hardware,

configure la dirección IP desde la consola local de la puerta de enlace para esa puerta de enlace. Las aplicaciones (como los clientes de NFS o SMB) se conectan a esta dirección IP. Puede acceder a la consola local de la puerta de enlace desde la consola del dispositivo de hardware con la opción Abrir consola de servicio.

Cómo configurar una dirección IP en su dispositivo para trabajar con las aplicaciones

1. En la consola de hardware, elija Abrir consola de servicio y, a continuación, presione `Enter` para abrir la página de inicio de sesión de la consola local de la puerta de enlace.
2. La página de inicio de sesión de la consola AWS Storage Gateway local le pide que inicie sesión para cambiar la configuración de la red y otros ajustes.

   La cuenta predeterminada es `admin` y la contraseña predeterminada es `password`.

   > **Note**
   >
   > Se recomienda cambiar la contraseña predeterminada introduciendo el número correspondiente para Consola de puerta de enlace en el menú principal Activación del dispositivo de AWS - Configuración y, a continuación, ejecutando el comando `passwd`. Para obtener información acerca de cómo ejecutar el comando, consulte Ejecución de comandos de Storage Gateway en la consola local. También puede establecer la contraseña desde la consola de Storage Gateway. Para obtener más información, consulte Ajuste de la contraseña de la consola local desde la consola de Storage Gateway.

3. La página Activación del dispositivo de AWS : Configuración incluye las siguientes opciones de menú:

   - Configuración de un proxy SOCKS o HTTP
   - Configuración de red
   - Prueba de la conectividad de red
   - Vista de una comprobación de recursos del sistema
   - Administración de la hora del sistema
   - Información sobre licencias
   - Símbolo del sistema

> **Note**
>
> Algunas opciones aparecen solo para tipos de puertas de enlace o plataformas de host específicos.

Ingrese el número correspondiente para navegar hasta la página Configuración de red.

4. Aplique alguna de las siguientes acciones para configurar la dirección IP de la puerta de enlace:

   - Para usar la dirección IP asignada por el servidor del protocolo de configuración dinámica de host (DHCP), ingrese el número correspondiente para Configurar DHCP y, a continuación, ingrese la información de configuración de DHCP válida en la página siguiente.
   - Para asignar una dirección IP estática, ingrese el número correspondiente para Configurar la IP estática y, a continuación, ingrese una dirección IP válida y la información de DNS en la página siguiente.

   > **Note**
   >
   > La dirección IP que especifique aquí debe estar en la misma subred que la dirección IP utilizada durante la activación del dispositivo de hardware.

Cómo salir de la consola local de la puerta de enlace

- Pulse la combinación de teclas `Crtl+]` (paréntesis de cierre). Aparece la consola de hardware.

> **Note**
>
> La combinación de teclas anterior es la única manera de salir de la consola local de la gateway.

Después de activar y configurar su dispositivo de hardware, este aparece en la consola. Ahora puede continuar con el procedimiento de instalación y configuración de la puerta de enlace en la consola de Storage Gateway. Para obtener instrucciones, consulte Configure su Amazon FSx File Gateway.

Eliminación del software de puerta de enlace del dispositivo de hardware

> **Note**
>
> Aviso de fin de disponibilidad: a partir del 12 de mayo de 2025, el dispositivo de AWS Storage Gateway hardware dejará de estar disponible. Los clientes actuales que dispongan del dispositivo de AWS Storage Gateway hardware pueden seguir utilizándolo y recibiendo asistencia hasta mayo de 2028. Como alternativa, puede utilizar el AWS Storage Gateway servicio para ofrecer a sus aplicaciones un acceso local y en la nube a un almacenamiento en la nube prácticamente ilimitado.

Si ya no necesita un Storage Gateway específico que haya implementado en un dispositivo de hardware, puede eliminar el software de puerta de enlace del dispositivo de hardware. Tras eliminar el software de puerta de enlace, tiene la opción de elegir implementar una nueva puerta de enlace en su lugar o eliminar el propio dispositivo de hardware de la consola de Storage Gateway. Para eliminar el software de la gateway de su dispositivo de hardware, realice el siguiente procedimiento.

Cómo eliminar una puerta de enlace de un dispositivo de hardware

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Elija Hardware en el panel de navegación situado en la parte izquierda de la página de la consola y, a continuación, elija el Nombre del dispositivo de hardware del que desea eliminar el software de la puerta de enlace.
3. En el menú desplegable Acciones, elija Eliminar puerta de enlace.

   Aparece el cuadro de diálogo de confirmación.
4. Compruebe que desea eliminar el software de la puerta de enlace del dispositivo de hardware especificado, escriba la palabra `remove` en el cuadro de confirmación.
5. Elija Eliminar para eliminar permanentemente el software de la puerta de enlace.

   > **Note**
   >
   > Después de eliminar el software de la puerta de enlace, no podrá deshacer la acción. En determinados tipos de gateway, puede perder datos tras su eliminación, sobre todo

datos almacenados. Para obtener más información sobre la eliminación de una gateway, consulte Eliminación de la puerta de enlace y eliminación de los recursos asociados.

Al eliminar una puerta de enlace, no se elimina el dispositivo de hardware de la consola. El dispositivo de hardware permanece para futuras implementaciones de gateway.

Eliminar el dispositivo de hardware AWS Storage Gateway

> **Note**
>
> Aviso de fin de disponibilidad: a partir del 12 de mayo de 2025, el dispositivo de AWS Storage Gateway hardware dejará de estar disponible. Los clientes actuales que dispongan del dispositivo de AWS Storage Gateway hardware pueden seguir utilizándolo y recibiendo asistencia hasta mayo de 2028. Como alternativa, puede utilizar el AWS Storage Gateway servicio para ofrecer a sus aplicaciones un acceso local y en la nube a un almacenamiento en la nube prácticamente ilimitado.

Si ya no necesita un dispositivo de hardware AWS Storage Gateway que ya haya activado, puede eliminarlo por completo de su AWS cuenta.

> **Note**
>
> Para mover el dispositivo a una AWS cuenta diferente o Región de AWS, primero debe eliminarlo mediante el siguiente procedimiento y, a continuación, abrir el canal de soporte y el contacto de la puerta de enlace Soporte para realizar un restablecimiento parcial. Para obtener más información, consulte activar el Soporte acceso para ayudar a solucionar los problemas de la puerta de enlace alojada en las instalaciones.

Cómo eliminar el dispositivo de hardware

1. Si ha instalado una puerta de enlace en el dispositivo de hardware, primero debe eliminar la puerta de enlace antes de eliminar el dispositivo. Para obtener instrucciones sobre cómo eliminar una puerta de enlace de su dispositivo de hardware, consulte Eliminación del software de puerta de enlace del dispositivo de hardware.

2. En la página Hardware de la consola de Storage Gateway, elija el dispositivo de hardware que desee eliminar.
3. En Actions (Acciones), elija Delete appliance (Eliminar dispositivo). Aparece el cuadro de diálogo de confirmación.
4. Compruebe que desea eliminar el dispositivo de hardware especificado, escriba la palabra eliminar en el cuadro de confirmación y seleccione Eliminar.

   Cuando se elimina el dispositivo de hardware, todos los recursos asociados a la puerta de enlace que están instalados en el dispositivo se eliminan, pero los datos existentes en el dispositivo de hardware no se eliminan.

Creación de la puerta de enlace

Las secciones de información general de esta página proporcionan una sinopsis de alto nivel de cómo funciona el proceso de creación de Storage Gateway. Para conocer step-by-step los procedimientos para crear un tipo específico de puerta de enlace mediante la consola Storage Gateway, consulte los temas siguientes:

- Creación y activación de una puerta de enlace de archivo de Amazon S3
- Crear y activar un Amazon FSx File Gateway
- Creación y activación de una puerta de enlace de cinta
- Creación y activación de una puerta de enlace de volumen

> **Important**
>
> 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.

Descripción general: activación de una puerta de enlace

La activación de la puerta de enlace implica configurar la puerta de enlace AWS, conectarla a ella, revisar la configuración y activarla.

Configuración de una puerta de enlace

Para configurar la Storage Gateway, primero debe elegir el tipo de puerta de enlace que desea crear y la plataforma host en la que ejecutará el dispositivo virtual de puerta de enlace. A continuación, descargue la plantilla del dispositivo virtual de puerta de enlace para la plataforma que elija e impleméntela en su entorno en las instalaciones. También puede implementar su Storage Gateway como un dispositivo de hardware físico que solicite a su distribuidor preferido o como una instancia de Amazon EC2 en AWS su entorno de nube. Al implementar el dispositivo de puerta de enlace, está asignando un espacio en disco físico local al host de virtualización.

Connect to AWS

El siguiente paso es conectar la puerta de enlace a AWS. Para ello, primero debe elegir el tipo de punto final de servicio que desea utilizar para las comunicaciones entre el dispositivo virtual de puerta de enlace y AWS los servicios en la nube. A este punto de conexión se puede acceder desde la Internet pública o solo desde su Amazon VPC, donde tiene el control total de la configuración de seguridad de la red. A continuación, especifique la dirección IP de la puerta de enlace o su clave de activación, que puede obtener conectándose a la consola local del dispositivo de puerta de enlace.

Revisión y activación

En este punto, podrá revisar la puerta de enlace y las opciones de conexión que elija, y hacer los cambios necesarios. Cuando todo esté configurado como desea, puede activar la puerta de enlace. Antes de empezar a utilizar la puerta de enlace activada, deberá configurar ciertos ajustes adicionales y crear sus recursos de almacenamiento.

Descripción general: configuración de la puerta de enlace

Después de activar Storage Gateway, debe configurar ciertos ajustes adicionales. En este paso, asignará el almacenamiento físico que aprovisionó en la plataforma host de la puerta de enlace para que el dispositivo de puerta de enlace lo utilice como caché o búfer de carga. Luego, configura los ajustes para ayudar a monitorear el estado de su puerta de enlace mediante Amazon CloudWatch Logs y CloudWatch alarmas, y agrega etiquetas para ayudar a identificar la puerta de enlace, si lo desea. Antes de empezar a utilizar la puerta de enlace activada y configurada, deberá crear sus recursos de almacenamiento.

Descripción general: recursos de almacenamiento

Después de activar y configurar Storage Gateway, debe crear recursos de almacenamiento en la nube para utilizarla. Según el tipo de puerta de enlace que haya creado, utilizará la consola de Storage Gateway para crear volúmenes, cintas o recursos compartidos de FSx archivos de Amazon S3 o Amazon para asociarlos a ella. Cada tipo de puerta de enlace utiliza sus recursos respectivos para emular el tipo de infraestructura de almacenamiento de red correspondiente y transfiere los datos que escriba en ella a la nube de AWS .

Creación de un sistema de archivos de Amazon FSx para Windows File Server

Para crear un Amazon FSx File Gateway en AWS Storage Gateway, el primer paso es crear un sistema de archivos Amazon FSx para Windows File Server. Si ya has creado un sistema de FSx archivos de Amazon, ve al siguiente paso,Crear y activar un Amazon FSx File Gateway.

> **Note**
>
> Se aplican las siguientes limitaciones al escribir en un sistema de FSx archivos de Amazon desde una pasarela de FSx archivos:
>
> - FSx El sistema de archivos de Amazon y FSx File Gateway deben ser propiedad de la misma AWS cuenta y estar ubicados en la misma AWS región.
> - Cada puerta de enlace puede admitir cinco sistemas de archivos adjuntos. Al asociar un sistema de archivos, la consola de Storage Gateway le notifica si la puerta de enlace seleccionada está al máximo de su capacidad. En ese caso, debe elegir una puerta de enlace diferente o desasociar un sistema de archivos para poder asociar otro.
> - FSx File Gateway admite cuotas de almacenamiento temporal (emite advertencias cuando los usuarios sobrepasan sus límites de datos), pero no admite cuotas fijas (impone límites de datos al denegar el acceso de escritura). Se admiten cuotas flexibles para todos los usuarios, excepto para el usuario FSx administrador de Amazon. Para obtener más información sobre cómo configurar las cuotas de almacenamiento, consulte Cuotas de almacenamiento en la Guía del usuario de Amazon FSx para Windows File Server.
> - No recomendamos utilizar el Sistema de archivos distribuido (DFS) de Microsoft para redirigir a los usuarios al sistema de FSx archivos de Amazon a través de FSx File Gateway. En su lugar, configure DFS para que redirija directamente al sistema de FSx archivos de Amazon tal y Nube de AWS como se describe en Agrupación de varios sistemas de archivos con espacios de nombres DFS de la Guía del usuario del servidor de archivos de FSx Amazon para Windows.
> - Algunas operaciones con archivos en la puerta de enlace de FSx archivos, como cambiar el nombre de las carpetas de nivel superior o los cambios de permisos, pueden provocar varias operaciones con archivos y provocar una gran I/O carga de trabajo en el sistema de archivos del servidor de archivos FSx de Windows. Si el sistema de archivos no tiene suficientes recursos de rendimiento para su carga de trabajo, es posible que elimine

las instantáneas, ya que da prioridad a la disponibilidad para la retención continua de instantáneas por I/O encima de la histórica.

En la FSx consola de Amazon, consulta la página Supervisión y rendimiento para ver si tu sistema de archivos está insuficientemente aprovisionado. Si es así, puede cambiar a un almacenamiento en SSD, aumentar la capacidad de rendimiento o aumentar las IOPS en SSD para gestionar su carga de trabajo.

Para crear un sistema de archivos FSx para Windows File Server

1. Abre Consola de administración de AWS at https://console.aws.amazon.com/fsx/home/ y elige la región en la que deseas crear tu puerta de enlace.
2. Siga las instrucciones de Introducción a Amazon FSx en la Guía del usuario de Amazon FSx para Windows File Server.

Crear y activar un Amazon FSx File Gateway

En esta sección, encontrará instrucciones sobre cómo crear, implementar y activar una puerta de enlace de archivo en AWS Storage Gateway.

Temas

- Configurar un Amazon FSx File Gateway
- Conecta tu Amazon FSx File Gateway a AWS
- Revisa la configuración y activa tu Amazon FSx File Gateway
- Configure su Amazon FSx File Gateway

Configurar un Amazon FSx File Gateway

Para configurar un nuevo FSx File Gateway

1. Abre Consola de administración de AWS at https://console.aws.amazon.com/storagegateway/home/ y elige el Región de AWS lugar donde quieres crear tu puerta de enlace.
2. Seleccione Crear puerta de enlace para abrir la página Configurar puerta de enlace.
3. En la sección Configuración de puerta de enlace, realice lo siguiente:

a. En Nombre de la puerta de enlace, introduzca un nombre para la puerta de enlace. Tras crear la puerta de enlace, puede buscar este nombre para encontrar la puerta de enlace en las páginas de la lista de la consola de AWS Storage Gateway .

b. En Zona horaria de la puerta de enlace, elija la zona horaria local de la parte del mundo en la que desee implementar la puerta de enlace.

4. En la sección Opciones de puerta de enlace, para el tipo de puerta de enlace, elija Amazon FSx File Gateway.

5. En la sección Opciones de plataforma, haga lo siguiente:

a. Para Plataforma host, elija la plataforma en la que desea implementar la puerta de enlace. A continuación, siga las instrucciones específicas de la plataforma que se muestran en la página de la consola de Storage Gateway para configurar la plataforma host. Puede elegir entre las siguientes opciones:

- VMware ESXi— Descargue, implemente y configure la máquina virtual de puerta de enlace mediante VMware ESXi.
- Microsoft Hyper-V: descargue, implemente y configure la máquina virtual de puerta de enlace mediante Microsoft Hyper-V.
- Linux KVM: descargue, implemente y configure la máquina virtual de puerta de enlace mediante máquina virtual basada en el kernel (KVM) de Linux. Consulte el aws-storage-gateway archivo.xml proporcionado para ver las configuraciones de arranque sugeridas. Se requiere el modo de arranque UEFI con el arranque seguro desactivado (loader_secure=no) para File Gateway 2.x, Volume Gateway 3.x y Tape Gateway 3.x.
- Amazon EC2: configure y lance una instancia de Amazon EC2 para alojar la puerta de enlace.
- Dispositivo de hardware: solicite un dispositivo de hardware físico dedicado para alojar su puerta de enlace. AWS

b. En Confirmar la configuración de la puerta de enlace, seleccione la casilla de verificación para confirmar que ha realizado los pasos de implementación de la plataforma host que ha elegido. Este paso no se aplica a la plataforma host del dispositivo de hardware.

6. Ahora que su puerta de enlace está configurada, debe elegir cómo desea que se conecte y con qué se comunique AWS. Elija Paso siguiente para continuar.

Conecta tu Amazon FSx File Gateway a AWS

Para conectar un nuevo FSx File Gateway a AWS

1. Si aún no lo ha hecho, complete el procedimiento descrito en Configurar un Amazon FSx File Gateway. Cuando haya terminado, seleccione Siguiente para abrir la AWS página Conectar a en la AWS Storage Gateway consola.
2. En la sección Opciones de punto final, para Punto final de servicio, elija el tipo de punto final con el que se comunicará su puerta de enlace AWS. Puede elegir entre las siguientes opciones:

   - Acceso público: su puerta de enlace se comunica AWS a través de la Internet pública. Si selecciona esta opción, utilice la casilla de verificación del Punto de conexión habilitado para el Estándar federal de procesamiento de información (FIPS) para especificar si la conexión debe cumplir los estándares federales de procesamiento de información (FIPS).

     > **Note**
     >
     > Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un terminal compatible con FIPS. Para obtener más información, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.
     > El punto de conexión de servicio de FIPS solo está disponible en algunas Regiones de AWS . Para obtener más información, consulte Puntos de conexión y cuotas de AWS Storage Gateway en la Referencia general de AWS.

   - Alojado en VPC: su puerta de enlace se comunica AWS a través de una conexión privada con su nube privada virtual (VPC), lo que le permite controlar la configuración de la red. Si selecciona esta opción, debe especificar un punto de conexión de VPC existente eligiendo su ID de punto de conexión de VPC en la lista desplegable. También puede proporcionar el nombre del sistema de nombres de dominio (DNS) o la dirección IP del punto de conexión de VPC.
3. En la sección Opciones de conexión de puerta de enlace, en Opciones de conexión, elija cómo identificar la puerta de enlace en AWS. Puede elegir entre las siguientes opciones:

   - Dirección IP: indique la dirección IP de la puerta de enlace en el campo correspondiente. Esta dirección IP debe ser pública o accesible desde su red actual y debe poder conectarse a ella desde su navegador web.

Puede obtener la dirección IP de la puerta de enlace iniciando sesión en la consola local de la puerta de enlace en su cliente hipervisor o copiándola en la página de detalles de la instancia de Amazon EC2.

- Clave de activación: proporcione la clave de activación de la puerta de enlace en el campo correspondiente. Puede generar una clave de activación mediante la consola local de la puerta de enlace. Si la dirección IP de la puerta de enlace no está disponible, elija esta opción.

4. Ahora que ha elegido cómo quiere que se conecte su puerta de enlace AWS, debe activarla. Elija Paso siguiente para continuar.

Revisa la configuración y activa tu Amazon FSx File Gateway

Para activar un nuevo FSx File Gateway

1. Si aún no lo ha hecho, complete los procedimientos que se describen en los siguientes temas:

   - Configurar un Amazon FSx File Gateway
   - Conecta tu Amazon FSx File Gateway a AWS

   Cuando haya terminado, elija Siguiente para abrir la página Revisar y activar en la consola de AWS Storage Gateway .
2. Revise los detalles iniciales de la puerta de enlace de cada sección de la página.
3. Si una sección contiene errores, elija Editar para volver a la página de configuración correspondiente y realizar los cambios.

   > **Important**
   >
   > No puede modificar las opciones de la puerta de enlace ni la configuración de la conexión después de activar la puerta de enlace.

4. Ahora que ha activado la puerta de enlace, debe realizar la primera configuración para asignar los discos de almacenamiento local y configurar el registro. Elija Paso siguiente para continuar.

Configure su Amazon FSx File Gateway

Para realizar la configuración por primera vez en una nueva FSx puerta de enlace de archivos

1. Si aún no lo ha hecho, complete los procedimientos que se describen en los siguientes temas:

   - Configurar un Amazon FSx File Gateway
   - Conecta tu Amazon FSx File Gateway a AWS
   - Revisa la configuración y activa tu Amazon FSx File Gateway

   Cuando haya terminado, seleccione Siguiente para abrir la página Configurar puerta de enlace en la consola de AWS Storage Gateway .
2. En la sección Configurar almacenamiento, use las listas desplegables para asignar al menos un disco local con una capacidad mínima de 150 gibibytes (GiB) a la memoria caché. Los discos locales que se enumeran en esta sección corresponden al almacenamiento físico que aprovisionó en su plataforma host.
3. En la sección del grupo de CloudWatch registros, elige cómo configurar Amazon CloudWatch Logs para supervisar el estado de tu puerta de enlace. Puede elegir entre las siguientes opciones:

   - Crear un nuevo grupo de registro: configure un nuevo grupo de registro para supervisar la puerta de enlace.
   - Uso de un grupo de registro existente: elija un grupo de registro existente en el menú desplegable correspondiente.
   - Desactiva el registro: no utilices Amazon CloudWatch Logs para supervisar tu puerta de enlace.

   > **Note**
   >
   > Para recibir los registros de estado de Storage Gateway, los siguientes permisos deben estar presentes en la política de recursos del grupo de registros. *highlighted section*Sustitúyala por la información ResourceArn del grupo de registros específico para su implementación.
   >
   > ```
   > "Sid": "AWSLogDeliveryWrite20150319",
   >       "Effect": "Allow",
   > ```

```
      "Principal": {
        "Service": [
          "delivery.logs.amazonaws.com"
        ]
      },
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:eu-west-1:1234567890:log-group:/foo/bar:log-stream:*"
```

El elemento “Recurso” solo es necesario si desea que los permisos se apliquen de forma explícita a un grupo de registros individual.

4. En la sección de CloudWatch alarmas, elige cómo configurar CloudWatch las alarmas de Amazon para que te notifiquen cuando las métricas de tu pasarela se desvíen de los límites definidos. Puede elegir entre las siguientes opciones:

   - Cree las alarmas recomendadas por Storage Gateway: cree todas las CloudWatch alarmas recomendadas automáticamente al crear la puerta de enlace. Para obtener más información sobre las alarmas recomendadas, consulte Descripción de CloudWatch las alarmas.

     > **Note**
     >
     > Esta función requiere permisos CloudWatch de política que no se conceden automáticamente como parte de la política de acceso total preconfigurada de Storage Gateway. Asegúrese de que su política de seguridad conceda los siguientes permisos antes de intentar crear CloudWatch las alarmas recomendadas:
     >
     > - `cloudwatch:PutMetricAlarm`: crear alarmas
     > - `cloudwatch:DisableAlarmActions`: desactivar acciones de alarma
     > - `cloudwatch:EnableAlarmActions`: activar acciones de alarma
     > - `cloudwatch:DeleteAlarms`: eliminar alarmas

   - Cree una alarma personalizada: configure una nueva CloudWatch alarma para recibir notificaciones sobre las métricas de su puerta de enlace. Selecciona Crear alarma para definir las métricas y especificar las acciones de alarma en la CloudWatch consola de Amazon.

Para obtener instrucciones, consulta Uso de CloudWatch alarmas de Amazon en la Guía del CloudWatch usuario de Amazon.

- Sin alarma: no utilices CloudWatch las alarmas para recibir notificaciones sobre las métricas de tu puerta de enlace.

5. (Opcional) En la sección Etiquetas, seleccione Agregar etiqueta nueva y, a continuación, introduzca un par clave-valor que distinga mayúsculas de minúsculas para ayudarle a buscar y filtrar la puerta de enlace en las páginas de la lista de la consola de AWS Storage Gateway . Repita este paso para agregar todas las etiquetas que necesite.
6. (Opcional) En la sección Verificar la configuración de VMware alta disponibilidad, si la puerta de enlace está implementada en un VMware host que forma parte de un clúster de VMware alta disponibilidad (HA), elija Verificar VMware la alta disponibilidad para comprobar si la configuración de alta disponibilidad funciona correctamente.

   > **Note**
   >
   > Esta sección solo aparece para las puertas de enlace que se ejecutan en la plataforma VMware host.
   > Este paso no es necesario para completar el proceso de configuración de la puerta de enlace. Puede comprobar la configuración de alta disponibilidad de la puerta de enlace en cualquier momento. La verificación tarda unos minutos y reinicia la máquina virtual (VM) de Storage Gateway.

7. Elija Configurar para terminar de crear la puerta de enlace.

   Para comprobar el estado de la nueva puerta de enlace, búsquela en la página Información general sobre la puerta de enlace de la consola de AWS Storage Gateway .

Ahora que ha creado la puerta de enlace, debe asociar un sistema de archivos para utilizarla. Para obtener instrucciones, consulte Adjuntar un sistema de archivos de Amazon FSx for Windows File Server.

Si no tienes un sistema de FSx archivos de Amazon existente para adjuntar, debes crear uno. Para obtener instrucciones, consulta Cómo empezar a usar Amazon FSx.

Activación de una puerta de enlace en una nube privada virtual

Puede crear una conexión privada entre su dispositivo de puerta de enlace en las instalaciones y una infraestructura de almacenamiento basada en la nube. Puede usar esta conexión para activar su puerta de enlace y configurarla para transferir datos a los servicios AWS de almacenamiento sin comunicarse a través de la Internet pública. Con el servicio Amazon VPC, puede lanzar AWS recursos, incluidos los puntos finales de la interfaz de red privada, en una nube privada virtual (VPC) personalizada. Una VPC le permite controlar la configuración de red, como el intervalo de direcciones IP, las subredes, las tablas de enrutamiento y las puertas de enlace de red. Para obtener más información VPCs, consulte ¿Qué es Amazon VPC? en la Guía del usuario de Amazon VPC.

Para activar la puerta de enlace en una VPC, utilice la consola de Amazon VPC para crear un punto de conexión de VPC para Storage Gateway y obtenga el ID del punto de conexión de VPC. A continuación, especifique este ID de punto de conexión de VPC al crear y activar la puerta de enlace. Para obtener más información, consulte Connect your Amazon FSx File Gateway AWS a.

Para configurar su puerta de enlace de FSx archivos para transferir datos a través de la VPC, debe establecer una VPN o un AWS DirectConnect enlace entre la VPC del servidor de archivos de Amazon FSx para Windows y la red en la que está desplegada la puerta de enlace.

> **Note**
>
> Debe activar la puerta de enlace en la misma región en la que creó el punto de conexión de VPC para Storage Gateway.

Crear un punto de conexión de VPC para Storage Gateway

Siga estas instrucciones para crear un punto de enlace de la VPC. Si ya tiene un punto de conexión de VPC para Storage Gateway, puede usarlo.

Cómo crear un punto de conexión de VPC para Storage Gateway

1. Inicie sesión en la consola de Amazon VPC Consola de administración de AWS y ábrala en. https://console.aws.amazon.com/vpc/
2. En el panel de navegación, elija Endpoints (Puntos de enlace) y, a continuación, elija Create Endpoint (Crear punto de enlace).
3. En la página Crear punto de conexión, elija Servicios de AWS en Categoría de servicio.

4. En Nombre de servicio, elija `com.amazonaws.region.storagegateway`. Por ejemplo, `com.amazonaws.us-east-2.storagegateway`.
5. En VPC, elija su VPC y anote sus zonas de disponibilidad y subredes.
6. Compruebe que la opción Habilitar nombre de DNS no esté seleccionada.
7. En Security group (Grupo de seguridad), elija el grupo de seguridad que desea utilizar para su VPC. Puede aceptar el grupo de seguridad predeterminado. Compruebe que los siguientes puertos TCP están permitidos en su grupo de seguridad:

   - TCP 443
   - TCP 1026
   - TCP 1027
   - TCP 1028
   - TCP 1031
   - TCP 2222
8. Seleccione Crear punto de conexión. El estado inicial del punto de enlace espending (pendiente). Cuando se crea el punto de enlace, anote el ID del punto de enlace de la VPC que acaba de crear.
9. Cuando se cree el punto de enlace, elija Endpoints (Puntos de enlace) y, a continuación, elija el nuevo punto de enlace de la VPC.
10. En la pestaña Detalles del punto de conexión de Storage Gateway seleccionado, en Nombres de DNS, utilice el primer nombre de DNS que no especifique una zona de disponibilidad. El nombre de DNS debería ser similar al siguiente ejemplo: `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

Ahora que ha creado un punto de conexión de VPC, puede crear su puerta de enlace. Para obtener más información, consulte Crear y activar un Amazon FSx File Gateway.

Para obtener información sobre cómo obtener una clave de activación, consulte Obtención de una clave de activación para la puerta de enlace.

Configurar ajustes de acceso de dominio de Microsoft Active Directory

En este paso, configurará los ajustes de acceso para unir su Amazon FSx File Gateway a un dominio de Microsoft Active Directory.

Cómo configurar los ajustes de Active Directory

1. En la consola Storage Gateway, seleccione sistemas de FSx archivos en el menú de navegación.
2. Seleccione Adjuntar sistema de FSx archivos.
3. En la página Confirmar puerta de enlace, elija la puerta de enlace que desee unir a su dominio de Active Directory en el menú desplegable.

   Si no tiene una puerta de enlace de archivo de FSx, cree una. Asegúrese de que la puerta de enlace pueda resolver el nombre del controlador de dominio de Active Directory. Para obtener información, consulte Requisitos previos.
4. Introduzca valores para la configuración de Active Directory:

   > **Note**
   >
   > Si la puerta de enlace ya está unida a un dominio, no es necesario que vuelva a unirla. Continúe con el paso siguiente.

   - En el campo Nombre de dominio, introduzca el nombre de dominio de Active Directory que desea utilizar.
   - En el campo Usuario de dominio, introduzca el nombre de usuario del usuario de Active Directory que desee usar para unir la puerta de enlace al dominio. Este usuario debe tener los permisos necesarios. Para obtener más información, consulte Requisitos de permiso de la cuenta de servicio de Active Directory.
   - En el campo Contraseña de dominio, escriba la contraseña para el usuario.
   - En el campo Unidad organizativa (opcional), puede especificar la unidad organizativa a la que pertenece Active Directory.

> **Note**
>
> Si deja este campo en blanco, al unirse a un dominio se crea una cuenta de equipo de Active Directory en el contenedor predeterminado del equipo (que no es una unidad organizativa), con el ID de puerta de enlace de la puerta de enlace como nombre de cuenta (por ejemplo, SGW-1234ADE). No es posible personalizar el nombre de esta cuenta.
>
> Si su entorno de Active Directory requiere que configure previamente las cuentas para facilitar el proceso de unión al dominio, tendrá que crear esta cuenta con antelación.
>
> Si su entorno de Active Directory tiene una unidad organizativa designada para los nuevos objetos de equipo, debe especificarla al unirse al dominio.

- Introduzca un valor para los Controladores de dominio (opcional).

5. Seleccione Siguiente para abrir la página del sistema Adjuntar FSx archivos.

Paso siguiente

Adjunte un sistema de archivos de Amazon FSx para Windows File Server

Adjunte un sistema de archivos de Amazon FSx para Windows File Server

Debe disponer de un sistema de archivos FSx para Windows File Server antes de poder adjuntarlo a una pasarela de FSx archivos. Si no dispone de un sistema de archivos, debe crear uno. Para obtener instrucciones, consulta el paso 1: Crea tu sistema de archivos en la Guía del usuario del servidor de archivos de Amazon FSx para Windows.

El siguiente paso es adjuntar un sistema de FSx archivos de Amazon a la pasarela. Al adjuntar un sistema de FSx archivos de Amazon, todos los archivos compartidos del sistema de archivos se ponen a disposición de Amazon FSx File Gateway (FSx File Gateway) para que los monte.

> **Note**
>
> Se aplican las siguientes limitaciones al escribir en un sistema de FSx archivos de Amazon desde Amazon FSx File Gateway:
>
> - Su sistema de FSx archivos de Amazon y su FSx File Gateway deben ser propiedad de la misma persona Cuenta de AWS y estar ubicados en el mismo lugar Región de AWS.
> - Cada puerta de enlace puede admitir hasta cinco sistemas de archivos asociados. Al asociar un sistema de archivos, la consola de Storage Gateway le notifica si la puerta de enlace seleccionada tiene capacidad. En ese caso, debe elegir una puerta de enlace diferente o desasociar un sistema de archivos para poder asociar otro.
> - FSx File Gateway admite cuotas de almacenamiento temporal (que le avisan cuando los usuarios sobrepasan sus límites de datos), pero no admite cuotas estrictas (que imponen límites de datos al denegar el acceso de escritura). Se admiten cuotas flexibles para todos los usuarios, excepto para el usuario FSx administrador de Amazon. Para obtener más información sobre cómo configurar las cuotas de almacenamiento, consulta Cuotas de almacenamiento en la Guía del FSx usuario de Amazon.
> - No recomendamos utilizar el Sistema de archivos distribuido (DFS) de Microsoft para redirigir a los usuarios al sistema de FSx archivos de Amazon a través de FSx File Gateway. En su lugar, configure DFS para que redirija directamente al sistema de FSx archivos de Amazon tal y Nube de AWS como se describe en Agrupación de varios sistemas de archivos con espacios de nombres DFS de la Guía del usuario del servidor de archivos de FSx Amazon para Windows.

Para adjuntar un sistema de FSx archivos de Amazon

1. En la consola Storage Gateway, en la página Sistemas de FSx archivos > Adjuntar sistema de FSx archivos, complete los siguientes campos de la sección de configuración del sistema de FSx archivos:

   - Para FSx el nombre del sistema de archivos, elija el sistema de archivos que desee adjuntar en la lista desplegable.
   - En el caso de la dirección IP del punto final local, introduzca la dirección IP de la puerta de enlace que los clientes utilizarán para buscar los archivos compartidos en el sistema de FSx archivos.

   > **Note**
   >
   > - Debe especificar una dirección IP para cada sistema de archivos asociado a la puerta de enlace.
   > - En el caso de EC2 las puertas de enlace de Amazon, puede especificar la dirección IP privada de la EC2 instancia, a menos que ya la esté utilizando otro sistema de archivos, en cuyo caso debe añadir una nueva dirección privada a la puerta de enlace y, a continuación, reiniciarla. Para obtener más información, consulta Múltiples direcciones IP en la Guía del EC2 usuario de Amazon.
   > - Para las puertas de enlace en las instalaciones, puede especificar la dirección IP de la interfaz de red principal (estática o DHCP), a menos que ya la esté utilizando un sistema de archivos diferente, en cuyo caso debe proporcionar una dirección IP diferente de la misma subred que la interfaz principal, que estará disponible como IP virtual. No utilice una dirección IP asignada a ninguna interfaz de red que no sea la principal.

2. En la sección Configuración de la cuenta de servicio, proporciona las credenciales de inicio de sesión de la cuenta de servicio asociadas al sistema de FSx archivos de Amazon.

   > **Note**
   >
   > Esta cuenta de servicio debe tener los privilegios de Operador de Backup del servicio Active Directory asociado a sus sistemas de FSx archivos de Amazon o tener permisos equivalentes.

> **Important**
>
> Para garantizar que existen permisos suficientes para los archivos, las carpetas y los metadatos de archivos, le recomendamos que convierta la cuenta de servicio en miembro del grupo de administradores del sistema de archivos.
> Si utiliza AWS Directory Service Microsoft Active Directory con Amazon FSx for Windows File Server, la cuenta de servicio debe ser miembro del grupo de FSx administradores AWS delegados.
> Si utiliza un Active Directory autogestionado con Amazon FSx for Windows File Server, le recomendamos que la cuenta de servicio sea miembro del grupo de administradores de sistemas de archivos delegados personalizados que especificó para la administración del sistema de archivos al crear el sistema de FSx archivos de Amazon.
> Si optó por no crear un grupo de administradores de sistemas de archivos delegado personalizado al crear el sistema de FSx archivos de Amazon, el grupo predeterminado es Domain Admins. Si bien puede convertir la cuenta de servicio en miembro de este grupo, no se recomienda hacerlo como práctica recomendada.
> Para obtener más información, consulta Cómo delegar privilegios en tu cuenta de FSx servicio de Amazon en la Guía del usuario de Amazon FSx para Windows File Server.

3. En la sección Registros de auditoría, selecciona Grupos de registros existentes y elige el registro que deseas usar para monitorear el acceso a tu sistema de FSx archivos de Amazon. Puede crear uno nuevo. Si no desea monitorear el sistema, elija Deshabilitar registro.
4. Para Configuración de actualización de caché automatizada, elija Establecer intervalo de actualización y especifique un intervalo entre 5 minutos y 30 días.
5. (Opcional) En la sección Etiquetas, elija Agregar etiqueta nueva para agregar una o más claves y un valor para etiquetar los ajustes.
6. Elija Next (Siguiente) y revise la configuración. Para cambiar la configuración, puede elegir Editar en cada sección.
7. Cuando haya terminado, seleccione Finish.

Paso siguiente

Monta y usa tu recurso compartido de FSx archivos de Amazon

Monta y usa tu recurso compartido de FSx archivos de Amazon

Antes de montar tu recurso compartido de archivos en el cliente, espera a que el estado del sistema de FSx archivos de Amazon cambie a Disponible. Una vez montado el recurso compartido de archivos, puede empezar a utilizar su Amazon FSx File Gateway (FSx File Gateway).

Temas

- Montar el recurso compartido de archivos SMB en el cliente
- Pruebe su puerta de enlace FSx de archivos

Montar el recurso compartido de archivos SMB en el cliente

En este paso, monte el recurso compartido de archivos SMB y asígnelo a una unidad a la que el cliente pueda obtener acceso. La sección de puerta de enlace de archivo de la consola muestra los comandos de montaje compatibles que se pueden utilizar para los clientes de SMB. A continuación, se muestran algunas opciones adicionales para probar.

Puede utilizar varios métodos para montar recursos compartidos de archivos SMB, entre los que se incluyen los siguientes:

- El comando `net use`: no se conserva cuando el sistema se reinicia, a menos que se utilice el conmutador `/persistent:(yes:no)`.
- La utilidad de línea de comandos `CmdKey`: crea una conexión persistente con un recurso compartido de archivos SMB montado que permanece después de un reinicio.
- Una unidad de red asignada en el explorador de archivos: configura el recurso compartido de archivos montado para volver a conectarse al iniciar sesión y solicitar la introducción de las credenciales de red.
- PowerShell script: puede ser persistente y puede ser visible o invisible para el sistema operativo mientras está montado.

> **Note**
>
> Si es un usuario de Microsoft Active Directory, póngase en contacto con el administrador para asegurarse de que dispone de acceso al recurso compartido de archivos SMB antes de montarlo en el sistema local.
> Amazon FSx File Gateway no admite el bloqueo de SMB ni los atributos extendidos de SMB.

Cómo montar un recurso compartido de archivos SMB para los usuarios de Active Directory mediante el comando net use

1. Asegúrese de que tiene acceso al recurso compartido de archivos SMB antes de montarlo en el sistema local.
2. Para los clientes de Microsoft Active Directory, escriba el siguiente comando en el símbolo del sistema:

   ```
   net use [WindowsDriveLetter]: \\[Gateway IP Address]\[Name of the share on the FSx file system]
   ```

Para montar un recurso compartido de archivos SMB en Windows mediante CmdKey

1. Pulse la tecla de Windows y escriba **cmd** para ver el elemento de menú del símbolo del sistema.
2. Abra el menú contextual (haga clic con el botón derecho) del símbolo del sistema y elija Ejecutar como administrador.
3. Introduzca el siguiente comando:

   ```
   C:\>cmdkey /add:[Gateway VM IP address] /user:[DomainName]\[UserName] /pass:[Password]
   ```

> **Note**
>
> Al montar recursos compartidos de archivos, puede que sea preciso volver a montar el recurso compartido de archivos después de reiniciar el cliente.

Cómo montar un recurso compartido de archivos SMB mediante el explorador de archivos de Windows

1. Pulse la tecla de Windows y escriba **`File Explorer`** en el cuadro de búsqueda de Windows o pulse **`Win+E`**.
2. En el panel de navegación, elija Este PC. A continuación, en la pestaña Equipo, seleccione Asignar unidad de red.
3. En el cuadro de diálogo Asignar unidad de red, elija una letra de unidad en Unidad.
4. En Carpeta, escriba **`\\`*`[File Gateway IP]`*`\`*`[SMB File Share Name]`** o elija Examinar para seleccionar el recurso compartido de archivos SMB desde el cuadro de diálogo.
5. (Opcional) Seleccione Reconnect at sign-up si desea que el punto de montaje se conserve tras los reinicios.
6. (Opcional) Seleccione Conectar con otras credenciales si desea que el usuario introduzca las credenciales de inicio de sesión de Active Directory o la contraseña de la cuenta de usuario invitado.
7. Elija Finish para finalizar el punto de montaje.

Pruebe su puerta de enlace FSx de archivos

Puede copiar archivos y directorios en la unidad asignada. Los archivos se cargan automáticamente en su sistema FSx de archivos del servidor de archivos de Windows.

Para subir archivos desde tu cliente de Windows a Amazon FSx

1. En el cliente Windows, vaya a la unidad en la que montó el sistema de archivos. El nombre de la unidad va precedido del nombre del sistema de archivos.
2. Copie los archivos o un directorio en la unidad.

> **Note**
>
> Las puertas de enlace de archivo no admiten la creación de enlaces físicos ni simbólicos en un recurso compartido de archivos.

Administración de los recursos de Amazon FSx File Gateway

En las siguientes secciones se proporciona información sobre cómo administrar los recursos de Amazon FSx File Gateway (FSx File Gateway), incluida la conexión y desconexión de los sistemas de FSx archivos de Amazon y la configuración de los ajustes de Microsoft Active Directory.

Temas

- Descripción del estado de la puerta de enlace
- Descripción de los estados del sistema de archivos
- Edite la información básica de una pasarela de FSx archivos
- Establecer un nivel de seguridad para la puerta de enlace
- Edición de la configuración de Active Directory para n FSx File Gateway
- Edición de la configuración de un sistema de FSx archivos de Amazon
- Separar un sistema de FSx archivos de Amazon

Descripción del estado de la puerta de enlace

Cada puerta de enlace de su implementación de AWS Storage Gateway tiene un estado asociado que le indica de un vistazo cuál es el estado de la puerta de enlace. En la mayoría de los casos, el estado indica que la puerta de enlace funciona normalmente y que no se requiere ninguna intervención por parte del usuario. En ocasiones, el estado indica algún problema; en este caso, podría o no ser preciso que intervenga.

Puede ver el estado de cada puerta de enlace de su implementación en la página Puertas de enlace de la consola de Storage Gateway. El estado de la puerta de enlace aparece en la columna Estado junto al nombre de la puerta de enlace. Una puerta de enlace que funciona correctamente suele tener el estado `RUNNING`.

En la tabla siguiente, encontrará una descripción de cada estado de puerta de enlace, y si debe hacer algo según cada estado. El estado de una puerta de enlace debe ser `RUNNING` la totalidad o la mayor parte del tiempo que se esté usando.

Status	Significado
`RUNNING`	La puerta de enlace está configurada correctamente y se encuentra disponible para su uso.
`OFFLINE`	La puerta de enlace puede mostrar un estado `OFFLINE` por uno o varios de los motivos siguientes: • La puerta de enlace no puede llegar a los puntos de conexión del servicio de Storage Gateway. • La puerta de enlace se cerró inesperadamente. • La puerta de enlace tiene asociado un disco de caché que está desconectado, se ha modificado o ha fallado.

Descripción de los estados del sistema de archivos

Puede ver el estado de un sistema de archivos de un vistazo consultando su estado. Si el estado indica que el sistema de archivos funciona normalmente, no se requiere ninguna intervención por parte del usuario. Si el estado indica que hay un problema, puede investigarlo para determinar si es necesario tomar medidas.

Puede ver el estado de un sistema de archivos en la consola de Storage Gateway, en la columna Estado. Un sistema de archivos que funciona correctamente muestra el estado DISPONIBLE. Este debería ser el estado la mayoría de las veces.

En la siguiente tabla se describen los estados de los archivos compartidos, su significado y si es necesario tomar alguna medida.

Status	Significado
DISPONIBLE	El sistema de archivos está configurado correctamente y se encuentra disponible para su uso. Este es el estado estándar de un sistema de archivos que funciona correctamente.
CREAR	El sistema de archivos aún no se ha creado completamente y no está listo para su uso. El estado CREATING es transitorio. No hay que hacer nada más. Si el sistema de archivos se queda atascado en este estado,

Status	Significado
	probablemente se deba a que la máquina virtual de la puerta de enlace perdió la conexión con ella AWS.
ACTUALIZANDO	La configuración del sistema de archivos se está actualizando actualmente. El estado ACTUALIZANDO es transitorio. No hay que hacer nada más. Si un sistema de archivos se bloquea en este estado, probablemente se deba a que la máquina virtual de la puerta de enlace perdió la conexión con él AWS.
ELIMINANDO	Se está eliminando el sistema de archivos. El sistema de archivos no se elimina hasta que se hayan cargado todos los datos AWS. El estado DELETING es transitorio y no se requiere ninguna acción.
FORCE_DELETING	El sistema de archivos se está eliminando de forma forzada. El sistema de archivos se elimina inmediatamente y los datos no se cargan en él AWS. El estado FORCE_DELETING es transitorio y no se requiere ninguna acción.
ERROR	El sistema de archivos se encuentra en mal estado. Es necesario tomar medidas. Algunas causas posibles incluyen problemas con las credenciales o los privilegios de acceso, problemas de conectividad o espacio de almacenamiento insuficiente en el sistema de archivos. Cuando se resuelve el problema que ha provocado el mal estado, el archivo recupera el estado DISPONIBLE.

Edite la información básica de una pasarela de FSx archivos

Puede usar la consola Storage Gateway para editar la información básica de una puerta de enlace existente, incluidos el nombre de la puerta de enlace, la zona horaria y el grupo de CloudWatch registros.

Cómo editar la información básica de una puerta de enlace existente

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Elija Puertas de enlace y, a continuación, elija la puerta de enlace para la que desee editar la información básica.

3. En el menú desplegable Acciones, seleccione Editar información de la puerta de enlace.
4. En Nombre de la puerta de enlace, introduzca un nombre para la puerta de enlace. Puede buscar este nombre para encontrar la puerta de enlace en las páginas de la lista de la consola de Storage Gateway.

   > **Note**
   >
   > Los nombres de las puertas de enlace deben tener entre 2 y 255 caracteres y no pueden incluir una barra inclinada (\ o /).
   > Al cambiar el nombre de una puerta de enlace, se desconectarán todas CloudWatch las alarmas configuradas para monitorear la puerta de enlace. Para volver a conectar las alarmas, actualice las GatewayNamede cada alarma de la CloudWatch consola.

5. En Zona horaria de la puerta de enlace, elija la zona horaria local de la parte del mundo en la que desee implementar la puerta de enlace.
6. En Elige cómo configurar el grupo de registros, elige cómo configurar Amazon CloudWatch Logs para supervisar el estado de tu puerta de enlace. Puede elegir entre las siguientes opciones:

   - Crear un nuevo grupo de registro: configure un nuevo grupo de registro para supervisar la puerta de enlace.
   - Uso de un grupo de registro existente: elija un grupo de registro existente en el menú desplegable correspondiente.
   - Desactiva el registro: no utilices Amazon CloudWatch Logs para supervisar tu puerta de enlace.

7. Cuando termine de modificar la configuración que quiere cambiar, elija Guardar cambios.

Establecer un nivel de seguridad para la puerta de enlace

Puede configurar el nivel de seguridad SMB de su puerta de enlace de FSx archivos para especificar si la puerta de enlace debe requerir la firma del bloque de mensajes del servidor (SMB) o el cifrado SMB.

Cómo configurar el nivel de seguridad

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.

2. Elija Puertas de enlace y, a continuación, elija la puerta de enlace para la que desee editar los ajustes de SMB.
3. En el menú desplegable Acciones, elija Editar configuración de SMB y, a continuación, elija Configuración de seguridad de SMB.
4. En Security level (Nivel de seguridad) elija una de las siguientes opciones:

> **Note**
>
> Para obtener información sobre cómo configurar este ajuste mediante la AWS API, consulte Actualizar la SMBSecurity estrategia en la referencia de la AWS Storage Gateway API.
> Un nivel de seguridad más alto puede afectar al rendimiento de la puerta de enlace.

- Cifrado obligatorio: si elige esta opción, FSx File Gateway solo permite conexiones desde SMBv3 clientes que utilicen algoritmos de cifrado AES de 256 bits. No se permiten los algoritmos de 128 bits. Esta opción es recomendable para entornos que manejen información confidencial. Funciona con clientes SMB en Microsoft Windows 8, Windows Server 2012 o posterior.
- Exigir el cifrado: si elige esta opción, FSx File Gateway solo permite las conexiones desde SMBv3 clientes que tengan el cifrado activado. Se permiten algoritmos de 256 y 128 bits. Esta opción es recomendable para entornos que manejen información confidencial. Funciona con clientes SMB en Microsoft Windows 8, Windows Server 2012 o posterior.
- Forzar la firma: si elige esta opción, FSx File Gateway solo permite conexiones desde SMBv2 SMBv3 clientes que tengan activada la firma. Esta opción funciona con clientes SMB en Microsoft Windows Vista, Windows Server 2008 o posterior.

> **Note**
>
> El nivel de seguridad predeterminado de FSx File Gateway es el cifrado obligatorio.

5. Seleccione Save.

Edición de la configuración de Active Directory para n FSx File Gateway

Para usar su Microsoft Active Directory corporativo o AWS Managed Microsoft AD para el acceso autenticado por el usuario a su sistema de FSx archivos de Amazon, edite la configuración SMB de su puerta de enlace y proporcione sus credenciales de dominio de Active Directory. De este modo, la puerta de enlace puede unirse al dominio de Active Directory, lo que permite a los miembros del dominio tener acceso al sistema de archivos.

> **Note**
>
> Con Directory Service, puede crear un servicio de dominio de Active Directory alojado en. Nube de AWS
> Para utilizarla AWS Managed Microsoft AD con una puerta de enlace de Amazon EC2, debe crear la instancia de Amazon EC2 en la misma VPC que la, añadir el grupo de seguridad AWS Managed Microsoft AD_WorkspaceMembers a la instancia de Amazon EC2 y unirse al dominio de AD con las credenciales de administrador de. AWS Managed Microsoft AD
> Para obtener más información al respecto, consulte la Guía de administración. AWS Managed Microsoft ADAWS Directory Service
> Para obtener más información acerca de Amazon EC2, consulte la Documentación de Amazon Elastic Compute Cloud.

Cómo activar la autenticación con Active Directory

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Elija Puertas de enlace y, a continuación, elija la puerta de enlace para la que desee editar los ajustes de SMB.
3. En el menú desplegable Acciones, elija Editar configuración de SMB y, a continuación, elija Configuración de Active Directory.
4. En el campo Nombre de dominio, introduzca el nombre de dominio de Active Directory al que desea que se una la puerta de enlace.

   > **Note**
   >
   > Active Directory status (Estado de Active Directory) muestra Detached (Desvinculado) cuando una gateway no se ha unido nunca a un dominio.

Su cuenta de servicio de Active Directory debe tener los permisos necesarios. Para obtener más información, consulte Requisitos de permiso de la cuenta de servicio de Active Directory.

Al unirse a un dominio, se crea una cuenta de equipo de Active Directory en el contenedor predeterminado del equipo (que no es una unidad organizativa), con el ID de puerta de enlace de la puerta de enlace como nombre de cuenta (por ejemplo, SGW-1234ADE). No es posible personalizar el nombre de esta cuenta.

Si su entorno de Active Directory requiere que configure previamente las cuentas para facilitar el proceso de unión al dominio, tendrá que crear esta cuenta con antelación.

Si su entorno de Active Directory tiene una unidad organizativa designada para los nuevos objetos de equipo, debe especificarla al unirse al dominio.

Si la puerta de enlace no puede unirse a un directorio de Active Directory, intente unirse con la dirección IP del directorio mediante la operación de JoinDomainAPI.

5. En los campos Usuario del dominio y Contraseña del dominio, introduzca las credenciales de la cuenta de servicio de Active Directory que la puerta de enlace utilizará para unirse al dominio.
6. (Opcional) En el caso de una Unidad organizativa (UO), introduzca la UO designada que Active Directory utiliza para los nuevos objetos de equipo.
7. (Opcional) Para los controladores de dominio (DC), introduzca el nombre de uno o varios DCs a través de los cuales la puerta de enlace se conectará a Active Directory. Puede introducir varios DCs como una lista separada por comas. Puede dejar este campo en blanco para permitir que DNS seleccione automáticamente un controlador de dominio.
8. Seleccione Save changes (Guardar cambios).

Edición de la configuración de un sistema de FSx archivos de Amazon

Tras crear un sistema de archivos del servidor de archivos de Amazon FSx para Windows, puede editar la configuración de CloudWatch los registros, la actualización automática de la caché y las credenciales de la cuenta de FSx servicio de Amazon.

Para editar la configuración FSx del sistema de archivos de Amazon

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. En el panel de navegación izquierdo, elija Sistema de archivos y, a continuación, elija el sistema de archivos cuya configuración desee editar.

3. En Acciones, elija Editar configuración del sistema de archivos.
4. En la sección de configuración del sistema de archivos, verifica la información de la puerta de enlace, la FSx ubicación de Amazon y la dirección IP.

   > **Note**
   >
   > No puede editar la dirección IP de un sistema de archivos después de asociarlo a una puerta de enlace. Para cambiar la dirección IP, debe desasociar y volver a asociar el sistema de archivos.

5. En la sección Registros de auditoría, elige una opción para usar grupos de CloudWatch registros para monitorear el acceso a los sistemas de FSx archivos de Amazon. También puede utilizar un grupo de registro existente.
6. En Configuración de actualización de caché automatizada, elija una opción. Puede elegir Establecer intervalo de actualización, establecer el tiempo en días, horas y minutos para actualizar la caché del sistema de archivos mediante el tiempo de vida (TTL).

   TTL es el tiempo transcurrido desde la última actualización. Cuando se accede al directorio después de ese período de tiempo, File Gateway actualiza el contenido del directorio desde el sistema de FSx archivos de Amazon.

   > **Note**
   >
   > Los valores de intervalo de actualización válidos oscilan entre 5 minutos y 30 días.

7. En la sección Configuración de la cuenta de servicio (opcional), introduzca un nombre de usuario y una Contraseña. Estas credenciales son para un usuario que tiene la función de administrador de Backup del servicio Active Directory asociado a sus sistemas de FSx archivos de Amazon.
8. Seleccione Save changes (Guardar cambios).

Separar un sistema de FSx archivos de Amazon

Al separar un sistema de archivos no se eliminan los datos en FSx Windows File Server. Los datos que se escriban en estos sistemas de archivos antes de separarlos seguirán cargándose en el servidor de archivos FSx de Windows.

Para separar un sistema de FSx archivos de Amazon

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Elija los sistemas de FSx archivos y, a continuación, seleccione uno o más sistemas de archivos para separarlos.
3. En Acciones, seleccione Desasociar sistema de archivos. Aparece el cuadro de diálogo de confirmación.
4. Compruebe que desea desasociar los sistemas de archivos especificados, escriba la palabra desasociar en el cuadro de confirmación y seleccione Desasociar.

Supervisión de Storage Gateway

Los temas de esta sección describen cómo monitorizar una puerta de enlace mediante Amazon CloudWatch, incluida la supervisión del almacenamiento en caché y otros recursos asociados a la puerta de enlace. Utilice la consola de Storage Gateway para ver las métricas y alarmas de la puerta de enlace. Por ejemplo, puede ver el número de bytes utilizados en las operaciones de lectura y escritura, el tiempo empleado en las operaciones de lectura y escritura y el tiempo que se tarda en recuperar los datos de la AWS nube. Con las métricas, puede realizar un seguimiento de la salud de la gateway y configurar alarmas que le avisen cuando una o varias métricas superen un umbral definido.

Storage Gateway proporciona CloudWatch métricas sin costo adicional. Las métricas de Storage Gateway se registran durante un periodo de dos semanas. Puede utilizar estas métricas para tener acceso a información histórica y obtener una mejor perspectiva del rendimiento de las puertas de enlace. Storage Gateway también proporciona CloudWatch alarmas, excepto las de alta resolución, sin cargo adicional. Para obtener más información sobre CloudWatch los precios, consulta los CloudWatch precios de Amazon. Para obtener más información al respecto CloudWatch, consulta la Guía del CloudWatch usuario de Amazon.

Temas

- Entender CloudWatch las alarmas- Obtenga información básica sobre CloudWatch las alarmas, incluidos los estados de las alarmas y las configuraciones recomendadas.
- Cree CloudWatch las alarmas recomendadas- Aprenda a configurar de forma rápida y automática todas las CloudWatch alarmas recomendadas como parte del proceso de configuración inicial de File Gateway.
- Crea una CloudWatch alarma personalizada- Aprenda a crear una CloudWatch alarma personalizada para monitorear una métrica específica utilizando criterios de evaluación específicos para activar estados de alarma y enviar notificaciones.
- Supervisión de su puerta de enlace de - Aprenda a ver CloudWatch los registros y los registros de auditoría y a encontrar información sobre las métricas específicas de la pasarela y del sistema de archivos compartidos que informa su pasarela.

Entender CloudWatch las alarmas

CloudWatch las alarmas supervisan la información sobre su puerta de enlace en función de métricas y expresiones. Puede añadir CloudWatch alarmas a la puerta de enlace y ver sus estados en la consola de Storage Gateway. Para obtener más información sobre las métricas que se utilizan para monitorear , consulte de enlace y Descripción de las métricas de uso del sistema de archivos. Para cada alarma, especifique las condiciones que activarán su estado de ALARMA. Los indicadores de estado de alarma de la consola de Storage Gateway se iluminan en rojo cuando están en estado de ALARMA, lo que facilita la supervisión del estado de forma proactiva. Puede configurar las alarmas para que invoquen acciones automáticamente en función de los cambios sostenidos de estado. Para obtener más información sobre CloudWatch las alarmas, consulta Uso de CloudWatch alarmas de Amazon en la Guía del CloudWatch usuario de Amazon.

> **Note**
>
> Si no tienes permiso para ver CloudWatch, no podrás ver las alarmas.

Para cada gateway activada, se recomienda crear las siguientes alarmas de CloudWatch:

- Espera de E/S de alto desempeño: `IoWaitpercent` >= 20 para 3 puntos de datos en 15 minutos
- Porcentaje de caché sucia: `CachePercentDirty` > 80 para 4 puntos de datos en 20 minutos
- Archivos que no se cargan: `FilesFailingUpload` >= 1 para 1 punto de datos en 5 minutos
- Error del sistema de archivos: `FileSystem-ERROR` >= 1 para 1 punto de datos en 5 minutos
- Notificaciones de estado: `HealthNotifications` >= 1 para 1 punto de datos en 5 minutos. Al configurar esta alarma, defina Tratamiento de datos faltantes como notBreaching.

  > **Note**
  >
  > Solo puede establecer una alarma de notificación de estado si la gateway tenía una notificación de estado anterior en CloudWatch.

Para las puertas de enlace en plataformas VMware host que forman parte de un clúster de VMware alta disponibilidad, también recomendamos esta CloudWatch alarma adicional:

- Notificaciones de disponibilidad: `AvailabilityNotifications` >= 1 para 1 punto de datos en 5 minutos. Al configurar esta alarma, defina Tratamiento de datos faltantes como notBreaching.

En la siguiente tabla se describen los estados CloudWatch de alarma.

Estado	Description (Descripción)
OK (Correcto)	La métrica o expresión está dentro del umbral definido.
Alarma	La métrica o expresión está fuera del umbral definido.
Datos insuficientes	La alarma acaba de iniciarse, la métrica no está disponible o no hay suficientes datos disponibles en la métrica para determinar el estado de la alarma.
Ninguna	No hay alarmas creadas para la gateway. Para crear una alarma nueva, consulte Cree una CloudWatch alarma personalizada para su puerta de enlace.
No disponible	Se desconoce el estado de la alarma. Elija Unavailable (No disponible) para ver la información de error en la pestaña Monitoring (Monitorización) .

Crear CloudWatch las alarmas recomendadas para su puerta de enlace

Al crear una nueva puerta de enlace mediante la consola Storage Gateway, puede optar por crear automáticamente todas CloudWatch las alarmas recomendadas como parte del proceso de configuración inicial. Para obtener más información, Configurar Amazon FSx File Gateway. Si desea añadir o actualizar CloudWatch las alarmas recomendadas para una puerta de enlace existente después de haber completado la configuración por primera vez, utilice el siguiente procedimiento.

Para agregar o actualizar CloudWatch las alarmas recomendadas para una puerta de enlace existente

> **Note**
>
> Esta función requiere permisos CloudWatch de política, que no se otorgan automáticamente como parte de la política de acceso total preconfigurada de Storage Gateway. Asegúrese de que su política de seguridad conceda los siguientes permisos antes de intentar crear CloudWatch las alarmas recomendadas:
>
> - `cloudwatch:PutMetricAlarm`: crear alarmas
> - `cloudwatch:DisableAlarmActions`: desactivar acciones de alarma
> - `cloudwatch:EnableAlarmActions`: activar acciones de alarma
> - `cloudwatch:DeleteAlarms`: eliminar alarmas

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa/.
2. En el panel de navegación de la parte izquierda de la página, elija Gateways y, a continuación, elija la puerta de enlace para la que desee crear las alarmas recomendadas CloudWatch .
3. En la página Detalles de la puerta de enlace, elija la pestaña Supervisión.
4. En Alarmas, elija Crear alarmas recomendadas. Las alarmas recomendadas se crean automáticamente.

   La sección Alarmas muestra todas las CloudWatch alarmas de una puerta de enlace específica. Aquí puede seleccionar y eliminar una o más alarmas, activar o desactivar las acciones de las alarmas y crear nuevas alarmas.

Cree una CloudWatch alarma personalizada para su puerta de enlace

CloudWatch utiliza Amazon Simple Notification Service (Amazon SNS) para enviar notificaciones de alarma cuando una alarma cambia de estado. Una alarma vigila una única métrica durante el periodo que especifique y realiza una o varias acciones en función del valor de la métrica relativo a un determinado umbral durante una serie de periodos de tiempo. La acción es una notificación que se envía a un tema de Amazon SNS. Puedes crear un tema de Amazon SNS al crear una CloudWatch

alarma. Para obtener más información sobre Amazon SNS, consulte ¿Qué es Amazon SNS? en la Guía para desarrolladores de Amazon Simple Notification Service.

Para crear una CloudWatch alarma en la consola Storage Gateway

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa/.
2. En el panel de navegación, elija Puertas de enlace y, a continuación, elija la puerta de enlace para la que desea crear la alarma.
3. En la página de detalles de la puerta de enlace, elija la pestaña Supervisión.
4. En Alarmas, seleccione Crear alarma para abrir la CloudWatch consola.
5. Usa la CloudWatch consola para crear el tipo de alarma que desees. Puede crear los siguientes tipos de alarma:

   - Alarma de umbral estático: alarma basada en un umbral establecido para una métrica elegida. La alarma pasa al estado ALARM cuando la métrica supera el umbral durante un número especificado de periodos de evaluación.

     Para crear una alarma de umbral estático, consulta Cómo crear una CloudWatch alarma basada en un umbral estático en la Guía del CloudWatch usuario de Amazon.
   - Alarma de detección de anomalías: la detección de anomalías extrae datos métricos pasados y crea un modelo de valores esperados. Establece un valor para el umbral de detección de anomalías y lo CloudWatch utiliza con el modelo para determinar el rango «normal» de valores de la métrica. Un valor mayor del umbral produce un intervalo mayor de valores “normales”. Puede elegir activar la alarma solo cuando el valor de la métrica esté por encima de la banda de valores esperados, solo cuando esté por debajo de la banda o cuando esté por encima o por debajo de la banda.

     Para crear una alarma de detección de anomalías, consulta Cómo crear una CloudWatch alarma basada en la detección de anomalías en la Guía CloudWatch del usuario de Amazon.
   - Alarma de expresión matemática métrica: alarma basada en una o más métricas utilizadas en una expresión matemática. A continuación, especifique la expresión, el umbral y los periodos de evaluación.

     Para crear una alarma de expresión matemática métrica, consulte Creación de una CloudWatch alarma basada en una expresión matemática métrica en la Guía del CloudWatch usuario de Amazon.

- Alarma compuesta: alarma que determina su estado observando los estados de otras alarmas. Una alarma compuesta puede ayudarle a reducir el ruido de las alarmas.

  Para crear una alarma compuesta, consulta Cómo crear una alarma compuesta en la Guía del CloudWatch usuario de Amazon.

6. Tras crear la alarma en la CloudWatch consola, vuelva a la consola de Storage Gateway. Para ver la alarma, realice una de las siguientes acciones:

   - En el panel de navegación, elija Puertas de enlace y, a continuación elija la puerta de enlace para la que desee ver alarmas. En la pestaña Detalles, en Alarmas, elija CloudWatch Alarmas.
   - En el panel de navegación, elija Puertas de enlace, elija la puerta de enlace cuyas alarmas desee ver y, a continuación, elija la pestaña Supervisión.

     La sección Alarmas muestra todas las CloudWatch alarmas de una pasarela específica. Aquí puede seleccionar y eliminar una o más alarmas, activar o desactivar las acciones de las alarmas y crear nuevas alarmas.
   - En el panel de navegación, elija Puertas de enlace y, a continuación, elija el estado de alarma de la puerta de enlace para el que desea ver las alarmas.

Para obtener información sobre cómo editar o eliminar una alarma, consulte Edición o eliminación de una CloudWatch alarma.

> **Note**
>
> Al eliminar una puerta de enlace mediante la consola de Storage Gateway, todas CloudWatch las alarmas asociadas a la puerta de enlace también se eliminan automáticamente.

Supervisión de su puerta de enlace de

Puede monitorear su puerta de enlace de y los recursos asociados AWS Storage Gateway mediante CloudWatch métricas y registros de auditoría de Amazon. También puede usar CloudWatch Events para recibir una notificación cuando se terminen las operaciones con los archivos.

Temas

- Obtener los registros de estado de File Gateway con CloudWatch grupos de registros

- Uso de CloudWatch las métricas de Amazon
- Información acerca de las métricas de gateway
- Descripción de las métricas de sistemas de archivos
- Descripción de los registros de auditoría de FSx

Obtener los registros de estado de File Gateway con CloudWatch grupos de registros

Puede usar Amazon CloudWatch Logs para obtener información sobre el estado de su y los recursos relacionados. Puede utilizar los registros para supervisar los errores que detecte la puerta de enlace. Además, puede utilizar los filtros de CloudWatch suscripción de Amazon para automatizar el procesamiento de la información de registro en tiempo real. Para obtener más información, consulta el artículo Procesamiento de datos de registro en tiempo real con suscripciones en la Guía del CloudWatch usuario de Amazon.

Por ejemplo, puede configurar un grupo de CloudWatch registros para monitorear su puerta de enlace y recibir notificaciones cuando su puerta de enlace de FSx archivos no pueda cargar archivos a un sistema de FSx archivos de Amazon. Puede configurar el grupo cuando active la puerta de enlace o cuando esta ya esté activada y en funcionamiento. Para obtener información acerca de cómo configurar un grupo de registros de CloudWatch al activar una gateway, consulte Configure su Amazon FSx File Gateway. Para obtener información general sobre los grupos de CloudWatch registros, consulte Trabajar con grupos de registros y transmisiones de registros en la Guía del CloudWatch usuario de Amazon.

Para obtener información sobre cómo solucionar los errores que pueda reportar , consulteSolución de problemas: problemas con la puerta de enlace de archivo.

Configurar un grupo de CloudWatch registros después de activar la puerta de enlace

El siguiente procedimiento muestra cómo configurar un grupo de CloudWatch registros después de activar la puerta de enlace.

Para configurar un grupo de CloudWatch registros para que funcione con su File Gateway

1. Inicie sesión en la consola Storage Gateway de su https://console.aws.amazon.com/storagegateway/casa Consola de administración de AWS y ábrala.
2. En el panel de navegación, elija Gateways y, a continuación, elija la puerta de enlace para la que desea configurar el grupo de CloudWatch registros.

3. En Acciones, seleccione Editar información de puerta de enlace.
4. En Elegir cómo configurar el grupo de registro, elija una de las siguientes opciones:

   - Cree un nuevo grupo de registros para crear un nuevo grupo de CloudWatch registros.
   - Use un grupo de registros existente para usar un grupo de CloudWatch registros que ya existe.

     Elija un grupo de registro de la Lista de grupos de registros existentes.
   - Desactive el registro si no quiere supervisar su puerta de enlace mediante grupos de CloudWatch registros.
5. Seleccione Save changes (Guardar cambios).
6. Para consultar los registros del estado de la puerta de enlace, haga lo siguiente:

   1. En el panel de navegación, elija Puertas de enlace y, a continuación, elija la puerta de enlace para la que ha configurado el grupo de CloudWatch registros.
   2. Seleccione la pestaña Detalles y, en Registros de salud, elija CloudWatchRegistros. La página de detalles del grupo de registros se abre en la CloudWatch consola.

Uso de CloudWatch las métricas de Amazon

Puede obtener datos de supervisión para su puerta de enlace de archivos mediante la API Consola de administración de AWS o la CloudWatch API. La consola muestra una serie de gráficos basados en los datos sin procesar de la CloudWatch API. La CloudWatch API también se puede utilizar a través de una de las AWS SDKsherramientas de la CloudWatch API de Amazon. En función de sus necesidades, es posible que prefiera utilizar los gráficos que se muestran en la consola o que se recuperan de la API.

Independientemente del método que utilice para trabajar con las métricas, debe especificar la siguiente información:

- La dimensión de las métricas con las que va a trabajar. Una dimensión es un par de nombre-valor que le ayuda a identificar una métrica de forma inequívoca. Las dimensiones de Storage Gateway son `GatewayId` y`GatewayName`. En la CloudWatch consola, puede usar la `Gateway Metrics` vista para seleccionar dimensiones específicas de la puerta de enlace. Para obtener más información sobre las dimensiones, consulta Dimensiones en la Guía del CloudWatch usuario de Amazon.
- El nombre de la métrica, como `ReadBytes`.

En la tabla siguiente se indican los tipos de datos de métricas de Storage Gateway que están disponibles para usted.

Espacio de CloudWatch nombres Amazon	Dimensión	Description (Descripción)
`AWS/StorageGateway`	`GatewayId` , `GatewayName`	Estas dimensiones filtran datos de métricas que describen aspectos de la gateway. Puede identificar una con la que trabajar especificando tanto las dimensiones como `GatewayId` las `GatewayName` dimensiones. Los datos de velocidad y latencia de una gateway se basan en todos los archivos compartidos en la gateway. Los datos se encuentran disponibles automáticamente en periodos de 5 minutos sin costo alguno.

Trabajar con métricas de gateway y de archivos es similar a trabajar con otras métricas de servicio. Puede encontrar información sobre algunas de las métricas más comunes en la documentación de CloudWatch que se muestra a continuación:

- Visualización de las métricas disponibles
- Obtener estadísticas de una métrica
- Creación de alarmas de CloudWatch

Información acerca de las métricas de gateway

En la siguiente tabla se describen las métricas que cubren FSx las pasarelas de archivos. Cada puerta de enlace tiene un conjunto de métricas asociado. Algunas métricas específicas de las pasarelas tienen el mismo nombre que determinadas métricas. file-system-specific Estas métricas representan el mismo tipo de medidas, pero se asignan a la puerta de enlace en lugar de al sistema de archivos.

Especifique siempre si desea trabajar con una puerta de enlace o un sistema de archivos a la hora de trabajar con una métrica concreta. En concreto, cuando trabaje con métricas de puertas de

enlace, debe especificar el `Gateway Name` de la puerta de enlace cuyos datos de métrica desee ver. Para obtener más información, consulte Uso de CloudWatch las métricas de Amazon.

> **Note**
>
> Algunas métricas solo devuelven puntos de datos cuando se han generado nuevos datos durante el período de supervisión más reciente.

En la siguiente tabla se describen las métricas que puede utilizar para obtener información sobre sus puertas de enlace de s.

Métrica	Description (Descripción)
`AvailabilityNotifications`	Esta métrica indica el número de notificaciones de estado relacionadas con la disponibilidad que generó la puerta de enlace durante el período del informe. Unidades: recuento
`CacheDirectorySize`	Esta métrica controla el tamaño de las carpetas en la caché de la puerta de enlace. El tamaño de la carpeta viene determinado por el número de archivos y subcarpetas de su primer nivel; no se incluye de forma recursiva en las subcarpetas. Utilice esta métrica con la estadística `Average` para medir el tamaño medio de una carpeta en la caché de la puerta de enlace. Utilice esta métrica con la estadística `Max` para medir el tamaño máximo de una carpeta en la caché de la puerta de enlace. Unidades: recuento
`CacheFileSize`	Esta métrica controla el tamaño de los archivos en la caché de la puerta de enlace.

Métrica	Description (Descripción)
	Utilice esta métrica con la estadística `Average` para medir el tamaño medio de un archivo en la caché de la puerta de enlace. Utilice esta métrica con la estadística `Max` para medir el tamaño máximo de un archivo en la caché de la puerta de enlace. Unidades: bytes
`CacheFree`	Esta métrica indica el número de bytes disponibles en la caché de la puerta de enlace. Unidades: bytes
`CacheHitPercent`	Porcentaje de operaciones de lectura de la aplicación desde la puerta de enlace que se sirven desde la caché. La muestra se obtiene al final del período de notificación. Cuando no hay operaciones de lectura de la aplicación desde la puerta de enlace, esta métrica registra un valor del 100 %. Unidad: porcentaje
`CachePercentDirty`	El porcentaje total de la memoria caché de la puerta de enlace que no se ha conservado. AWS La muestra se obtiene al final del período de notificación. Unidad: porcentaje
`CachePercentUsed`	Porcentaje total del almacenamiento en caché de la puerta de enlace que se utiliza. La muestra se obtiene al final del período de notificación. Unidad: porcentaje

Métrica	Description (Descripción)
`CacheUsed`	Esta métrica indica el número de bytes utilizados en la caché de la puerta de enlace. Unidades: bytes
`CloudBytesDownloaded`	El número total de bytes desde los que se descargó la puerta de enlace AWS durante el período del informe. Utilice esta métrica con la estadística `Sum` para medir la velocidad y con la estadística `Samples` para medir las operaciones de entrada/salida por segundo (IOPS). Unidades: bytes
`CloudBytesUploaded`	El número total de bytes en los que se cargó la puerta de enlace AWS durante el período del informe. Utilice esta métrica con la `Sum` estadística para medir el rendimiento y con la `Samples` estadística para medir input/output las operaciones por segundo (IOPS). Unidades: bytes

Métrica	Description (Descripción)
`FilesFailingUpload`	Esta métrica controla el número de archivos que no se pueden cargar en AWS. Estos archivos generarán notificaciones de estado que contienen más información sobre el problema. Use esta métrica con la estadística `Sum` para mostrar el número de archivos que no se pueden cargar en AWS actualmente. Unidades: recuento
`FileShares`	Esta métrica indica el número de recursos compartidos de archivos en la puerta de enlace. Unidades: recuento
`FileSystem-ERROR`	Esta métrica proporciona el número de asociaciones de sistemas de archivos en estas puertas de enlace que se encuentran en el estado ERROR. Si esta métrica indica que alguna asociación de sistemas de archivos está en estado ERROR, es probable que haya un problema con la puerta de enlace que pueda interrumpir el flujo de trabajo. Se recomienda crear una alarma para cuando esta métrica informe de un valor distinto de cero. Unidades: recuento

Métrica	Description (Descripción)
HealthNotifications	Esta métrica indica el número de notificaciones de estado que generó esta puerta de enlace en el período del informe. Unidades: recuento
IndexEvictions	Esta métrica indica el número de archivos cuyos metadatos se han desalojado del índice almacenado en la caché de metadatos de archivos para dejar espacio para nuevas entradas. La puerta de enlace mantiene este índice de metadatos, que se completa desde la AWS nube a pedido. Unidades: recuento
IndexFetches	Esta métrica indica el número de archivos para los que se han recuperado metadatos . La puerta de enlace mantiene un índice en caché de los metadatos de los archivos, que se rellena desde la AWS nube a pedido. Unidades: recuento
IoWaitPercent	Esta métrica indica el porcentaje de tiempo que la CPU está a la espera de recibir una respuesta del disco local. Unidad: porcentaje
MemTotalBytes	Esta métrica indica la cantidad total de memoria de la puerta de enlace. Unidades: bytes

Métrica	Description (Descripción)
`MemUsedBytes`	Esta métrica indica la cantidad de memoria utilizada en la puerta de enlace. Unidades: bytes
`RootDiskFreeBytes`	Esta métrica indica la cantidad de bytes disponibles en el disco raíz de la puerta de enlace. Si esta métrica indica que quedan menos de 20 GB libres, debe aumentar el tamaño del disco raíz. Para aumentar el tamaño del disco raíz, puede aumentar el tamaño del disco raíz existente en la máquina virtual. Cuando se reinicia la máquina virtual, la puerta de enlace reconoce el aumento de tamaño del disco raíz. Unidades: bytes
`SmbV2Sessions`	Esta métrica indica el número de SMBv2 sesiones que están activas en la puerta de enlace. Esta métrica se emite una vez para cada sistema de archivos asociado a la puerta de enlace. Utilice la estadística SUM para calcular el número total de SMBv2 sesiones activas en todos los sistemas de archivos. Unidades: recuento

Métrica	Description (Descripción)
`SmbV3Sessions`	Esta métrica indica el número de SMBv3 sesiones que están activas en la puerta de enlace. Esta métrica se emite una vez para cada sistema de archivos asociado a la puerta de enlace. Utilice la estadística SUM para calcular el número total de SMBv3 sesiones activas en todos los sistemas de archivos. Unidades: recuento
`TotalCacheSize`	Esta métrica indica el tamaño total de la caché. Unidades: bytes
`UserCpuPercent`	Esta métrica indica el porcentaje de tiempo que se dedica al procesamiento de la puerta de enlace. Unidad: porcentaje

Descripción de las métricas de sistemas de archivos

A continuación puede encontrar información acerca de las métricas de Storage Gateway que cubren los sistemas de archivos. Cada sistema de archivos tiene un conjunto de métricas asociado. Algunas de las métricas específicas de los sistemas de archivos tienen el mismo nombre que determinadas métricas específicas de puertas de enlace. Estas métricas representan el mismo tipo de medidas, pero se asignan al sistema de archivos.

Especifique siempre si desea trabajar con una métrica de puerta de enlace o de sistema de archivos antes de trabajar con una métrica. En concreto, cuando trabaje con métricas de sistema de archivos, debe especificar el `File system ID` que identifique el sistema de archivos cuyas métricas desea ver. Para obtener más información, consulte Uso de CloudWatch las métricas de Amazon.

> **Note**
>
> Algunas métricas solo devuelven puntos de datos cuando se han generado nuevos datos durante el período de supervisión más reciente.

En la siguiente tabla se describen las métricas de Storage Gateway que puede utilizar para obtener información acerca de los recursos compartidos de archivos.

Métrica	Description (Descripción)
`CacheHitPercent`	Porcentaje de operaciones de lectura de la aplicación desde los recursos compartidos de archivo que se sirven desde la caché. La muestra se obtiene al final del período de notificación. Cuando no hay operaciones de lectura de la aplicación desde el recurso compartido de archivos, esta métrica registra un valor del 100 %. Unidad: porcentaje
`CachePercentDirty`	La contribución del recurso compartido de archivos al porcentaje total de la caché de la puerta de enlace que no se ha almacenado de forma persistente en AWS. La muestra se obtiene al final del período de notificación. Utilice esta métrica con la estadística `Sum`. Lo ideal es que esta métrica se mantenga baja. **Note** Utilice la métrica `CachePercentDirty` de la puerta de enlace para ver el porcentaje total de la caché

Métrica	Description (Descripción)
	de la puerta de enlace que no se ha almacenado de forma persistente en AWS. Unidad: porcentaje
`CachePercentUsed`	Porcentaje de la caché de datos utilizada en toda la puerta de enlace. La muestra se obtiene al final del período de notificación. Esta métrica específica del recurso compartido de archivos indica el mismo valor que la métrica específica de la puerta de enlace correspondiente. Unidad: porcentaje
`CloudBytesUploaded`	El número total de bytes en los que se cargó la puerta de enlace AWS durante el período del informe. Utilice esta métrica con la estadística `Sum` para medir la velocidad y con la estadísti ca `Samples` para medir las operaciones de entrada/salida por segundo (IOPS). Unidades: bytes
`CloudBytesDownloaded`	El número total de bytes desde los que se descargó la puerta de enlace AWS durante el período del informe. Utilice esta métrica con la `Sum` estadística para medir el rendimiento y con la `Samples` estadística para medir input/output las operaciones por segundo (IOPS). Unidades: bytes

Métrica	Description (Descripción)
`FilesFailingUpload`	Esta métrica controla el número de archivos que no se pueden cargar en AWS. Estos archivos generarán notificaciones de estado que contienen más información sobre el problema. Use esta métrica con la estadística `Sum` para mostrar el número de archivos que no se pueden cargar en AWS actualmente. Unidades: recuento
`ReadBytes`	El número total de bytes leídos desde las aplicaciones en las instalaciones en el período de notificación para un recurso compartido de archivos. Utilice esta métrica con la estadística `Sum` para medir la velocidad y con la estadísti ca `Samples` para medir las operaciones de entrada/salida por segundo (IOPS). Unidades: bytes
`WriteBytes`	El número total de bytes escritos en las aplicaciones on-premises en el período de notificación. Utilice esta métrica con la estadística `Sum` para medir la velocidad y con la estadísti ca `Samples` para medir las operaciones de entrada/salida por segundo (IOPS). Unidades: bytes

Descripción de los registros de auditoría de FSx

Los registros de auditoría de Amazon FSx FSx File Gateway (File Gateway) proporcionan detalles sobre el acceso de los usuarios a los archivos y carpetas de una asociación de sistemas de archivos. Puede usar los registros de auditoría para supervisar las actividades de los usuarios y tomar medidas si se identifican patrones de actividad inapropiados. Los registros tienen un formato similar al de los eventos de registro de seguridad de Windows Server, a fin de garantizar la compatibilidad con las herramientas de procesamiento de registros existentes para los eventos de seguridad de Windows.

Operaciones

En la siguiente tabla se describen las operaciones de acceso a los File Gateway.

Nombre de operación	Definición
Leer datos	Leer el contenido de un archivo.
Escribir datos	Cambiar el contenido de un archivo.
Crear	Crear un nuevo archivo o carpeta.
Cambio de nombre	Cambiar el nombre de un archivo o carpeta existente.
Eliminar	Eliminar un archivo o carpeta.
Atributos de escritura	Actualice los metadatos del archivo o la carpeta (propietarioACLs, grupo, permisos).

Atributos

En la siguiente tabla se describen los atributos de acceso al FSx archivo de registro de auditoría de File Gateway.

Atributo	Definición
`securityDescriptor`	Muestra la lista de control de acceso discrecional (DACL) establecida en un objeto, en formato SDDL.

Atributo	Definición
`sourceAddress`	La dirección IP del equipo cliente de recurso compartido de archivos.
`SubjectDomainName`	El dominio de Directorio Activo (AD) al que pertenece la cuenta del cliente.
`SubjectUserName`	Nombre de usuario de Active Directory del cliente.
`source`	El ID de la `FileSystemAssociation` de Storage Gateway que se está auditando.
`mtime`	El momento en el que el contenido del objeto fue modificado, establecido por el cliente.
`version`	Versión del formato de registro de auditoría.
`ObjectType`	Define si el objeto es un archivo o una carpeta.
`locationDnsName`	El nombre DNS del sistema FSx File Gateway.
`objectName`	La ruta completa al objeto.
`ctime`	Hora en la que se modificó el contenido o los metadatos del objeto, establecida por el cliente.
`shareName`	Nombre del recurso compartido al que se está accediendo.
`operation`	Nombre de la operación de acceso a objetos.
`newObjectName`	La ruta de acceso completa al nuevo objeto después de que se haya cambiado el nombre.
`gateway`	El ID de Storage Gateway.

Atributo	Definición
`status`	El estado de la operación. Solo se registra el éxito (los errores se registran con la excepción de los errores que surgen de permisos denegados).
`fileSizeInBytes`	El tamaño del archivo en bytes, establecido por el cliente en el momento de la creación del archivo.

Atributos registrados por operación

En la siguiente tabla se describen los atributos del registro de auditoría de FSx File Gateway registrados en cada operación de acceso a los archivos.

	Leer datos	Escribir datos	Creación de una carpeta	Crear archivo	Cambiar nombre de archivo/carpeta	Eliminar archivo/carpeta	Atributos de escritura (cambiar ACL)	Atributos de escritura (chown)	Atributos de escritura (chmod)	Atributos de escritura (chgrp)
`securi escrip`							X			
`source ress`	X	X	X	X	X	X	X	X	X	X
`Subjec mainNa`	X	X	X	X	X	X	X	X	X	X
`Subjec erName`	X	X	X	X	X	X	X	X	X	X
`source`	X	X	X	X	X	X	X	X	X	X

	Leer datos	Escribir datos	Creación de una carpeta	Crear archivo	Cambiar nombre de archivo/carpeta	Eliminar archivo/carpeta	Atributos de escritura (cambiar ACL)	Atributos de escritura (chown)	Atributos de escritura (chmod)	Atributos de escritura (chgrp)
mtime			X	X						
versic	X	X	X	X	X	X	X	X	X	X
object e	X	X	X	X	X	X	X	X	X	X
locati nsName	X	X	X	X	X	X	X	X	X	X
object e	X	X	X	X	X	X	X	X	X	X
ctime			X	X						
shareN	X	X	X	X	X	X	X	X	X	X
operat	X	X	X	X	X	X	X	X	X	X
newObj Name					X					
gatewa	X	X	X	X	X	X	X	X	X	X
status	X	X	X	X	X	X	X	X	X	X
fileSi nBytes				X						

Mantenimiento de la puerta de enlace

Mantenimiento de su Amazon FSx File Gateway implica realizar un mantenimiento general para optimizar el rendimiento de su puerta de enlace. Estas tareas son comunes para todos los tipos de gateways.

Esta sección contiene los siguientes temas, que describen los conceptos y procedimientos relacionados con el mantenimiento de Amazon FSx File Gateway :

Temas

- Administración de actualizaciones de puertas de enlace: obtenga información sobre cómo activar o desactivar las actualizaciones de mantenimiento y modificar la programación de los periodos de mantenimiento de la puerta de enlace de archivo.
- Realización de tareas de mantenimiento con la consola local: obtenga información sobre cómo realizar tareas de mantenimiento mediante la consola local de la puerta de enlace.
- Apagado de la máquina virtual de puerta de enlace: obtenga información sobre qué hacer si necesita apagar o reiniciar la máquina virtual de puerta de enlace para realizar tareas de mantenimiento, por ejemplo, al aplicar un parche al hipervisor.
- Sustituir la puerta de enlace de archivos de existente por una nueva instancia— Aprenda a reemplazar su puerta de enlace de archivos de por una nueva instancia cuando desee mejorar el rendimiento o responder a una notificación para migrar la puerta de enlace.
- Eliminación de la puerta de enlace y eliminación de los recursos asociados— Aprenda a eliminar su puerta de enlace mediante la AWS Storage Gateway consola y a limpiar los recursos asociados para evitar que se le cobre por su uso continuo.

Administración de actualizaciones de puertas de enlace

Storage Gateway consta de un componente de servicios en la nube gestionados y un componente de dispositivo de puerta de enlace que se implementan de forma local o en una instancia de Amazon EC2 en AWS la nube. Ambos componentes reciben actualizaciones periódicas. Los temas de esta sección describen la cadencia de estas actualizaciones, cómo se aplican y cómo configurar los ajustes relacionados con las actualizaciones en las puertas de enlace de la implementación.

> **Important**
>
> Debe tratar el dispositivo de Storage Gateway como una máquina virtual administrada y no debe intentar acceder a su instalación o contenido ni modificarlos de forma alguna. Si intenta instalar o actualizar cualquier paquete de software mediante métodos distintos al mecanismo de actualización de la AWS puerta de enlace normal (por ejemplo, mediante SSM o herramientas de hipervisor), es posible que la puerta de enlace no funcione correctamente. Storage Gateway aplica parches al dispositivo de forma automática y periódica para mantener la seguridad y la estabilidad. Los dispositivos de Storage Gateway utilizan Amazon Linux como sistema operativo base. Puede comprobar el estado de los problemas relacionados con vulnerabilidades y exposiciones comunes (CVE) detectados en el Centro de Seguridad de Amazon Linux. Los parches de CVE se aplican automáticamente 30 días después de su publicación, tal y como se muestra en el Centro de Seguridad de Amazon Linux. Los parches se instalan durante el programa de mantenimiento de la puerta de enlace, siempre que la puerta de enlace esté en línea.
>
> Storage Gateway no admite la actualización manual de una puerta de enlace de Amazon EC2 mediante las directivas cloud-init. Si utiliza este método para actualizar una puerta de enlace, es posible que se produzcan problemas de interoperabilidad que le impidan activar o utilizar el dispositivo de puerta de enlace.

Frecuencia de actualización y comportamiento esperado

AWS actualiza el componente de servicios en la nube según sea necesario sin interrumpir las pasarelas implementadas. Los dispositivos de puerta de enlace implementados reciben los siguientes tipos de actualizaciones:

- Mantenimiento: actualizaciones periódicas que pueden incluir actualizaciones del sistema operativo y del software, correcciones para mejorar la estabilidad, el rendimiento y la seguridad, y el acceso a nuevas características.
- Urgentes: actualizaciones críticas que incluyen las correcciones necesarias para los problemas que afectan inmediatamente a la seguridad, el rendimiento o la durabilidad de la puerta de enlace. Las actualizaciones urgentes se pueden publicar en cualquier momento, fuera del ritmo normal de las actualizaciones mensuales de mantenimiento y características.

Todas las actualizaciones son acumulativas y actualizan las pasarelas a la versión actual cuando se aplican. Para obtener información sobre los cambios específicos incluidos en cada actualización, consulte .

Todas las actualizaciones del dispositivo de puerta de enlace pueden provocar una breve interrupción del servicio. El host de máquinas virtuales de la puerta de enlace no necesita reiniciarse durante las actualizaciones, pero la puerta de enlace no estará disponible durante un breve periodo de tiempo mientras el dispositivo de puerta de enlace se actualiza y se reinicia.

Cuando implemente y active la puerta de enlace, se establecerá un calendario de periodos de mantenimiento predeterminado. Puede modificar el calendario de periodos de mantenimiento en cualquier momento. También puede desactivar las actualizaciones de mantenimiento, pero le recomendamos que las deje activadas.

> **Note**
>
> Las actualizaciones urgentes se aplican de acuerdo con el calendario de periodos de mantenimiento, incluso si las actualizaciones de mantenimiento periódicas están desactivadas.

Antes de aplicar cualquier actualización a su puerta de enlace, se lo AWS notifica con un mensaje en la consola de Storage Gateway y en su Panel de AWS Health. Para obtener más información, consulte Panel de AWS Health. Para modificar la dirección de correo electrónico a la que se envían las notificaciones de actualización de software, consulte Actualizar los contactos alternativos de su AWS cuenta en la Guía de referencia de administración de AWS cuentas.

Cuando haya actualizaciones disponibles, la pestaña Detalles de la puerta de enlace muestra un mensaje de mantenimiento. Puede ver también la fecha y la hora en que se aplicó la última actualización correcta en la pestaña Detalles.

Activación o desactivación de las actualizaciones de mantenimiento

Cuando las actualizaciones de mantenimiento están activadas, la puerta de enlace las aplica automáticamente de acuerdo con la programación del periodo de mantenimiento configurado. Para obtener más información, consulte Modificar el programa del periodo de mantenimiento de la puerta de enlace.

Si las actualizaciones de mantenimiento están desactivadas, la puerta de enlace no las aplicará automáticamente, pero siempre podrá aplicarlas manualmente mediante la consola, la API o la CLI

de Storage Gateway. En ocasiones, las actualizaciones urgentes se aplicarán durante el periodo de mantenimiento configurado, independientemente de esta configuración.

> **Note**
>
> En el siguiente procedimiento se describe cómo activar o desactivar las actualizaciones de puerta de enlace mediante la consola de Storage Gateway. Para cambiar esta configuración mediante programación mediante la API, consulte la referencia de la API UpdateMaintenanceStartTimede Storage Gateway.

Para activar o desactivar las actualizaciones de mantenimiento mediante la consola de Storage Gateway:

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. En el panel de navegación, elija Puertas de enlace y, a continuación elija la puerta de enlace para la que desee configurar actualizaciones de mantenimiento.
3. Elija Acciones y, a continuación, elija Editar la configuración de mantenimiento.
4. Para las actualizaciones de mantenimiento, seleccione Activar o Desactivar.
5. Cuando haya finalizado, elija Guardar cambios.

Puede comprobar la configuración actualizada en la pestaña Detalles de la puerta de enlace seleccionada en la consola de Storage Gateway.

Modificación del programa de periodos de mantenimiento de la puerta de enlace

Si las actualizaciones de mantenimiento están activadas, la puerta de enlace las aplica automáticamente de acuerdo con la programación del periodo de mantenimiento. En ocasiones, las actualizaciones urgentes se aplicarán durante el periodo de mantenimiento configurado, independientemente de la configuración de las actualizaciones de mantenimiento.

> **Note**
>
> El siguiente procedimiento describe cómo modificar la programación del período de mantenimiento mediante la consola de Storage Gateway. Para cambiar esta

configuración mediante programación mediante la API, consulte la referencia de la API UpdateMaintenanceStartTimede Storage Gateway.

Para modificar la programación del periodo de mantenimiento mediante la consola de Storage Gateway:

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. En el panel de navegación, elija Puertas de enlace y, a continuación elija la puerta de enlace para la que desee configurar actualizaciones de mantenimiento.
3. Elija Acciones y, a continuación, elija Editar la configuración de mantenimiento.
4. En Hora de inicio del periodo de mantenimiento, haga lo siguiente:

   a. En Programar, elija Semanal o Mensual para establecer la cadencia del periodo de mantenimiento.

   b. Si elige Semanalmente, modifique los valores de Día de la semana y Hora para establecer el momento específico de cada semana en el que comenzará el periodo de mantenimiento.

      Si elige Mensualmente, modifique los valores de Día de la semana y Hora para establecer el momento específico durante cada mes en el que comenzará el periodo de mantenimiento.

      > **Note**
      >
      > El valor máximo que se puede establecer para el día del mes es 28. No es posible configurar el programa de mantenimiento para que comience los días 29 a 31.
      > Si recibe un error al ajustar esta configuración, es posible que el software de la puerta de enlace esté desactualizado. Considere actualizar primero la puerta de enlace manualmente y, a continuación, intentar configurar de nuevo el programa del periodo de mantenimiento.

5. Cuando haya finalizado, elija Guardar cambios.

Puede comprobar la configuración actualizada en la pestaña Detalles de la puerta de enlace seleccionada en la consola de Storage Gateway.

Aplicación de una actualización manualmente

Si hay una actualización de software disponible para la puerta de enlace, puede aplicarla manualmente siguiendo el procedimiento que se indica a continuación. Este proceso de actualización manual ignora la programación del periodo de mantenimiento y aplica la actualización inmediatamente, incluso si las actualizaciones de mantenimiento están desactivadas.

> **Note**
>
> El siguiente procedimiento describe cómo aplicar una actualización manualmente mediante la consola de Storage Gateway. Para realizar esta acción mediante programación mediante la API, consulte la referencia de la API UpdateGatewaySoftwareNowde Storage Gateway.

Para aplicar manualmente una actualización del software de la puerta de enlace mediante la consola de Storage Gateway:

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. En el panel de navegación, elija Puertas de enlace y, a continuación elija la puerta de enlace que desee administrar.

   Si hay una actualización disponible, la consola muestra un banner de notificación azul en la pestaña Detalles de la puerta de enlace, que incluye una opción para aplicar la actualización.
3. Elija Aplicar actualización ahora para actualizar inmediatamente la puerta de enlace.

   > **Note**
   >
   > Esta operación provoca una interrupción temporal en la funcionalidad de la puerta de enlace mientras se instala la actualización. Durante este tiempo, el estado de la puerta de enlace aparece OFFLINE en la consola de Storage Gateway. Una vez finalizada la instalación de la actualización, la puerta de enlace reanuda su funcionamiento normal y su estado cambia a RUNNING.

Puede comprobar que el software de la puerta de enlace se actualizó a la versión más reciente mediante la comprobación de la pestaña Detalles de la puerta de enlace seleccionada en la consola de Storage Gateway.

Realización de tareas de mantenimiento con la consola local

Esta sección contiene los siguientes temas, que proporcionan información sobre cómo realizar tareas de mantenimiento mediante la consola local del dispositivo de puerta de enlace. Puede realizar estas tareas accediendo a la consola local a través de la máquina virtual local en las instalaciones o la instancia de Amazon EC2 que aloja su dispositivo de puerta de enlace. La mayoría de las tareas son comunes entre las distintas plataformas de hosts, pero también hay algunas diferencias.

Temas

- Acceso a la consola local de la puerta de enlace- Aprenda a iniciar sesión en la consola local de una puerta de enlace local alojada en una máquina virtual basada en el núcleo de Linux (KVM) VMware ESXi o en una plataforma Microsoft Hyper-V Manager.
- Realización de tareas en la consola local de la máquina virtual: obtenga información sobre cómo usar la consola local para realizar tareas de configuración básicas y avanzadas para una puerta de enlace en las instalaciones, como configurar un proxy HTTP, ver el estado de los recursos del sistema o ejecutar comandos de terminal.
- Realización de tareas en la consola local de la puerta de enlace de Amazon EC2: obtenga información sobre cómo iniciar sesión en la consola local para realizar tareas de configuración básicas y avanzadas para una puerta de enlace de Amazon EC2, como configurar un proxy HTTP, ver el estado de los recursos del sistema o ejecutar comandos de terminal.

Acceso a la consola local de la puerta de enlace

La forma en que se obtiene acceso a la consola local de la máquina virtual depende del tipo de hipervisor en que se haya implementado la máquina virtual de la gateway. En esta sección, encontrará información sobre cómo acceder a la consola local de la máquina virtual de la máquina virtual basada en el núcleo de Linux (KVM) VMware ESXi y Microsoft Hyper-V Manager.

Temas

- Acceso a la consola local de la gateway con Linux KVM
- Acceder a la consola local de Gateway con VMware ESXi
- Acceso a la consola local de la gateway con Microsoft Hyper-V

Acceso a la consola local de la gateway con Linux KVM

Existen distintas formas de configurar máquinas virtuales que se ejecutan en KVM, en función de la distribución Linux que se esté utilizando. A continuación se indican las instrucciones para acceder a las opciones de configuración KVM desde la línea de comandos. Las instrucciones podrían variar según la implementación de KVM.

Cómo obtener acceso a la consola local de la puerta de enlace con KVM

1. Utilice el siguiente comando para enumerar los VMs que están disponibles actualmente en KVM.

   ```
   # virsh list
   ```

   El comando devuelve una lista VMs con la información de identificación, nombre y estado de cada uno. Anote el `Id` de la máquina virtual para la que desea lanzar la consola local de la puerta de enlace.

2. Utilice el siguiente comando para acceder a la consola local.

   ```
   # virsh console Id
   ```

   *Id*Sustitúyalo por el identificador de la máquina virtual que anotaste en el paso anterior.

   La consola local de AWS Appliance Gateway le pide que inicie sesión para cambiar la configuración de la red y otros ajustes.

3. Ingrese el nombre de usuario y la contraseña para iniciar sesión en la consola local de la puerta de enlace. Para obtener más información, consulte Inicio de sesión en la consola local de la puerta de enlace de archivo.

   Tras iniciar sesión, aparece el menú Activación del dispositivo de AWS : configuración. Puede seleccionar las opciones del menú para realizar las tareas de configuración de la puerta de enlace. Para obtener más información, consulte Realizar tareas en la consola local de la máquina virtual.

Acceder a la consola local de Gateway con VMware ESXi

Para acceder a la consola local de su puerta de enlace con VMware ESXi

1. En el cliente VMware vSphere, seleccione la máquina virtual de puerta de enlace.
2. Asegúrese de que la máquina virtual de la puerta de enlace esté encendida.

   > **Note**
   >
   > Si la máquina virtual de la puerta de enlace está encendida, aparece un icono de flecha verde con el icono de la máquina virtual en el panel del navegador de la máquina virtual en la parte izquierda de la ventana de la aplicación. Si la máquina virtual de la puerta de enlace no está activada, puede activarla mediante la elección del icono Encender verde en la Barra de herramientas en la parte superior de la ventana de la aplicación.

3. Elija la pestaña Consola en el panel de información principal, en la parte derecha de la ventana de la aplicación.

   Transcurridos unos instantes, la consola local de AWS Appliance Gateway le pedirá que inicie sesión para cambiar la configuración de la red y otros ajustes.

   > **Note**
   >
   > Para liberar el cursor de la ventana de la consola, pulse Ctrl+Alt.

4. Ingrese el nombre de usuario y la contraseña para iniciar sesión en la consola local de la puerta de enlace. Para obtener más información, consulte Inicio de sesión en la consola local de la puerta de enlace de archivo.

   Tras iniciar sesión, aparece el menú Activación del dispositivo de AWS : configuración. Puede seleccionar las opciones del menú para realizar las tareas de configuración de la puerta de enlace. Para obtener más información, consulte Realizar tareas en la consola local de la máquina virtual.

Acceso a la consola local de la gateway con Microsoft Hyper-V

Cómo obtener acceso a la consola local de la gateway (Microsoft Hyper-V)

1. Seleccione la máquina virtual del dispositivo de puerta de enlace en el panel Máquinas virtuales del lado izquierdo de la ventana de la aplicación Microsoft Hyper-V Manager.

2. Asegúrese de que la puerta de enlace esté encendida.

> **Note**
>
> Si la máquina virtual de la puerta de enlace está encendida, `Running` aparecerá en la columna Estado de la máquina virtual del panel Máquinas virtuales, en la parte izquierda de la ventana de la aplicación. Si la máquina virtual de la puerta de enlace no está activada, puede activarla mediante la elección de Iniciar en el panel Acciones en el lado derecho de la ventana de la aplicación.

3. Elija Conectar en el panel Acciones.

   Aparece la ventana Virtual Machine Connection. Si aparece una ventana de autenticación, escriba las credenciales proporcionados por el administrador del hipervisor.

   Transcurridos unos instantes, la consola local de AWS Appliance Gateway le pedirá que inicie sesión para cambiar la configuración de la red y otros ajustes.

4. Ingrese el nombre de usuario y la contraseña para iniciar sesión en la consola local de la puerta de enlace. Para obtener más información, consulte Inicio de sesión en la consola local de la puerta de enlace de archivo.

   Tras iniciar sesión, aparece el menú Activación del dispositivo de AWS : configuración. Puede seleccionar las opciones del menú para realizar las tareas de configuración de la puerta de enlace. Para obtener más información, consulte Realizar tareas en la consola local de la máquina virtual.

Realización de tareas en la consola local de la máquina virtual

En una puerta de enlace de archivo implementada en las instalaciones, puede realizar las siguientes tareas de mantenimiento utilizando la consola local del host de la máquina virtual. Estas tareas son comunes a los VMware hipervisores de máquinas virtuales basadas en el núcleo (KVM) de Microsoft Hyper-V y Linux.

Temas

- Inicio de sesión en la consola local de la puerta de enlace de archivo: obtenga información sobre cómo iniciar sesión en la consola local, donde puede configurar los ajustes de red de la puerta de enlace y cambiar la contraseña predeterminada.

- Configuración de un proxy HTTP- Aprenda a configurar Storage Gateway para enrutar todo el tráfico de AWS puntos finales a través de un servidor proxy.
- Configuración de red de la puerta de enlace: obtenga información sobre cómo configurar la puerta de enlace para utilizar DHCP o una dirección IP estática.
- Probar la conexión de red de la puerta de enlace: obtenga información sobre cómo usar la consola local de la puerta de enlace para probar la conectividad de la red.
- Visualización del estado de los recursos de sistema de la puerta de enlace: obtenga información sobre cómo comprobar los núcleos de la CPU virtuales de la puerta de enlace, el tamaño del volumen raíz y la RAM.
- Configuración de un servidor NTP (Network Time Protocol) para la puerta de enlace: obtenga información sobre cómo ver y editar las configuraciones del servidor NTP (Network Time Protocol) y sincronizar la hora de la puerta de enlace con el host del hipervisor.
- Ejecución de comandos de Storage Gateway en la consola local- Aprenda a ejecutar los comandos de la consola local para realizar tareas como guardar tablas de enrutamiento Soporte, conectarse a, etc.

Inicio de sesión en la consola local de la puerta de enlace de archivo

Cuando la MV está lista para el inicio de sesión, se muestra la pantalla de inicio de sesión. Si es la primera vez que inicia sesión en la consola local de la máquina virtual, utilice las credenciales temporales para iniciar sesión. Estas credenciales temporales proporcionan acceso a menús donde puede configurar los ajustes de red de la puerta de enlace y cambiar la contraseña de la consola local. El nombre de usuario inicial es `admin` y la contraseña temporal es `password`. La primera vez que inicie sesión debe cambiar la contraseña.

Cómo cambiar la contraseña temporal

1. En el menú principal Activación de dispositivo de AWS - Configuración, introduzca el número correspondiente para la Consola de puerta de enlace.
2. Ejecute el comando `passwd`. Para obtener información acerca de cómo ejecutar el comando, consulte Ejecución de comandos de Storage Gateway en la consola local.

Ajuste de la contraseña de la consola local desde la consola de Storage Gateway

También puede administrar la contraseña de la consola local desde la consola basada en web de Storage Gateway. Cualquier actualización correcta de la contraseña realizada con la consola basada

en web anulará la contraseña utilizada por la consola local de la máquina virtual de puerta de enlace, incluida la contraseña temporal si nunca ha iniciado sesión de forma local. Si no se puede acceder a la puerta de enlace a través de la red, se producirá un error en el proceso de actualización de la contraseña.

Cómo establecer la contraseña de la consola local en la consola de Storage Gateway

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. En el panel de navegación, elija Puertas de enlace y, a continuación, seleccione la puerta de enlace para la que desee establecer una nueva contraseña.
3. En Actions (Acciones), elija Set Local Console Password (Establecer contraseña de consola local).
4. En el cuadro de diálogo Set Local Console Password (Establecer contraseña de consola local), introduzca una contraseña nueva, confírmela y, a continuación, elija Save (Guardar).

   La nueva contraseña sustituye a la contraseña actual. El servicio Storage Gateway no guarda, almacena ni registra la contraseña, sino que la transmite de forma segura a través de un canal cifrado a la máquina virtual, donde se almacena de forma segura.

   > **Note**
   >
   > La contraseña puede contener cualquier carácter del teclado y pueden tener de 1 a 512 caracteres de longitud.

Configuración de un proxy HTTP

Las puertas de enlace de archivo admiten la configuración de un proxy HTTP.

> **Note**
>
> La única configuración de proxy que admiten las puertas de enlace de archivo es HTTP.

Si la gateway debe utilizar un servidor proxy para comunicarse con Internet, debe configurar los ajustes del proxy HTTP para la gateway. Para ello, especifique una dirección IP y un número de puerto para el host en el que se ejecuta el proxy. Una vez hecho esto, Storage Gateway enruta todo el AWS tráfico de puntos finales a través del servidor proxy. Las comunicaciones entre la puerta

de enlace y los puntos de conexión están cifradas, incluso cuando se utiliza el proxy HTTP. Para obtener más información sobre los requisitos de red para la gateway, consulte Requisitos de red y firewall.

Cómo configurar un proxy HTTP para una puerta de enlace de archivo

1. Inicie sesión en la consola local de la gateway:
   - Para obtener más información sobre cómo iniciar sesión en la consola VMware ESXi local, consulteAcceder a la consola local de Gateway con VMware ESXi.
   - Para obtener más información sobre el inicio de sesión en la consola local de Microsoft Hyper-V, consulte Acceso a la consola local de la gateway con Microsoft Hyper-V.
   - Para obtener más información sobre cómo iniciar sesión en la consola local de la máquina virtual de Linux basada en el kernel (KVM), consulte Acceso a la consola local de la gateway con Linux KVM.
2. En el menú principal Activación de dispositivo de AWS - Configuración, introduzca el número correspondiente para seleccionar Configurar proxy HTTP.
3. En el menú Configuración de proxy HTTP de activación de dispositivo de AWS , introduzca el número correspondiente a la tarea que desee realizar:
   - Configurar proxi HTTP: deberá proporcionar un nombre de host y un puerto para completar la configuración.
   - Ver la configuración de proxy HTTP actual: si no está configurado un proxy HTTP, se muestra el mensaje `HTTP Proxy not configured`. Si se ha configurado un proxy HTTP, se muestran el nombre de host y el puerto del proxy.
   - Eliminar la configuración de un proxy HTTP: se muestra el mensaje `HTTP Proxy Configuration Removed`.
4. Reinicie la máquina virtual para aplicar la configuración de HTTP.

Configuración de red de la puerta de enlace

La configuración de red predeterminada de la gateway es DHCP (Dynamic Host Configuration Protocol). Con DHCP, a la gateway se le asigna automáticamente una dirección IP. En algunos casos, es posible que tenga que asignar manualmente la IP de la gateway como una dirección IP estática, como se describe a continuación.

Cómo configurar la puerta de enlace para que utilice direcciones IP estáticas

1. Inicie sesión en la consola local de la gateway:
   - Para obtener más información sobre cómo iniciar sesión en la consola VMware ESXi local, consulteAcceder a la consola local de Gateway con VMware ESXi.
   - Para obtener más información sobre el inicio de sesión en la consola local de Microsoft Hyper-V, consulte Acceso a la consola local de la gateway con Microsoft Hyper-V.
   - Para obtener más información sobre el inicio de sesión en la consola local de KVM, consulte Acceso a la consola local de la gateway con Linux KVM.
2. En el menú principal Activación de dispositivo de AWS - Configuración, introduzca el número correspondiente para seleccionar Configuración de red.
3. En el menú Configuración de red, realice una de las siguientes tareas:

Cómo llevar a cabo esta tarea	Haga lo siguiente
Obtener información sobre el adaptador de red	Introduzca el número correspondiente para seleccionar Describir el adaptador. Aparecerá una lista de nombres de adaptador y se le pedirá que introduzca el nombre de un adaptador, por ejemplo, **`eth0`**. Si el adaptador que especifique está en uso, se mostrará la siguiente información acerca del adaptador: • Dirección MAC (Media Access Control) • Dirección IP • Máscara de red • Dirección IP de la gateway • Estado de habilitación de DHCP

Cómo llevar a cabo esta tarea	Haga lo siguiente
	Al configurar una dirección IP estática o al configurar el adaptador predeterminado de la puerta de enlace, se utilizan los nombres de los adaptadores que aparecen aquí.
Configurar el enrutamiento DHCP	Introduzca el número correspondiente para seleccionar Configurar DHCP. Se le pedirá que configure la interfaz de red para utilizar DHCP.

Cómo llevar a cabo esta tarea	Haga lo siguiente
Configurar una dirección IP estática para la gateway	Introduzca el número correspondiente para seleccionar Configurar IP estática. Se le pedirá que introduzca la siguiente información para configurar una IP estática: • Nombre del adaptador de red • Dirección IP • Máscara de red • Dirección de la gateway predeterminada • Dirección DNS (Domain Name Service) principal • Dirección DNS secundaria **Important** Si la puerta de enlace ya se ha activado, debe cerrarla y reiniciarla desde la consola de Storage Gateway para que la configuración surta efecto. Para obtener más información, consulte Apagado de la máquina virtual de puerta de enlace. Si la puerta de enlace utiliza más de una interfaz de red, debe configurar todas las

Cómo llevar a cabo esta tarea	Haga lo siguiente
	interfaces activas para que utilicen DHCP o direcciones IP estáticas. Por ejemplo, suponga que la máquina virtual de la gateway utiliza dos interfaces configura das como DHCP. Si más tarde establece una interfaz en una IP estática, la otra interfaz se desactivará. Para activar la interfaz en este caso, debe establecerla en una IP estática. Si ambas interfaces se establecen inicialme nte para que utilicen direcciones IP estáticas y, a continuación, configura la gateway para que utilice DHCP, ambas interfaces utilizarán DHCP.

Cómo llevar a cabo esta tarea	Haga lo siguiente
Configuración de un nombre de host para la puerta de enlace	Introduzca el número correspondiente para seleccionar Configurar nombre de host. Se le solicitará que elija si la puerta de enlace utilizará un nombre de host estático que usted especifique o si adquirirá uno automáticamente a través de DCHP o rDNS. Si selecciona Estático, se le solicitará que proporcione un nombre de host estático, como `testgateway.example.com` . Ingrese y para aplicar la configuración. **Note** Si configura un nombre de host estático para la puerta de enlace, asegúrese de que el nombre de host proporcionado esté en el dominio al que está unida la puerta de enlace. Debe crear un registro A en el sistema DNS que dirija la dirección IP de la puerta de enlace a su nombre de host estático.
Ver la configuración del nombre de host de la puerta de enlace	Introduzca el número correspondiente para seleccionar Ver configuración de nombre de host. Se muestran el nombre de host, el modo de adquisición, el dominio y el ámbito de Active Directory de la puerta de enlace.

Cómo llevar a cabo esta tarea	Haga lo siguiente
Restablecer toda la configuración de red de la gateway a DHCP	Introduzca el número correspondiente para seleccionar Restablecer todo a DHCP. Todas las interfaces de red se configuran para utilizar DHCP. **Important** Si la puerta de enlace ya se ha activado, debe cerrarla y reiniciarla desde la consola de Storage Gateway para que la configuración surta efecto. Para obtener más información, consulte Apagado de la máquina virtual de puerta de enlace.
Establecer el adaptador de ruta predeterminada del gateway	Introduzca el número correspondiente para seleccionar Establecer adaptador predeterminado. Se mostrarán los adaptadores disponibles para la puerta de enlace y se le pedirá que elija uno de los adaptadores, por ejemplo, **`eth0`**.
Editar la configuración de DNS de la gateway	Introduzca el número correspondiente para seleccionar Editar configuración de DNS. Se muestran los adaptadores disponibles de los servidores DNS primario y secundario. Se le pedirá que proporcione la dirección IP nueva.

Cómo llevar a cabo esta tarea	Haga lo siguiente
Ver la configuración de DNS de la ruta de enlace	Introduzca el número correspondiente para seleccionar Ver configuración de DNS. Se muestran los adaptadores disponibles de los servidores DNS primario y secundario. **Note** En algunas versiones del VMware hipervisor, puede editar la configuración del adaptador en este menú.
Ver tablas de ruteo	Introduzca el número correspondiente para seleccionar Ver rutas. Se muestra la ruta predeterminada de la gateway.

Probar la conexión de red de la puerta de enlace

Puede utilizar la consola local de la puerta de enlace para probar la conexión de red. Esta prueba puede ser útil para solucionar problemas de red con la gateway.

Cómo probar la conexión de red de la puerta de enlace

1. Inicie sesión en la consola local de la gateway:

   - Para obtener más información sobre cómo iniciar sesión en la consola VMware ESXi local, consulteAcceder a la consola local de Gateway con VMware ESXi.
   - Para obtener más información sobre el inicio de sesión en la consola local de Microsoft Hyper-V, consulte Acceso a la consola local de la gateway con Microsoft Hyper-V.
   - Para obtener más información sobre el inicio de sesión en la consola local de KVM, consulte Acceso a la consola local de la gateway con Linux KVM.

2. En el menú principal Activación de dispositivo de AWS - Configuración, introduzca el número correspondiente para seleccionar Probar conexión de red.

   Si la puerta de enlace ya se ha activado, la prueba de conexión comienza inmediatamente. En el caso de las puertas de enlace que aún no se han activado, debe especificar el tipo de punto final y tal Región de AWS como se describe en los pasos siguientes.
3. Si la puerta de enlace aún no está activada, introduzca el número correspondiente para seleccionar el tipo de punto de conexión de la puerta de enlace.
4. Si ha seleccionado el tipo de punto final público, introduzca el número correspondiente para seleccionar el Región de AWS que desee probar. Para ver los puntos de enlace de AWS servicio compatibles Regiones de AWS y una lista de los que puede usar con Storage Gateway, consulte los AWS Storage Gateway puntos de enlace y las cuotas en. Referencia general de AWS

A medida que avanza la prueba, cada punto de conexión muestra [APROBADA] o [ERROR], lo que indica el estado de la conexión de la siguiente manera:

Mensaje	Description (Descripción)
[PASSED]	Storage Gateway tiene conexión de red.
[FAILED]	Storage Gateway no tiene conexión de red.

Visualización del estado de los recursos de sistema de la puerta de enlace

Cuando la gateway se inicia, comprueba sus núcleos de CPU virtuales, el tamaño del volumen raíz y la RAM. Acto seguido, determina si estos recursos del sistema son suficientes para que la gateway funcione correctamente. Puede ver los resultados de esta comprobación en la consola local de la gateway.

Para ver el estado de un recurso del sistema, consulte

1. Inicie sesión en la consola local de la gateway:

   - Para obtener más información sobre cómo iniciar sesión en la VMware ESXi consola, consulteAcceder a la consola local de Gateway con VMware ESXi.
   - Para obtener más información sobre el inicio de sesión en la consola local de Microsoft Hyper-V, consulte Acceso a la consola local de la gateway con Microsoft Hyper-V.

- Para obtener más información sobre el inicio de sesión en la consola local de KVM, consulte Acceso a la consola local de la gateway con Linux KVM.

2. En el menú principal Activación de dispositivo de AWS - Configuración, introduzca el número correspondiente para seleccionar Ver comprobación de recursos del sistema.

   Cada recurso muestra [CORRECTO], [ADVERTENCIA] o [ERROR], lo que indica el estado del recurso de la siguiente manera:

Mensaje	Description (Descripción)
[OK]	El recurso ha superado la comprobación de recursos del sistema.
[WARNING]	El recurso no satisface los requisitos recomendados, pero la puerta de enlace continuará funcionando. Storage Gateway muestra un mensaje en el que se describen los resultados de la comprobación de recursos.
[FAIL]	El recurso no satisface los requisitos mínimos. Es posible que la puerta de enlace no funcione correctamente. Storage Gateway muestra un mensaje en el que se describen los resultados de la comprobación de recursos.

   La consola también muestra el número de errores y advertencias junto a la opción de menú de comprobación de recursos.

Configuración de un servidor NTP (Network Time Protocol) para la puerta de enlace

Puede ver y editar las configuraciones del servidor NTP (Network Time Protocol) y sincronizar la hora de la máquina virtual de la gateway con el host del hipervisor.

Cómo administrar la hora del sistema

1. Inicie sesión en la consola local de la gateway:

- Para obtener más información sobre cómo iniciar sesión en la consola VMware ESXi local, consulteAcceder a la consola local de Gateway con VMware ESXi.
- Para obtener más información sobre el inicio de sesión en la consola local de Microsoft Hyper-V, consulte Acceso a la consola local de la gateway con Microsoft Hyper-V.
- Para obtener más información sobre el inicio de sesión en la consola local de KVM, consulte Acceso a la consola local de la gateway con Linux KVM.

2. En el menú principal Activación de dispositivo de AWS - Configuración, introduzca el número correspondiente para seleccionar Administración de la hora del sistema.
3. En el menú Administración de la hora del sistema, introduzca el número correspondiente para realizar una de las siguientes tareas.

Cómo llevar a cabo esta tarea	Haga lo siguiente
Ver y sincronizar la hora de la máquina virtual con la hora del servidor NTP.	Introduzca el número correspondiente para seleccionar Ver y sincronizar la hora del sistema. Se muestra la hora actual de la máquina virtual. La puerta de enlace de archivo determina la diferencia horaria entre la máquina virtual de puerta de enlace y la hora del servidor NTP, y le pide que sincronice la hora de la máquina virtual con la hora de NTP. Una vez que la gateway esté implement ada y en funcionamiento, es posible que en algunos casos la hora de la MV se desvíe. Por ejemplo, supongamos que hay una interrupc ión prolongada de la red y el host del hiperviso r y la gateway no reciben actualizaciones de hora. En este caso, la hora de la máquina virtual de la gateway será diferente de la hora real. Cuando hay una desviación de hora, se produce una discrepancia entre las horas declaradas cuando se producen operaciones

Cómo llevar a cabo esta tarea	Haga lo siguiente
	tales como las instantáneas y las horas reales a las que se producen las operaciones. En el caso de una puerta de enlace implement ada VMware ESXi, basta con configurar la hora del host del hipervisor y sincronizar la hora de la máquina virtual con el host para evitar la pérdida de tiempo. Para obtener más información, consulte Sincronice la hora de la máquina virtual con la hora del host VMware. En el caso de gateways implementadas en Microsoft Hyper-V, debe comprobar periódica mente la hora de la MV. Para obtener más información, consulte Sincronización de la hora de la máquina virtual con la hora del host KVM de Hyper-V o Linux. Para una gateway implementada en KVM, puede comprobar y sincronizar la hora de la máquina virtual mediante la interfaz de línea de comandos `virsh` para KVM.
Editar la configuración del servidor NTP	Introduzca el número correspondiente para seleccionar Editar configuración de NTP. El sistema le pedirá que proporcione un servidor NTP preferido y uno secundario.
Ver la configuración del servidor NTP	Introduzca el número correspondiente para seleccionar Ver configuración de NTP. Se mostrará la configuración del servidor NTP.

Ejecución de comandos de Storage Gateway en la consola local

La consola local de la máquina virtual de Storage Gateway contribuye a proporcionar un entorno seguro para la configuración y el diagnóstico de problemas de la puerta de enlace. Con los comandos de la consola local, puede realizar tareas de mantenimiento, como guardar tablas de enrutamiento Soporte, conectarse a, etc.

Cómo ejecutar un comando de configuración o diagnóstico

1. Inicie sesión en la consola local de la gateway:
   - Para obtener más información sobre cómo iniciar sesión en la consola VMware ESXi local, consulteAcceder a la consola local de Gateway con VMware ESXi.
   - Para obtener más información sobre el inicio de sesión en la consola local de Microsoft Hyper-V, consulte Acceso a la consola local de la gateway con Microsoft Hyper-V.
   - Para obtener más información sobre el inicio de sesión en la consola local de KVM, consulte Acceso a la consola local de la gateway con Linux KVM.
2. En el menú principal Activación de dispositivo de AWS - Configuración, introduzca el número correspondiente para seleccionar Consola de puerta de enlace.
3. En la línea de comandos de la consola de la puerta de enlace, introduzca **h**.

   La consola muestra el menú COMANDOS DISPONIBLES con los comandos disponibles:

Comando	Función
dig	Recopilar los resultados de dig para la solución de problemas de DNS.
exit	Volver al menú de configuración.
h	Mostrar la lista de comandos disponibles.
ifconfig	Visualizar o configurar las interfaces de red. **Note** Recomendamos configurar los ajustes de red o IP mediante la consola de

Comando	Función
	Storage Gateway o la opción de menú de la consola local dedicada. Para obtener instrucciones, consulte Configuración de red de la puerta de enlace.
ip	Mostrar/manipular el enrutamiento, los dispositivos y los túneles. **Note** Recomendamos configurar los ajustes de red o IP mediante la consola de Storage Gateway o la opción de menú de la consola local dedicada. Para obtener instrucciones, consulte Configuración de red de la puerta de enlace.
iptables	Herramienta de administración para el filtrado IPv4 de paquetes y la NAT.
ncport	Probar la conexión a un puerto TCP específico en una red.
nping	Recopilar los resultados de nping para la solución de problemas de red.
open-support-channel	Connect to AWS Support. Para obtener instrucciones sobre cómo activar el acceso al AWS soporte, consulte de enlace EC2.
passwd	Actualizar tokens de autenticación.
save-iptables	Mantener tablas de IP.

Comando	Función
save-routing-table	Guardar una entrada de la tabla de enrutamie nto recién agregada.
tcptraceroute	Recopilar la salida de traceroute del tráfico TCP a un destino.
sslcheck	Devuelve el resultado con el emisor del certificado **Note** Storage Gateway utiliza la verificación del emisor del certificado y no admite la inspección de SSL. Si este comando devuelve un emisor distinto de aws-appliance@amazon.com, es probable que se trate de una aplicación que esté realizando una inspección de SSL. En ese caso, recomendamos omitir la inspección de SSL para el dispositivo de Storage Gateway.

4. En la línea de comandos de la consola de la puerta de enlace, introduzca el comando correspondiente a la función que desee utilizar y siga las instrucciones.

Para obtener información sobre un comando, escriba **`man`** + *`command name`* en la línea de comandos.

Realización de tareas en la consola local de la puerta de enlace de Amazon EC2

Algunas tareas de mantenimiento requieren que inicie sesión en la consola local cuando ejecute una puerta de enlace implementada en una instancia de Amazon EC2. En esta sección se describe cómo iniciar sesión en la consola local y realizar tareas de mantenimiento.

Temas

- Inicio de sesión en la consola local de la puerta de enlace de Amazon EC2: obtenga información sobre cómo conectarse a la consola local de la puerta de enlace de la instancia de Amazon EC2 e iniciar sesión en la puerta de enlace mediante la utilización de un cliente de Secure Shell (SSH).
- Direccionamiento de la puerta de enlace implementada en Amazon EC2 a través de un proxy HTTP- Aprenda a configurar un proxy Socket Secure versión 5 (SOCKS5) entre una instancia de Amazon EC2 AWS y una puerta de enlace implementada en una instancia de Amazon EC2.
- Probar la conexión de red de la puerta de enlace: obtenga información sobre cómo utilizar la consola local de la puerta de enlace para probar la conectividad de red entre la puerta de enlace y varios recursos de la red.
- Visualización del estado de los recursos de sistema de la puerta de enlace: obtenga información sobre cómo utilizar la consola local de la puerta de enlace para comprobar los núcleos de la CPU virtual de la puerta de enlace, el tamaño del volumen raíz y la RAM.
- Ejecución de comandos de Storage Gateway en la consola local para la puerta de enlace de Amazon EC2: obtenga información sobre cómo ejecutar comandos de la consola local para realizar tareas como guardar tablas de enrutamiento, conectarse a Soporte, etc.
- Configuración de red de la puerta de enlace de Amazon EC2: obtenga información sobre cómo usar la consola local para ver y configurar los ajustes de red, como el DNS y el nombre de host de una puerta de enlace en una instancia de Amazon EC2.

Inicio de sesión en la consola local de la puerta de enlace de Amazon EC2

Inicie sesión en la consola local de la puerta de enlace en una instancia de Amazon EC2 mediante el uso de un cliente de Secure Shell (SSH). Para obtener información detallada, consulte Conexión con la instancia en la Guía del usuario de Amazon EC2. Para conectarse de esta manera, necesitará el par de claves SSH que ha especificado al lanzar la instancia. Para obtener información sobre los pares de claves de Amazon EC2, consulte Pares de claves de Amazon EC2 en la Guía del usuario de Amazon EC2.

Cómo iniciar sesión en la consola local de la puerta de enlace

1. Conéctese a la instancia de Amazon EC2 mediante SSH e inicie sesión como usuario administrador.
2. Tras iniciar sesión, verá el menú principal Activación de dispositivo de AWS - Configuración, desde el que puede realizar diversas tareas.

Cómo obtener información sobre esta tarea	Consulte este tema
Configurar un proxy HTTP para la gateway	Direccionamiento de la puerta de enlace implementada en Amazon EC2 a través de un proxy HTTP
Configurar la red para la gateway	Configuración de red de la puerta de enlace de Amazon EC2
Probar la conectividad de red	Probar la conexión de red de la puerta de enlace
Ver una comprobación de recursos del sistema	Visualización del estado de los recursos de sistema de la puerta de enlace.
Ejecute los comandos de la consola de Storage Gateway	Ejecución de comandos de Storage Gateway en la consola local para la puerta de enlace de Amazon EC2

Para cerrar la gateway, escriba **0**.

Para salir de la sesión de configuración, introduzca **x**.

Direccionamiento de la puerta de enlace implementada en Amazon EC2 a través de un proxy HTTP

Storage Gateway es compatible con la configuración de un proxy Socket Secure versión 5 (SOCKS5) entre la puerta de enlace implementada en Amazon EC2 y AWS.

Si la gateway debe utilizar un servidor proxy para comunicarse con Internet, debe configurar los ajustes del proxy HTTP para la gateway. Para ello, especifique una dirección IP y un número de puerto para el host en el que se ejecuta el proxy. Una vez hecho esto, Storage Gateway enruta todo el AWS tráfico de puntos finales a través del servidor proxy. Las comunicaciones entre la puerta de enlace y los puntos de conexión están cifradas, incluso cuando se utiliza el proxy HTTP.

Cómo dirigir el tráfico de Internet de la gateway a través de un servidor proxy local

1. Inicie sesión en la consola local de la gateway. Para obtener instrucciones, consulte Inicio de sesión en la consola local de la puerta de enlace de Amazon EC2.
2. En el menú principal Activación de dispositivo de AWS - Configuración, introduzca el número correspondiente para seleccionar Configurar proxy HTTP.
3. En el menú Configuración de proxy HTTP de activación de dispositivo de AWS , introduzca el número correspondiente a la tarea que desee realizar:

   - Configurar proxi HTTP: deberá proporcionar un nombre de host y un puerto para completar la configuración.
   - Ver la configuración de proxy HTTP actual: si no está configurado un proxy HTTP, se muestra el mensaje `HTTP Proxy not configured`. Si se ha configurado un proxy HTTP, se muestran el nombre de host y el puerto del proxy.
   - Eliminar la configuración de un proxy HTTP: se muestra el mensaje `HTTP Proxy Configuration Removed`.

Probar la conexión de red de la puerta de enlace

Puede utilizar la consola local de la puerta de enlace para probar la conexión de red. Esta prueba puede ser útil para solucionar problemas de red con la gateway.

Cómo probar la conexión de red de la puerta de enlace

1. Inicie sesión en la consola local de la gateway. Para obtener instrucciones, consulte Inicio de sesión en la consola local de la puerta de enlace de Amazon EC2.
2. En el menú principal Activación de dispositivo de AWS - Configuración, introduzca el número correspondiente para seleccionar Probar conexión de red.

   Si la puerta de enlace ya se ha activado, la prueba de conexión comienza inmediatamente. En el caso de las puertas de enlace que aún no se han activado, debe especificar el tipo de punto final y tal Región de AWS como se describe en los pasos siguientes.
3. Si la puerta de enlace aún no está activada, introduzca el número correspondiente para seleccionar el tipo de punto de conexión de la puerta de enlace.
4. Si ha seleccionado el tipo de punto final público, introduzca el número correspondiente para seleccionar el Región de AWS que desee probar. Para ver los puntos de enlace de AWS servicio

compatibles Regiones de AWS y una lista de los que puede usar con Storage Gateway, consulte los AWS Storage Gateway puntos de enlace y las cuotas en. Referencia general de AWS

A medida que avanza la prueba, cada punto de conexión muestra [APROBADA] o [ERROR], lo que indica el estado de la conexión de la siguiente manera:

Mensaje	Description (Descripción)
[PASSED]	Storage Gateway tiene conexión de red.
[FAILED]	Storage Gateway no tiene conexión de red.

Visualización del estado de los recursos de sistema de la puerta de enlace

Cuando la puerta de enlace de archivo se inicia, comprueba sus núcleos de CPU virtuales, el tamaño del volumen raíz y la RAM. Acto seguido, determina si los recursos del sistema disponibles son suficientes para que la puerta de enlace funcione correctamente. Puede ver los resultados de la comprobación de los recursos del sistema mediante la consola local de la puerta de enlace.

Para ver el estado de un recurso del sistema, consulte

1. Inicie sesión en la consola local de la puerta de enlace de archivo de Amazon EC2. Para obtener instrucciones, consulte Inicio de sesión en la consola local de la puerta de enlace de Amazon EC2.
2. En el menú principal Activación de dispositivo de AWS - Configuración, introduzca el número correspondiente para seleccionar Ver comprobación de recursos del sistema.

   La consola local de la puerta de enlace muestra [OK], [WARNING] o [FAIL] para indicar el estado del recurso de la siguiente manera:

Mensaje	Description (Descripción)
[OK]	El recurso ha superado la comprobación de recursos del sistema.
[WARNING]	El recurso no satisface los requisitos recomendados, pero la puerta de enlace

Mensaje	Description (Descripción)
	continuará funcionando. La consola local de la puerta de enlace muestra un mensaje en el que se describen los resultados de la comprobación de recursos.
[FAIL]	El recurso no satisface los requisitos mínimos. Es posible que la puerta de enlace no funcione correctamente. La consola local de la puerta de enlace muestra un mensaje en el que se describen los resultados de la comprobación de recursos.

La consola local también muestra el número de errores y advertencias junto a la opción de menú de comprobación de recursos.

Ejecución de comandos de Storage Gateway en la consola local para la puerta de enlace de Amazon EC2

La AWS Storage Gateway consola ayuda a proporcionar un entorno seguro para configurar y diagnosticar problemas con la puerta de enlace. Con los comandos de la consola, puede realizar tareas de mantenimiento, como guardar tablas de enrutamiento o conectarse a Soporte ellas.

Cómo ejecutar un comando de configuración o diagnóstico

1. Inicie sesión en la consola local de la gateway. Para obtener instrucciones, consulte Inicio de sesión en la consola local de la puerta de enlace de Amazon EC2.
2. En el menú principal Activación de dispositivo de AWS - Configuración, introduzca el número correspondiente para seleccionar Consola de puerta de enlace.
3. En la línea de comandos de la consola de la puerta de enlace, introduzca **h**.

   La consola muestra el menú COMANDOS DISPONIBLES con los comandos disponibles:

Comando	Función
dig	Recopilar los resultados de dig para la solución de problemas de DNS.
exit	Volver al menú de configuración.
h	Mostrar la lista de comandos disponibles.
ifconfig	Visualizar o configurar las interfaces de red. **Note** Recomendamos configurar los ajustes de red o IP mediante la consola de Storage Gateway o la opción de menú de la consola local dedicada. Para obtener instrucciones, consulte Configuración de red de la puerta de enlace.
ip	Mostrar/manipular el enrutamiento, los dispositivos y los túneles. **Note** Recomendamos configurar los ajustes de red o IP mediante la consola de Storage Gateway o la opción de menú de la consola local dedicada. Para obtener instrucciones, consulte Configuración de red de la puerta de enlace.
iptables	Herramienta de administración para el filtrado IPv4 de paquetes y la NAT.

Comando	Función
ncport	Probar la conexión a un puerto TCP específico en una red.
nping	Recopilar los resultados de nping para la solución de problemas de red.
open-support-channel	Connect to AWS Support.
save-iptables	Mantener tablas de IP.
save-routing-table	Guardar una entrada de la tabla de enrutamie nto recién agregada.
tcptraceroute	Recopilar la salida de traceroute del tráfico TCP a un destino.

4. En la línea de comandos de la consola de la puerta de enlace, introduzca el comando correspondiente a la función que desee utilizar y siga las instrucciones.

Para obtener información sobre un comando, escriba **`man`** + *`command name`* en la línea de comandos.

Configuración de red de la puerta de enlace de Amazon EC2

Puede ver y configurar la red para la puerta de enlace de archivo de Amazon EC2 mediante la consola local de la puerta de enlace.

Cómo configurar la red

1. Inicie sesión en la consola local de la puerta de enlace de archivo de Amazon EC2. Para obtener instrucciones, consulte Inicio de sesión en la consola local de la puerta de enlace de Amazon EC2.
2. En el menú principal Activación de dispositivo de AWS - Configuración, introduzca el número correspondiente para seleccionar Configuración de red.
3. En el menú Activación de dispositivo de AWS - Configuración de red, introduzca el número correspondiente a la tarea que desee realizar:

- Editar configuración de DNS: la consola local de la puerta de enlace muestra los adaptadores disponibles para los servidores DNS principal y secundario. A continuación, la consola le pide que proporcione la nueva dirección IP.
- Ver configuración de DNS: la consola local de la puerta de enlace muestra los adaptadores disponibles para los servidores DNS principal y secundario.
- Configurar nombre de host: la consola local de la puerta de enlace le solicitará que elija si la puerta de enlace utilizará un nombre de host estático que usted especifique o si adquirirá un nombre de host automáticamente a través de DCHP o rDNS.

  > **Note**
  >
  > Si configura un nombre de host estático para la puerta de enlace, debe crear un registro A en el sistema DNS que dirija la dirección IP de la puerta de enlace a su nombre de host estático.

- Ver configuración de nombre de host: la consola local de la puerta de enlace muestra el nombre de host, el modo de adquisición, el dominio y el ámbito de Active Directory para la puerta de enlace de archivo de Amazon EC2.

Apagado de la máquina virtual de puerta de enlace

Puede que tenga que apagar la máquina virtual o reiniciarla para realizar tareas de mantenimiento, como aplicar un parche al hipervisor. Apague las máquinas virtuales de puerta de enlace en las instalaciones mediante la interfaz del hipervisor y las instancias de Amazon EC2 con la consola de Amazon EC2.

> **Important**
>
> Si detiene e inicia una puerta de enlace de Amazon EC2 que utiliza almacenamiento efímero, esta se desconectará permanentemente. Esto sucede porque se ha reemplazado el disco de almacenamiento físico. No hay una solución para este problema. La única solución es eliminar la puerta de enlace y activar una nueva en una nueva instancia de EC2.

Sustituir la puerta de enlace de archivos de existente por una nueva instancia

Puede reemplazar una puerta de enlace de archivos de existente por una nueva instancia a medida que aumenten sus necesidades de datos y rendimiento, o si recibe una AWS notificación para migrar su puerta de enlace. Puede que tenga que hacerlo si quiere trasladar la puerta de enlace a una plataforma de host mejor o a instancias de Amazon EC2 más nuevas, o si desea actualizar el hardware del servidor subyacente.

> **Important**
>
> Utilice estas instrucciones únicamente para migrar dispositivos de puerta de enlace que ejecuten la versión 1.x. No puede utilizarlos para migrar dispositivos de puerta de enlace que ejecuten versiones anteriores.

> **Note**
>
> La migración solo se puede realizar entre puertas de enlace del mismo tipo. Por ejemplo, no puede migrar la configuración o los datos de una puerta de enlace de FSx archivos a una puerta de enlace de archivos S3.

Para reemplazar la puerta de enlace de FSx File Gateway por una nueva instancia con un disco de caché vacío y un nuevo ID de puerta de enlace:

1. Detenga cualquier aplicación que esté grabando en la puerta de enlace de archivos de existente. Compruebe que la métrica `CachePercentDirty` de la pestaña Supervisión es `0` antes de configurar las asociaciones de sistemas de archivos en la nueva puerta de enlace.
2. Utilice AWS Command Line Interface (AWS CLI) para recopilar y guardar la información de configuración sobre su puerta de enlace de archivos de existente y los sistemas de archivos asociados de la siguiente manera:

    a. Guarde la información de configuración de la puerta de enlace para la puerta de enlace de archivos de .

```
aws storagegateway describe-gateway-information --gateway-arn
 "arn:aws:storagegateway:us-east-2:123456789012:gateway/sgw-12A3456B"
```

Este comando devuelve un bloque JSON que contiene los metadatos de una puerta de enlace, por ejemplo, su nombre, las interfaces de red, la zona horaria configurada y el estado (es decir, si la puerta de enlace se está ejecutando o no).

b. Guarde la configuración del bloque de mensajes del servidor (SMB) de la puerta de enlace de .

```
aws storagegateway describe-smb-settings --gateway-arn
 "arn:aws:storagegateway:us-east-2:123456789012:gateway/sgw-12A3456B"
```

Este comando devuelve un bloque JSON que contiene el nombre de dominio de Microsoft Active Directory al que se ha unido la puerta de enlace.

c. Guarde la información de uso compartido de archivos para cada sistema de archivos asociado a la puerta de enlace de :

Utilice el siguiente comando para cada sistema de archivos asociado.

```
aws storagegateway describe-file-system-associations --file-system-
association-arn-list "arn:aws:storagegateway:us-east-2:123456789012:fs-
association/fsa-987A654B"
```

Este comando devuelve un bloque JSON que contiene los metadatos del sistema de archivos, por ejemplo, su ARN de ubicación, el destino del registro de auditoría, los atributos de actualización de la caché, las direcciones IP configuradas y las etiquetas.

3. Cree una nueva puerta de enlace de archivos con los mismos ajustes y configuración que la puerta de enlace anterior. Si es necesario, consulte la información que guardó en el paso 2.
4. Cree nuevas asociaciones de sistemas de archivos para la nueva puerta de enlace con los mismos ajustes y configuración que los sistemas de archivos que se configuraron en la puerta de enlace anterior. Si es necesario, consulte la información que guardó en el paso 2.
5. Compruebe que la nueva puerta de enlace funciona correctamente y, a continuación, reasigne o transfiera a los clientes de los sistemas de archivos antiguos a los nuevos de la manera que mejor se adapte a su entorno.

6. Confirme que la nueva puerta de enlace funciona correctamente y, a continuación, elimine la puerta de enlace anterior de la consola de Storage Gateway.

> **Important**
>
> Antes de eliminar una puerta de enlace de archivos de , asegúrese de que actualmente no haya ninguna aplicación grabando en la memoria caché de esa puerta de enlace. Si elimina la puerta de enlace mientras se esté utilizando, puede producirse pérdida de datos.

> **Warning**
>
> Cuando se elimina una puerta de enlace, no se puede recuperar.

7. Elimine la máquina virtual de puerta de enlace anterior o la instancia de Amazon EC2.

Eliminación de la puerta de enlace y eliminación de los recursos asociados

Si no planea continuar utilizando la gateway, considere la posibilidad de eliminar la gateway y los recursos asociados. La eliminación de recursos evita incurrir en cargos por recursos que no planee continuar utilizando y ayuda a reducir la factura mensual.

Al eliminar una puerta de enlace, deja de aparecer en la consola AWS Storage Gateway de administración y sus conexiones al sistema de archivos se cierran. El procedimiento para eliminar una gateway es el mismo para todos los tipos de gateway; sin embargo, según el tipo de gateway que desee borrar y el host en el que esté implementada, debe seguir instrucciones específicas para eliminar los recursos asociados.

Puede eliminar una puerta de enlace mediante la consola de Storage Gateway o mediante programación. A continuación puede encontrar información sobre cómo eliminar una puerta de enlace mediante la consola de Storage Gateway. Si desea eliminar la puerta de enlace mediante programación, consulte Referencia de la API de AWS Storage Gateway..

Eliminación de la puerta de enlace mediante la consola de Storage Gateway

El procedimiento para eliminar una gateway es el mismo para todos los tipos de gateway. Sin embargo, según el tipo de gateway que desee eliminar y el host en el que se haya implementado la gateway, es posible que tenga que realizar tareas adicionales para eliminar los recursos asociados a la gateway. La eliminación de estos recursos le ayudará a evitar pagar por recursos que no planee utilizar.

> **Note**
>
> Para puertas de enlace implementadas en una instancia de Amazon EC2, la instancia continúa existiendo hasta que la elimine.
> Para puerta de enlaces implementadas en una máquina virtual (VM), después de eliminar la puerta de enlace, la puerta de enlace continúa existiendo en el entorno de virtualización. Para eliminar la máquina virtual, utilice el cliente VMware vSphere, Microsoft Hyper-V Manager o el cliente de máquina virtual basada en el núcleo de Linux (KVM) para conectarse al host y eliminar la máquina virtual. Tenga en cuenta que no es posible reutilizar la MV de la gateway eliminada para activar una nueva gateway.

Cómo eliminar una puerta de enlace

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Elija puertas de enlace y, a continuación, seleccione una o más puertas de enlace para eliminarlas.
3. En Actions (Acciones), elija Delete gateway (Eliminar la gateway). Aparece el cuadro de diálogo de confirmación.

> **Warning**
>
> Antes de realizar este paso, asegúrese de que no haya aplicaciones escribiendo en los volúmenes de la puerta de enlace. Si elimina la gateway mientras se esté utilizando, puede producirse pérdida de datos. Cuando se elimina una gateway, no se puede recuperar.

4. Compruebe que desea eliminar las puertas de enlace especificadas, escriba la palabra eliminar en el cuadro de confirmación y seleccione Eliminar.
5. (Opcional) Si desea proporcionar comentarios sobre la puerta de enlace eliminada, complete el cuadro de diálogo de comentarios y, a continuación, seleccione Enviar. De lo contrario, elija Omitir.

> **Important**
>
> Después de eliminar una puerta de enlace dejará de pagar cargos por el software, pero persistirán recursos como el bucket de Amazon S3 y las instancias de Amazon EC2. Puede eliminar la puerta de enlace de la instancia de Amazon EC2 después de eliminar la puerta de enlace de archivo.

Rendimiento y optimización

En esta sección se describen las directrices y las prácticas recomendadas para optimizar el rendimiento de la puerta de enlace de archivo.

Temas

- Guía básica de rendimiento para File Gateway
- Optimizing Gateway Performance
- Maximización del rendimiento de la puerta de enlace de archivo de S3
- Optimización de la puerta de enlace de archivo de S3 para copias de seguridad de bases de datos de SQL Server

Guía básica de rendimiento para File Gateway

En esta sección, encontrará instrucciones para el aprovisionamiento de hardware para su máquina virtual de FSx File Gateway. Las configuraciones de instancias que se indican en la tabla son ejemplos y se proporcionan como referencia.

Para un rendimiento óptimo, el tamaño del disco en caché debe ajustarse al tamaño del conjunto de trabajo activo. El uso de varios discos locales para la caché aumenta el rendimiento de escritura mediante el acceso en paralelo a los datos e incrementa la velocidad de E/S (IOPS).

> **Note**
>
> No recomendamos el uso del almacenamiento efímero. Para obtener información sobre el uso del almacenamiento efímero, consulte Uso del almacenamiento efímero con puertas de enlace de EC2.
> El límite de tamaño recomendado para los directorios individuales de los sistemas de archivos que se conectan a la puerta de enlace de archivo de 10 000 archivos por directorio. Puede usar la puerta de enlace de archivo con directorios que tengan más de 10 000 archivos, pero es posible que el rendimiento se vea afectado.

En la siguiente tabla, las operaciones de lectura de aciertos de la caché son lecturas de los datos de archivos que se obtienen desde la caché. Las operaciones de lectura errónea de la caché son lecturas de los datos de archivos que se proporcionan desde Amazon FSx para Windows File Server.

La siguiente tabla muestra un ejemplo de configuración de FSx File Gateway.

FSx Rendimiento de File Gateway en clientes Windows

Configuración de ejemplo	Protocolo	Rendimiento de escritura (tamaños de archivos 1 GB)	Rendimiento de lectura de aciertos de la caché	Rendimiento de lectura de errores de la caché
Disco raíz: 80 GB, io1 SSD, 4000 IOPS Discos caché: 2 discos NVME de 2 TiB Rendimiento mínimo de red: 10 Gbps CPU: 32 vCPU | RAM: 24 GB	SMBv3 - 1 hilo	162 MiB/sec (1,4 Gbps)	403 MiB/sec (3,4 Gbps)	288 MiB/sec (2,4 Gbps)
	SMBv3 - 8 hilos	511 MiB/sec (4,3 Gbps)	571 MiB/sec (4,8 Gbps)	567 MiB/sec (4,8 Gbps)

> **Note**
>
> El rendimiento puede variar en función de la configuración de la plataforma de host y el ancho de banda de la red. El rendimiento de escritura disminuye con el tamaño del archivo, y el rendimiento más alto que se puede lograr para archivos pequeños (menos de 32 MiB) es de 16 archivos por segundo.

Optimizing Gateway Performance

A continuaciónnuación encontrará información sobre cómo optimizar el rendimiento de la gateway. La orientación se basa en la adición de recursos a la gateway y la adición de recursos al servidor de aplicaciones.

Añada recursos a la gateway

Puede optimizar el rendimiento de la gateway añadiendo recursos a la misma mediante uno o varios de los métodos siguientes.

Utilice discos de mayor rendimiento

Para optimizar el rendimiento de la puerta de enlace, puede añadir discos de alto rendimiento, como unidades de estado sólido (SSDs) y una NVMe controladora. También puede asociar discos virtuales a la MV directamente desde una red de área de almacenamiento (SAN) en lugar de Microsoft Hyper-V NTFS. La mejora del rendimiento del disco generalmente se traduce en un mejor rendimiento y en más input/output operaciones por segundo (IOPS). Para obtener más información sobre cómo agregar discos, consulte Configuración de almacenamiento en caché adicional.

Para medir el rendimiento, utilice las métricas `ReadBytes` y `WriteBytes` con la estadística `Samples` de Amazon CloudWatch . Por ejemplo, la estadística `Samples` de la métrica `ReadBytes` durante un periodo muestra de 5 minutos, dividida por 300 segundos devuelve las IOPS. Por regla general, cuando revise estas métricas por una gateway, busque tendencias de bajo rendimiento y bajas IOPS, que indican cuellos de botella.

> **Note**
>
> CloudWatch las métricas no están disponibles para todas las puertas de enlace. Para obtener información sobre métricas de puertas de enlace, consulte Supervisión de su puerta de enlace de .

Añada recursos de CPU al host de la gateway

El requisito mínimo para un servidor de alojamiento de gateway son cuatro procesadores virtuales. Para optimizar el rendimiento de la gateway, compruebe que los cuatro procesadores virtuales asignados a la máquina virtual de la gateway están respaldados por cuatro núcleos. Además, confirme que no está sobresuscribiendo el servidor CPUs anfitrión.

Cuando agrega más CPUs al servidor host de la puerta de enlace, aumenta la capacidad de procesamiento de la puerta de enlace. De este modo, la puerta de enlace podrá gestionar, paralelamente, el almacenamiento de los datos de la aplicación en el almacenamiento local y la carga de estos datos en para Windows File Server. CPUs Además, ayuda a garantizar que su

puerta de enlace reciba suficientes recursos de CPU cuando el host se comparte con otros VMs. Proporcionar suficientes recursos de CPU tiene el efecto general de mejorar el rendimiento.

Storage Gateway admite el uso de 24 CPUs en el servidor host de la puerta de enlace. Puede usar 24 CPUs para mejorar significativamente el rendimiento de su puerta de enlace. Le recomendamos la siguiente configuración de gateway para el servidor de alojamiento de la gateway:

- 24 CPUs.
- 16 GiB de RAM reservada para puertas de enlace de archivo
  - 16 GiB de RAM reservados para puertas de enlace con un tamaño de caché de hasta 16 TiB
  - 32 GiB de RAM reservados para puertas de enlace con un tamaño de caché de 16 TiB a 32 TiB
  - 48 GiB de RAM reservados para puertas de enlace con un tamaño de caché de 32 TiB a 64 TiB
- Disco 1 asociado a controlador paravirtual 1, que se utiliza como caché de la gateway de la manera siguiente:
  - SSD con un NVMe controlador.
- Adaptador de red 1 configurado en red de MV 1:
  - Utilice la red VM 1 y añada VMXnet3 (10 Gbps) para utilizarla en la ingestión.
- Adaptador de red 2 configurado en red de MV 2:
  - Utilice la red VM 2 y añada una VMXnet3 (10 Gbps) para conectarla. AWS

Respalde los discos virtuales de la gateway con discos físicos independientes

Cuando aprovisione discos para una puerta de enlace, le recomendamos encarecidamente que no aprovisione discos locales para el almacenamiento local que utilicen el mismo disco de almacenamiento físico subyacente. Por ejemplo VMware ESXi, los recursos de almacenamiento físico subyacentes se representan como un almacén de datos. Al implementar la máquina virtual de gateway, debe elegir el almacén de datos en el que se almacenarán los archivos de la máquina virtual. Cuando aprovisione un disco virtual (por ejemplo, como búfer de carga), puede almacenar el disco virtual en el mismo almacén de datos que la máquina virtual o en un almacén de datos diferente.

Si tiene más de un almacén de datos, le recomendamos encarecidamente que elija un almacén de datos para cada tipo de almacenamiento local que esté creando. Un almacén de datos respaldado por un único disco físico subyacente puede dar lugar a un bajo rendimiento. Por

ejemplo, cuando se utiliza el mismo disco para respaldar tanto el almacenamiento en caché como para el búfer de carga en una configuración de gateway. Del mismo modo, un almacén de datos respaldado por una configuración RAID que no sea de alto rendimiento, como RAID 1, puede dar lugar a un bajo rendimiento.

Añada recursos al entorno de aplicaciones

Aumente el ancho de banda entre el servidor de aplicaciones y la gateway

Para optimizar el rendimiento de la puerta de enlace, asegúrese de que el ancho de banda de la red entre la aplicación y la puerta de enlace puede sostener las necesidades de la aplicación. Puede utilizar las métricas `ReadBytes` y `WriteBytes` de la puerta de enlace para medir el rendimiento de datos total.

Para la aplicación, compare el rendimiento medido con el rendimiento deseado. Si el rendimiento medido es inferior al deseado, un aumento del ancho de banda entre la aplicación y la gateway puede aumentar el rendimiento si la red es el cuello de botella. Del mismo modo, puede aumentar el ancho de banda entre la MV y los discos locales, si no están conectados directamente.

Añada recursos de CPU al entorno de aplicaciones

Si la aplicación puede utilizar recursos de CPU adicionales, añadir más CPUs puede ayudar a la aplicación a escalar su I/O carga.

Algunas operaciones con archivos en la puerta de enlace de FSx archivos, como cambiar el nombre de las carpetas de nivel superior o los cambios de permisos, pueden provocar varias operaciones con archivos y provocar una I/O carga elevada en el sistema de archivos del servidor de archivos de Windows. FSx Si el sistema de archivos no tiene suficientes recursos de rendimiento para su carga de trabajo, es posible que elimine las instantáneas, ya que da prioridad a la disponibilidad para la retención continua de instantáneas por I/O encima de la histórica.

En la FSx consola de Amazon, consulta la página Supervisión y rendimiento para ver si tu sistema de archivos está insuficientemente aprovisionado. Si es así, puede cambiar a un almacenamiento en SSD, aumentar la capacidad de rendimiento o aumentar las IOPS en SSD para gestionar su carga de trabajo.

Maximización del rendimiento de la puerta de enlace de archivo de S3

En las siguientes secciones se describen las prácticas recomendadas para maximizar el rendimiento entre los clientes de NFS y SMB, la puerta de enlace de archivo de S3 y Amazon S3. Las directrices que se proporcionan en cada sección contribuyen gradualmente a mejorar el rendimiento general. Si bien ninguna de estas recomendaciones es obligatoria y no son interdependientes, se han seleccionado y ordenado de forma lógica para probar y ajustar las implementaciones de S3 File Gateway. Soporte Al implementar y probar estas sugerencias, tenga en cuenta que cada implementación de la puerta de enlace de archivo de S3 es única, por lo que los resultados pueden variar.

La puerta de enlace de archivo de S3 proporciona una interfaz de archivos para almacenar y recuperar objetos de Amazon S3 mediante protocolos de archivos NFS o SMB estándares del sector, con una asignación 1:1 nativa entre el archivo y el objeto. Puede implementar S3 File Gateway como una máquina virtual local en su VMware entorno KVM de Microsoft Hyper-V o Linux, o en la AWS nube como una instancia de Amazon EC2. La puerta de enlace de archivo de S3 no está diseñada para sustituir completamente a la NAS empresarial. La puerta de enlace de archivo de S3 emula un sistema de archivos, pero no lo es. El uso de Amazon S3 como almacenamiento interno duradero genera una sobrecarga adicional en cada I/O operación, por lo que evaluar el rendimiento de S3 File Gateway con respecto a un NAS o servidor de archivos existente no es una comparación equivalente.

Implementar la puerta de enlace en la misma ubicación que los clientes

Se recomienda implementar el dispositivo virtual de puerta de enlace de archivo de S3 en una ubicación física con la menor latencia de red posible entre este y sus clientes de NFS o SMB. A la hora de elegir una ubicación para la puerta de enlace, tenga en cuenta lo siguiente:

- Una menor latencia de la red en la puerta de enlace puede ayudar a mejorar el rendimiento de los clientes de NFS o SMB.
- La puerta de enlace de archivo de S3 está diseñada para tolerar una latencia de red más alta entre la puerta de enlace y Amazon S3 que entre la puerta de enlace y los clientes.
- Para las instancias de la puerta de enlace de archivo de S3 implementadas en Amazon EC2, se recomienda mantener la puerta de enlace y los clientes de NFS o SMB en el mismo grupo de ubicación. Para obtener más información, consulte Grupos de ubicación para instancias de Amazon EC2 en la Guía del usuario de Amazon Elastic Compute Cloud.

Reducir los cuellos de botella causados por la lentitud de los discos

Recomendamos monitorear la `IoWaitPercent` CloudWatch métrica para identificar los cuellos de botella en el rendimiento que pueden resultar de la lentitud de los discos de almacenamiento en su S3 File Gateway. Al intentar optimizar los problemas de rendimiento relacionados con los discos, tenga en cuenta lo siguiente:

- `IoWaitPercent` indica el porcentaje de tiempo que la CPU está a la espera de recibir una respuesta de los discos raíz o de caché.
- Cuando `IoWaitPercent` es superior al 5 o 10 %, esto suele indicar un cuello de botella en el rendimiento de la puerta de enlace provocado por discos con bajo rendimiento. Esta métrica debe estar lo más cerca posible del 0 %, lo que significa que la puerta de enlace nunca espera en el disco, lo que ayuda a optimizar los recursos de la CPU.
- Puede consultar `IoWaitPercent` la pestaña Supervisión de la consola Storage Gateway o configurar CloudWatch las alarmas recomendadas para que le notifiquen automáticamente si la métrica supera un umbral específico. Para obtener más información, consulte Crear CloudWatch las alarmas recomendadas para la puerta de enlace.
- Le recomendamos que utilice una unidad SSD NVMe o una unidad SSD para los discos raíz y caché de la puerta de enlace, a fin de minimizar el riesgo`IoWaitPercent`.

Ajustar la asignación de recursos de la máquina virtual para los discos de CPU, RAM y caché

Al intentar optimizar el rendimiento de la puerta de enlace de archivo de S3, es importante asignar suficientes recursos a la máquina virtual de puerta de enlace, incluidos los discos de CPU, RAM y caché. Los requisitos mínimos de recursos virtuales de 4 CPUs, 16 GB de RAM y 150 GB de almacenamiento en caché suelen ser adecuados solo para cargas de trabajo más pequeñas. Al asignar recursos virtuales a cargas de trabajo más grandes, se recomienda lo siguiente:

- Aumente el número asignado CPUs a entre 16 y 48, en función del uso típico de la CPU que genere su S3 File Gateway. Puede supervisar el uso de la CPU mediante la métrica `UserCpuPercent`. Para obtener más información, consulte Descripción de métricas de la puerta de enlace.
- Aumente la RAM asignada a entre 32 y 64 GB.

> **Note**
>
> La puerta de enlace de archivo S3 no puede utilizar más de 64 GB de RAM.

- Utilice NVMe un SSD para los discos raíz y el disco de caché, y ajuste el tamaño de los discos de caché para adaptarlos al conjunto de datos de trabajo máximo que planea escribir en la puerta de enlace. Para obtener más información, consulte las mejores prácticas de tamaño de caché de S3 File Gateway en el YouTube canal oficial de Amazon Web Services.
- Añada al menos 4 discos de caché virtuales a la puerta de enlace, en lugar de utilizar un único disco grande. Varios discos virtuales pueden mejorar el rendimiento incluso si comparten el mismo disco físico subyacente, pero las mejoras suelen ser mayores cuando los discos virtuales se encuentran en discos físicos subyacentes diferentes.

  Por ejemplo, si quiere implementar 12 TB de caché, puede utilizar una de las siguientes configuraciones:

  - 4 discos de caché de 3 TB
  - 8 discos de caché de 1,5 TB
  - 12 discos de caché de 1 TB

  Esto no solo permite una administración más eficiente del rendimiento, sino también de la máquina virtual a lo largo del tiempo. A medida que cambie su carga de trabajo, puede aumentar gradualmente la cantidad de discos de caché y la capacidad total de caché, al tiempo que mantiene el tamaño original de cada disco virtual individual para preservar la integridad de la puerta de enlace.

  Para obtener más información, consulte Cálculo de la cantidad de almacenamiento en disco local.

Cuando implemente la puerta de enlace de archivo de S3 como una instancia de Amazon EC2, tenga en cuenta lo siguiente:

- El tipo de instancia que elija puede afectar significativamente al rendimiento de la puerta de enlace. Amazon EC2 ofrece una amplia flexibilidad para ajustar la asignación de recursos para la instancia de la puerta de enlace de archivo de S3.
- Para ver los tipos de instancia de Amazon EC2 recomendados para la puerta de enlace de archivo de S3, consulte Requisitos para los tipos de instancia de Amazon EC2.

- Puede cambiar el tipo de instancia de Amazon EC2 que aloja una puerta de enlace de archivo de S3 activa. Esto le permite ajustar fácilmente la generación de hardware y la asignación de recursos de Amazon EC2 para encontrar una proporción ideal price-to-performance. Para cambiar el tipo de instancia, utilice el siguiente procedimiento en la consola de Amazon EC2:

  1. Detenga la instancia de Amazon EC2.
  2. Cambie el tipo de instancia de Amazon EC2.
  3. Encienda la instancia de Amazon EC2.

  > **Note**
  >
  > Si detiene una instancia que aloja una puerta de enlace de archivo de S3, se interrumpirá temporalmente el acceso a los recursos compartidos de archivos. Asegúrese de programar un período de mantenimiento si es necesario.

- La price-to-performance proporción de una instancia Amazon EC2 se refiere a la potencia de cálculo que obtiene por el precio que paga. Por lo general, las instancias Amazon EC2 de nueva generación ofrecen la mejor price-to-performance relación, con un hardware más nuevo y un rendimiento mejorado a un costo relativamente menor en comparación con las generaciones anteriores. Factores como el tipo de instancia, la región y los patrones de uso influyen en esta relación, por lo que es importante seleccionar la instancia adecuada para su carga de trabajo específica a fin de optimizar la rentabilidad.

Ajustar el nivel de seguridad de SMB

El SMBv3 protocolo permite tanto la firma como el cifrado SMB, lo que tiene algunas desventajas en cuanto a rendimiento y seguridad. Para optimizar el rendimiento, puede ajustar el nivel de seguridad de SMB de la puerta de enlace para especificar cuáles de estas características de seguridad se aplican a las conexiones de los clientes. Para obtener más información, consulte Establecer un nivel de seguridad para la puerta de enlace.

A la hora de ajustar el nivel de seguridad de SMB, tenga en cuenta lo siguiente:

- El nivel de seguridad predeterminado para la puerta de enlace de archivo de S3 Aplicar cifrado. Esta configuración aplica tanto el cifrado como la firma de las conexiones de los clientes de SMB a los recursos compartidos de archivos de la puerta de enlace, lo que significa que todo el tráfico del cliente a la puerta de enlace está cifrado. Esta configuración no afecta al tráfico desde la puerta de enlace a AWS, que siempre está cifrado.

La puerta de enlace limita cada conexión de cliente cifrada a una sola vCPU. Por ejemplo, si solo tiene un cliente cifrado, ese cliente estará limitado a solo 1 vCPU, incluso si se CPUs asignan 4 o más v a la puerta de enlace. Por este motivo, el rendimiento de las conexiones cifradas desde un único cliente a la puerta de enlace de archivo de S3 suele tener cuellos de botella entre 40 y 60 MB/s.

- Si sus requisitos de seguridad le permiten adoptar una postura más flexible, puede cambiar el nivel de seguridad a negociado con el cliente, lo que deshabilitará el cifrado SMB y solo aplicará la firma SMB. Con esta configuración, las conexiones de los clientes a la puerta de enlace pueden utilizar múltiples vCPUs, lo que normalmente se traduce en un aumento del rendimiento.

> **Note**
>
> Tras cambiar el nivel de seguridad de SMB de la puerta de enlace de archivo de S3, debe esperar a que el estado del recurso compartido de archivos cambie de Actualizado a Disponible en la consola de la Storage Gateway y, a continuación, desconectar y volver a conectar los clientes de SMB para que se aplique la nueva configuración.

Utilizar varios subprocesos y clientes para paralelizar las operaciones de escritura

Es difícil lograr el máximo rendimiento con una puerta de enlace de archivo de S3 que utilice solo un cliente de NFS o SMB para escribir un archivo a la vez, ya que la escritura secuencial desde un único cliente es una operación de subproceso único. En su lugar, se recomienda usar varios subprocesos de cada cliente de NFS o SMB para escribir varios archivos en paralelo y usar varios clientes de NFS o SMB simultáneamente en la puerta de enlace de archivo de S3 para maximizar el rendimiento de la puerta de enlace.

El uso de varios subprocesos puede mejorar considerablemente el rendimiento. Sin embargo, el uso de más subprocesos requiere más recursos del sistema, lo que puede afectar negativamente al rendimiento si la puerta de enlace no tiene el tamaño adecuado para soportar el aumento de carga. En una implementación típica, cabe esperar un mejor rendimiento de procesamiento a medida que agrega más subprocesos y clientes, hasta alcanzar las limitaciones máximas de hardware y ancho de banda para la puerta de enlace. Se recomienda experimentar con distintos números de subprocesos para encontrar el equilibrio óptimo entre la velocidad y el uso de recursos del sistema para la configuración específica de hardware y red.

Tenga en cuenta la siguiente información sobre las herramientas habituales que pueden ayudar a probar la configuración de subprocesos y clientes:

- Puede probar el rendimiento de escritura de varios subprocesos mediante herramientas como la robocopia para copiar un conjunto de archivos en un recurso compartido de archivos de la puerta de enlace. De forma predeterminada, la robocopia utiliza 8 subprocesos al copiar archivos, pero se pueden especificar hasta 128 subprocesos.

  Para utilizar varios subprocesos con robocopia, añada el conmutador `/MT:n` al comando, donde n indica el número de subprocesos que desea utilizar. Por ejemplo:

  ```
  robocopy C:\source D:\destination /MT:64
  ```

  Este comando utilizará 64 subprocesos para la operación de copia.

  > **Note**
  >
  > No se recomienda utilizar el Explorador de Windows para arrastrar y soltar archivos cuando se intenta obtener el máximo rendimiento, ya que este método se limita a un único subproceso y copia los archivos secuencialmente.

  Para obtener más información, consulte robocopy en el sitio web de Microsoft Learn.
- También puede realizar pruebas con herramientas comunes de análisis comparativo de almacenamiento, como DISKSPD o FIO. Estas herramientas disponen de opciones para ajustar la cantidad de subprocesos, la profundidad de E/S y otros parámetros para adaptarlos a los requisitos de carga de trabajo específicos.

  DiskSpd permite controlar el número de hilos mediante el `-t` parámetro. Por ejemplo:

  ```
  diskspd -c10G -d300 -r -w50 -t64 -o32 -b1M -h -L C:\testfile.dat
  ```

  Este comando de ejemplo hace lo siguiente:

  - Crea un archivo de prueba de 10 GB (`-c1G`)
  - Se ejecuta durante 300 segundos (`-d300`)
  - Realiza una I/O prueba aleatoria con un 50% de lecturas y un 50% de escrituras (`-r -w50`)
  - Utiliza 64 subprocesos (`-t64`)
  - Establece la profundidad de cola en 32 por subproceso (`-o32`)

- Utiliza un tamaño de bloque de 1 MB (`-b1M`)
- Deshabilita el almacenamiento en caché de hardware y software (`-h -L`)

Para obtener más información, consulte Use DISKSPD to test workload storage performance en el sitio web de Microsoft Learn.

- FIO usa el parámetro `numjobs` para controlar el número de subprocesos paralelos. Por ejemplo:

```
fio --name=mixed_test --rw=randrw --rwmixread=70 --bs=1M -- iodepth=64
--size=10G --runtime=300 --numjobs=64 --ioengine=libaio --direct=1 --
group_reporting
```

Este comando de ejemplo hace lo siguiente:

- Realiza una I/O prueba aleatoria (`--rw=randrw`)
- Realiza un 70 % de lecturas y un 30 % de escrituras (`--rwmixread=70`)
- Utiliza un tamaño de bloque de 1 MB (`--bs=1M`)
- Establece la I/O profundidad en 64 (`--iodepth=64`)
- Realiza pruebas en un archivo de 10 GB (`--size=10G`)
- Se ejecuta durante 5 minutos (`--runtime=300`)
- Crea 64 trabajos paralelos (subprocesos) (`--numjobs=64`)
- Utiliza un motor asíncrono I/O () `--ioengine=libaio`
- Agrupa los resultados para facilitar el análisis (`--group_reporting`)

Para obtener más información, consulte la página del manual de Linux fio.

-

Desactivar la actualización automática de la caché

La característica de actualización automática de la caché permite a la puerta de enlace de archivo de S3 actualizar los metadatos automáticamente, para ayudar a capturar cualquier cambio que los usuarios o las aplicaciones realicen en el conjunto de archivos escribiéndolos directamente en el bucket de Amazon S3, en lugar de hacerlo a través de la puerta de enlace. Para obtener más información, consulte Actualización de la caché de objetos del bucket de Amazon S3.

Para optimizar el rendimiento de la puerta de enlace, se recomienda desactivar esta característica en las implementaciones en las que todas las lecturas y escrituras del bucket de Amazon S3 se realicen a través de la puerta de enlace de archivo de S3.

A la hora de configurar la actualización automática de la caché, tenga en cuenta lo siguiente:

- Si necesita utilizar la actualización automática de la caché porque los usuarios o las aplicaciones de la implementación a veces escriben directamente en Amazon S3, se recomienda configurar el intervalo de tiempo más largo posible entre las actualizaciones, aquel que mejor se adapte a las necesidades de su empresa. Un intervalo de actualización de la caché más prolongado ayuda a reducir la cantidad de operaciones de metadatos que la puerta de enlace debe realizar al explorar directorios o modificar archivos.

  Por ejemplo: configure la actualización automática de la caché en 24 horas, en lugar de 5 minutos, si es tolerable para su carga de trabajo.
- El intervalo de tiempo mínimo es de 5 minutos. El intervalo máximo es 30 días.
- Si decide configurar un intervalo de actualización de la caché muy corto, se recomienda probar la experiencia de navegación de directorios de los clientes de NFS y SMB. El tiempo que se tarda en actualizar la caché de la puerta de enlace puede aumentar considerablemente en función del número de archivos y subdirectorios del bucket de Amazon S3.

Aumentar el número de subprocesos del cargador de Amazon S3

De forma predeterminada, la puerta de enlace de archivo de S3 abre 8 subprocesos para la carga de datos de Amazon S3, lo que proporciona suficiente capacidad de carga para la mayoría de las implementaciones habituales. Sin embargo, es posible que una puerta de enlace reciba datos de clientes de NFS y SMB a una velocidad superior a la que puede cargar en Amazon S3 con la capacidad estándar de 8 subprocesos, lo que puede provocar que la caché local alcance su límite de almacenamiento.

En circunstancias específicas, Soporte puede aumentar el número de subprocesos de carga de Amazon S3 para su puerta de enlace de 8 a 40, lo que permite cargar más datos en paralelo. En función del ancho de banda y de otros factores específicos de la implementación, esto puede aumentar considerablemente el rendimiento de carga y ayudar a reducir la cantidad de almacenamiento en caché necesaria para soportar la carga de trabajo.

Recomendamos usar la `CachePercentDirty` CloudWatch métrica para monitorear la cantidad de datos almacenados en los discos de caché de la puerta de enlace local que aún no se han cargado

en Amazon S3 y ponerse en contacto con nosotros Soporte para determinar si aumentar el número de subprocesos de carga podría mejorar el rendimiento de su S3 File Gateway. Para obtener más información, consulte Descripción de métricas de la puerta de enlace.

> **Note**
>
> Esta configuración consume recursos adicionales de la CPU de la puerta de enlace. Se recomienda supervisar el uso de la CPU de la puerta de enlace y aumentar los recursos de CPU asignados si es necesario.

Aumentar la configuración de tiempo de espera de SMB

Cuando la puerta de enlace de archivo de S3 copia archivos de gran tamaño en un recurso compartido de archivos SMB, el tiempo de espera de la conexión del cliente de SMB puede agotarse después de un período prolongado.

Se recomienda ampliar el tiempo de espera de las sesiones de SMB para sus clientes de SMB a 20 minutos o más, según el tamaño de los archivos y la velocidad de escritura de la puerta de enlace. El valor predeterminado es 300 segundos o 5 minutos. Para obtener más información, consulte El trabajo de copia de seguridad de la puerta de enlace falla o se producen errores al escribir en la puerta de enlace.

Activar el bloqueo oportunista para las aplicaciones compatibles

El bloqueo oportunista, u “oplocks”, está activado de forma predeterminada para cada nueva puerta de enlace de archivo de S3. Al usar oplocks con aplicaciones compatibles, el cliente agrupa varias operaciones más pequeñas en operaciones más grandes, lo que resulta más eficiente para el cliente, la puerta de enlace y la red. Se recomienda mantener activado el bloqueo oportunista si utiliza aplicaciones que aprovechan el almacenamiento en caché local del lado del cliente, como Microsoft Office, Adobe Suite y muchas otras, ya que puede mejorar considerablemente el rendimiento.

Si se desactiva el bloqueo oportunista, las aplicaciones que admiten oplocks suelen abrir archivos grandes (de 50 MB o más) con mucha más lentitud. Este retraso se debe a que la puerta de enlace envía los datos en partes de 4 KB, lo que se traduce en un rendimiento alto I/O y bajo.

Ajustar la capacidad de la puerta de enlace en función del tamaño del conjunto de archivos de trabajo

El parámetro de capacidad de la puerta de enlace especifica el número máximo de archivos para los que la puerta de enlace almacenará los metadatos en su caché local. De forma predeterminada, la capacidad de la puerta de enlace está establecida en Pequeña, lo que significa que la puerta de enlace almacena metadatos de hasta 5 millones de archivos. La configuración predeterminada es idónea para la mayoría de las cargas de trabajo, aunque haya cientos de millones o incluso miles de millones de objetos en Amazon S3, ya que solo se accede activamente a un pequeño subconjunto de archivos en un momento dado en una implementación típica. Este grupo de archivos se denomina “conjunto de trabajo”.

Si su carga de trabajo accede con regularidad a un conjunto de trabajo de archivos de más de 5 millones, la puerta de enlace tendrá que realizar frecuentes expulsiones de caché, que son pequeñas operaciones de E/S que se almacenan en la RAM y persisten en el disco raíz. Esto puede afectar negativamente al rendimiento de la puerta de enlace, ya que la puerta de enlace obtiene datos nuevos de Amazon S3.

Puede supervisar la métrica `IndexEvictions` para determinar el número de archivos cuyos metadatos se expulsaron de la memoria caché y dejar espacio para nuevas entradas. Para obtener más información, consulte Descripción de métricas de la puerta de enlace.

Se recomienda utilizar la acción de la API `UpdateGatewayInformation` para aumentar la capacidad de la puerta de enlace y adaptarla al número de archivos del conjunto de trabajo habitual. Para obtener más información, consulte UpdateGatewayInformation.

> **Note**
>
> El aumento de la capacidad de la puerta de enlace requiere RAM y capacidad de disco raíz adicionales.
>
> - Los discos pequeños (5 millones de archivos) requieren al menos 16 GB de RAM y 80 GB de disco raíz.
> - El tamaño mediano (10 millones de archivos) requiere al menos 32 GB de RAM y 160 GB de disco raíz.
> - El disco grande (20 millones de archivos) requiere 64 GB de RAM y 240 GB de disco raíz.

> **Important**
>
> La capacidad de la puerta de enlace no se puede reducir.

Implementar varias puertas de enlace para cargas de trabajo más grandes

Se recomienda dividir la carga de trabajo en varias puertas de enlace siempre que sea posible, en lugar de consolidar muchos recursos compartidos de archivos en una sola puerta de enlace grande. Por ejemplo, puede aislar un recurso compartido de archivos muy utilizado en una puerta de enlace y agrupar los recursos compartidos de archivos que se utilizan con menos frecuencia en otra puerta de enlace.

Al planificar una implementación con varias puertas de enlace y recursos compartidos de archivos, tenga en cuenta lo siguiente:

- El número máximo de recursos compartidos de archivos en una sola puerta de enlace es de 50, pero el número de recursos compartidos de archivos gestionados por una puerta de enlace puede afectar al rendimiento de la puerta de enlace. Para obtener más información, consulte Directrices de rendimiento para puertas de enlace con varios recursos compartidos de archivos.
- Los recursos de cada puerta de enlace de archivo de S3 se comparten entre todos los recursos compartidos de archivos, sin necesidad de particionarlos.
- Un único recurso compartido de archivos con un uso intensivo puede afectar al rendimiento de otros recursos compartidos de archivos de la puerta de enlace.

> **Note**
>
> No se recomienda crear varios recursos compartidos de archivos que estén asignados a la misma ubicación de Amazon S3 desde varias puertas de enlace, a menos que al menos una de ellas sea de solo lectura.
> Las escrituras simultáneas en el mismo archivo desde varias puertas de enlace se consideran un escenario multiescritura, lo que puede provocar problemas de integridad de los datos.

Optimización de la puerta de enlace de archivo de S3 para copias de seguridad de bases de datos de SQL Server

Las copias de seguridad de bases de datos son un caso de uso común y recomendado para la puerta de enlace de archivo de S3, que proporciona una retención de datos rentable a corto y largo plazo al almacenar las copias de seguridad de las bases de datos en Amazon S3, con la capacidad de cambiar el ciclo de vida para reducir los costes de los niveles de almacenamiento según sea necesario. Con esta solución, puede reducir la necesidad de aplicaciones de copia de seguridad empresariales mediante herramientas integradas, como SQL Server Management Studio y Oracle RMAN.

En las siguientes secciones se describen las prácticas recomendadas para ajustar la implementación de la puerta de enlace de archivo de S3 a fin de optimizar el rendimiento y ofrecer un soporte rentable para cientos de terabytes de copias de seguridad de bases de datos de SQL. Las directrices que se proporcionan en cada sección contribuyen gradualmente a mejorar el rendimiento general. Si bien ninguna de estas recomendaciones es obligatoria y no son interdependientes, se han seleccionado y ordenado de forma lógica para probar y ajustar las implementaciones de S3 File Gateway. Soporte Al implementar y probar estas sugerencias, tenga en cuenta que cada implementación de la puerta de enlace de archivo de S3 es única, por lo que los resultados pueden variar.

La puerta de enlace de archivo de S3 proporciona una interfaz de archivos para almacenar y recuperar objetos de Amazon S3 mediante protocolos de archivos NFS o SMB estándares del sector, con una asignación 1:1 nativa entre el archivo y el objeto. Puede implementar S3 File Gateway como una máquina virtual local en su VMware entorno KVM de Microsoft Hyper-V o Linux, o en la AWS nube como una instancia de Amazon EC2. La puerta de enlace de archivo de S3 no está diseñada para sustituir completamente a la NAS empresarial. La puerta de enlace de archivo de S3 emula un sistema de archivos, pero no lo es. El uso de Amazon S3 como almacenamiento interno duradero genera una sobrecarga adicional en cada I/O operación, por lo que evaluar el rendimiento de S3 File Gateway con respecto a un NAS o servidor de archivos existente no es una comparación equivalente.

Implementar la puerta de enlace en la misma ubicación que los servidores SQL

Recomendamos implementar el dispositivo virtual de puerta de enlace de archivo de S3 en una ubicación física con la menor latencia de red posible entre este y los servidores SQL. A la hora de elegir una ubicación para la puerta de enlace, tenga en cuenta lo siguiente:

- Una menor latencia de la red en la puerta de enlace puede ayudar a mejorar el rendimiento de los clientes de SMB, como los servidores SQL.
- La puerta de enlace de archivo de S3 está diseñada para tolerar una latencia de red más alta entre la puerta de enlace y Amazon S3 que entre la puerta de enlace y los clientes.
- Para las instancias de la puerta de enlace de archivo de S3 implementadas en Amazon EC2, se recomienda mantener la puerta de enlace y los servidores SQL en el mismo grupo de ubicación. Para obtener más información, consulte Grupos de ubicación para instancias de Amazon EC2 en la Guía del usuario de Amazon Elastic Compute Cloud.

Reducir los cuellos de botella causados por la lentitud de los discos

Recomendamos monitorear la `IoWaitPercent` CloudWatch métrica para identificar los cuellos de botella en el rendimiento que pueden resultar de la lentitud de los discos de almacenamiento en su S3 File Gateway. Al intentar optimizar los problemas de rendimiento relacionados con los discos, tenga en cuenta lo siguiente:

- `IoWaitPercent` indica el porcentaje de tiempo que la CPU está a la espera de recibir una respuesta de los discos raíz o de caché.
- Cuando `IoWaitPercent` es superior al 5 o 10 %, esto suele indicar un cuello de botella en el rendimiento de la puerta de enlace provocado por discos con bajo rendimiento. Esta métrica debe estar lo más cerca posible del 0 %, lo que significa que la puerta de enlace nunca espera en el disco, lo que ayuda a optimizar los recursos de la CPU.
- Puede consultar `IoWaitPercent` la pestaña Supervisión de la consola Storage Gateway o configurar CloudWatch las alarmas recomendadas para que le notifiquen automáticamente si la métrica supera un umbral específico. Para obtener más información, consulte Crear CloudWatch las alarmas recomendadas para la puerta de enlace.
- Le recomendamos que utilice una unidad SSD NVMe o una unidad SSD para los discos raíz y caché de la puerta de enlace, a fin de minimizar el riesgo`IoWaitPercent`.

Ajustar la asignación de recursos de la máquina virtual de puerta de enlace de archivo de S3 para los discos de CPU, RAM y caché

Al intentar optimizar el rendimiento de la puerta de enlace de archivo de S3, es importante asignar suficientes recursos a la máquina virtual de puerta de enlace, incluidos los discos de CPU, RAM y caché. Los requisitos mínimos de recursos virtuales de 4 CPUs, 16 GB de RAM y 150 GB de almacenamiento en caché suelen ser adecuados solo para cargas de trabajo más pequeñas. Al asignar recursos virtuales a cargas de trabajo más grandes, se recomienda lo siguiente:

- Aumente el número asignado CPUs a entre 16 y 48, en función del uso típico de la CPU que genere su S3 File Gateway. Puede supervisar el uso de la CPU mediante la métrica `UserCpuPercent`. Para obtener más información, consulte Descripción de métricas de la puerta de enlace.
- Aumente la RAM asignada a entre 32 y 64 GB.

  > **Note**
  >
  > La puerta de enlace de archivo S3 no puede utilizar más de 64 GB de RAM.

- Utilice NVMe un SSD para los discos raíz y el disco de caché, y ajuste el tamaño de los discos de caché para adaptarlos al conjunto de datos de trabajo máximo que planea escribir en la puerta de enlace. Para obtener más información, consulte las mejores prácticas de tamaño de caché de S3 File Gateway en el YouTube canal oficial de Amazon Web Services.
- Añada al menos 4 discos de caché virtuales a la puerta de enlace, en lugar de utilizar un único disco grande. Varios discos virtuales pueden mejorar el rendimiento incluso si comparten el mismo disco físico subyacente, pero las mejoras suelen ser mayores cuando los discos virtuales se encuentran en discos físicos subyacentes diferentes.

  Por ejemplo, si quiere implementar 12 TB de caché, puede utilizar una de las siguientes configuraciones:

  - 4 discos de caché de 3 TB
  - 8 discos de caché de 1,5 TB
  - 12 discos de caché de 1 TB

  Esto no solo permite una administración más eficiente del rendimiento, sino también de la máquina virtual a lo largo del tiempo. A medida que cambie su carga de trabajo, puede aumentar gradualmente la cantidad de discos de caché y la capacidad total de caché, al tiempo que

mantiene el tamaño original de cada disco virtual individual para preservar la integridad de la puerta de enlace.

Para obtener más información, consulte Cálculo de la cantidad de almacenamiento en disco local.

Cuando implemente la puerta de enlace de archivo de S3 como una instancia de Amazon EC2, tenga en cuenta lo siguiente:

- El tipo de instancia que elija puede afectar significativamente al rendimiento de la puerta de enlace. Amazon EC2 ofrece una amplia flexibilidad para ajustar la asignación de recursos para la instancia de la puerta de enlace de archivo de S3.
- Para ver los tipos de instancia de Amazon EC2 recomendados para la puerta de enlace de archivo de S3, consulte Requisitos para los tipos de instancia de Amazon EC2.
- Puede cambiar el tipo de instancia de Amazon EC2 que aloja una puerta de enlace de archivo de S3 activa. Esto le permite ajustar fácilmente la generación de hardware y la asignación de recursos de Amazon EC2 para encontrar una proporción ideal price-to-performance. Para cambiar el tipo de instancia, utilice el siguiente procedimiento en la consola de Amazon EC2:

  1. Detenga la instancia de Amazon EC2.
  2. Cambie el tipo de instancia de Amazon EC2.
  3. Encienda la instancia de Amazon EC2.

  > **Note**
  >
  > Si detiene una instancia que aloja una puerta de enlace de archivo de S3, se interrumpirá temporalmente el acceso a los recursos compartidos de archivos. Asegúrese de programar un período de mantenimiento si es necesario.

- La price-to-performance proporción de una instancia Amazon EC2 se refiere a la potencia de cálculo que obtiene por el precio que paga. Por lo general, las instancias Amazon EC2 de nueva generación ofrecen la mejor price-to-performance relación, con un hardware más nuevo y un rendimiento mejorado a un costo relativamente menor en comparación con las generaciones anteriores. Factores como el tipo de instancia, la región y los patrones de uso influyen en esta relación, por lo que es importante seleccionar la instancia adecuada para su carga de trabajo específica a fin de optimizar la rentabilidad.

Mejorar el rendimiento de los clientes de SMB mediante el ajuste del nivel de seguridad de la puerta de enlace de archivo de S3

El SMBv3 protocolo permite tanto la firma como el cifrado SMB, lo que tiene algunas desventajas en cuanto a rendimiento y seguridad. Para optimizar el rendimiento, puede ajustar el nivel de seguridad de SMB de la puerta de enlace para especificar cuáles de estas características de seguridad se aplican a las conexiones de los clientes. Para obtener más información, consulte Establecer un nivel de seguridad para la puerta de enlace.

A la hora de ajustar el nivel de seguridad de SMB, tenga en cuenta lo siguiente:

- El nivel de seguridad predeterminado para la puerta de enlace de archivo de S3 Aplicar cifrado. Esta configuración aplica tanto el cifrado como la firma de las conexiones de los clientes de SMB a los recursos compartidos de archivos de la puerta de enlace, lo que significa que todo el tráfico del cliente a la puerta de enlace está cifrado. Esta configuración no afecta al tráfico desde la puerta de enlace a AWS, que siempre está cifrado.

  La puerta de enlace limita cada conexión de cliente cifrada a una sola vCPU. Por ejemplo, si solo tiene un cliente cifrado, ese cliente estará limitado a solo 1 vCPU, incluso si se CPUs asignan 4 o más v a la puerta de enlace. Por este motivo, el rendimiento de las conexiones cifradas desde un único cliente a la puerta de enlace de archivo de S3 suele tener cuellos de botella entre 40 y 60 MB/s.
- Si sus requisitos de seguridad le permiten adoptar una postura más flexible, puede cambiar el nivel de seguridad a negociado con el cliente, lo que deshabilitará el cifrado SMB y solo aplicará la firma SMB. Con esta configuración, las conexiones de los clientes a la puerta de enlace pueden utilizar múltiples vCPUs, lo que normalmente se traduce en un aumento del rendimiento.

> **Note**
>
> Tras cambiar el nivel de seguridad de SMB de la puerta de enlace de archivo de S3, debe esperar a que el estado del recurso compartido de archivos cambie de Actualizado a Disponible en la consola de la Storage Gateway y, a continuación, desconectar y volver a conectar los clientes de SMB para que se aplique la nueva configuración.

Mejorar el rendimiento de los de clientes SMB mediante la división de las copias de seguridad de SQL en varios archivos

- Es difícil lograr el máximo rendimiento con una puerta de enlace de archivo de S3 en la que solo un servidor SQL escribe un archivo a la vez, ya que la escritura secuencial desde un único servidor SQL es una operación de un solo subproceso. En su lugar, se recomienda usar varios subprocesos de cada servidor SQL para escribir varios archivos en paralelo y usar varios servidores SQL simultáneamente en la puerta de enlace de archivo de S3 para maximizar el rendimiento de la puerta de enlace. Con las copias de seguridad de SQL, la división de las copias de seguridad en varios archivos permite que cada archivo utilice un subproceso independiente, que escribirá varios archivos simultáneamente en el recurso compartido de archivos de la puerta de enlace de archivo de S3. Cuantos más subprocesos tenga, mayor rendimiento podrá lograr, hasta los límites de la puerta de enlace.
- SQL Server permite escribir en varios archivos al mismo tiempo durante una sola operación de copia de seguridad. Por ejemplo, puede especificar varios destinos de archivo mediante comandos de T-SQL o mediante SQL Server Management Studio (SSMS). Cada archivo utiliza un subproceso independiente para enviar los datos desde el servidor SQL al recurso compartido de archivos de la puerta de enlace. Este enfoque permite un mejor I/O rendimiento, lo que puede mejorar considerablemente la velocidad y la eficiencia de las copias de seguridad.

Al configurar las copias de seguridad de los servidores SQL, tenga en cuenta lo siguiente:

- Al dividir las copias de seguridad en varios archivos, los administradores de SQL Server pueden optimizar los tiempos de las copias de seguridad y administrar las copias de seguridad de grandes bases de datos de manera más eficaz.
- La cantidad de archivos utilizados depende de la configuración de almacenamiento y de los requisitos de rendimiento del servidor. Para bases de datos de gran tamaño, recomendamos dividir las copias de seguridad en varios archivos más pequeños de entre 10 GB y 20 GB cada uno.
- No hay un límite estricto en cuanto al número de archivos en los que SQL Server puede escribir durante una copia de seguridad, pero esta elección debe basarse en consideraciones prácticas, como la arquitectura de almacenamiento y el ancho de banda de la red.

Para obtener más información, consulte lo siguiente:

- Realizar copias de seguridad de SQL Server entre un 43 y un 67 % más rápido al escribir en varios archivos

- Almacene fácilmente sus copias de seguridad de SQL Server en Amazon S3 mediante Puerta de enlace de archivo

Evitar errores al copiar archivos de gran tamaño mediante el aumento la configuración de tiempo de espera de SMB

Cuando la puerta de enlace de archivo de S3 copia archivos de copia de seguridad de SQL gran tamaño en un recurso compartido de archivos SMB, el tiempo de espera de la conexión del cliente de SMB puede agotarse después de un período prolongado. Se recomienda ampliar el tiempo de espera de las sesiones de SMB para sus clientes de SMB de SQL Server a 20 minutos o más, según el tamaño de los archivos y la velocidad de escritura de la puerta de enlace. El valor predeterminado es 300 segundos o 5 minutos. Para obtener más información, consulte El trabajo de copia de seguridad de la puerta de enlace falla o se producen errores al escribir en la puerta de enlace.

Aumentar el número de subprocesos del cargador de Amazon S3

De forma predeterminada, la puerta de enlace de archivo de S3 abre 8 subprocesos para la carga de datos de Amazon S3, lo que proporciona suficiente capacidad de carga para la mayoría de las implementaciones habituales. Sin embargo, es posible que una puerta de enlace reciba datos de servidores SQL a una velocidad superior a la que puede cargar en Amazon S3 con la capacidad estándar de 8 subprocesos, lo que puede provocar que la caché local alcance su límite de almacenamiento.

En circunstancias específicas, Soporte puede aumentar el número de subprocesos de carga de Amazon S3 para su puerta de enlace de 8 a 40, lo que permite cargar más datos en paralelo. En función del ancho de banda y de otros factores específicos de la implementación, esto puede aumentar considerablemente el rendimiento de carga y ayudar a reducir la cantidad de almacenamiento en caché necesaria para soportar la carga de trabajo.

Recomendamos usar la `CachePercentDirty` CloudWatch métrica para monitorear la cantidad de datos almacenados en los discos de caché de la puerta de enlace local que aún no se han cargado en Amazon S3 y ponerse en contacto con nosotros Soporte para determinar si aumentar el número de subprocesos de carga podría mejorar el rendimiento de su S3 File Gateway. Para obtener más información, consulte Descripción de métricas de la puerta de enlace.

> **Note**
>
> Esta configuración consume recursos adicionales de la CPU de la puerta de enlace. Se recomienda supervisar el uso de la CPU de la puerta de enlace y aumentar los recursos de CPU asignados si es necesario.

Desactivar la actualización automática de la caché

La característica de actualización automática de la caché permite a la puerta de enlace de archivo de S3 actualizar los metadatos automáticamente, para ayudar a capturar cualquier cambio que los usuarios o las aplicaciones realicen en el conjunto de archivos escribiéndolos directamente en el bucket de Amazon S3, en lugar de hacerlo a través de la puerta de enlace. Para obtener más información, consulte Actualización de la caché de objetos del bucket de Amazon S3.

Para optimizar el rendimiento de la puerta de enlace, se recomienda desactivar esta característica en las implementaciones en las que todas las lecturas y escrituras del bucket de Amazon S3 se realicen a través de la puerta de enlace de archivo de S3.

A la hora de configurar la actualización automática de la caché, tenga en cuenta lo siguiente:

- Si necesita utilizar la actualización automática de la caché porque los usuarios o las aplicaciones de la implementación a veces escriben directamente en Amazon S3, se recomienda configurar el intervalo de tiempo más largo posible entre las actualizaciones, aquel que mejor se adapte a las necesidades de su empresa. Un intervalo de actualización de la caché más prolongado ayuda a reducir la cantidad de operaciones de metadatos que la puerta de enlace debe realizar al explorar directorios o modificar archivos.

  Por ejemplo: configure la actualización automática de la caché en 24 horas, en lugar de 5 minutos, si es tolerable para su carga de trabajo.
- El intervalo de tiempo mínimo es de 5 minutos. El intervalo máximo es 30 días.
- Si decide configurar un intervalo de actualización de la caché muy corto, se recomienda probar la experiencia de navegación de directorios de los servidores SQL. El tiempo que se tarda en actualizar la caché de la puerta de enlace puede aumentar considerablemente en función del número de archivos y subdirectorios del bucket de Amazon S3.

Implementar varias puertas de enlace para soportar la carga de trabajo

Storage Gateway puede admitir copias de seguridad de SQL para entornos grandes con cientos de bases de datos SQL, varios servidores SQL y cientos de terabytes de datos de copia de seguridad al dividir la carga de trabajo en varias puertas de enlace.

Al planificar una implementación con varias puertas de enlace y servidores SQL, tenga en cuenta lo siguiente:

- Por lo general, una sola puerta de enlace puede cargar hasta 20 TB por día, con suficientes recursos de hardware y ancho de banda. Puede aumentar este límite hasta 40 TB por día mediante el aumento del número de subprocesos del cargador de Amazon S3.
- Recomendamos realizar una proof-of-concept prueba para medir el rendimiento y tener en cuenta todas las variables de la implementación. Después de determinar el rendimiento máximo de la carga de trabajo de copia de seguridad de SQL, puede escalar la cantidad de puertas de enlace para cumplir con sus requisitos.
- Se recomienda diseñar la solución teniendo en cuenta el crecimiento, ya que la cantidad y el tamaño de las bases de datos pueden aumentar con el tiempo. Para seguir escalando y soportando una carga de trabajo cada vez mayor, puede implementar puertas de enlace adicionales según sea necesario.

Recursos adicionales para cargas de trabajo de copia de seguridad de bases de datos

- Almacene copias de seguridad de SQL Server en Amazon S3 mediante AWS Storage Gateway
- Almacene fácilmente sus copias de seguridad de SQL Server en Amazon S3 mediante Puerta de enlace de archivo
- Uso AWS Storage Gateway para almacenar copias de seguridad de bases de datos Oracle en Amazon S3
- Realización de copias de seguridad de bases de datos Oracle en Amazon S3 a escala
- Integre una base de datos SAP ASE en Amazon S3 mediante AWS Storage Gateway
- Cómo utiliza One AWS Hero las copias AWS Storage Gateway de seguridad en la nube
- Prácticas recomendadas de dimensionamiento de la caché de la puerta de enlace de archivo de S3

Seguridad en AWS Storage Gateway

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 AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener información sobre los programas de cumplimiento que se aplican a AWS Storage Gateway, consulte AWS Servicios dentro del alcance por programa de cumplimiento AWS .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo puede aplicar el modelo de responsabilidad compartida cuando se utiliza Storage Gateway. En los siguientes temas, se le mostrará cómo configurar Storage Gateway para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a usar otros AWS servicios que le ayudan a monitorear y proteger los recursos de Storage Gateway.

Protección de datos en AWS Storage Gateway

El modelo de se aplica a protección de datos en AWS Storage Gateway. 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, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. Exigimos 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 la información confidencial almacenada 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, consulte 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 Storage Gateway u otro Servicios de AWS dispositivo mediante la consola AWS CLI, la API o AWS SDKs. Cualquier dato que introduzca en etiquetas o campos de formato libre utilizados para los nombres se pueden 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 mediante AWS KMS

Amazon FSx File Gateway admite el cifrado SMB hasta la última especificación SMB v3.1.1, que incluye AES 128 CCM y AES 128 GCM. Los clientes compatibles se conectarán automáticamente mediante el cifrado. Además, FSx File Gateway utiliza el cifrado SMB cuando se comunica con Windows File Server in. FSx AWS Debe configurar un Direct Connect enlace y establecer las

políticas adecuadas para permitir el paso del tráfico SMB y el tráfico de administración hacia él. AWS AWS

Cifrado de un sistema de archivos

Para obtener más información, consulte Cifrado de datos en Amazon FSx en la Guía del usuario del servidor de archivos de Amazon FSx para Windows.

Cuando AWS KMS lo utilices para cifrar tus datos, ten en cuenta lo siguiente:

- Los datos se cifran en reposo en la nube. Es decir, los datos se cifran en Amazon FSx.
- Los usuarios de IAM deben tener los permisos necesarios para llamar a las operaciones de la AWS KMS API. Para obtener más información, consulte Uso de políticas de IAM con AWS KMS en la Guía para desarrolladores de AWS Key Management Service .

> **Important**
>
> Cuando utilice una AWS KMS clave para el cifrado del lado del servidor, debe elegir una clave simétrica. Storage Gateway no es compatible con claves asimétricas. Para obtener más información, consulte Uso de claves simétricas y asimétricas en la guía para desarrolladores de AWS Key Management Service .

Para obtener más información al respecto AWS KMS, consulte ¿Qué es? AWS Key Management Service

Administración de identidades y accesos para AWS Storage Gateway

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar AWS los recursos de SGW. El IAM es un servicio Servicio de AWS que puede utilizar sin coste adicional.

Temas

- Público

- Autenticación con identidades
- Administración del acceso con políticas
- Cómo funciona AWS Storage Gateway con IAM
- Ejemplos de políticas basadas en identidad para AWS Storage Gateway
- Solución de problemas AWS de identidad y acceso a Storage Gateway
- Uso de etiquetas para controlar el acceso a la puerta de enlace y a los recursos

Público

La forma de usar AWS Identity and Access Management (IAM) varía según la función que desempeñes:

- Usuario del servicio: solicite permisos al administrador si no puede acceder a las características (consulte Solución de problemas AWS de identidad y acceso a Storage Gateway).
- Administrador del servicio: determine el acceso de los usuarios y envíe las solicitudes de permiso (consulte Cómo funciona AWS Storage Gateway con IAM).
- Administrador de IAM: escribe las políticas para administrar el acceso (consulte Ejemplos de políticas basadas en identidad para AWS Storage Gateway).

Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Debe autenticarse como usuario de Usuario raíz de la cuenta de AWS IAM o asumir una función de IAM.

Puede iniciar sesión como una identidad federada con las credenciales de una fuente de identidad, como AWS IAM Identity Center (IAM Identity Center), la autenticación de inicio de sesión único o las credenciales. Google/Facebook Para obtener más información sobre el inicio de sesión, consulte Cómo iniciar sesión en la Cuenta de AWS en la Guía del usuario de AWS Sign-In .

Para el acceso programático, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte AWS Signature Version 4 para solicitudes de API en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear un Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz que tiene acceso completo a todos Servicios de AWS los recursos. Se

recomiendaencarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver las tareas que requieren credenciales de usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio empresarial, del proveedor de identidades web o al Directory Service que se accede Servicios de AWS mediante credenciales de una fuente de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, se recomienda AWS IAM Identity Center. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad con permisos específicos para una sola persona o aplicación. Recomendamos el uso de credenciales temporales en lugar de usuarios de IAM con credenciales de larga duración. Para obtener más información, consulte Exigir a los usuarios humanos que utilicen la federación con un proveedor de identidad para acceder AWS mediante credenciales temporales en la Guía del usuario de IAM.

Un grupo de IAM especifica un conjunto de usuarios de IAM y facilita la administración de los permisos para grupos grandes de usuarios. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un Rol de IAM es una identidad con permisos específicos que proporciona credenciales temporales. Puede asumir un rol cambiando de un rol de usuario a uno de IAM (consola) o llamando a una AWS CLI operación de AWS API. Para obtener más información, consulte Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM son útiles para el acceso de usuario federado, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon EC2. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Administración del acceso con políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política define los permisos cuando están asociados a una identidad o un recurso. AWS evalúa estas políticas cuando un director hace una solicitud. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre los documentos de políticas de JSON, consulte Información general de políticas de JSON en la Guía del usuario de IAM.

Mediante las políticas, los administradores especifican quién tiene acceso a qué, definiendo qué entidad principal puede realizar acciones sobre qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM crea políticas de IAM y las agrega a roles, que los usuarios pueden asumir posteriormente. Las políticas de IAM definen permisos independientemente del método que se utilice para realizar la operación.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de política de permisos JSON que asocia a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Las políticas basadas en identidad pueden ser políticas insertadas (incrustadas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener información sobre cómo elegir entre políticas administradas e insertadas, consulte Selección entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de políticas JSON que se asocian a un recurso. Los ejemplos incluyen las Políticas de confianza de roles de IAM y las Políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Debe especificar una entidad principal en una política basada en recursos.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer los permisos máximos que conceden los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM. Para obtener más información, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations .
- Políticas de control de recursos (RCPs): establece los permisos máximos disponibles para los recursos de tus cuentas. Para obtener más información, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para obtener más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona AWS Storage Gateway con IAM

Antes de usar IAM para administrar el acceso a la AWS SGW, averigüe qué funciones de IAM están disponibles para su uso con la SGW. AWS

Funciones de IAM que puede usar con AWS Storage Gateway

Característica de IAM	AWS Soporte para SGW
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No

Característica de IAM	AWS Soporte para SGW
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
ACLs	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Sesiones de acceso directo (FAS)	Sí
Roles de servicio	Sí
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo funcionan AWS SGW y otros AWS servicios con la mayoría de las funciones de IAM, consulte los AWS servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas de SGW basadas en la identidad AWS

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de la política de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en la identidad para SGW AWS

Para ver ejemplos de políticas de AWS SGW basadas en la identidad, consulte. Ejemplos de políticas basadas en identidad para AWS Storage Gateway

Políticas basadas en recursos dentro de SGW AWS

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 basada en 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. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones políticas para SGW AWS

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de AWS SGW, consulte Acciones definidas por AWS Storage Gateway en la Referencia de autorización de servicios.

Las acciones políticas en AWS SGW utilizan el siguiente prefijo antes de la acción:

```
sgw
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "sgw:action1",
      "sgw:action2"
         ]
```

Para ver ejemplos de políticas de AWS SGW basadas en la identidad, consulte. Ejemplos de políticas basadas en identidad para AWS Storage Gateway

Recursos de políticas para SGW AWS

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). En el caso de las acciones que no admiten permisos por recurso, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de los tipos de recursos de AWS SGW y sus tipos ARNs, consulte Recursos definidos por AWS Storage Gateway en la Referencia de autorización de servicios. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte Actions Defined by AWS Storage Gateway.

Para ver ejemplos de políticas de AWS SGW basadas en la identidad, consulte. Ejemplos de políticas basadas en identidad para AWS Storage Gateway

Claves de condición de la política para SGW AWS

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puede crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de claves de condición de AWS SGW, consulte Claves de condición de AWS Storage Gateway en la Referencia de autorización de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Actions Defined by AWS Storage Gateway.

Para ver ejemplos de políticas de AWS SGW basadas en la identidad, consulte. Ejemplos de políticas basadas en identidad para AWS Storage Gateway

ACLs AWS en SGW

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 SGW AWS

Compatibilidad con ABAC (etiquetas en las políticas): parcial

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos denominados etiquetas. Puede adjuntar etiquetas a las entidades y AWS los recursos de IAM y, a continuación, diseñar políticas de ABAC para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con SGW AWS

Compatibilidad con credenciales temporales: sí

Las credenciales temporales proporcionan acceso a AWS los recursos a corto plazo y se crean automáticamente cuando se utiliza la federación o se cambia de rol. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM y Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Sesiones de acceso directo para AWS SGW

Admite sesiones de acceso directo (FAS): sí

Las sesiones de acceso directo (FAS) utilizan los permisos del operador principal que realiza la llamada Servicio de AWS, junto con los que solicitan, Servicio de AWS para realizar solicitudes a los servicios descendentes. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Sesiones de acceso directo.

Funciones de servicio para SGW AWS

Compatible con roles de servicio: sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Crear un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de la AWS SGW. Edite las funciones de servicio solo cuando AWS SGW le dé instrucciones para hacerlo.

Funciones vinculadas al servicio para SGW AWS

Compatible con roles vinculados al servicio: sí

Un rol vinculado al 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 más información sobre cómo crear o administrar roles vinculados a servicios, consulta Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en identidad para AWS Storage Gateway

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de AWS SGW. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por AWS SGW, incluido el formato de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de AWS Storage Gateway en la Referencia de autorización del servicio. ARNs

Temas

- Prácticas recomendadas sobre las políticas
- Uso de la consola SGW AWS
- Cómo permitir a los usuarios consultar sus propios permisos

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear, acceder o eliminar los recursos de AWS SGW de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están

disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.

- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de la consola SGW AWS

Para acceder a la consola AWS Storage Gateway, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver los detalles sobre los recursos de AWS SGW de su Cuenta de AWS cuenta. Si crea una política basada en identidades que sea más restrictiva que

el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS API. En su lugar, permita el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la consola de AWS SGW, adjunte también la AWS SGW *ConsoleAccess* o la política *ReadOnly* AWS gestionada 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 administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
```

```
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Solución de problemas AWS de identidad y acceso a Storage Gateway

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas habituales que pueden surgir al trabajar con AWS SGW e IAM.

Temas

- No estoy autorizado a realizar ninguna acción en SGW AWS
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de AWS SGW

No estoy autorizado a realizar ninguna acción en SGW AWS

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 `sgw:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 sgw: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 `sgw:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibe un error que indica que no está autorizado a realizar la `iam:PassRole` acción, sus políticas deben actualizarse para que pueda transferir una función a AWS SGW.

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 al servicio. Para ello, debe tener permisos para transferir la función al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en AWS SGW. 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 su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

> **Important**
>
> Storage Gateway puede asumir roles de servicio existentes que se transfieren mediante la acción de política `iam:PassRole`, pero no admite las políticas de IAM que utilizan la clave de contexto `iam:PassedToService` para limitar la acción a servicios específicos.
> Para obtener más información, consulte los siguientes temas en la Guía del usuario de AWS Identity and Access Management :
>
> - IAM: transfiera una función de IAM a un servicio específico AWS
> - Otorgar permisos a un usuario para transferir un rol a un servicio AWS
> - Claves disponibles para IAM

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de AWS SGW

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que respaldan políticas basadas en recursos o listas de control de acceso (ACLs), puede usar esas políticas para permitir que las personas accedan a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si AWS SGW admite estas funciones, consulte. Cómo funciona AWS Storage Gateway con IAM
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (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 para controlar el acceso a la puerta de enlace y a los recursos

Para controlar el acceso a los recursos y las acciones de la puerta de enlace, puede utilizar políticas AWS Identity and Access Management (IAM) basadas en etiquetas. Puede proporcionar el control de dos maneras:

1. Control del acceso a los recursos de una gateway basándose en las etiquetas de dichos recursos.
2. Controlar las etiquetas que se pueden pasar en una condición de solicitud de IAM.

Para obtener información sobre cómo utilizar etiquetas para controlar el acceso, consulte Control del acceso mediante etiquetas.

Control del acceso a un recurso en función de las etiquetas

Para controlar las acciones que puede realizar un usuario o un rol en un recurso de gateway, puede utilizar etiquetas en el recurso de gateway. Por ejemplo, es posible que desee permitir o denegar acciones de la API específicas en un recurso de gateway de archivos en función del par clave-valor de la etiqueta del recurso.

En el siguiente ejemplo, se permite a un usuario o un rol realizar las acciones `ListTagsForResource`, `ListFileShares` y `DescribeNFSFileShares` con todos los recursos. La política se aplica únicamente si la clave de la etiqueta del recurso es `allowListAndDescribe` y tiene el valor `yes`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:ListTagsForResource",
                "storagegateway:ListFileShares",
                "storagegateway:DescribeNFSFileShares"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/allowListAndDescribe": "yes"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:*"
            ],
            "Resource": "arn:aws:storagegateway:us-east-1:111122223333:*/*"
        }
    ]
```

```
}
```

Control del acceso en función de las etiquetas de una solicitud de IAM

Para controlar lo que un usuario puede hacer en un recurso de puerta de enlace, puede utilizar condiciones en una política de IAM basada en etiquetas. Por ejemplo, puede escribir una política que permite o deniega a un usuario la posibilidad de realizar operaciones de la API específicas en función de la etiqueta que se proporcionó al crear el recurso.

En el siguiente ejemplo, la primera instrucción permite a un usuario crear una gateway únicamente si el par clave-valor de la etiqueta que se proporcionó al crear la gateway es **`Department`** y **`Finance`**. Al utilizar la operación de la API, tendrá que añadir esta etiqueta a la solicitud de activación.

La segunda instrucción permite al usuario crear un recurso compartido de archivos Network File System (NFS) o Server Message Block (SMB) en una gateway solo si el par clave-valor de la etiqueta de la gateway coincide con **`Department`** y **`Finance`**. Además, el usuario debe añadir una etiqueta al recurso compartido de archivos, y el par clave-valor de la etiqueta debe ser **`Department`** y **`Finance`**. Las etiquetas de un recurso compartido de archivos se añaden al crearlo. No hay permisos para las operaciones `RemoveTagsFromResource` ni `AddTagsToResource`, por lo que el usuario no puede realizar estas operaciones en la gateway ni en el recurso compartido de archivos.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "storagegateway:ActivateGateway"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/Department":"Finance"
            }
         }
      },
      {
         "Effect":"Allow",
```

```
            "Action":[
               "storagegateway:CreateNFSFileShare",
               "storagegateway:CreateSMBFileShare"
            ],
            "Resource":"*",
            "Condition":{
               "StringEquals":{
                  "aws:ResourceTag/Department":"Finance",
                  "aws:RequestTag/Department":"Finance"
               }
            }
         }
      ]
}
```

Validación de conformidad para AWS Storage Gateway

Los auditores externos evalúan la seguridad y el cumplimiento de AWS Storage Gateway como parte de varios programas de AWS cumplimiento. Estos incluyen SOC, PCI, ISO, FedRAMP, HIPAA, MTCS, C5, K-ISMS, ENS High, OSPAR y HITRUST CSF.

Para obtener una lista de AWS los servicios incluidos en el ámbito de los programas de conformidad específicos, consulte AWS Servicios incluidos en el ámbito de aplicación por programa de conformidad y . 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 en el ámbito de la conformidad al usar Storage Gateway viene determinada por la confidencialidad de los datos, los objetivos de conformidad de la empresa y las leyes y regulaciones aplicables. AWS proporciona los siguientes recursos para ayudarlo con los requisitos de conformidad:

- Guías de inicio rápido sobre : estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en la seguridad y el cumplimiento. AWS
- Documento técnico sobre cómo diseñar una arquitectura basada en la seguridad y el cumplimiento de la HIPAA: en este documento técnico se describe cómo pueden utilizar las empresas para crear aplicaciones que cumplan con la HIPAA. AWS

- AWS Recursos de cumplimiento Recursos de de trabajo y guías puede aplicarse a su sector y ubicación.
- Evaluación de los recursos con las reglas de 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 CSPM— Este AWS servicio proporciona una visión integral del estado de su seguridad AWS que le ayuda a comprobar su conformidad con los estándares y las mejores prácticas del sector de la seguridad.

Resiliencia en AWS Storage Gateway

La infraestructura AWS global se basa en distintas zonas Regiones de AWS de disponibilidad.

Una Región de AWS es una ubicación física en todo el mundo donde los centros de datos están agrupados. Cada grupo de centros de datos lógicos se denomina zona de disponibilidad (AZ). Cada uno Región de AWS consta de un mínimo de tres aislados y separados físicamente AZs dentro de un área geográfica. A diferencia de otros proveedores de servicios en la nube, que suelen definir una región como un único centro de datos, el diseño de múltiples zonas de disponibilidad de cada uno de Región de AWS ellos ofrece claras ventajas. Cada zona de disponibilidad tiene alimentación, refrigeración y seguridad física independientes y está conectada a través de ultra-low-latency redes redundantes. Si su implementación requiere centrarse en la alta disponibilidad, puede configurar los servicios y los recursos en varios para lograr una mayor AZs tolerancia a los errores.

Regiones de AWS cumplen con los niveles más altos de seguridad de infraestructura, cumplimiento y protección de datos. Todo el tráfico intermedio AZs está cifrado. El rendimiento de la red es suficiente para realizar una replicación sincrónica entre AZs ellas. AZs facilitan la partición de servicios y recursos para lograr una alta disponibilidad. Si su implementación está dividida AZs, es mejor aislar sus recursos y protegerlos de problemas como cortes de energía, rayos, tornados, terremotos y más. AZs están separados físicamente por una distancia significativa de cualquier otra zona de disponibilidad, aunque todas se encuentran a menos de 100 km (60 millas) una de la otra.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura AWS global.

Además de la infraestructura AWS global, Storage Gateway es compatible con VMware vSphere High Availability (VMware HA) para ayudar a proteger las cargas de trabajo de almacenamiento contra fallos de hardware, hipervisor o red. Para obtener más información, consulte Uso de VMware vSphere High Availability con Storage Gateway Uso de Gateway.

Seguridad de la infraestructura en AWS Storage Gateway

Como servicio gestionado, AWS Storage Gateway está protegido por los procedimientos de seguridad de red AWS global que se describen en Security Pillar: AWS Well-Architected Framework.

Las llamadas a la API AWS publicadas se utilizan para acceder a Storage Gateway a través de la red. Los clientes deben admitir el protocolo de seguridad de la capa de transporte (TLS) 1.2. Los clientes también deben ser compatibles con conjuntos de cifrado con confidencialidad directa total (PFS) tales como Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puedes utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

> **Note**
>
> Debe tratar el dispositivo AWS Storage Gateway como una máquina virtual administrada y no debe intentar acceder a su instalación ni modificarla de ninguna manera. El intento de instalar un software de escaneo o actualizar cualquier paquete de software mediante métodos distintos al mecanismo de actualización de la puerta de enlace normal puede provocar un mal funcionamiento de la puerta de enlace y afectar a nuestra capacidad de admitir o reparar la puerta de enlace.
>
> AWS revisa, analiza y CVEs corrige periódicamente. Incorporamos correcciones para estos problemas en Storage Gateway como parte de nuestro ciclo de lanzamiento de software normal. Por lo general, estos ajustes se aplican como parte del proceso normal de actualización de la puerta de enlace durante los periodos de mantenimiento programados. Para obtener más información sobre las actualizaciones de la puerta de enlace, consulte Administrar las actualizaciones de la puerta de enlace mediante la AWS Storage Gateway consola.

AWS Prácticas recomendadas de seguridad

AWS proporciona una serie de características de seguridad que debe tener en cuenta a la hora de desarrollar e implementar sus propias políticas de seguridad. Estas prácticas recomendadas

son directrices generales y no suponen una solución de seguridad completa. Puesto que es posible que estas prácticas no sean adecuadas o suficientes para el entorno, considérelas como consideraciones útiles en lugar de como normas. Para obtener más información, consulte AWS Prácticas recomendadas de seguridad de .

Inicio de sesión y supervisión AWS Storage Gateway

Storage Gateway 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 Storage Gateway. CloudTrail captura todas las llamadas a la API de Storage Gateway como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de Storage Gateway y las llamadas de código a las operaciones de la API de Storage Gateway. Si crea una ruta, puede activar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Storage Gateway. Si no configura un registro, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a Storage Gateway, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía AWS CloudTrail del usuario.

Información sobre Storage Gateway en CloudTrail

CloudTrail se activa en su AWS cuenta al crear la cuenta. Cuando se produce una actividad en Storage Gateway, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los eventos recientes en su AWS cuenta. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para obtener un registro continuo de los eventos de su AWS cuenta, incluidos los eventos de Storage Gateway, cree un registro. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando crea una ruta en la consola, la ruta se aplica a todas AWS las regiones. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. 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 Integraciones y servicios 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 las acciones de Storage Gateway están registradas y documentadas en el tema Acciones. Por ejemplo, las llamadas a las `ActivateGateway` `ShutdownGateway` acciones y las llamadas generan entradas en los archivos de CloudTrail registro. `ListGateways`

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 archivos de registro de Storage Gateway

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 la acción.

```
{ "Records": [{
                "eventVersion": "1.02",
                "userIdentity": {
                "type": "IAMUser",
                "principalId": "AIDAII5AUEPBH2M7JTNVC",
                "arn": "arn:aws:iam::111122223333:user/StorageGateway-team/JohnDoe",
```

```
                "accountId": "111122223333",
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                 "userName": "JohnDoe"
               },
                  "eventTime": "2014-12-04T16:19:00Z",
                  "eventSource": "storagegateway.amazonaws.com",
                  "eventName": "ActivateGateway",
                  "awsRegion": "us-east-2",
                  "sourceIPAddress": "192.0.2.0",
                  "userAgent": "aws-cli/1.6.2 Python/2.7.6 Linux/2.6.18-164.el5",
                   "requestParameters": {
                                          "gatewayTimezone": "GMT-5:00",
                                          "gatewayName": "cloudtrailgatewayvtl",
                                          "gatewayRegion": "us-east-2",
                                          "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
                                          "gatewayType": "VTL"
                                               },
                                               "responseElements": {
                                                                      "gatewayARN":
 "arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayvtl"
                                               },
                                               "requestID":
 "54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
                                               "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
                                               "eventType": "AwsApiCall",
                                               "apiVersion": "20130630",
                                               "recipientAccountId": "444455556666"
             }]
}
```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la ListGateways acción.

```
{
 "Records": [{
               "eventVersion": "1.02",
               "userIdentity": {
                                "type": "IAMUser",
                                "principalId": "AIDAII5AUEPBH2M7JTNVC",
                                "arn": "arn:aws:iam::111122223333:user/StorageGateway-
team/JohnDoe",
```

```
                                "accountId:" 111122223333", " accessKeyId ":"
 AKIAIOSFODNN7EXAMPLE",
                                " userName ":" JohnDoe "
                                },

                                " eventTime ":" 2014 - 12 - 03T19: 41: 53Z ",
                                " eventSource ":" storagegateway.amazonaws.com ",
                                " eventName ":" ListGateways ",
                                " awsRegion ":" us-east-2 ",
                                " sourceIPAddress ":" 192.0.2.0 ",
                                " userAgent ":" aws - cli / 1.6.2 Python / 2.7.6
 Linux / 2.6.18 - 164.el5 ",
                                " requestParameters ":null,
                                " responseElements ":null,
                                "requestID ":"
 6U2N42CU37KAO8BG6V1I23FRSJ1Q8GLLE1QEU3KPGG6F0KSTAUU0 ",
                                " eventID ":" f76e5919 - 9362 - 48ff - a7c4 -
 d203a189ec8d ",
                                " eventType ":" AwsApiCall ",
                                " apiVersion ":" 20130630 ",
                                " recipientAccountId ":" 444455556666"
             }]
}
```

Solución de problemas relacionados con la implementación de Storage Gateway

A continuación, puede encontrar información sobre las prácticas recomendadas y la solución de problemas relacionados con las puertas de enlace, las plataformas de host, los sistemas de archivos, la alta disponibilidad, la recuperación de datos y las instantáneas. La información sobre la solución de problemas de las puertas de enlace en las instalaciones cubre las puertas de enlace implementadas en las plataformas de virtualización compatibles. La información de solución de problemas de alta disponibilidad abarca las puertas de enlace que se ejecutan en la plataforma VMware vSphere High Availability (HA).

Temas

- Solución de problemas: problemas sin conexión de puerta de enlace: obtenga información sobre cómo diagnosticar los problemas que pueden provocar que la puerta de enlace aparezca sin conexión en la consola de Storage Gateway.
- Solución de problemas: problemas relacionados con Active Directory: obtenga información sobre qué hacer si recibe mensajes de error como `NETWORK_ERROR`, `TIMEOUT` o `ACCESS_DENIED` al tratar de unir su puerta de enlace de archivo a un dominio de Microsoft Active Directory.
- Solución de problemas: problemas de activación de la puerta de enlace: obtenga información sobre qué hacer si recibe un mensaje de error interno al intentar activar la Storage Gateway.
- Solución de problemas: problemas relacionados con la puerta de enlace en las instalaciones- Obtenga información sobre los problemas habituales que se pueden producir al trabajar con las puertas de enlace locales y cómo permitir la conexión Soporte a ellas para facilitar la solución de problemas.
- Solución de problemas: problemas con la configuración de Microsoft Hyper-V: obtenga información sobre los problemas habituales que podrían surgir al implementar Storage Gateway en la plataforma de Microsoft Hyper-V.
- Solución de problemas: problemas con la puerta de enlace de Amazon EC2: encuentre información sobre los problemas habituales que pueden surgir al trabajar con puertas de enlace implementadas en Amazon EC2.
- Solución de problemas: problemas con el dispositivo de hardware- Aprenda a resolver los problemas que puedan surgir con el dispositivo de hardware AWS Storage Gateway.

- Solución de problemas: problemas con la puerta de enlace de archivo- Encuentre información que le ayude a entender la causa de los errores y las notificaciones de estado que aparecen en los CloudWatch registros de su File Gateway.
- Solución de problemas: problemas de alta disponibilidad- Obtenga información sobre qué hacer si tiene problemas con las pasarelas que se implementan en un entorno de alta VMware disponibilidad.

Solución de problemas: puerta de enlace sin conexión en la consola de Storage Gateway

Utilice la siguiente información de solución de problemas para determinar qué hacer si la consola de AWS Storage Gateway muestra que la puerta de enlace está desconectada.

La puerta de enlace puede mostrarse como desconectada por uno o varios de los motivos siguientes:

- La puerta de enlace no puede llegar a los puntos de conexión del servicio de Storage Gateway.
- La puerta de enlace se cerró inesperadamente.
- Se desconectó o modificó un disco caché asociado a la puerta de enlace, o se produjo un error.

Para volver a conectar la puerta de enlace, identifique y resuelva el problema que provocó que la puerta de enlace se desconectara.

Comprobación del firewall o el proxy asociados

Si configuró la puerta de enlace para usar un proxy o la colocó detrás de un firewall, revise las reglas de acceso del proxy o el firewall. El proxy o el firewall deben permitir el tráfico hacia y desde los puertos de red y los puntos de conexión de servicio requeridos por Storage Gateway. Para obtener más información, consulte Requisitos de red y firewall.

Comprobación para una inspección continua de SSL o de paquetes exhaustiva del tráfico de la puerta de enlace

Si actualmente se está realizando una inspección profunda de paquetes o SSL en el tráfico de red entre la puerta de enlace y la puerta de enlace AWS, es posible que la puerta de enlace no pueda

comunicarse con los puntos finales de servicio necesarios. Para que la puerta de enlace vuelva a estar en línea, debe desactivar la inspección.

Compruebe la métrica IOWait porcentual tras un reinicio o una actualización de software

Tras reiniciar o actualizar el software, compruebe si la métrica `IOWaitPercent` de la puerta de enlace de archivo es 10 o superior. Esto puede provocar que la puerta de enlace tarde en responder mientras reconstruye la caché de índices en RAM. Para obtener más información, consulte Solución de problemas: uso de CloudWatch métricas.

Comprobación de si hay un corte de energía o un error de hardware en el host del hipervisor

Un corte de energía o un error de hardware en el host del hipervisor de la puerta de enlace pueden provocar que la puerta de enlace se cierre inesperadamente y no se pueda acceder a ella. Tras restablecer la alimentación y la conectividad de red, se volverá a poder acceder a la puerta de enlace.

Cuando la puerta de enlace vuelva a estar en línea, asegúrese de tomar las medidas necesarias para recuperar los datos. Para obtener información, consulte Prácticas recomendadas: recuperación de datos .

Comprobación de si hay problemas con un disco de caché asociado

La puerta de enlace se puede desconectar si al menos uno de los discos de caché asociados a la puerta de enlace se ha eliminado, modificado, redimensionado o está dañado.

Si se ha eliminado un disco de caché en funcionamiento del host del hipervisor:

1. Apague la gateway.
2. Vuelva a agregar el disco.

   > **Note**
   >
   > Asegúrese de agregar el disco al mismo nodo de disco.

3. Reinicie la gateway.

Si un disco de caché está dañado, se reemplazó o se cambió su tamaño:

- Siga el procedimiento del método 2 descrito en Reemplazo de la puerta de enlace de archivo de S3 existente por una nueva instancia para configurar una nueva puerta de enlace y volver a descargar la información del disco de caché de la nube de AWS .

Solución de problemas: problemas al unir la puerta de enlace a Active Directory

Utilice la siguiente información sobre solución de problemas para determinar qué hacer si recibe mensajes de error como `NETWORK_ERROR`, `TIMEOUT` o `ACCESS_DENIED` al tratar de unir la puerta de enlace de archivo con un dominio de Microsoft Active Directory.

Para resolver estos errores, realice las siguientes comprobaciones y configuraciones.

Confirme que la puerta de enlace puede llegar al controlador de dominio mediante la ejecución de una prueba de ping

Para ejecutar una prueba de nping:

1. Conéctese a la consola local de la puerta de enlace mediante el software de administración del hipervisor (VMware, Hyper-V o KVM) para las puertas de enlace en las instalaciones, o mediante ssh para las puertas de enlace de Amazon EC2.
2. Introduzca el número correspondiente para seleccionar Consola de puerta de enlace y, a continuación, introduzca h para ver todos los comandos disponibles. Para probar la conectividad entre la máquina virtual de Storage Gateway y el dominio, ejecute el siguiente comando:

   ```
   nping -d corp.domain.com -p 389 -c 1 -t tcp
   ```

   > **Note**
   >
   > Reemplace `corp.domain.com` por el nombre de DNS de su dominio de Active Directory y reemplace `389` por el puerto LDAP de su entorno.
   > Compruebe que ha abierto los puertos necesarios en su firewall.

A continuación, se ofrece un ejemplo de una prueba de nping satisfactoria en la que la puerta de enlace pudo llegar al controlador de dominio:

```
nping -d corp.domain.com -p 389 -c 1 -t tcp

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2022-06-30 16:24 UTC
SENT (0.0553s) TCP 10.10.10.21:9783 > 10.10.10.10:389 S ttl=64 id=730 iplen=40
 seq=2597195024 win=1480
RCVD (0.0556s) TCP 10.10.10.10:389 > 10.10.10.21:9783 SA ttl=128 id=22332 iplen=44
 seq=4170716243 win=8192 <mss 8961>

Max rtt: 0.310ms | Min rtt: 0.310ms | Avg rtt: 0.310ms
Raw packets sent: 1 (40B) | Rcvd: 1 (44B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 1.09 seconds<br>
```

El siguiente es un ejemplo de una prueba de nping en la que no hay conectividad con el destino `corp.domain.com` ni respuesta desde este:

```
nping -d corp.domain.com -p 389 -c 1 -t tcp

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2022-06-30 16:26 UTC
SENT (0.0421s) TCP 10.10.10.21:47196 > 10.10.10.10:389  S ttl=64 id=30318 iplen=40
 seq=1762671338 win=1480

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Raw packets sent: 1 (40B) | Rcvd: 0 (0B) | Lost: 1 (100.00%)
Nping done: 1 IP address pinged in 1.07 seconds
```

Compruebe las opciones de DHCP configuradas para la VPC de la instancia de puerta de enlace de Amazon EC2

Si la puerta de enlace de archivo se ejecuta en una instancia de Amazon EC2, debe asegurarse de que el conjunto de opciones de DHCP esté correctamente configurado y conectado a la nube privada virtual (VPC) de Amazon que contiene la instancia de puerta de enlace. Para obtener más información, consulte Conjuntos de opciones de DHCP en la VPC de Amazon.

Confirme que la puerta de enlace puede resolver el dominio ejecutando una consulta de búsqueda

Si la puerta de enlace no puede resolver el dominio, la puerta de enlace no puede unirse al dominio.

Para ejecutar una consulta de búsqueda:

1. Conéctese a la consola local de la puerta de enlace mediante el software de administración del hipervisor (VMware, Hyper-V o KVM) para las puertas de enlace en las instalaciones, o mediante ssh para las puertas de enlace de Amazon EC2.
2. Introduzca el número correspondiente para seleccionar Consola de puerta de enlace y, a continuación, introduzca h para ver todos los comandos disponibles. Para probar si la puerta de enlace puede resolver el dominio, ejecute el siguiente comando:

   ```
   dig -d corp.domain.com
   ```

   > **Note**
   >
   > Reemplace `corp.domain.com` por el nombre de DNS del dominio de Active Directory.

A continuación se muestra un ejemplo de una respuesta correcta:

```
; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.amzn2.5.2 <<>> corp.domain.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24817
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;corp.domain.com.        IN    A

;; ANSWER SECTION:
corp.domain.com.    600    IN    A    10.10.10.10
corp.domain.com.    600    IN    A    10.10.20.10

;; Query time: 0 msec
;; SERVER: 10.10.20.228#53(10.10.20.228)
;; WHEN: Thu Jun 30 16:36:32 UTC 2022
;; MSG SIZE  rcvd: 78
```

Compruebe la configuración y los roles del controlador de dominio

Compruebe que el controlador de dominio no esté configurado como de solo lectura y que tenga funciones suficientes para que se unan los equipos. Para probarlo, intente unir otros servidores de la misma subred de la VPC que la máquina virtual de puerta de enlace al dominio.

Compruebe que la puerta de enlace esté unida al controlador de dominio más cercano

Como práctica recomendada, le recomendamos unir la puerta de enlace a un controlador de dominio que esté geográficamente cerca del dispositivo de puerta de enlace. Si el dispositivo de puerta de enlace no puede comunicarse con el controlador de dominio en 20 segundos debido a la latencia de la red, es posible que se agote el tiempo de espera del proceso de unión al dominio. Por ejemplo, es posible que se agote el tiempo de espera del proceso si el dispositivo de puerta de enlace se encuentra en EE. UU. Este (Virginia del Norte) Región de AWS y el controlador de dominio se encuentra en Asia Pacífico (Singapur Región de AWS).

> **Note**
>
> Para aumentar el valor de tiempo de espera predeterminado de 20 segundos, puede ejecutar el comando join-domain en AWS Command Line Interface (AWS CLI) e incluir la `--timeout-in-seconds` opción de aumentar el tiempo. También puedes usar la llamada a la JoinDomain API e incluir el `TimeoutInSeconds` parámetro para aumentar el tiempo. El valor del tiempo de espera máximo es de 3600 segundos.
> Si recibes errores al ejecutar AWS CLI comandos, asegúrate de usar la AWS CLI versión más reciente.

Confirmar que Active Directory crea nuevos objetos de equipo en la unidad organizativa (UO) predeterminada

Asegúrese de que Microsoft Active Directory no tiene ningún objeto de política de grupo que cree nuevos objetos de equipo en cualquier ubicación que no sea la UO predeterminada. Para poder unir la puerta de enlace al dominio de Active Directory, debe existir un nuevo objeto de equipo en la UO predeterminada. Algunos entornos de Active Directory están personalizados OUs para tener distintos objetos recién creados. Para garantizar que haya un nuevo objeto de equipo para la máquina virtual de puerta de enlace en la OU predeterminada, intente crear el objeto de equipo

manualmente en el controlador de dominio antes de unir la puerta de enlace al dominio. También puede ejecutar el comando join-domain mediante la AWS CLI. A continuación, especifique la opción para `--organizational-unit`.

> **Note**
>
> El proceso de creación del objeto de equipo se denomina pre-ensayo.

Comprobar los registros de eventos del controlador de dominio

Si no puede unir la puerta de enlace al dominio después de realizar todas las demás comprobaciones y configuraciones descritas en las secciones anteriores, le recomendamos que examine los registros de eventos del controlador de dominio. Compruebe si hay algún error en el visor de eventos del controlador de dominio. Compruebe que las consultas de la puerta de enlace hayan llegado al controlador de dominio.

Solución de problemas: error interno durante la activación de la puerta de enlace

Las solicitudes de activación de Storage Gateway atraviesan dos rutas de red. Las solicitudes de activación entrantes que envía un cliente se conectan a la máquina virtual (VM) de la puerta de enlace o a la instancia de Amazon Elastic Compute Cloud (Amazon EC2) a través del puerto 80. Si la puerta de enlace recibe correctamente la solicitud de activación, la puerta de enlace se comunica con los puntos de conexión de Storage Gateway para recibir una clave de activación. Si la puerta de enlace no puede llegar a los puntos de conexión de Storage Gateway, la puerta de enlace responde al cliente con un mensaje de error interno.

Utilice la siguiente información de solución de problemas para determinar qué hacer si recibe un mensaje de error interno al intentar activar AWS Storage Gateway.

> **Note**
>
> - Asegúrese de implementar nuevas puertas de enlace con la versión del archivo de imagen de máquina virtual más reciente o de Imagen de máquina de Amazon (AMI). Recibirá un error interno si intenta activar una puerta de enlace que utiliza una AMI desactualizada.

- Asegúrese de seleccionar el tipo de puerta de enlace correcto que pretende implementar antes de descargar la AMI. Los archivos.ova y AMIs para cada tipo de puerta de enlace son diferentes y no son intercambiables.

Resolución de errores al activar la puerta de enlace mediante un punto de conexión público

Para resolver los errores de activación al activar la puerta de enlace mediante un punto de conexión público, realice las siguientes comprobaciones y configuraciones.

Comprobación de los puertos necesarios

Para las puertas de enlace implementadas en las instalaciones, compruebe que los puertos estén abiertos en el firewall local. Para puertas de enlace implementadas en una instancia de Amazon EC2, compruebe que los puertos estén abiertos en el grupo de seguridad de la instancia. Para confirmar que los puertos están abiertos, ejecute un comando telnet en el punto de conexión público desde un servidor. Este servidor debe estar en la misma subred que la puerta de enlace. Por ejemplo, los siguientes comandos telnet prueban la conexión al puerto 443:

```
telnet d4kdq0yaxexbo.cloudfront.net 443
telnet storagegateway.region.amazonaws.com 443
telnet dp-1.storagegateway.region.amazonaws.com 443
telnet proxy-app.storagegateway.region.amazonaws.com 443
telnet client-cp.storagegateway.region.amazonaws.com 443
telnet anon-cp.storagegateway.region.amazonaws.com 443
```

Para confirmar que la propia puerta de enlace puede llegar al punto de conexión, acceda a la consola de máquina virtual local de la puerta de enlace (para las puertas de enlace implementadas en las instalaciones). O bien, puede utilizar SSH en la instancia de la puerta de enlace (para las puertas de enlace implementadas en Amazon EC2). A continuación, ejecute una prueba de conectividad de red. Confirme que la prueba devuelve `[PASSED]`. Para obtener más información, consulte Testing your gateway's network connectivity.

> **Note**
>
> El nombre de usuario de inicio de sesión predeterminado para la consola de la puerta de enlace es `admin` y la contraseña predeterminada es `password`.

Asegúrese de que la seguridad del firewall no modifique los paquetes enviados desde la puerta de enlace a los puntos de conexión públicos

Las inspecciones de SSL, las inspecciones exhaustivas de paquetes u otras formas de seguridad mediante firewall pueden interferir con los paquetes enviados desde la puerta de enlace. El protocolo de enlace SSL produce un error si el certificado SSL se modifica con respecto a lo esperado del punto de conexión de activación. Para confirmar que no hay ninguna inspección de SSL en curso, ejecute un comando de OpenSSL en el punto de conexión de activación principal (`anon-cp.storagegateway.region.amazonaws.com`) del puerto 443. Debe ejecutar este comando desde una máquina que se encuentre en la misma subred que la puerta de enlace:

```
$ openssl s_client -connect  anon-cp.storagegateway.region.amazonaws.com:443 -
servername anon-cp.storagegateway.region.amazonaws.com
```

> **Note**
>
> Sustitúyalos por *region* los suyos. Región de AWS

Si no hay ninguna inspección de SSL en curso, el comando devuelve una respuesta similar a la siguiente:

```
$ openssl s_client -connect anon-cp.storagegateway.us-east-2.amazonaws.com:443 -
servername anon-cp.storagegateway.us-east-2.amazonaws.com
CONNECTED(00000003)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-2.amazonaws.com
verify return:1
---
Certificate chain
 0 s:/CN=anon-cp.storagegateway.us-east-2.amazonaws.com
   i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
 1 s:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
   i:/C=US/O=Amazon/CN=Amazon Root CA 1
 2 s:/C=US/O=Amazon/CN=Amazon Root CA 1
   i:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
```

```
 3 s:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
   i:/C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification Authority
---
```

Si hay una inspección de SSL en curso, la respuesta muestra una cadena de certificados alterada, similar a la siguiente:

```
$ openssl s_client -connect  anon-cp.storagegateway.ap-southeast-1.amazonaws.com:443 -
servername anon-cp.storagegateway.ap-southeast-1.amazonaws.com
CONNECTED(00000003)
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.ap-southeast-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

El punto de conexión de activación solo acepta los protocolos de enlace de SSL si reconoce el certificado SSL. Esto significa que el tráfico saliente de la puerta de enlace hacia los puntos de conexión debe estar exento de las inspecciones realizadas por los firewalls de la red. Es posible que estas inspecciones sean una inspección de SSL o una inspección profunda de paquetes.

Comprobación de la sincronización horaria de la puerta de enlace

Los sesgos horarios excesivos pueden provocar errores en el protocolo de enlace de SSL. En el caso de las puertas de enlace en las instalaciones, puede utilizar la consola de máquina virtual local de la puerta de enlace para comprobar la sincronización horaria de la puerta de enlace. El sesgo horario no debe ser superior a 60 segundos. Para obtener más información, consulte Sincronización de la hora de la MV de la gateway.

La opción Administración del tiempo del sistema no está disponible en las puertas de enlace alojadas en instancias de Amazon EC2. Para asegurarse de que las puertas de enlace de Amazon

EC2 pueden sincronizar correctamente la hora, confirme que la instancia de Amazon EC2 puede conectarse a la siguiente lista de grupos de servidores NTP a través de los puertos UDP y TCP 123:

- time.aws.com
- 0.amazon.pool.ntp.org
- 1.amazon.pool.ntp.org
- 2.amazon.pool.ntp.org
- 3.amazon.pool.ntp.org

Resolución de errores al activar la puerta de enlace mediante un punto de conexión de VPC de Amazon

Para resolver los errores de activación al activar la puerta de enlace mediante un punto de conexión de Amazon Virtual Private Cloud (Amazon VPC), realice las siguientes comprobaciones y configuraciones.

Comprobación de los puertos necesarios

Asegúrese de que los puertos necesarios del firewall local (para las puertas de enlace implementadas en las instalaciones) o del grupo de seguridad (para las puertas de enlace implementadas en Amazon EC2) estén abiertos. Los puertos necesarios para conectar una puerta de enlace a un punto de conexión de VPC de Storage Gateway difieren de los necesarios al conectar una puerta de enlace a puntos de conexión públicos. Se requieren los siguientes puertos para conectarse a un punto de conexión de VPC de Storage Gateway:

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

Para obtener más información, consulte Creating a VPC endpoint for Storage Gateway.

Además, compruebe el grupo de seguridad que está conectado al punto de conexión de VPC de Storage Gateway. Es posible que el grupo de seguridad predeterminado asociado al punto de

conexión no permita los puertos necesarios. Cree un nuevo grupo de seguridad que permita el tráfico desde el rango de direcciones IP de la puerta de enlace a través de los puertos necesarios. A continuación, asocie ese grupo de seguridad al punto de conexión de VPC.

> **Note**
>
> Utilice la consola de Amazon VPC para verificar el grupo de seguridad que está conectado al punto de conexión de VPC. Consulte el punto de conexión de VPC de Storage Gateway desde la consola y, a continuación, elija la pestaña Grupos de seguridad.

Para confirmar que los puertos necesarios están abiertos, puede ejecutar comandos telnet en el punto de conexión de VPC de Storage Gateway. Debe ejecutar estos comandos desde un servidor que esté en la misma subred que la puerta de enlace. Puede ejecutar las pruebas en el primer nombre de DNS que no especifique una zona de disponibilidad. Por ejemplo, los siguientes comandos telnet prueban las conexiones de puerto necesarias con el nombre de DNS vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 443
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1026
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1027
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1028
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1031
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 2222
```

Asegúrese de que la seguridad del firewall no modifique los paquetes enviados desde la puerta de enlace al punto de conexión de VPC de Amazon de Storage Gateway

Las inspecciones de SSL, las inspecciones exhaustivas de paquetes u otras formas de seguridad mediante firewall pueden interferir con los paquetes enviados desde la puerta de enlace. El protocolo de enlace SSL produce un error si el certificado SSL se modifica con respecto a lo esperado del punto de conexión de activación. Para confirmar que no hay ninguna inspección de SSL en curso, ejecute un comando de OpenSSL en el punto de conexión de VPC de Storage Gateway. Debe ejecutar este comando desde una máquina que se encuentre en la misma subred que la puerta de enlace. Ejecute el comando para cada puerto requerido:

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:443 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1026 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1028 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1031 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:2222 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

Si no hay ninguna inspección de SSL en curso, el comando devuelve una respuesta similar a la siguiente:

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-1.amazonaws.com
verify return:1
---
Certificate chain
 0 s:CN = anon-cp.storagegateway.us-east-1.amazonaws.com
   i:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
 1 s:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
   i:C = US, O = Amazon, CN = Amazon Root CA 1
 2 s:C = US, O = Amazon, CN = Amazon Root CA 1
   i:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
```

```
 3 s:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
   i:C = US, O = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification
 Authority
---
```

Si hay una inspección de SSL en curso, la respuesta muestra una cadena de certificados alterada, similar a la siguiente:

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.us-
east-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.us-east-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

El punto de conexión de activación solo acepta los protocolos de enlace de SSL si reconoce el certificado SSL. Esto significa que el tráfico saliente de la puerta de enlace hacia el punto de conexión de VPC debe estar exento de las inspecciones realizadas por los firewalls de la red. Es posible que estas inspecciones sean inspecciones de SSL o inspecciones profundas de paquetes.

Comprobación de la sincronización horaria de la puerta de enlace

Los sesgos horarios excesivos pueden provocar errores en el protocolo de enlace de SSL. En el caso de las puertas de enlace en las instalaciones, puede utilizar la consola de máquina virtual local de la puerta de enlace para comprobar la sincronización horaria de la puerta de enlace. El sesgo horario no debe ser superior a 60 segundos. Para obtener más información, consulte Sincronización de la hora de la MV de la gateway.

La opción Administración del tiempo del sistema no está disponible en las puertas de enlace alojadas en instancias de Amazon EC2. Para asegurarse de que las puertas de enlace de Amazon EC2 pueden sincronizar correctamente la hora, confirme que la instancia de Amazon EC2 puede conectarse a la siguiente lista de grupos de servidores NTP a través de los puertos UDP y TCP 123:

- 0.amazon.pool.ntp.org
- 1.amazon.pool.ntp.org
- 2.amazon.pool.ntp.org
- 3.amazon.pool.ntp.org

Comprobación de un proxy HTTP y confirmación de la configuración del grupo de seguridad asociado

Antes de la activación, compruebe si tiene un proxy HTTP en Amazon EC2 configurado en la máquina virtual de puerta de enlace en las instalaciones como un proxy Squid en el puerto 3128. En este caso, confirme lo siguiente:

- El grupo de seguridad adjunto al proxy HTTP en Amazon EC2 debe tener una regla de entrada. Esta regla de entrada debe permitir el tráfico del proxy Squid en el puerto 3128 desde la dirección IP de la máquina virtual de la puerta de enlace.
- El grupo de seguridad adjunto al punto de conexión de VPC de Amazon EC2 debe tener reglas de entrada. Estas reglas de entrada deben permitir el tráfico en los puertos 1026-1028, 1031, 2222 y 443 desde la dirección IP del proxy HTTP en Amazon EC2.

Resuelva los errores al activar la puerta de enlace mediante un punto de conexión público y hay un punto de conexión de VPC de Storage Gateway en la misma VPC

Para resolver los errores al activar la puerta de enlace mediante un punto de conexión público cuando hay un punto de conexión de Amazon Virtual Private Cloud (Amazon VPC) en la misma VPC, realice las siguientes comprobaciones y configuraciones.

Confirmar que la configuración Habilitar nombre de DNS privado no esté habilitada en el punto de conexión de VPC de Storage Gateway

Si la opción Habilitación de nombre de DNS privado está habilitada, no podrá activar ninguna puerta de enlace desde esa VPC al punto de conexión público.

Para desactivar la opción de nombre de DNS privado:

1. Abra la Consola de Amazon VPC.
2. En el panel de navegación, elija Puntos de conexión.
3. Elija el punto de conexión de VPC de Storage Gateway.
4. Elija Acciones.
5. Elija Administrar nombres de DNS privados.
6. Para Habilitar nombre de DNS privado, borre Habilitar para este punto de conexión.
7. Elija Modificar nombres de DNS privados para guardar la configuración.

Solución de problemas: problemas relacionados con la puerta de enlace en las instalaciones

A continuación, encontrará información sobre los problemas habituales que pueden surgir al trabajar con las puertas de enlace locales y sobre cómo permitir la conexión Soporte a la puerta de enlace para ayudarle a solucionar problemas.

En la siguiente tabla se muestran los problemas habituales que podría encontrar al trabajar con gateways locales.

Problema	Acción que ejecutar
No se encuentra la dirección IP de la gateway.	Utilice el cliente del hipervisor para conectarse al host y buscar la dirección IP de la gateway. • Para VMware ESXi, la dirección IP de la máquina virtual se encuentra en el cliente de vSphere, en la pestaña Resumen. • Para Microsoft Hyper-V, la dirección IP de la MV puede encontrar se al iniciar sesión en la consola local.

Problema	Acción que ejecutar
	Si continúa teniendo problemas para encontrar la dirección IP de la gateway: • Compruebe que la MV esté activada. Solo cuando está activada la MV se asigna una dirección IP a la gateway. • Espere a que la MV termine de configurarse. Si acaba de activar la MV, la gateway puede tardar varios minutos en finalizar la secuencia de arranque.
Tiene problemas de red o de firewall.	• Asigne permisos a los puertos adecuados para la gateway. • Si utiliza un firewall o un router para filtrar o limitar el tráfico de red, debe configurar el firewall y el router para dar permiso a los puntos de conexión de servicio para mantener comunicaciones de salida con AWS. Para obtener más información sobre los requisitos de red y firewall, consulte Requisitos de red y firewall.

Problema	Acción que ejecutar
La activación de la puerta de enlace produce un error al hacer clic en el botón Proceder a la activación de la consola de administración de Storage Gateway.	• Compruebe que la MV de la gateway permita el acceso haciendo ping a la MV desde el cliente. • Compruebe que la MV tenga conectividad de red a Internet. De lo contrario, deberá configurar un proxy SOCKS. Para obtener más información sobre cómo hacerlo, consulte Probar la conexión de red de la puerta de enlace. • Compruebe que el host tenga la hora correcta, que el host esté configurado para sincronizar la hora de forma automática con un servidor NTP (Network Time Protocol) y que la MV de la gateway tenga la hora correcta. Para obtener información sobre la sincronización de la hora de los hosts del hipervisor, consulte. VMs Configuración de un servidor NTP (Network Time Protocol) para la puerta de enlace • Tras realizar estos pasos, puede reintentar la implementación de la puerta de enlace mediante la consola de Storage Gateway y el asistente Configurar y activar puerta de enlace. • Compruebe que la máquina virtual tiene al menos 16 GB de RAM. La asignación de la puerta de enlace produce un error si hay menos de 16 GB de RAM. Para obtener más información, consulte Requisitos de configuración de la puerta de enlace de archivo.

Problema	Acción que ejecutar
Debe mejorar el ancho de banda entre la puerta de enlace y AWS.	Puede mejorar el ancho de banda de la puerta de enlace AWS configurando la conexión a Internet AWS en un adaptador de red (NIC) independiente del que conecta las aplicaciones y la máquina virtual de la puerta de enlace. Este enfoque resulta útil si tiene una conexión con un ancho de banda elevado AWS y quiere evitar la contención del ancho de banda, especialmente durante una restauración instantánea. Para necesidades de carga de trabajo de alto rendimiento, puede usar Direct Connect para establecer una conexión de red dedicada entre la puerta de enlace en las instalaciones y AWS. Para medir el ancho de banda de la conexión desde la puerta de enlace AWS, utilice las `CloudBytesUploaded` métricas `CloudBytesDownloaded` y de la puerta de enlace. Para obtener más información sobre este tema, consulte Rendimiento y optimización. Mejorar la conectividad a Internet ayuda a garantizar que el búfer de carga no se llene.

Problema	Acción que ejecutar

El rendimiento hacia o desde la gateway disminuye a cero.	• En la pestaña Gateway de la consola Storage Gateway, compruebe que las direcciones IP de la máquina virtual de puerta de enlace son las mismas que las que ve al utilizar el software cliente del hipervisor (es decir, el cliente VMware vSphere o Microsoft Hyper-V Manager). Si encuentra una discrepancia, reinicie la puerta de enlace desde la consola de Storage Gateway, como se muestra en Apagado de la máquina virtual de puerta de enlace. Tras el reinicio, las direcciones de la lista Direcciones IP de la pestaña Puerta de enlace de la consola de Storage Gateway deberían coincidir con las direcciones IP de la puerta de enlace, las cuales determina desde el cliente del hipervisor.
	  • Para VMware ESXi, la dirección IP de la máquina virtual se encuentra en el cliente de vSphere, en la pestaña Resumen.
	  • Para Microsoft Hyper-V, la dirección IP de la MV puede encontrarse al iniciar sesión en la consola local.
	• Compruebe la conectividad de la puerta de enlace AWS tal y como se describe enProbar la conexión de red de la puerta de enlace.
	• Compruebe la configuración del adaptador de red de la puerta de enlace del cliente de administración del hipervisor y asegúrese de que todas las interfaces que desee activar para la puerta de enlace estén activadas.
	• Compruebe la configuración del adaptador de red de la puerta de enlace en la consola local de la puerta de enlace. Para obtener instrucciones, consulte Configuración de red de la puerta de enlace.
	
	Puedes ver el rendimiento desde y hacia tu puerta de enlace desde la CloudWatch consola de Amazon. Para obtener más información sobre cómo medir el rendimiento desde y hacia tu puerta de enlace AWS, consulta. Rendimiento y optimización

Problema	Acción que ejecutar
Tiene problemas para importar (implementar) Storage Gateway en Microsoft Hyper-V.	Consulte Solución de problemas: configuración de Microsoft Hyper-V, donde se explican algunos de los problemas comunes de implementar una gateway en Microsoft Hyper-V.
Recibirá un mensaje que indica: “Los datos que se han escrito en el volumen en la puerta de enlace no se almacenan de forma segura en AWS”.	Recibirá este mensaje si la máquina virtual de la gateway se creó a partir de un clon o de una instantánea de otra máquina virtual de gateway. Si este no es el caso, póngase en contacto con Soporte.

Activar el Soporte acceso para ayudar a solucionar los problemas de la puerta de enlace alojada en las instalaciones

Storage Gateway proporciona una consola local que puede utilizar para realizar varias tareas de mantenimiento, como permitir el acceso Soporte a la puerta de enlace para ayudarle a solucionar problemas de la puerta de enlace. De forma predeterminada, el Soporte acceso a la puerta de enlace está desactivado. Active este acceso mediante la consola local del host. Para Soporte acceder a su puerta de enlace, primero debe iniciar sesión en la consola local del host, ir a la consola de Storage Gateway y, a continuación, conectarse al servidor de soporte.

Para activar el Soporte acceso a la puerta de enlace

1. Inicie sesión en la consola local del host.
   - VMware ESXi — para obtener más información, consulteAcceder a la consola local de Gateway con VMware ESXi.
   - Microsoft Hyper-V: para obtener más información, consulte Acceso a la consola local de la gateway con Microsoft Hyper-V.
2. Cuando se le solicite, introduzca el número correspondiente para seleccionar Consola de puerta de enlace.
3. Introduzca **h** para abrir la lista de comandos disponibles.
4. Realice una de las siguientes acciones:

- Si la puerta de enlace está utilizando un punto de conexión público, en la ventana COMANDOS DISPONIBLES introduzca **`open-support-channel`** para conectar con el servicio de atención al cliente de Storage Gateway. Permitir el puerto TCP 22 para poder abrir un canal de soporte en AWS. Cuanto conecte con el servicio de atención al cliente, Storage Gateway le asignará un número de soporte. Apunte el número de soporte.
- Si la gateway está utilizando un punto de enlace de la VPC, en la ventana AVAILABLE COMMANDS (COMANDOS DISPONIBLES), introduzca **`open-support-channel`**. Si la puerta de enlace no está activada, proporcione el punto de conexión de VPC o la dirección IP para conectar con el servicio de atención al cliente de Storage Gateway. Permitir el puerto TCP 22 para poder abrir un canal de soporte en AWS. Cuanto conecte con el servicio de atención al cliente, Storage Gateway le asignará un número de soporte. Apunte el número de soporte.

> **Note**
>
> El número de canal no es un número de puerto Protocol/User Datagram Protocol (TCP/UDP (Control de transmisión). En lugar de ello, la puerta de enlace realiza una conexión Secure Shell (SSH) (TCP 22) a los servidores de Storage Gateway y proporciona el canal de soporte para la conexión.

5. Una vez establecido el canal de soporte, proporcione su número de servicio de soporte para Soporte que Soporte pueda ayudarlo a solucionar problemas.
6. Cuando se complete la sesión de soporte, introduzca **`q`** para finalizarla. No cierre la sesión hasta que el servicio de soporte de Amazon Web Services le notifique que la sesión de soporte se ha completado.
7. Introduzca **`exit`** para cerrar sesión en la consola de Storage Gateway.
8. Siga las instrucciones para salir de la consola local.

Solución de problemas: configuración de Microsoft Hyper-V

En la siguiente tabla se muestran los problemas habituales que podrían surgir al implementar Storage Gateway en la plataforma de Microsoft Hyper-V.

Problema	Acción que ejecutar
Se intenta importar una puerta de enlace y se recibe el mensaje de error siguiente: “Se ha producido un error al intentar importar la máquina virtual. Se ha producido un error al importar. Imposible encontrar los archivos de importación de la máquina virtual en la ubicación […]. Solo puede importar una máquina virtual si utilizó Hyper-V para crearla y exportarla”.	Este error puede producirse por las razones siguientes: • Si no apunta a la raíz de los archivos de origen de la gateway sin comprimir. La última parte de la ubicación que especifique en el cuadro de diálogo Importar máquina virtual debe ser `AWS-Storage-Gateway` . Por ejemplo: `C:\prod-gateway\unzippedSourceVM\AWS-Storage-Gateway\` . • Si ya ha implementado una gateway, pero no seleccionó la opción Copy the virtual machine (Copia la máquina virtual) ni activó la opción Duplicate all files (Duplicar todos los archivos) en el cuadro de diálogo Import Virtual Machine (Importar máquina virtual), la máquina virtual se creó en la ubicación donde tiene los archivos de la gateway sin comprimir y no puede volver a importarla desde esta ubicación. Para solucionar este problema, obtenga una copia nueva de los archivos de origen de la gateway sin comprimir y cópiela en una nueva ubicación. Utilice la nueva ubicación como origen de la importación. Si planea crear varias puertas de enlace desde una ubicación de archivos de origen descomprimida, debe seleccionar Copiar la máquina virtual y marcar la casilla Duplicar todos los archivos en el cuadro de diálogo Importar máquina virtual.
Se intenta importar una puerta de enlace y se recibe el mensaje de error siguiente: “Se ha producido un error al intentar importar la máquina virtual. Se ha producido un error al importar. La tarea de importación no pudo copiar	Si ya ha implementado una gateway e intenta reutilizar las carpetas predeterminadas donde se almacenan los archivos del disco duro virtual y los archivos de configuración de máquinas virtuales, se producirá este error. Para solucionar este problema, especifique las nuevas ubicaciones en Servidor, en el panel situado a la izquierda del cuadro de diálogo de configuración de Hyper-V.

Problema	Acción que ejecutar
el archivo de [...]: el archivo existe. (0x80070050)”	
Se intenta importar una puerta de enlace y se recibe el mensaje de error siguiente: “Se ha producido un error al intentar importar la máquina virtual. Se ha producido un error al importar. Import failed because the virtual machine must have a new identifier. Select a new identifier and try the import again."	Al importar la puerta de enlace, asegúrese de que selecciona la opción Copiar la máquina virtual y de que marca la casilla Duplicar todos los archivos en el cuadro de diálogo Importar máquina virtual para crear un nuevo ID único para la máquina virtual.
Se intenta iniciar una máquina virtual de puerta de enlace y se recibe el mensaje de error siguiente: “Se ha producido un error al intentar iniciar las máquinas virtuales seleccionadas. La configuración del procesador de particiones secundario no es compatible con la partición principal . No se pudo inicializar “AWS-Storage-Gateway”. (ID de máquina virtual [...])”	Es probable que este error se deba a una discrepancia de CPU entre lo necesario CPUs para la puerta de enlace y lo disponible CPUs en el host. Asegúrese de que el número de CPU de MV sea compatible con el hipervisor subyacente. Para obtener más información sobre los requisitos de Storage Gateway, consulte Requisitos de configuración de la puerta de enlace de archivo.

Problema	Acción que ejecutar
Se intenta iniciar una máquina virtual de puerta de enlace y se recibe el mensaje de error siguiente: “Se ha producido un error al intentar iniciar las máquinas virtuales seleccionadas. No se pudo inicializar “AWS-Storage-Gateway”. (ID de máquina virtual [...]) No se pudo crear la partición : los recursos del sistema son insuficientes para completar el servicio solicitado. (0x800705AA)”	Es probable que este error se deba a una discrepancia de RAM entre la RAM requerida para la gateway y la RAM disponible en el host. Para obtener más información sobre los requisitos de Storage Gateway, consulte Requisitos de configuración de la puerta de enlace de archivo.
Las actualizaciones del software de la gateway y de las instantáneas se producen a horas ligeramente diferentes de lo esperado.	El reloj de la MV de la gateway puede desviarse de la hora real, lo que se conoce como deriva del reloj. Compruebe y corrija la hora de la MV mediante la opción de sincronización de hora de la consola de la gateway local. Para obtener más información, consulte Configuración de un servidor NTP (Network Time Protocol) para la puerta de enlace.
Debe colocar los archivos de Microsoft Hyper-V Storage Gateway sin comprimir en el sistema de archivos del host.	Acceda al host como lo hace en un servidor de Microsoft Windows típico. Por ejemplo, si el host del hipervisor se llama `hyperv-server` , puede utilizar la siguiente ruta UNC `\\hyperv-server\c$` , en la que se asume que el nombre `hyperv-server` se puede resolver o está definido en el archivo del host local.
Se le solicitan credenciales al conectarse al hipervisor.	Agregue sus credenciales de usuario como administrador local para el host del hipervisor a través de la herramienta Sconfig.cmd.

Problema	Acción que ejecutar
Es posible que observe un rendimiento de red deficiente si activa la cola de máquinas virtuales (VMQ) para un host Hyper-V que utilice un adaptador de red Broadcom.	Para obtener información sobre una solución alternativa, consulte la documentación de Microsoft y consulte Rendimiento de red deficiente en máquinas virtuales en el host Hyper-V de Windows Server 2012 si VMQ se ha activado.

Solución de problemas: problemas con la puerta de enlace de Amazon EC2

En las secciones siguientes, encontrará los problemas habituales que podría encontrar al trabajar con la puerta de enlace implementada en Amazon EC2. Para obtener más información sobre la diferencia entre una puerta de enlace en las instalaciones y una puerta de enlace implementada en Amazon EC2 consulte Implemente un host Amazon EC2 predeterminado para File Gateway FSx.

Temas

- La puerta de enlace no se ha activado poco tiempo después
- No encuentra la instancia de la puerta de enlace de EC2 en la lista de instancias
- Desea conectarse a la instancia de puerta de enlace con la consola serie de Amazon EC2
- Quiere ayudar Soporte a solucionar los problemas de su puerta de enlace Amazon EC2

La puerta de enlace no se ha activado poco tiempo después

Compruebe lo siguiente en la consola de Amazon EC2:

- El puerto 80 está abierto en el grupo de seguridad que ha asociado a la instancia. Para obtener más información sobre cómo agregar una regla de grupo de seguridad, consulte Agregación de una regla de grupo de seguridad en la Guía del usuario de Amazon EC2.
- La instancia de la gateway está marcada como en ejecución. En la consola de Amazon EC2, el valor de Estado de la instancia debe ser EN EJECUCIÓN.

- Asegúrese de que el tipo de instancia de Amazon EC2 cumple los requisitos mínimos, tal y como se describe en Requisitos de almacenamiento.

Después de corregir el problema, intente activar la gateway de nuevo. Para ello, abra la consola de Storage Gateway, seleccione Implementar una nueva puerta de enlace en Amazon EC2 y vuelva a introducir la dirección IP de la instancia.

No encuentra la instancia de la puerta de enlace de EC2 en la lista de instancias

Si no asignó a la instancia una etiqueta de recurso y tiene muchas instancias en funcionamiento, puede ser difícil saber qué instancia lanzó. En este caso, puede realizar las siguientes acciones para encontrar la instancia de la gateway:

- Compruebe el nombre la Imagen de máquina de Amazon (AMI) en la pestaña Description (Descripción) de la instancia. Una instancia basada en la AMI de Storage Gateway debe empezar con el texto **`aws-storage-gateway-ami`**.
- Si tiene varias instancias basadas en la AMI de Storage Gateway, compruebe el momento de lanzar la instancia para encontrar la instancia correcta.

Desea conectarse a la instancia de puerta de enlace con la consola serie de Amazon EC2

Puede utilizar la consola serie de Amazon EC2 para solucionar problemas de arranque, configuración de red y otros. Para obtener instrucciones y consejos de solución de problemas, consulte Amazon EC2 Serial Console en la Guía del usuario de Amazon Elastic Compute Cloud.

Quiere ayudar Soporte a solucionar los problemas de su puerta de enlace Amazon EC2

Storage Gateway proporciona una consola local que puede utilizar para realizar varias tareas de mantenimiento, como permitir el acceso Soporte a la puerta de enlace para ayudarle a solucionar problemas de la puerta de enlace. De forma predeterminada, el Soporte acceso a la puerta de enlace está desactivado. Active este acceso mediante la consola local de Amazon EC2. Inicie sesión en la consola local de Amazon EC2 mediante Secure Shell (SSH). Para iniciar sesión correctamente

mediante SSH, el grupo de seguridad de la instancia debe tener una regla que abra el puerto TCP 22.

> **Note**
>
> Si agrega una nueva regla a un grupo de seguridad existente, la nueva regla se aplicará a todas las instancias que utilicen ese grupo de seguridad. Para obtener más información sobre los grupos de seguridad y cómo agregar una regla de grupo de seguridad, consulte Grupos de seguridad de Amazon EC2 en la Guía del usuario de Amazon EC2.

Para permitir la Soporte conexión a su puerta de enlace, primero inicie sesión en la consola local de la instancia de Amazon EC2, navegue hasta la consola de Storage Gateway y, a continuación, proporcione el acceso.

Para activar el Soporte acceso a una puerta de enlace implementada en una instancia de Amazon EC2

1. Inicie sesión en la consola local para la instancia de Amazon EC2. Para obtener instrucciones, vaya a Conexión a la instancia en la Guía del usuario de Amazon EC2.

   Puede utilizar el siguiente comando para iniciar sesión en la consola local de la instancia EC2.

   ```
   ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
   ```

   > **Note**
   >
   > *PRIVATE-KEY*Es el `.pem` archivo que contiene el certificado privado del par de claves EC2 que utilizó para lanzar la instancia de Amazon EC2. Para obtener más información, consulte Recuperación de la clave pública para el par de claves en la Guía del usuario de Amazon EC2.
   > *INSTANCE-PUBLIC-DNS-NAME*Es el nombre público del Sistema de nombres de dominio (DNS) de la instancia de Amazon EC2 en la que se ejecuta la puerta de enlace. Para obtener este nombre de DNS público, seleccione la instancia de Amazon EC2 en la consola de EC2 y haga clic en la pestaña Descripción.

2. En el símbolo del sistema, introduzca **`6 - Command Prompt`** para abrir la consola del canal de Soporte .

3. Introduzca **h** para abrir la ventana AVAILABLE COMMANDS (COMANDOS DISPONIBLES).
4. Realice una de las siguientes acciones:

   - Si la puerta de enlace está utilizando un punto de conexión público, en la ventana COMANDOS DISPONIBLES introduzca **`open-support-channel`** para conectar con el servicio de atención al cliente de Storage Gateway. Permitir el puerto TCP 22 para poder abrir un canal de soporte en AWS. Cuanto conecte con el servicio de atención al cliente, Storage Gateway le asignará un número de soporte. Apunte el número de soporte.
   - Si la gateway está utilizando un punto de enlace de la VPC, en la ventana AVAILABLE COMMANDS (COMANDOS DISPONIBLES), introduzca **`open-support-channel`**. Si la puerta de enlace no está activada, proporcione el punto de conexión de VPC o la dirección IP para conectar con el servicio de atención al cliente de Storage Gateway. Permitir el puerto TCP 22 para poder abrir un canal de soporte en AWS. Cuanto conecte con el servicio de atención al cliente, Storage Gateway le asignará un número de soporte. Apunte el número de soporte.

   > **Note**
   >
   > El número de canal no es un número de puerto Protocol/User Datagram Protocol (TCP/UDP (Control de transmisión). En lugar de ello, la puerta de enlace realiza una conexión Secure Shell (SSH) (TCP 22) a los servidores de Storage Gateway y proporciona el canal de soporte para la conexión.

5. Una vez establecido el canal de soporte, proporcione su número de servicio de soporte para Soporte que Soporte pueda ayudarlo a solucionar problemas.
6. Cuando se complete la sesión de soporte, introduzca **`q`** para finalizarla. No cierre la sesión hasta que el servicio de soporte de Amazon Web Services le notifique que la sesión de soporte se ha completado.
7. Introduzca **`exit`** para salir de la consola de Storage Gateway.
8. Siga los menús de la consola para cerrar sesión en la instancia de Storage Gateway.

Solución de problemas: problemas con el dispositivo de hardware

> **Note**
>
> Aviso de fin de disponibilidad: a partir del 12 de mayo de 2025, el dispositivo de AWS Storage Gateway hardware dejará de estar disponible. Los clientes actuales que dispongan del dispositivo de AWS Storage Gateway hardware pueden seguir utilizándolo y recibiendo asistencia hasta mayo de 2028. Como alternativa, puede utilizar el AWS Storage Gateway servicio para ofrecer a sus aplicaciones un acceso local y en la nube a un almacenamiento en la nube prácticamente ilimitado.

En los temas siguientes se analizan los problemas que pueden surgir con el dispositivo de hardware AWS Storage Gateway y se ofrecen sugerencias para solucionarlos.

Temas

- No puede determinar la dirección IP del servicio
- ¿Cómo se restablece la configuración de fábrica?
- ¿Cómo se realiza un reinicio remoto?
- ¿Cómo se obtiene soporte de iDRAC de Dell?
- No puede encontrar el número de serie del dispositivo hardware
- Dónde obtener soporte para el dispositivo de hardware

No puede determinar la dirección IP del servicio

Cuando intente conectarse a un servicio, asegúrese de que está utilizando la dirección IP del servicio y no la dirección IP del host. Configure la dirección IP del servicio en la consola del servicio y la dirección IP del host en la consola del hardware. Verá la consola del hardware cuando inicie el dispositivo de hardware. Para ir a la consola de servicio desde la consola del hardware, seleccione Open Service Console (Abra la consola de servicio).

¿Cómo se restablece la configuración de fábrica?

Si necesita restablecer los valores de fábrica de su dispositivo, póngase en contacto con el equipo del dispositivo de hardware AWS Storage Gateway para obtener asistencia, tal y como se describe en la siguiente sección de soporte.

¿Cómo se realiza un reinicio remoto?

Si necesita realizar un reinicio remoto del dispositivo, puede hacerlo mediante la interfaz de administración iDRAC de Dell. Para obtener más información, consulte Ciclo de alimentación DRAC9 virtual: apague los PowerEdge servidores Dell EMC de forma remota en el InfoHub sitio web de Dell Technologies.

¿Cómo se obtiene soporte de iDRAC de Dell?

El PowerEdge servidor Dell incluye la interfaz de administración iDRAC de Dell. Le recomendamos lo siguiente:

- Si utiliza la interfaz de administración iDRAC, debe cambiar la contraseña predeterminada. Para obtener más información sobre las credenciales de iDRAC, consulte Dell PowerEdge : ¿Cuáles son las credenciales de inicio de sesión predeterminadas para iDRAC? .
- Asegúrese de que el firmware sea up-to-date para evitar violaciones de seguridad.
- Mover la interfaz de red del iDRAC a un puerto normal (`em`) puede provocar problemas de rendimiento o impedir el funcionamiento normal del dispositivo.

No puede encontrar el número de serie del dispositivo hardware

Puede encontrar el número de serie de su dispositivo de hardware AWS Storage Gateway mediante la consola Storage Gateway.

Para encontrar el número de serie del dispositivo de hardware:

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Elija Hardware en el menú de navegación del lado izquierdo de la página.
3. Seleccione el dispositivo de hardware de la lista.
4. Localice el campo del número de serie en la pestaña Detalles del dispositivo.

Dónde obtener soporte para el dispositivo de hardware

Para ponerse en contacto con AWS el soporte técnico de su dispositivo de hardware, consulte Soporte.

Es posible que el Soporte equipo le pida que active el canal de soporte para solucionar los problemas de la puerta de enlace de forma remota. No necesita que este puerto esté abierto para el funcionamiento normal de la gateway, pero es necesario para la solución de problemas. Puede activar el canal de soporte desde la consola del hardware, como se muestra en el siguiente procedimiento.

Para abrir un canal de soporte para AWS

1. Abra la consola del hardware.
2. Elija Abrir canal de soporte en la parte inferior de la página principal de la consola de hardware y, a continuación, pulse `Enter`.

   El número de puerto asignado debe aparecer en 30 segundos si no hay problemas de firewall o de conectividad de red. Por ejemplo:

   Estado: Abierto en el puerto 19599
3. Anote el número de puerto e indíquelo en Soporte.

Solución de problemas: problemas con la puerta de enlace de archivo

Puede configurar su File Gateway para escribir entradas de registro en un grupo de CloudWatch registros de Amazon. Si lo hace, recibirá notificaciones acerca del estado de la puerta de enlace y de los errores que esta detecta. Puede encontrar información sobre estas notificaciones de errores y estado en CloudWatch los registros.

En las siguientes secciones puede encontrar información que le ayudará a comprender la causa de cada notificación de estado y error y cómo solucionar los problemas.

Temas

- Error: FileMissing
- Error: FsxFileSystemAuthenticationFailure
- Error: FsxFileSystemConnectionFailure
- Error: FsxFileSystemFull
- Error: GatewayClockOutOfSync
- Error: InvalidFileState

- Error: ObjectMissing
- Error: DroppedNotifications
- Notificación: HardReboot
- Notificación: reinicio
- Solución de problemas: problemas relacionados con el dominio de Active Directory
- Solución de problemas: uso de métricas CloudWatch

Error: FileMissing

El error `FileMissing` es similar al error `ObjectMissing` y los pasos para resolverlo son idénticos. Puede producirse un `FileMissing` error cuando un escritor que no sea el File Gateway especificado elimina el archivo especificado de Amazon FSx. Cualquier carga posterior a Amazon FSx o cualquier recuperación del objeto FSx por parte de Amazon fallará.

Para resolver un error FileMissing

1. Guarde la copia más reciente del archivo en el sistema de archivos local del cliente SMB (necesitará una copia del archivo en el paso 3).
2. Elimine el archivo de la puerta de enlace de archivo utilizando el cliente SMB.
3. Copia la última versión del archivo que guardaste en el paso 1 en Amazon FSx con tu cliente SMB. Haga esto mediante la puerta de enlace de archivo.

Error: FsxFileSystemAuthenticationFailure

Se puede producir un error `FsxFileSystemAuthenticationFailure` cuando las credenciales proporcionadas al asociar el sistema de archivos hayan caducado o se hayan revocado sus privilegios.

Para resolver un FsxFileSystemAuthenticationFailure error

1. Asegúrese de que las credenciales proporcionadas en el momento de adjuntar el sistema de FSx archivos de Amazon siguen siendo válidas.
2. Asegúrese de que el usuario dispone de todos los permisos necesarios, tal y como se describe en Adjuntar un sistema de archivos de Amazon FSx para Windows File Server.

Error: FsxFileSystemConnectionFailure

Puede aparecer un `FsxFileSystemConnectionFailure` error cuando no se puede acceder al FSx servidor de Amazon desde la máquina de puerta de enlace.

Para resolver un error FsxFileSystemConnectionFailure

1. Asegúrese de que todas las reglas de firewall y VPC permitan la conexión entre la máquina de puerta de enlace y el servidor de Amazon FSx .
2. Asegúrese de que el FSx servidor de Amazon esté funcionando.

Error: FsxFileSystemFull

Puede aparecer un `FsxFileSystemFull` error si no hay suficiente espacio libre en el disco en el sistema de FSx archivos de Amazon.

Para resolver un FsxFileSystemFull error

- Aumente el espacio de almacenamiento del sistema de FSx archivos de Amazon.

Error: GatewayClockOutOfSync

Puede producirse un `GatewayClockOutOfSync` error cuando la puerta de enlace detecte una diferencia de 5 minutos o más entre la hora del sistema local y la hora notificada por los servidores de AWS Storage Gateway. Los problemas de sincronización del reloj pueden afectar negativamente a la conectividad entre la puerta de enlace y AWS. Si el reloj de la puerta de enlace no está sincronizado, pueden producirse errores de E/S en las conexiones NFS y SMB, y los usuarios de SMB podrían experimentar errores de autenticación.

Para resolver un GatewayClockOutOfSync error

- Compruebe la configuración de red entre la puerta de enlace y el servidor NTP. Para obtener más información sobre la sincronización de la hora de la máquina virtual de puerta de enlace y la actualización de la configuración del servidor NTP, consulte Configuración de un servidor NTP (Network Time Protocol) para la puerta de enlace.

Error: InvalidFileState

Se puede detectar un error `InvalidFileState` cuando un escritor que no sea la puerta de enlace especificada modifica el archivo especificado en el recurso compartido de archivos especificado. Como resultado, el estado del archivo en la puerta de enlace no coincide con su estado en Amazon FSx. Cualquier carga o recuperación posterior del archivo desde Amazon FSx podría fallar.

Para resolver un error InvalidFileState

1. Guarde la copia más reciente del archivo en el sistema de archivos local del cliente SMB (necesitará una copia del archivo en el paso 4). Si la versión del archivo en Amazon FSx es la más reciente, descarga esa versión. Puedes hacerlo accediendo directamente al FSx recurso compartido de Amazon mediante cualquier cliente SMB.
2. Elimina el archivo FSx directamente en Amazon.
3. Elimine el archivo de la puerta de enlace utilizando el cliente SMB.
4. Con tu cliente SMB, copia la última versión del archivo que guardaste en el paso 1, a través de File Gateway, a Amazon FSx.

Error: ObjectMissing

Puede producirse un `ObjectMissing` error cuando un escritor que no sea el File Gateway especificado elimina el archivo especificado de Amazon FSx. Cualquier carga posterior a Amazon FSx o cualquier recuperación del objeto FSx por parte de Amazon fallará.

Para resolver un error ObjectMissing

1. Guarde la copia más reciente del archivo en el sistema de archivos local del cliente SMB (necesitará una copia del archivo en el paso 3).
2. Elimine el archivo de la puerta de enlace de archivo utilizando el cliente SMB.
3. Copia la última versión del archivo que guardaste en el paso 1 en Amazon FSx con tu cliente SMB. Haga esto mediante la puerta de enlace de archivo.

Error: DroppedNotifications

Es posible que aparezca un `DroppedNotifications` error en lugar de otros tipos de entradas de CloudWatch registro esperadas si el espacio de almacenamiento libre en el disco raíz de la puerta de enlace es inferior a 1 GB o si se generan más de 100 notificaciones de estado en un intervalo de 1

minuto. En estas circunstancias, la puerta de enlace deja de generar notificaciones de CloudWatch registro detalladas como medida de precaución.

Para resolver un error DroppedNotifications

1. Compruebe la métrica `Root Disk Usage` de la pestaña Supervisión de la puerta de enlace en la consola de Storage Gateway para determinar si el espacio disponible en el disco raíz se está agotando.
2. Aumente el tamaño del disco de almacenamiento raíz de la puerta de enlace si el espacio disponible es inferior a 1 GB. Consulte la documentación del hipervisor de la máquina virtual para obtener instrucciones.

   Para aumentar el tamaño del disco raíz de las puertas de enlace de Amazon EC2, consulte Solicitar modificaciones a los volúmenes de EBS en la Guía del usuario de Amazon Elastic Compute Cloud.

   > **Note**
   >
   > No es posible aumentar el tamaño del disco raíz del dispositivo de hardware de AWS Storage Gateway.

3. Reinicie la gateway.

Notificación: HardReboot

Puede recibir una notificación `HardReboot` cuando la MV de la gateway se reinicia de forma inesperada. Este reinicio se puede deber a una pérdida de potencia, un fallo de hardware u otro evento. En el VMware caso de las puertas de enlace, un restablecimiento realizado por vSphere High Availability Application Monitoring puede provocar este evento.

Cuando la puerta de enlace se ejecute en un entorno de este tipo, compruebe la presencia de la `HealthCheckFailure` notificación y consulte el registro de VMware eventos de la máquina virtual.

Notificación: reinicio

Puede recibir una notificación de reinicio cuando la MV de la gateway se reinicia. Puede reiniciar la VM de una puerta de enlace mediante la consola de gestión de hipervisor de VM o la consola de Storage Gateway. También puede llevar a cabo el reinicio de la gateway mediante el software de la gateway durante el ciclo de mantenimiento de la gateway.

Si la hora del reinicio se encuentra dentro de un periodo de 10 minutos desde la hora de inicio de mantenimiento configurada de la gateway, es probable que este reinicio sea un evento normal y no sea signo de ningún problema. Si el reinicio se produce significativamente fuera del periodo de mantenimiento, compruebe si la gateway se ha reiniciado de forma manual.

Solución de problemas: problemas relacionados con el dominio de Active Directory

FSx File Gateway no genera mensajes de registro específicos para problemas de dominio de Active Directory. Si tiene problemas para unir la puerta de enlace al dominio de Active Directory, haga lo siguiente:

- Compruebe que la puerta de enlace no esté intentando utilizar un controlador de dominio de solo lectura (RODC) para unirse al dominio.
- Compruebe que la puerta de enlace está configurada para utilizar los servidores DNS correctos.

  Por ejemplo, si intenta unir una instancia de puerta de enlace de Amazon EC2 a un Active Directory AWS administrado, compruebe que la opción de DHCP establecida para su VPC de EC2 especifique los servidores DNS de Active Directory administrados. AWS

  Los servidores DNS que se configuran mediante el conjunto de opciones de DHCP de la VPC se proporcionan a todas las instancias de EC2 de la VPC. Si desea especificar un servidor DNS para una puerta de enlace individual, puede hacerlo mediante la consola local EC2 de esa puerta de enlace.

  Para las puertas de enlace en las instalaciones, especifique un servidor DNS mediante la consola local de la máquina virtual.
- Compruebe la conectividad de la red de la puerta de enlace ejecutando los siguientes comandos desde el símbolo del sistema de la consola local de la puerta de enlace. Sustituya las variables resaltadas por el nombre de dominio y las direcciones IP reales de la implementación.

  ```
  dig -d ExampleDomainName
  ncport -d ExampleDomainControllerIPAddress -p 445
  ncport -d ExampleDomainControllerIPAddress -p 389
  ```
- Compruebe que su cuenta de servicio de Active Directory tenga los permisos necesarios. Para obtener más información, consulte Requisitos de permiso de la cuenta de servicio de Active Directory.

- Compruebe que la puerta de enlace se une a la unidad organizativa (UO) correcta.

  Al unirse a un dominio, se crea una cuenta de equipo de Active Directory en el contenedor predeterminado del equipo (que no es una unidad organizativa), con el ID de puerta de enlace de la puerta de enlace como nombre de cuenta (por ejemplo, SGW-1234ADE). No es posible personalizar el nombre de esta cuenta.

  Si su entorno de Active Directory tiene una unidad organizativa designada para los nuevos objetos de equipo, debe especificarla al unirse al dominio.

  Si encuentra errores de denegación de acceso al intentar unirse a la UO designada, póngase en contacto con el administrador del dominio de Active Directory. Es posible que el administrador necesite preparar la cuenta de equipo de la puerta de enlace antes de que pueda unirse al dominio. Para obtener más información, consulte ¿Cómo puedo solucionar problemas relacionados con la unión de la puerta de enlace de archivo de Storage Gateway a un dominio para la autenticación de Microsoft Active Directory? .

- Compruebe que el nombre de host de la puerta de enlace se pueda resolver en el DNS ejecutando el siguiente comando desde el símbolo del sistema de la consola local de la puerta de enlace. Sustituya la variable resaltada por el nombre de host real de la puerta de enlace.

  ```
  dig -d ExampleHostName -r A
  ```

  Si configuró un nombre de host personalizado para la puerta de enlace, debe agregar manualmente un registro A de DNS que apunte a su dirección IP.

- Compruebe que la latencia de la red entre la puerta de enlace y el controlador de dominio sea razonablemente baja. El tiempo de espera para la consulta de unión a un dominio puede agotarse si la puerta de enlace no recibe una respuesta del controlador de dominio en 20 segundos.

  Si une la puerta de enlace al dominio mediante el comando JoinDomainCLI, puede agregar el `--timeout-in-seconds` indicador para aumentar el tiempo de espera hasta un máximo de 3600 segundos.

- Compruebe que el usuario de Active Directory que está utilizando para unir la puerta de enlace al dominio tenga los privilegios necesarios para hacerlo.

Solución de problemas: uso de métricas CloudWatch

A continuación, encontrará información sobre las acciones para abordar los problemas mediante el uso de CloudWatch las métricas de Amazon con Storage Gateway.

Temas

- La puerta de enlace reacciona lentamente al examinar directorios
- La puerta de enlace no responde
- No ves los archivos en tu sistema de FSx archivos de Amazon
- No ves instantáneas antiguas en tu sistema de FSx archivos de Amazon
- Tu puerta de enlace tarda en transferir datos a Amazon FSx
- El trabajo de copia de seguridad de la puerta de enlace falla o se producen errores al escribir en la puerta de enlace

La puerta de enlace reacciona lentamente al examinar directorios

Si File Gateway reacciona con lentitud cuando ejecutas el ls comando o navegas por los directorios, comprueba las `IndexEviction` CloudWatch métricas `IndexFetch` y:

- Si la `IndexFetch` métrica es superior a 0 cuando ejecuta un `ls` comando o navega por directorios, su File Gateway se inició sin información sobre el contenido del directorio afectado y tuvo que acceder al servidor de archivos de FSx para Windows. Los esfuerzos posteriores para mostrar el contenido de ese directorio deberían realizarse más rápidamente.
- Si la métrica de `IndexEviction` es mayor que 0, significa que la puerta de enlace de archivo ha alcanzado el límite de lo que puede gestionar en la caché en ese momento. En este caso, la puerta de enlace de archivo tiene que liberar espacio de almacenamiento del directorio al que se ha accedido menos recientemente para crear un nuevo directorio. Si esto ocurre con frecuencia y hay un impacto en el rendimiento, póngase en contacto con Soporte.

  Analice Soporte el contenido del sistema de FSx archivos de Amazon relacionado y las recomendaciones para mejorar el rendimiento en función de su caso de uso.

La puerta de enlace no responde

Si la puerta de enlace de archivo no responde, realice las siguientes acciones:

- Si se ha producido una actualización de software o un reinicio recientemente, compruebe la métrica `IOWaitPercent`. Esta métrica muestra el porcentaje de tiempo que la CPU está inactiva cuando hay una I/O solicitud de disco pendiente. En algunos casos, puede ser elevado (10 o más) y se puede producir después de que el servidor se haya reiniciado o actualizado. En estos casos, se puede producir un efecto embudo en la puerta de enlace de archivo a causa de un disco raíz lento, ya que reanuda la caché de índice en la RAM. Puede solucionar este problema mediante el uso de un disco físico más rápido para el disco raíz.
- Si la métrica `MemUsedBytes` es igual o prácticamente igual que la métrica `MemTotalBytes`, la puerta de enlace de archivo se está ejecutando fuera de la RAM disponible. Asegúrese de que la puerta de enlace de archivo tenga el menos la RAM mínima requerida. Si ya la tiene, considere añadir más RAM a la puerta de enlace de archivo en función de la carga de trabajo y el caso de uso.

  Si el recurso compartido de archivos es SMB, el problema también podría deberse al número de clientes SMB conectados a dicho recurso. Para ver el número de clientes que están conectados en cualquier momento, compruebe la métrica `SMBV(1/2/3)Sessions`. Si hay muchos clientes conectados, es posible que necesite añadir más RAM a la puerta de enlace de archivo.

No ves los archivos en tu sistema de FSx archivos de Amazon

Si observas que los archivos de la pasarela no se reflejan en el sistema de FSx archivos de Amazon, comprueba la `FilesFailingUpload` métrica. Si la métrica indica que algunos archivos no se cargan correctamente, compruebe las notificaciones de estado. Cuando los archivos no se pueden cargar, la puerta de enlace genera una notificación de salud con más detalles sobre el problema.

No ves instantáneas antiguas en tu sistema de FSx archivos de Amazon

Algunas operaciones con archivos en la puerta de enlace de FSx archivos, como cambiar el nombre de las carpetas de nivel superior o los cambios de permisos, pueden provocar varias operaciones con archivos y provocar una gran I/O carga en el sistema de archivos del servidor FSx de archivos de Windows. Si el sistema de archivos no tiene suficientes recursos de rendimiento para su carga de trabajo, es posible que elimine las instantáneas, ya que da prioridad a la disponibilidad para la retención continua de instantáneas por I/O encima de la histórica.

En la FSx consola de Amazon, consulta la página Supervisión y rendimiento para ver si tu sistema de archivos está insuficientemente aprovisionado. Si es así, puede cambiar a un almacenamiento en SSD, aumentar la capacidad de rendimiento o aumentar las IOPS en SSD para gestionar su carga de trabajo.

Tu puerta de enlace tarda en transferir datos a Amazon FSx

Si su puerta de enlace de archivos tarda en transferir datos a Amazon FSx for Windows File Server, haga lo siguiente:

- Si la `CachePercentDirty` métrica es 80 o superior, su File Gateway escribe los datos en el disco más rápido de lo que puede cargar los datos en Amazon FSx para Windows File Server. Considere aumentar el ancho de banda para cargar desde su puerta de enlace de archivos, añadir uno o más discos de caché, ralentizar las escrituras del cliente o aumentar la capacidad de rendimiento del servidor de archivos Amazon FSx for Windows asociado.
- Si la métrica `CachePercentDirty` es baja, compruebe la métrica `IoWaitPercent`. Si `IoWaitPercent` es mayor que 10, es posible que se produzca un efecto embudo en la puerta de enlace de archivo por la velocidad del disco en caché local. Recomendamos utilizar discos de disco de estado sólido (SSD) locales para la memoria caché, preferiblemente NVM Express ()NVMe. Si dichos discos no están disponibles, intente utilizar varios discos en caché desde discos físicos independientes para mejorar el rendimiento.

El trabajo de copia de seguridad de la puerta de enlace falla o se producen errores al escribir en la puerta de enlace

Si el trabajo de copia de seguridad de la puerta de enlace de archivo falla o se producen errores al escribir en la puerta de enlace de archivo, realice las siguientes acciones:

- Si la métrica `CachePercentDirty` es del 90 por ciento o superior, la puerta de enlace de archivo no puede aceptar nuevas escrituras en el disco porque no hay suficiente espacio disponible en el disco de caché. Para ver la rapidez con la que File Gateway se carga en para Windows File Server, consulte la `CloudBytesUploaded` métrica. Compare esa métrica con la métrica `WriteBytes`, que muestra a qué velocidad escribe archivos el cliente en la puerta de enlace de archivo. Si el cliente SMB escribe en su puerta de enlace de archivos más rápido de lo que puede cargar en para Windows File Server, añada más discos de caché para cubrir como mínimo el tamaño del trabajo de copia de seguridad. También puede aumentar el ancho de banda de carga.
- Si una copia de un archivo grande como un trabajo de copia de seguridad falla, pero la métrica `CachePercentDirty` es inferior al 80 por ciento, es posible que la puerta de enlace de archivo esté alcanzando el tiempo de espera de la sesión del lado del cliente. En el caso de SMB, puede aumentar este tiempo de espera mediante el comando. PowerShell `Set-SmbClientConfiguration -SessionTimeout 300` Al ejecutar este comando, el tiempo de espera se establece en 300 segundos.

Notificaciones de estado de alta disponibilidad

Al ejecutar la puerta de enlace en la plataforma VMware vSphere High Availability (HA), es posible que reciba notificaciones de estado. Para obtener más información sobre las notificaciones de estado, consulte Solución de problemas: problemas de alta disponibilidad.

Solución de problemas: problemas de alta disponibilidad

A continuación puede encontrar información acerca de las acciones que debe realizar si experimenta problemas de disponibilidad.

Temas

- Notificaciones de estado
- Métricas

Notificaciones de estado

Cuando ejecuta la puerta de enlace en VMware vSphere HA, todas las puertas de enlace producen las siguientes notificaciones de estado en el grupo de registros de Amazon CloudWatch configurado. Estas notificaciones van a un flujo de registro denominado `AvailabilityMonitor`.

Temas

- Notificación: reinicio
- Notificación: HardReboot
- Notificación: HealthCheckFailure
- Notificación: AvailabilityMonitorTest

Notificación: reinicio

Puede recibir una notificación de reinicio cuando la MV de la gateway se reinicia. Puede reiniciar la VM de una puerta de enlace mediante la consola de gestión de hipervisor de VM o la consola de Storage Gateway. También puede llevar a cabo el reinicio de la gateway mediante el software de la gateway durante el ciclo de mantenimiento de la gateway.

Acción necesaria

Si la hora del reinicio se encuentra dentro de un periodo de 10 minutos desde la hora de inicio de mantenimiento configurada de la gateway, es probable que sea un evento normal y no sea signo de ningún problema. Si el reinicio se produce significativamente fuera del periodo de mantenimiento, compruebe si la gateway se ha reiniciado de forma manual.

Notificación: HardReboot

Puede recibir una notificación `HardReboot` cuando la MV de la gateway se reinicia de forma inesperada. Este reinicio se puede deber a una pérdida de potencia, un fallo de hardware u otro evento. En el VMware caso de las puertas de enlace, un restablecimiento realizado por vSphere High Availability Application Monitoring puede provocar este evento.

Acción necesaria

Cuando la puerta de enlace se ejecute en un entorno de este tipo, compruebe la presencia de la `HealthCheckFailure` notificación y consulte el registro de VMware eventos de la máquina virtual.

Notificación: HealthCheckFailure

En el caso de una puerta de enlace en VMware vSphere HA, puede recibir una `HealthCheckFailure` notificación cuando se produzca un error en una comprobación de estado y se solicite el reinicio de la máquina virtual. Este evento también se produce durante una prueba para monitorizar la disponibilidad y se indica mediante una notificación `AvailabilityMonitorTest`. En este caso, la notificación `HealthCheckFailure` es normal.

> **Note**
>
> Esta notificación es solo para VMware puertas de enlace.

Acción necesaria

Si este evento se produce de forma repetida sin una notificación `AvailabilityMonitorTest`, compruebe si la infraestructura de la MV presenta algún problema (almacenamiento, memoria, etc.). Si necesita ayuda adicional, póngase en contacto con Soporte.

Notificación: AvailabilityMonitorTest

En el caso de una puerta de enlace en VMware vSphere HA, puede recibir una `AvailabilityMonitorTest` notificación cuando ejecute una prueba del sistema de supervisión de disponibilidad y aplicaciones en. VMware

Métricas

La métrica `AvailabilityNotifications` está disponible en todas las gateways. Esta métrica es un recuento del número de notificaciones de estado relacionadas con la disponibilidad que ha generado la gateway. Utilice la estadística `Sum` para comprobar si se está produciendo algún evento relacionado con la disponibilidad en la gateway. Consulte con el grupo de CloudWatch registro configurado para obtener más información sobre los eventos.

Prácticas recomendadas para la puerta de enlace de archivo

Esta sección contiene los siguientes temas, que proporcionan información sobre las prácticas recomendadas para trabajar con puertas de enlace, recursos compartidos de archivos, buckets y datos. Le recomendamos que se familiarice con la información que se describe en esta sección e intente seguir estas directrices para evitar problemas con AWS Storage Gateway. Para obtener orientación adicional sobre diagnóstico y solución de problemas comunes que pueden surgir con la implementación, consulte Solución de problemas relacionados con la implementación de Storage Gateway.

Temas

- Prácticas recomendadas: recuperación de los datos
- Restauración a partir de copias de seguridad o instantáneas directamente en Amazon FSx
- limpieza de recursos innecesarios

Prácticas recomendadas: recuperación de los datos

Aunque es infrecuente, es posible que su gateway se enfrente a un error irrecuperable. Este error puede producir en la máquina virtual (VM), en la propia gateway, en el almacenamiento local o en otro lugar. Si se produce un error, le recomendamos que siga las instrucciones de la sección adecuada, a continuación, para recuperar los datos.

> **Important**
>
> Storage Gateway no permite recuperar la máquina virtual de una puerta de enlace a partir de una instantánea creada por el hipervisor o desde la imagen de máquina de Amazon (AMI) de Amazon EC2. Si la MV de la gateway no funciona correctamente, active una nueva gateway y recupere los datos para esa gateway utilizando las instrucciones siguientes.

Recuperación de un cierre inesperado de una máquina virtual

Si la MV se cierra de forma inesperada, por ejemplo, durante un corte de suministro eléctrico, el acceso a la gateway dejará de ser posible. Cuando se restablezca el suministro eléctrico y la conectividad de red, volverá a ser posible el acceso a la gateway y empezará a funcionar

normalmente. A continuación se muestran algunas de las acciones que puede llevar a cabo en ese momento para facilitar la recuperación de los datos:

- Si una interrupción del suministro eléctrico provoca problemas de conectividad de red, puede solucionar el problema. Para obtener más información sobre cómo probar la conectividad de red, consulte Probar la conexión de red de la puerta de enlace.

Recuperación de los datos a partir de un disco de la caché que no funciona correctamente

Si el disco de la caché encuentra un error, le recomendamos que haga lo siguiente para recuperar los datos en función de la situación:

- Si el error se produjo porque se retiró del host un disco de la caché, cierre la puerta de enlace, vuelva a agregar el disco y reinicie la puerta de enlace.

Recuperación de los datos de un centro de datos inaccesible

Si una puerta de enlace o un centro de datos deja de ser accesible por algún motivo, puede recuperar los datos en otra puerta de enlace de un centro de datos diferente o en una puerta de enlace alojada en una instancia de Amazon EC2. Si no tiene acceso a otro centro de datos, le recomendamos crear la puerta de enlace en una instancia de Amazon EC2. Los pasos que siga dependerán del tipo de gateway cuyos datos intenta recuperar.

Cómo recuperar datos de una puerta de enlace de archivo en un centro de datos inaccesible

En el caso de File Gateway, debe asignar un nuevo sistema de archivos de archivos al para Windows File Server que contiene los datos que desea recuperar.

1. Cree y active una nueva puerta de enlace de archivo en un host de Amazon EC2. Para obtener más información, consulte Implemente un host Amazon EC2 predeterminado para File Gateway FSx.
2. Cree un nuevo sistema de archivos en la puerta de enlace de EC2 que ha creado. Para obtener más información, consulte Crear un sistema de archivos FSx para Windows File Server.
3. Monte el sistema de archivos en su cliente y asígnelo al para el servidor de archivos de Windows que contiene los datos que desea recuperar. Para obtener más información, consulte Montaje y uso de un recurso compartido de archivos.

Restauración a partir de copias de seguridad o instantáneas directamente en Amazon FSx

En algunos casos, es posible que tengas que restaurar los datos de tu sistema de FSx archivos de Amazon directamente, mediante una copia de seguridad o una instantánea de un momento anterior. En estos casos, existe el riesgo de que se cree un escenario de doble grabación entre la aplicación de copia de seguridad y la puerta de enlace de FSx archivos, lo que puede provocar que los archivos se atasquen o no coincidan. Para evitar problemas al restaurar el sistema de FSx archivos de Amazon a partir de copias de seguridad o instantáneas, utilice el siguiente procedimiento.

> **Note**
>
> Los datos en caché almacenados actualmente en su FSx File Gateway no serán válidos después de restaurar el sistema de FSx archivos de Amazon a partir de una copia de seguridad o instantánea mediante este procedimiento.

Para evitar problemas al restaurar el sistema de FSx archivos de Amazon a partir de copias de seguridad o instantáneas

1. Desconecte el sistema de FSx archivos Amazon de FSx File Gateway mediante la consola Storage Gateway.
2. Restaure la copia de seguridad o la instantánea directamente en su sistema de FSx archivos de Amazon.
3. Vuelva a conectar el sistema de FSx archivos Amazon a FSx File Gateway mediante la consola Storage Gateway.

limpieza de recursos innecesarios

Recomendamos eliminar los recursos de Storage Gateway para evitar cambios imprevistos o innecesarios. Por ejemplo, si creó una puerta de enlace como ejercicio de demostración o prueba, considere la posibilidad de eliminar de la implementación dicha puerta y su dispositivo virtual. Utilice el siguiente procedimiento para eliminar recursos.

Cómo eliminar los recursos innecesarios

1. Si no tiene previsto seguir utilizando una puerta de enlace, elimínela. Para obtener más información, consulte Eliminación de la puerta de enlace y eliminación de los recursos asociados.
2. Elimine la máquina virtual de Storage Gateway desde el host en las instalaciones. Si creó la puerta de enlace en una instancia de Amazon EC2, termine la instancia.

Recursos adicionales de Storage Gateway

Esta sección contiene los siguientes temas, que ofrecen información y recursos adicionales relacionados con la configuración y el uso de AWS Storage Gateway:

Temas

- Configuración del host: obtenga información sobre cómo implementar y configurar un host de máquina virtual para la puerta de enlace.
- Uso de Storage Gateway con VMware HA- Aprenda a configurar Storage Gateway para que funcione con las funciones de alta disponibilidad de VMware vSphere.
- Obtención de la clave de activación: obtenga información sobre dónde encontrar la clave de activación que debe proporcionar al implementar una nueva puerta de enlace.
- Usando Direct Connect: obtenga información sobre cómo crear una conexión de red dedicada entre la puerta de enlace en las instalaciones y la nube de AWS .
- Permisos de Active Directory: obtenga información sobre qué permisos debe tener su cuenta de servicio para poder unir la puerta de enlace al dominio de Active Directory.
- Obtención de la dirección IP para el dispositivo de puerta de enlace: obtenga información sobre dónde encontrar la dirección IP del host de la máquina virtual de la puerta de enlace, que debe proporcionar al implementar una nueva puerta de enlace.
- Comprensión de los recursos y los recursos IDs- Aprenda a AWS identificar los recursos y subrecursos que crea Storage Gateway.
- Etiquetado de recursos: obtenga información sobre cómo usar las etiquetas de metadatos para clasificar los recursos y facilitar su administración.
- Componentes de código abierto: obtenga información sobre las herramientas y licencias de terceros que se utilizan para ofrecer la funcionalidad de Storage Gateway.
- Cuotas: obtenga información sobre los límites y las cuotas de la puerta de enlace de archivo, incluidas las limitaciones mínimas y máximas de los recursos compartidos de archivos y los discos de caché locales.

Implementación y configuración del host de la máquina virtual de la puerta de enlace

En los siguientes temas se proporciona información acerca de cómo configurar la plataforma de host de la máquina virtual para la puerta de enlace.

Temas

- Implemente un host Amazon EC2 predeterminado para File Gateway FSx
- Implemente un host Amazon EC2 personalizado para File Gateway FSx
- Modificación de las opciones de metadatos de la instancia de Amazon EC2
- Sincronización de la hora de la máquina virtual con la hora del host KVM de Hyper-V o Linux
- Sincronice la hora de la máquina virtual con la hora del host VMware
- Configuración de adaptadores de red para la puerta de enlace
- Uso de VMware vSphere High Availability con Storage Gateway

Implemente un host Amazon EC2 predeterminado para File Gateway FSx

En este tema se enumeran los pasos para implementar un host de Amazon EC2 utilizando las especificaciones predeterminadas.

Puede implementar y activar un en una instancia de Amazon Elastic Compute Cloud (Amazon EC2). La imagen de máquina de Amazon (AMI) de AWS Storage Gateway se encuentra disponible como AMI de la comunidad.

> **Note**
>
> La comunidad Storage Gateway AMIs está publicada y cuenta con el apoyo total de AWS. Puede ver que el editor es AWS un proveedor verificado.

1. Para configurar la instancia de Amazon EC2, elija Amazon EC2 como Plataforma host en la sección Opciones de plataforma del flujo de trabajo. Para obtener instrucciones sobre la configuración de la instancia de Amazon EC2, consulte Gateway Implementación de una instancia de Amazon EC2 para alojar su Amazon File Gateway. FSx

2. Seleccione Launch instance para abrir la plantilla AWS Storage Gateway AMI en la consola Amazon EC2 y personalizar ajustes adicionales, como los tipos de instancia, los ajustes de red y configurar el almacenamiento.
3. Si lo desea, puede seleccionar Usar la configuración predeterminada en la consola de Storage Gateway para implementar una instancia de Amazon EC2 con la configuración predeterminada.

   La instancia de Amazon EC2 que crea Usar la configuración predeterminada tiene las siguientes especificaciones predeterminadas:

   - Tipo de instancia: m5.xlarge
   - Configuración de red
     - En VPC, elija la VPC en la que desea que se ejecute la instancia de EC2.
     - En Subred, especifique la subred en la que debe lanzarse la instancia de EC2.

     > **Note**
     >
     > Las subredes de VPC aparecerán en el menú desplegable solo si tienen activada la configuración de asignación automática de direcciones IP públicas desde la consola de administración de la VPC.

     - Asignar una IP pública de forma automática: Activada
     - Se crea un grupo de seguridad de EC2 y se asocia a la instancia de EC2. El grupo de seguridad tiene las siguientes reglas de puerto de entrada:

     > **Note**
     >
     > Necesitará que el puerto 80 esté abierto durante la activación de la puerta de enlace. El puerto se cierra inmediatamente después de la activación. A partir de entonces, solo se puede acceder a la instancia de EC2 a través de los demás puertos de la VPC seleccionada.
     > Solo se puede acceder a los recursos compartidos de archivos de la puerta de enlace desde los hosts de la misma VPC que la puerta de enlace. Si es necesario acceder a los recursos compartidos de archivos desde hosts externos a la VPC, debe actualizar las reglas del grupo de seguridad correspondientes.

Para editar los grupos de seguridad en cualquier momento, vaya a la página de detalles de la instancia de Amazon EC2, seleccione Seguridad, vaya a Detalles del grupo de seguridad y elija el ID del grupo de seguridad.

Puerto	Protocolo	Protocolo del sistema de archivos				
80	TCP	Acceso HTTP para la activación				
137	UDP	NetBIOS				
138	UDP	NetBIOS				
139	TCP, UDP	SMB				
389	TCP	LDAP				
445	TCP	SMB				

- Configurar almacenamiento

Configuración predeterminada	Volumen raíz de AMI	Caché de volumen 2				
Nombre de dispositivo		'/dev/sdb'				

Configuración predeterminada	Volumen raíz de AMI	Caché de volumen 2				
Tamaño	80 GiB	165 GiB				
Tipo de volumen	gp3	gp3				
IOPS	3 000	3 000				
Eliminar al finalizar	Sí	Sí				
Encriptado	No	No				
Rendimiento	125	125				

Implemente un host Amazon EC2 personalizado para File Gateway FSx

Puede implementar y activar un en una instancia de Amazon Elastic Compute Cloud (Amazon EC2). La imagen de máquina de Amazon (AMI) de AWS Storage Gateway se encuentra disponible como AMI de la comunidad.

> **Note**
>
> La comunidad Storage Gateway AMIs está publicada y cuenta con el apoyo total de AWS. Puede ver que el editor es AWS un proveedor verificado.
> File Gateway AMIs utiliza la siguiente convención de nomenclatura. El número de versión adjunto al nombre de la AMI cambia con cada versión publicada.
> `aws-storage-gateway-FILE_FSX_SMB-2.2.3`

Para implementar una instancia de Amazon EC2 para alojar su Amazon File Gateway FSx

1. Empiece configurando una nueva puerta de enlace mediante la consola de Storage Gateway. Para obtener instrucciones, consulte de enlace de FSx archivos de Amazon. Cuando llegue a la sección Opciones de plataforma, elija Amazon EC2 como Plataforma host y, a continuación, siga los pasos siguientes para lanzar la instancia de Amazon EC2 que alojará la puerta de enlace de archivo.
2. Elija Launch instance para abrir la plantilla de AWS Storage Gateway AMI en la consola Amazon EC2, donde podrá configurar ajustes adicionales.

   Utilice Quicklaunch para lanzar la instancia de Amazon EC2 con la configuración predeterminada. Para obtener más información sobre las especificaciones predeterminadas de Quicklaunch de Amazon EC2, consulte Especificaciones de configuración de Quicklaunch para Amazon EC2.
3. En Nombre, ingrese un nombre descriptivo para la instancia de Amazon EC2. Una vez implementada la instancia, puede usar este nombre para buscarla en las páginas de la lista de la consola de Amazon EC2.
4. En la sección Tipo de instancia, para el tipo de instancia, elija la configuración de hardware de su instancia. La configuración del hardware debe cumplir con ciertos requisitos mínimos para ser compatible con su puerta de enlace. Recomendamos comenzar por el tipo de instancia m5.xlarge, que cumple los requisitos mínimos de hardware para que la puerta de enlace funcione correctamente. Para obtener más información, consulte Requisitos para los tipos de instancia de Amazon EC2.

   Puede cambiar el tamaño de la instancia después de lanzarla, si es necesario. Para obtener más información, consulte Cambio de tamaño de la instancia en la Guía del usuario de Amazon EC2.

   > **Note**
   >
   > Algunos tipos de instancias, especialmente la i3 EC2, utilizan NVMe discos SSD. Estos pueden causar problemas al iniciar o detener la puerta de enlace de archivo; por ejemplo, se pueden perder datos de la caché. Supervisa la CloudWatch métrica de `CachePercentDirty` Amazon y solo inicia o detiene tu sistema cuando ese parámetro lo esté`0`. Para obtener más información sobre las métricas de monitoreo de su gateway, consulte las métricas y dimensiones de Storage Gateway en la CloudWatch documentación.

5. En la sección Par de claves (inicio de sesión), en Nombre del par de claves: obligatorio, elija el par de claves que desea usar para conectarse de forma segura a su instancia. Si es necesario, puede crear un nuevo par de claves. Para obtener más información, consulte Crear un par de claves en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux.
6. En la sección Configuración de red, revise los ajustes preconfigurados y elija Editar para realizar cambios en los siguientes campos:

   a. En VPC: obligatorio, elija la VPC en la que desee lanzar la instancia de Amazon EC2. Para obtener más información, consulte Cómo funciona Amazon VPC en la Guía del usuario de Amazon Virtual Private Cloud.

   b. (Opcional) En Subred, elija la subred en la que desee lanzar la instancia de Amazon EC2.

   c. En Auto-assign Public IP (Autoasignar IP pública), elija Enable (Habilitar).
7. En la subsección Firewall (grupos de seguridad), revise los ajustes preconfigurados. Si lo desea, puede cambiar el nombre y la descripción predeterminados del nuevo grupo de seguridad que se va a crear para su instancia de Amazon EC2 o aplicar reglas de firewall de un grupo de seguridad existente.
8. En la subsección Reglas de grupos de seguridad de entrada, agregue reglas de firewall para abrir los puertos que los clientes utilizarán para conectarse a su instancia. Para obtener más información sobre los puertos necesarios para Amazon FSx File Gateway, consulte de puertos. Para obtener más información sobre la agregación de reglas de firewall, consulte Reglas del grupo de seguridad en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux.

   > **Note**
   >
   > Amazon FSx File Gateway requiere que el puerto TCP 80 esté abierto para el tráfico entrante y el acceso HTTP único durante la activación de la puerta de enlace. Tras la activación, puede cerrar este puerto.
   > Además, debe abrir el puerto TCP 445 para el acceso SMB, el puerto UDP 137 para el acceso NetBIOS, el puerto UDP 138 para el acceso NetBIOS y el puerto TCP 389 para el acceso LDAP.
9. En la subsección Configuración de red avanzada, revise los ajustes preconfigurados y realice los cambios necesarios.
10. En la sección Configurar almacenamiento, elija Agregar volumen nuevo para agregar almacenamiento a la instancia de la puerta de enlace de archivos.

> **Important**
>
> Debe agregar al menos un volumen de Amazon EBS con una capacidad mínima de 150 GiB para el almacenamiento en caché, además del volumen raíz preconfigurado. Para aumentar el rendimiento, recomendamos asignar varios volúmenes de EBS para el almacenamiento en caché de al menos 150 GiB cada uno.

11. En la subsección Detalles avanzados, revise los ajustes preconfigurados y realice los cambios necesarios.
12. Elija Lanzar instancia para lanzar su nueva instancia de puerta de enlace de Amazon EC2 con los ajustes configurados.
13. Para comprobar que la nueva instancia se lanzó correctamente, vaya a la página Instancias de la consola de Amazon EC2 y busque la nueva instancia por su nombre. Asegúrese de que el Estado de la instancia se muestre En ejecución con una marca de verificación verde y de que la Comprobación de estado se haya completado y muestre una marca de verificación verde.
14. Seleccione la instancia de la página de detalles. Copie la dirección IP pública de la sección de resumen de instancias y, a continuación, vuelva a la página Configurar puerta de enlace de la consola de Storage Gateway para reanudar la configuración de (Amazon FSx File Gateway).

Puede determinar el ID de AMI que se utilizará para lanzar un File Gateway mediante la consola Storage Gateway o consultando el almacén de AWS Systems Manager parámetros.

Para determinar la ID de AMI, lleve a cabo alguna de las siguientes operaciones:

- Empiece configurando una nueva puerta de enlace mediante la consola de Storage Gateway. Para obtener instrucciones, consulte de enlace de FSx archivos de Amazon. Cuando llegue a la sección Opciones de plataforma, elija Amazon EC2 como plataforma host y, a continuación, elija Launch instance para abrir la plantilla de AWS Storage Gateway AMI en la consola de Amazon EC2.

  Se le redirigirá a la página de AMI de la comunidad EC2, donde podrá ver el ID de AMI de su AWS región en la URL.
- Consulta del almacén de parámetros de Systems Manager. Puede usar la API AWS CLI o Storage Gateway para consultar el parámetro público de Systems Manager en el espacio de nombres `/aws/service/storagegateway/ami/FILE_FSX_SMB/latest`. Por ejemplo, si utiliza el siguiente comando de CLI, se devuelve el ID de la AMI actual Región de AWS que especifique.

```
aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/
FILE_FSX_SMB/latest
```

El comando de la CLI devuelve un resultado similar al siguiente.

```
{
    "Parameter": {
        "Type": "String",
        "LastModifiedDate": 1561054105.083,
        "Version": 18,
         "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/
FILE_FSX_SMB/latest",
         "Name": "/aws/service/storagegateway/ami/FILE_FSX_SMB/latest",,
        "Value": "ami-033d1edba5606cffb"
    }
}
```

Modificación de las opciones de metadatos de la instancia de Amazon EC2

El servicio de metadatos de instancias (IMDS) es un componente de la instancia que proporciona acceso seguro a los metadatos de la instancia de Amazon EC2. Se puede configurar una instancia para que acepte las solicitudes de metadatos entrantes que usen la versión 1 (IMDSv1) del IMDS o para que todas las solicitudes de metadatos usen la versión 2 (IMDSv2) del IMDS. IMDSv2 utiliza solicitudes orientadas a la sesión y mitiga varios tipos de vulnerabilidades que podrían utilizarse para intentar acceder al IMDS. Para obtener más información IMDSv2, consulte Cómo funciona Instance Metadata Service versión 2 en la Guía del usuario de Amazon Elastic Compute Cloud.

Se recomienda que necesite IMDSv2 para todas las instancias de Amazon EC2 que alojan Storage Gateway. IMDSv2 es obligatorio de forma predeterminada en todas las instancias de gateway recién lanzadas. Si tiene instancias existentes que aún están configuradas para aceptar solicitudes de IMDSv1 metadatos, consulte Requerir el uso de IMDSv2 en la Guía del usuario de Amazon Elastic Compute Cloud para obtener instrucciones sobre cómo modificar las opciones de metadatos de la instancia para requerir el uso de IMDSv2. La aplicación de este cambio no requiere un reinicio de la instancia.

Sincronización de la hora de la máquina virtual con la hora del host KVM de Hyper-V o Linux

En el caso de una puerta de enlace VMware ESXi instalada, basta con configurar la hora del host del hipervisor y sincronizar la hora de la máquina virtual con el host para evitar la pérdida de tiempo. Para obtener más información, consulte Sincronice la hora de la máquina virtual con la hora del host VMware. Para una puerta de enlace implementada en Microsoft Hyper-V o Linux KVM, le recomendamos que compruebe periódicamente la hora de la máquina virtual mediante el procedimiento que se describe a continuación.

Visualización y sincronización de la hora de la máquina virtual de una puerta de enlace de hipervisor con un servidor de Network Time Protocol (NTP)

1. Inicie sesión en la consola local de la gateway:
   - Para obtener más información sobre el inicio de sesión en la consola local de Microsoft Hyper-V, consulte Acceso a la consola local de la gateway con Microsoft Hyper-V.
   - Para obtener más información sobre cómo iniciar sesión en la consola local de la máquina virtual basada en el kernel (KVM) de Linux, consulte Acceso a la consola local de la gateway con Linux KVM.
2. En la pantalla del menú principal de Configuración de Storage Gateway, ingrese el número correspondiente para seleccionar Administración de la hora del sistema.
3. En la pantalla del menú Administración de la hora del sistema, ingrese el número correspondiente para seleccionar Ver y sincronizar la hora del sistema.

   La consola local de la puerta de enlace muestra la hora actual del sistema y la compara con la hora indicada por el servidor NTP. A continuación, indica la discrepancia exacta entre ambas horas en segundos.
4. Si la discrepancia horaria es superior a 60 segundos, ingrese **y** para sincronizar la hora del sistema con la hora de NTP. De lo contrario, escriba **n**.

   La sincronización de la hora puede tardar unos instantes.

Sincronice la hora de la máquina virtual con la hora del host VMware

Para activar la gateway correctamente, debe asegurarse de que la hora de la máquina virtual esté sincronizada con la hora del host y de que esta última esté configurada de forma correcta. En esta

sección, primero se sincroniza la hora de la máquina virtual con la hora del host. A continuación, se comprueba la hora del host. Después, si es preciso, se establece la hora del host y se configura este último para que sincronice la hora automáticamente con un servidor NTP (Network Time Protocol).

> **Important**
>
> Sincronizar la hora de la máquina virtual con la hora del host es imprescindible para que la gateway se active correctamente.

Cómo sincronizar la hora de la máquina virtual con la hora del host

1. Configure la hora de la máquina virtual.

   a. En el cliente de vSphere, haga clic con el botón derecho en el nombre de la máquina virtual de puerta de enlace en el panel de la izquierda de la ventana de la aplicación para abrir el menú contextual para la máquina virtual y, a continuación, elija Editar configuración.

      Se abrirá el cuadro de diálogo Virtual Machine Properties (Propiedades de la máquina virtual).

   b. Seleccione la pestaña Opciones y, a continuación, seleccione VMware Herramientas en la lista de opciones.

   c. Marque la opción Sincronizar tiempo del invitado con el host en la sección Avanzadas situada a la derecha del cuadro de diálogo de propiedades de la máquina virtual, y, a continuación, elija Aceptar.

      La máquina virtual sincronizará su hora con la del host.

2. Configurar la hora del host.

   Es importante asegurarse de que el reloj del host esté establecido en la hora correcta. Si no ha configurado el reloj del host, siga estos pasos para configurarlo y sincronizarlo con un servidor NTP.

   a. En el cliente de VMware vSphere, seleccione el nodo host de vSphere en el panel izquierdo y, a continuación, elija la pestaña Configuración.

   b. Seleccione Time Configuration (Configuración de tiempo) en el panel Software y, a continuación, elija el enlace Properties (Propiedades).

      Aparecerá el cuadro de diálogo Time Configuration (Configuración de tiempo).

c. En Fecha y hora, defina la fecha y la hora del host de vSphere.

d. Configure el host para que sincronice la hora automáticamente con un servidor de NTP.

   i. Elija Opciones en el cuadro de diálogo Configuración de hora. A continuación, en el cuadro de diálogo Opciones de NTP Daemon (ntpd), elija Configuración de NTP en el panel izquierdo.

   ii. Elija Add (Añadir) para agregar un nuevo servidor NTP.

   iii. En el cuadro de diálogo Add NTP Server (Añadir servidor NTP), escriba la dirección IP o el nombre de dominio completo de un servidor NTP y, a continuación, elija OK (Aceptar).

   Puede usar `pool.ntp.org` como nombre de dominio.

   iv. En el cuadro de diálogo Opciones de NTP Daemon (ntpd), elija Generales en el panel de la izquierda.

   v. En Comandos de servicio, elija Iniciar para iniciar el servicio.

   Tenga en cuenta que si cambia esta referencia del servidor NTP o agrega otra más adelante, tendrá que reiniciar el servicio para utilizar el nuevo servidor.

e. Elija OK (Aceptar) para cerrar el cuadro de diálogo NTP Daemon (ntpd) Options (Opciones de NTP Daemon (ntpd)).

f. Elija OK (Aceptar) para cerrar el cuadro de diálogo Time Configuration (Configuración de tiempo).

Configuración de adaptadores de red para la puerta de enlace

Storage Gateway utiliza un único adaptador de red VMXNET3 (10 GbE) de forma predeterminada, pero puede configurar su puerta de enlace para que utilice más de un adaptador de red, de modo que se pueda acceder a él desde varias direcciones IP. Es posible que desee hacerlo en las siguientes situaciones:

- Maximización del rendimiento: quizá desee maximizar el rendimiento para una puerta de enlace cuando los adaptadores de red sean un cuello de botella.
- Separación de aplicaciones: quizá necesite separar la manera en que las aplicaciones escriben en los volúmenes de una puerta de enlace. Por ejemplo, quizá desee que una aplicación de almacenamiento crítica utilice exclusivamente un adaptador determinado definido para la gateway.

- Restricciones de la red: el entorno de su aplicación puede requerir que mantenga los recursos compartidos de archivos y los iniciadores que se conectan a ellos en una red aislada. Esta red es diferente de la red mediante la cual la gateway se comunica con AWS.

En un caso de uso típico de varios adaptadores, un adaptador se configura como la ruta por la que se comunica la puerta de enlace AWS (es decir, como la puerta de enlace predeterminada). Excepto para este adaptador, los iniciadores deben estar en la misma subred que el adaptador que contiene los recursos compartidos de archivo a los que se conecte. De lo contrario, puede que la comunicación con los objetivos reales no sea posible. Si un destino está configurado en el mismo adaptador con el que se utiliza para la comunicación AWS, el tráfico de archivos compartidos para ese destino y el AWS tráfico fluyen a través del mismo adaptador.

En algunos casos, podría configurar un adaptador para que se conecte con la consola de Storage Gateway y, a continuación, añadir un segundo adaptador. En este caso, Storage Gateway configurará automáticamente la tabla de enrutamiento para que utilice el segundo adaptador como ruta preferida. Para obtener instrucciones sobre cómo configurar varios adaptadores, consulte los temas siguientes:

Temas

- Configuración de la puerta de enlace para múltiples NICs conexiones en un VMware ESXi host
- Configuración de su puerta de enlace para varios NICs servidores en Microsoft Hyper-V

Configuración de la puerta de enlace para múltiples NICs conexiones en un VMware ESXi host

El siguiente procedimiento supone que la máquina virtual de puerta de enlace ya tiene un adaptador de red definido y describe cómo añadir un adaptador VMware ESXi.

Para configurar la puerta de enlace para que utilice un adaptador de red adicional en el VMware ESXi host

1. Apague la gateway.
2. En el cliente VMware vSphere, seleccione la máquina virtual de puerta de enlace.

   La MV puede mantenerse activada para este procedimiento.
3. En el cliente, abra el menú contextual (haga clic con el botón derecho) de la MV de la gateway y elija Edit Settings (Editar configuración).

4. En la pestaña Hardware del cuadro de diálogo Virtual Machine Properties (Propiedades de la MV), elija Add (Agregar) para agregar un dispositivo.
5. Siga el asistente para agregar hardware para agregar un adaptador de red.

   a. En el panel Device Type (Tipo de dispositivo), elija Ethernet Adapter (Adaptador de Ethernet) para agregar un adaptador y, a continuación, elija Next (Siguiente).

   b. En el panel Network Type (Tipo de red), asegúrese de que Se haya seleccionado Connect at power on (Conectar al inicio) para Type (Tipo) y, a continuación, elija Next (Siguiente).

      Se recomienda utilizar el adaptador de VMXNET3 red con Storage Gateway. Para obtener más información sobre los tipos de adaptadores que pueden aparecer en la lista de adaptadores, consulte Tipos de adaptadores de red en la ESXi documentación de vCenter Server.

   c. En el panel Ready to Complete (Listo para completar), revise la información y, a continuación, elija Finish (Finalizar).
6. Elija la pestaña Resumen de la VM y elija Ver todo junto al cuadro Dirección IP. En la ventana Direcciones IP de máquina virtual se muestran todas las direcciones IP que se pueden utilizar para obtener acceso a la puerta de enlace. Confirme que aparece una segunda dirección IP para la gateway.

   > **Note**
   >
   > Pueden pasar unos momentos hasta que los cambios del adaptador surtan efecto y el resumen de información de la MV se actualice.

7. En la consola de Storage Gateway, active la puerta de enlace.
8. En el panel Navegación de la consola de Storage Gateway, elija Puertas de enlace y elija la puerta de enlace a la que ha agregado el adaptador. Confirme que la segunda dirección IP aparece en la pestaña Details.

Para obtener información sobre las tareas de la consola local comunes a los VMware hosts de Hyper-V y KVM, consulte Realización de tareas en la consola local de la máquina virtual

Configuración de su puerta de enlace para varios NICs servidores en Microsoft Hyper-V

En el siguiente procedimiento se supone que la MV de la gateway ya tiene un adaptador de red definido y que está agregando un segundo adaptador. Este procedimiento muestra cómo añadir un adaptador para el host Microsoft Hyper-V.

Cómo configurar la puerta de enlace de modo que utilice un adaptador de red adicional en un host Microsoft Hyper-V

1. En la consola de Storage Gateway, desactive la puerta de enlace.
2. En Microsoft Hyper-V Manager, seleccione la máquina virtual de la puerta de enlace del panel Máquinas virtuales.
3. Si la máquina virtual de la puerta de enlace no está ya desactivada, haga clic con el botón derecho en el nombre de la máquina virtual para abrir el menú contextual y, a continuación, elija Desactivar.
4. Haga clic con el botón derecho en el nombre de la máquina virtual de la puerta de enlace para abrir el menú contextual y, a continuación, elija Configuración.
5. En el cuadro de diálogo Configuración, en Hardware, elija Agregar hardware.
6. En el panel Agregar hardware, en la parte derecha del cuadro de diálogo Configuración, elija Adaptador de red y, a continuación, elija Agregar para agregar un dispositivo.
7. Configure el adaptador de red y, a continuación, elija Apply para aplicar la configuración.
8. En el cuadro de diálogo Configuración, en Hardware, confirme que se ha agregado el nuevo adaptador de red a la lista de hardware y, a continuación, elija Aceptar.
9. Active la puerta de enlace mediante la consola de Storage Gateway.
10. En el panel de Navegación de la consola de Storage Gateway, elija Puertas de enlace y elija la puerta de enlace a la que ha agregado el adaptador. Confirme que una segunda dirección IP aparece en la pestaña Detalles.

Para obtener información sobre las tareas de la consola local comunes a los VMware hosts de Hyper-V y KVM, consulte Realización de tareas en la consola local de la máquina virtual

Uso de VMware vSphere High Availability con Storage Gateway

Storage Gateway proporciona alta disponibilidad VMware mediante un conjunto de comprobaciones de estado a nivel de aplicación integradas con VMware vSphere High Availability (HA). VMware Este

enfoque protege las cargas de trabajo de almacenamiento de los fallos de hardware, hipervisor o red. También protege de los errores de software, como los tiempos de espera de conexión y los recursos compartidos de archivos o la falta de disponibilidad de volumen.

Con esta integración, una puerta de enlace implementada en un VMware entorno local o en VMware Cloud On se recupera AWS automáticamente de la mayoría de las interrupciones del servicio. Esta operación se suele realizar en menos de 60 segundos sin pérdidas de datos.

> **Note**
>
> Le recomendamos que haga lo siguiente si implementa Storage Gateway en un clúster de VMware alta disponibilidad:
>
> - Implemente el paquete descargable VMware ESX .ova que contiene la máquina virtual Storage Gateway en un solo host de un clúster.
> - Cuando implemente el paquete .ova, seleccione un almacén de datos que no sea local para un host. En su lugar, utilice un almacén de datos accesible para todos los hosts del clúster. Si selecciona un almacén de datos local para un host y el host produce un error, es posible que la fuente de datos no permita el acceso a otros hosts del clúster y la conmutación por error a otro host no tenga éxito.
> - Con clústeres, si implementa el paquete .ova en el clúster, seleccione un host cuando se le solicite que lo haga. Además, puede implementar directamente en un host de un clúster.

En los siguientes temas se describe cómo implementar Storage Gateway en un clúster VMware de alta disponibilidad:

Temas

- Configure su clúster de vSphere HA VMware
- Configurar el tipo de puerta de enlace
- Implementar la gateway
- (Opcional) Agregue opciones de anulación para otras opciones VMs del clúster
- Activar la gateway
- Pruebe su configuración VMware de alta disponibilidad

Configure su clúster de vSphere HA VMware

En primer lugar, si aún no ha creado un VMware clúster, cree uno. Para obtener información sobre cómo crear un VMware clúster, consulte Crear un clúster de vSphere HA en la VMware documentación.

A continuación, configure el VMware clúster para que funcione con Storage Gateway.

Para configurar el VMware clúster

1. En la página Editar la configuración del clúster de VMware vSphere, asegúrese de que la supervisión de máquinas virtuales esté configurada para la supervisión de máquinas virtuales y aplicaciones. Para ello, defina los valores siguientes de cada opción:

   - Respuesta a un error del host: reinicie VMs
   - Respuesta al aislamiento del host: apague y reinicie VMs
   - Datastore with PDL (Almacén de datos con PDL): Disabled (Deshabilitado)
   - Datastore with APD (Almacén de datos con APD): Disabled (Deshabilitado)
   - VM Monitoring (Monitorización de MV): VM and Application Monitoring (Monitorización de aplicaciones y MV)
2. Ajuste la sensibilidad del clúster mediante la configuración de los siguientes valores:

   - Failure interval: después de este intervalo, la máquina virtual se reinicia si no se recibe un latido de la máquina virtual.
   - Minimum uptime: el clúster espera este tiempo después de que una máquina virtual comience a supervisar los latidos de las herramientas de la máquina virtual.
   - Maximum per-VM resets: el clúster reinicia la máquina virtual un máximo de estas veces dentro del intervalo de tiempo máximo de reinicios.
   - Maximum resets time window: el intervalo de tiempo en el que se cuentan los reinicios máximos por máquina virtual.

   Si no está seguro de los valores que tiene que establecer, utilice esta configuración de ejemplo:

   - Failure interval (Intervalo de error): **30** segundos
   - Minimum uptime (Tiempo de actividad mínimo): **120** segundos
   - Maximum per-VM resets (Reinicios máximos por MV): **3**

- Maximum resets time window (Periodo de tiempo de reinicio máximo): **1** hora

Si tiene otros en VMs ejecución en el clúster, puede que desee establecer estos valores específicamente para su máquina virtual. No puede hacerlo hasta que implemente la MV desde la imagen .ova. Para obtener más información acerca de la configuración de estos valores, consulte (Opcional) Agregue opciones de anulación para otras opciones VMs del clúster.

Configurar el tipo de puerta de enlace

Utilice el siguiente procedimiento para configurar la puerta de enlace

Cómo descargar la imagen .ova según el tipo de puerta de enlace

- Descargue la imagen .ova según el tipo de gateway desde:
  - Puerta de enlace de archivos: Crear y activar un Amazon FSx File Gateway

Implementar la gateway

En el clúster configurado, implemente la imagen .ova en uno de los hosts del clúster. Para obtener instrucciones, consulte Implementar una plantilla de OVF u OVA en la documentación en línea de VMware vSphere.

Cómo implementar la imagen .ova de la puerta de enlace

1. Implemente la imagen .ova en uno de los hosts del clúster.
2. Asegúrese de que los almacenes de datos que selecciona para el disco raíz y la caché están disponibles para todos los hosts del clúster.

(Opcional) Agregue opciones de anulación para otras opciones VMs del clúster

Si tiene otros en VMs ejecución en su clúster, es posible que desee establecer los valores del clúster específicamente para cada máquina virtual. Para obtener instrucciones, consulte Personalización de una máquina virtual individual en la documentación en línea de VMware vSphere.

Para añadir opciones de anulación para otras de VMs su clúster

1. En la página Resumen de VMware vSphere, elija el clúster para abrir la página del clúster y, a continuación, elija Configurar.

2. Seleccione la pestaña Configuration (Configuración) y, a continuación, seleccione VM Overrides (Anulaciones de MV).
3. Adición de una nueva opción de anulación de VM para cambiar cada valor.

   Establezca los siguientes valores para cada opción en vSphere HA: supervisión de máquina virtual:

   - Supervisión de máquina virtual: invalidación habilitada - supervisión de máquina virtual y aplicaciones
   - Confidencialidad de supervisión de máquina virtual: invalidación habilitada - supervisión de máquina virtual y aplicaciones
   - Supervisión de máquina virtual: personalizar
   - Intervalo de error: **30** segundos
   - Tiempo de actividad mínimo: **120** segundos
   - Maximum per-VM resets (Reinicios máximos por MV): **5**
   - Periodo máximo de reinicios: en **1** horas

Activar la gateway

Después de implementar el archivo.ova en su VMware entorno, active la puerta de enlace mediante la consola Storage Gateway. Para obtener instrucciones, consulte y activar su Amazon FSx File Gateway.

Pruebe su configuración VMware de alta disponibilidad

Después de activar la gateway, pruebe la configuración.

Para probar la configuración de VMware alta disponibilidad

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. En el panel de navegación, elija Gateways y, a continuación, elija la puerta de enlace en la que desee probar su alta disponibilidad VMware .
3. En Acciones, elija Verificar alta disponibilidad VMware.
4. En el cuadro Verificar la configuración de VMware alta disponibilidad que aparece, selecciona Aceptar.

> **Note**
>
> Al probar la configuración de VMware alta disponibilidad, se reinicia la máquina virtual de la puerta de enlace e interrumpe la conectividad con la puerta de enlace. La prueba puede tardar unos minutos en completarse.

Si la prueba se realiza correctamente, el estado de Verified (Verificado) aparece en la pestaña de detalles de la gateway en la consola.

5. Seleccione Salir.

Puede encontrar información sobre los eventos de VMware alta disponibilidad en los grupos de CloudWatch registros de Amazon. Para obtener más información, consulte Obtener los registros de estado de File Gateway con CloudWatch grupos de registros.

Obtención de una clave de activación para la puerta de enlace

Para recibir una clave de activación para la puerta de enlace, realice una solicitud web a la máquina virtual (VM) de la puerta de enlace. La máquina virtual devuelve un redireccionamiento que contiene la clave de activación, la cual se transfiere como uno de los parámetros de la acción de la API de `ActivateGateway` para especificar la configuración de la puerta de enlace. Para obtener más información, consulte la referencia ActivateGatewayde la API de Storage Gateway.

> **Note**
>
> Las claves de activación de la puerta de enlace caducan en 30 minutos si no se utilizan.

La solicitud que realiza a la máquina virtual de puerta de enlace incluye la AWS región en la que se produce la activación. La URL que devuelve el redireccionamiento en la respuesta contiene un parámetro de cadena de consulta llamado `activationkey`. Este parámetro de cadena de consulta es su clave de activación. El formato de la cadena de consulta tiene el aspecto siguiente: `http://`*`gateway_ip_address`*`/?activationRegion=`*`activation_region`*. El resultado de esta consulta devuelve la región y la clave de activación.

La URL también incluye `vpcEndpoint`, el ID del punto de conexión de VPC para las puertas de enlace que se conectan mediante el tipo de punto de conexión de VPC.

> **Note**
>
> El dispositivo de hardware AWS Storage Gateway, las plantillas de imágenes de máquinas virtuales y las Amazon Machine Images (AMI) de Amazon EC2 vienen preconfigurados con los servicios HTTP necesarios para recibir y responder a las solicitudes web que se describen en esta página. No es obligatorio ni recomendable instalar ningún servicio adicional en la puerta de enlace.

Temas

- Linux (curl)
- Linux (bash/zsh)
- Microsoft Windows PowerShell
- Mediante la consola local

Linux (curl)

En los siguientes ejemplos se muestra cómo obtener una clave de activación con Linux (curl).

> **Note**
>
> Sustituya las variables resaltadas por valores reales de la puerta de enlace. Los valores aceptables son los siguientes:
>
> - *`gateway_ip_address`*- La IPv4 dirección de su puerta de enlace, por ejemplo `172.31.29.201`
> - *`gateway_type`*- El tipo de puerta de enlace que desea activar`STORED`, como`CACHED`,`VTL`,`FILE_S3`, o`FILE_FSX_SMB`.
> - *`region_code`*- La región en la que quieres activar tu puerta de enlace. Consulte Puntos de conexión regionales en la Guía de referencia general de AWS . Si no se especifica este parámetro o si el valor proporcionado está mal escrito o no coincide con una región válida, el comando utilizará la región `us-east-1` de forma predeterminada.

- *vpc_endpoint*- El nombre del punto de conexión de VPC de su puerta de enlace, por ejemplo. `vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com`

Para obtener la clave de activación de un punto de conexión público:

```
curl "http://gateway_ip_address/?activationRegion=region_code&no_redirect"
```

Para obtener la clave de activación de un punto de conexión de VPC:

```
curl "http://gateway_ip_address/?
activationRegion=region_code&vpcEndpoint=vpc_endpoint&no_redirect"
```

Linux (bash/zsh)

En el siguiente ejemplo se muestra cómo utilizar Linux (bash/zsh) para recuperar la respuesta HTTP, analizar los encabezados HTTP y obtener la clave de activación.

```
function get-activation-key() {
  local ip_address=$1
  local activation_region=$2
  if [[ -z "$ip_address" || -z "$activation_region" || -z "$gateway_type" ]]; then
    echo "Usage: get-activation-key ip_address activation_region gateway_type"
    return 1
  fi

  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region&gatewayType=$gateway_type"); then
    activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
    echo "$activation_key_param" | cut -f2 -d=
  else
    return 1
  fi
}
```

Microsoft Windows PowerShell

El siguiente ejemplo muestra cómo utilizar Microsoft Windows PowerShell para obtener la respuesta HTTP, analizar los encabezados HTTP y obtener la clave de activación.

```
function Get-ActivationKey {
  [CmdletBinding()]
  Param(
    [parameter(Mandatory=$true)][string]$IpAddress,
    [parameter(Mandatory=$true)][string]$ActivationRegion,
    [parameter(Mandatory=$true)][string]$GatewayType
  )
  PROCESS {
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion&gatewayType=$GatewayType" -MaximumRedirection 0 -
ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

Mediante la consola local

En el siguiente ejemplo se muestra cómo utilizar la consola local para generar y mostrar una clave de activación.

Cómo obtener una clave de activación para la puerta de enlace desde la consola local

1. Inicie sesión en la consola local como administrador.
2. Tras iniciar sesión y ver el menú principal Activación del dispositivo de AWS - Configuración, seleccione `0` para elegir Obtener clave de activación.
3. Seleccione Storage Gateway como opción de familia de puertas de enlace.
4. Cuando se le solicite, introduzca el Región de AWS lugar en el que desea activar la puerta de enlace.
5. Introduzca 1 para punto de conexión público o 2 para punto de conexión de VPC como tipo de red.

6. Introduzca 1 para estándar o 2 estándar federal de procesamiento de información (FIPS) como tipo de punto de conexión.

Uso Direct Connect con Storage Gateway

Direct Connect vincula su red interna a la nube de Amazon Web Services. Al usarlo Direct Connect con Storage Gateway, puede crear una conexión para las necesidades de carga de trabajo de alto rendimiento, proporcionando una conexión de red dedicada entre su puerta de enlace local y. AWS

Storage Gateway utiliza puntos de conexión públicos. Con una Direct Connect conexión establecida, puede crear una interfaz virtual pública para permitir que el tráfico se enrute a los puntos finales de Storage Gateway. La interfaz virtual pública omite a los proveedores de Internet en su ruta de acceso a la red. El punto final público del servicio Storage Gateway puede estar en la misma AWS región que la Direct Connect ubicación o en una AWS región diferente.

La siguiente ilustración muestra un ejemplo de cómo Direct Connect funciona con Storage Gateway. arquitectura de red que muestra Storage Gateway conectado a la nube mediante conexión AWS directa.

En el siguiente procedimiento se supone que ha creado una gateway funcional.

Para usar Direct Connect con Storage Gateway

1. Cree y establezca una AWS Direct Connect conexión entre su centro de datos local y su terminal Storage Gateway. Para obtener más información sobre cómo crear una conexión, consulte Introducción a Direct Connect en la Guía del usuario de Direct Connect .
2. Connect el dispositivo Storage Gateway local al Direct Connect router.
3. Cree una interfaz virtual pública y configure su router local según sea necesario. Para obtener más información, consulte Creación de una interfaz virtual en la Guía del usuario de Direct Connect .

Para obtener más información Direct Connect, consulte ¿Qué es? Direct Connect en la Guía Direct Connect del usuario.

Requisitos de permisos de la cuenta de servicio de Active Directory

Si planea usar Microsoft Active Directory para proporcionar acceso autenticado por el usuario a los sistemas de archivos de archivos de su propiedad AWS Storage Gateway, debe asegurarse de tener

una cuenta de servicio de Active Directory y de que la cuenta de servicio tiene permisos delegados para unir los equipos a su dominio. Una cuenta de servicio es una cuenta de usuario de Active Directory a la que se ha delegado permiso para realizar determinadas tareas. Debe proporcionar las credenciales de nombre de usuario y contraseña de esta cuenta al unir Storage Gateway al dominio de Active Directory.

Es necesario delegar a la cuenta de servicio de Active Directory los siguientes permisos en la UO a la que se va a unir a la puerta de enlace:

- Capacidad para crear y eliminar objetos del equipo
- Capacidad de restablecer las contraseñas
- La capacidad de modificar los permisos
- Capacidad de restringir la lectura y escritura de datos en las cuentas
- Capacidad validada para leer y escribir las restricciones de la cuenta
- Capacidad validada para escribir en el nombre de entidad principal del servicio
- Capacidad validada para escribir en el nombre de host DNS

Estos representan el conjunto mínimo de permisos que se necesitan para unir objetos informáticos al Active Directory. 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.

Obtención de la dirección IP para el dispositivo de puerta de enlace

Después de elegir un host e implementar la MV de la gateway, conecte y active la gateway. Para ello, necesita la dirección IP de la MV de la gateway. Obtenga la dirección IP de la consola local de la gateway. Inicie sesión en la consola local y obtenga la dirección IP de la parte superior de la página de la consola.

Para las gateways implementadas en las instalaciones, obtenga también la dirección IP del hipervisor. Para puertas de enlace de Amazon EC2, también puede obtener la dirección IP de la instancia de Amazon EC2 desde la consola de administración de Amazon EC2. Para encontrar información cómo obtener la dirección IP de la gateway, consulte uno de los siguientes enlaces:

- VMware anfitrión: Acceder a la consola local de Gateway con VMware ESXi
- Host HyperV: Acceso a la consola local de la gateway con Microsoft Hyper-V

- Host de máquina virtual de Linux basada en el kernel (KVM): Acceso a la consola local de la gateway con Linux KVM
- Host EC2: Obtención de una dirección IP de un host Amazon EC2

Cuando encuentre la dirección IP, anótela. A continuación, vuelva a la consola de Storage Gateway y escriba la dirección IP en la consola.

Obtención de una dirección IP de un host Amazon EC2

Para obtener la dirección IP de la instancia de Amazon EC2 donde está implementada la puerta de enlace, inicie sesión en la consola local de la instancia de EC2. A continuación, obtenga la dirección IP de la parte superior de la página de la consola. Para obtener instrucciones, consulte .

También puede obtener la dirección IP desde la consola de administración de Amazon EC2. Le recomendamos que utilice la dirección IP pública para la activación. Para obtener la dirección IP pública, utilice el procedimiento 1. Si, en su lugar, decide utilizar la dirección IP elástica, consulte el procedimiento 2.

Procedimiento 1: conectarse a la gateway mediante la dirección IP pública

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instances y, a continuación, seleccione la instancia EC2 en la que está implementada la gateway.
3. Elija la pestaña Description en la parte inferior y, a continuación, anote la dirección IP pública. Utilice esta dirección IP para conectar con la gateway. Vuelva a la consola de Storage Gateway y escriba la dirección IP.

Si desea utilizar la dirección IP elástica para la activación, utilice el procedimiento siguiente.

Procedimiento 2: conectarse a la gateway mediante la dirección IP elástica

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instances y, a continuación, seleccione la instancia EC2 en la que está implementada la gateway.
3. Elija la pestaña Description en la parte inferior y, a continuación, anote el valor de Elastic IP. Utilice esta dirección IP elástica para conectar con la gateway. Vuelva a la consola de Storage Gateway y escriba la dirección IP elástica.

Descripción de los recursos y recursos de Storage Gateway IDs

En Storage Gateway, el recurso principal es una puerta de enlace, pero otros tipos de recursos son recursos compartidos de archivos. Los recursos compartidos de archivos se conocen como subrecursos y no existen a menos que estén asociados a una puerta de enlace.

Estos recursos y subrecursos tienen nombres de recursos de Amazon (ARNs) exclusivos asociados a ellos, como se muestra en esta tabla.

Tipo de recurso	Formato de ARN
ARN de gateway	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`*
ARN de recurso compartido de archivos	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:share/`*`share-id`*

¿Trabajando con Resource IDs

Cuando se crea un recurso, Storage Gateway asigna al recurso un ID de recurso único. Este ID de recurso forma parte del ARN de recurso. Un ID de recurso adopta la forma de un identificador de recurso, seguido de un guion y una combinación única de ocho letras y números. Por ejemplo, un ID de gateway presenta la forma `sgw-12A3456B` en la que `sgw` es el identificador de recurso para puestas de enlace.

Los ID de recursos de Storage Gateway aparecen en mayúsculas. No obstante, cuando utilice estos ID de recurso con la API de Amazon EC2, Amazon EC2 espera que los ID de recursos estén en minúsculas. Debe cambiar los ID de recursos a minúsculas para utilizarlos con la API de EC2. Por ejemplo, en Storage Gateway el ID para un volumen podría ser `vol-1122AABB`. Cuando utilice este ID con la API de EC2, debe cambiarlo a `vol-1122aabb`. De lo contrario, la API de EC2 podría no comportarse según lo previsto.

> **Important**
>
> IDs para los volúmenes de Storage Gateway y las instantáneas de Amazon EBS creadas a partir de los volúmenes de gateway están cambiando a un formato más largo. A partir de diciembre de 2016, todos los nuevos volúmenes e instantáneas se crearán con una cadena de 17 caracteres. A partir de abril de 2016, podrá utilizarlas durante más tiempo IDs para probar sus sistemas con el nuevo formato. Para obtener más información, consulte Longer EC2 y EBS Resource. IDs
> Por ejemplo, un ARN de volumen con el formato de ID de volumen más largo tendrá un aspecto similar al siguiente: `arn:aws:storagegateway:us-west-2:111122223333:gateway/sgw-12A3456B/volume/vol-1122AABBCCDDEEFFG`.
> Un ID de instantánea con el formato de ID más largo tendrá un aspecto similar al siguiente: `snap-78e226633445566ee`.
> Para obtener más información, consulte Anuncio: Heads-up: el volumen y la instantánea de Storage Gateway más largos estarán disponibles IDs en 2016.

Etiquetado de recursos de Storage Gateway

En Storage Gateway, puede utilizar etiquetas para administrar los recursos. Las etiquetas permiten agregar metadatos a los recursos y asignarles categorías para facilitar su administración. Cada etiqueta consta de un par clave-valor, que usted define. Puede agregar etiquetas a gateways, volúmenes y cintas virtuales. Puede buscar y filtrar estos recursos en función de las etiquetas que agregue.

Por ejemplo, puede usar etiquetas para identificar recursos de Storage Gateway utilizados por cada departamento de la organización. Podría etiquetar gateways y volúmenes utilizados por el departamento de contabilidad de este tipo: (`key=department` y `value=accounting`). A continuación, puede filtrar por esta etiqueta para identificar todas las gateways y volúmenes utilizados por el departamento de contabilidad y utilizar la información para determinar el costo. Para obtener más información, consulte Uso de etiquetas de asignación de costos y Trabajar con Tag Editor.

Si archiva una cinta virtual etiquetada, la cinta mantiene sus etiquetas en el archivo. Del mismo modo, si recupera una cinta del archivo en otra gateway, las etiquetas se mantienen en la nueva gateway.

Para la puerta de enlace de archivo, puede utilizar etiquetas para controlar el acceso a los recursos. Para obtener información acerca de cómo hacerlo, consulte Uso de etiquetas para controlar el acceso a la puerta de enlace y a los recursos.

Las etiquetas no tiene ningún significado semántico, sino que se interpretan como cadenas de caracteres.

Se aplican las siguientes restricciones a las etiquetas:

- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas.
- El número máximo de etiquetas para cada recurso es de 50.
- Las etiquetas no pueden empezar por `aws:`. Este prefijo se reserva para uso de AWS .
- Los caracteres válidos para la propiedad clave son números y letras UTF-8, el espacio y los caracteres especiales + - = . _ : / y @.

Trabajo con etiquetas

Puede trabajar con etiquetas a través de la consola de Storage Gateway, la API de Storage Gateway o la interfaz de la línea de comandos (CLI) de Storage Gateway. Los siguientes procedimientos muestran cómo agregar, editar y eliminar una etiqueta de la consola.

Cómo agregar una etiqueta

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. En el panel de navegación , elija el recurso que desea etiquetar.

   Por ejemplo, para etiquetar una gateway, elija Gateways y, a continuación, elija la gateway que desee etiquetar en la lista de gateways.
3. Elija Tags (Etiquetas) y, a continuación, elija Add/edit tags (Añadir o editar etiquetas).
4. En el cuadro de diálogo Add/edit tags (Añadir o editar etiquetas), elija Create tag (Crear etiqueta).
5. Escriba una clave para Key (Clave) y un valor para Value (Valor). Por ejemplo, puede escribir **`Department`** para la clave y **`Accounting`** para el valor.

   > **Note**
   >
   > Puede dejar en blanco el cuadro Value (Valor).

6. Elija Create Tag (Crear etiqueta) para agregar más etiquetas. Puede agregar varias etiquetas a un recurso.
7. Cuando haya acabado de agregar etiquetas, elija Save (Guardar).

Cómo editar una etiqueta

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Elija el recurso cuya etiqueta desea editar.
3. Elija Tags (Etiquetas) para abrir el cuadro de diálogo Add/edit tags (Añadir o editar etiquetas).
4. Elija el icono del lápiz que aparece junto a la etiqueta que desea editar y, a continuación, edite la etiqueta.
5. Cuando haya acabado de editar la etiqueta, elija Save (Guardar).

Cómo eliminar una etiqueta

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Elija el recurso cuya etiqueta desea eliminar.
3. Elija Tags (Etiquetas) y, a continuación, elija Add/edit tags (Añadir o editar etiquetas) para abrir el cuadro de diálogo Add/edit tags (Añadir o editar etiquetas).
4. Elija el icono X situado junto a la etiqueta que desea eliminar y, a continuación, elija Save (Guardar).

Trabajar con componentes de código abierto para AWS Storage Gateway

En esta sección, se describen las herramientas y licencias de terceros de las que dependemos para ofrecer la funcionalidad de AWS Storage Gateway .

Temas

- Componentes de código abierto para Storage Gateway
- Componentes de código abierto para Amazon FSx File Gateway

Componentes de código abierto para Storage Gateway

Se utilizan varias herramientas y licencias de terceros para ofrecer la funcionalidad para la puerta de enlace de volumen, la puerta de enlace de cinta y la puerta de enlace de archivo de Amazon S3.

Utilice los siguientes enlaces para descargar el código fuente de algunos componentes de software de código abierto que se incluyen con el AWS Storage Gateway software:

- Para los dispositivos Storage Gateway implementados en VMware ESXi: sources.tar
- Para los dispositivos de Storage Gateway implementados en Microsoft Hyper-V: sources_hyperv.tar
- Para los dispositivos de Storage Gateway implementados en la máquina virtual basada en el kernel (KVM) de Linux: sources_KVM.tar

Este producto incluye software desarrollado por el proyecto OpenSSL para su uso en el conjunto de herramientas de OpenSSL (http://www.openssl.org/). Para obtener las licencias pertinentes para todas las herramientas de terceros dependientes, consulte Licencias de terceros.

Componentes de código abierto para Amazon FSx File Gateway

Se utilizan varias herramientas y licencias de terceros para ofrecer la funcionalidad de Amazon FSx File Gateway (FSx File Gateway).

Utilice los siguientes enlaces para descargar el código fuente de algunos componentes de software de código abierto que se incluyen con el software FSx File Gateway:

- Para la versión 7 de julio de 2021 de Amazon FSx File Gateway: -open-source.tgz sgw-file-fsx-smb
- Para la versión de Amazon FSx File Gateway 06/04/2021: -20210406-open-source.tgz sgw-file-fsx-smb

Este producto incluye software desarrollado por el proyecto OpenSSL para su uso en el conjunto de herramientas de OpenSSL (http://www.openssl.org/). Para obtener las licencias pertinentes para todas las herramientas de terceros dependientes, consulte los siguientes enlaces:

- Para la versión de Amazon FSx File Gateway 7 de julio de 2021: licencia de terceros.
- Para la versión del 6 de abril de 2021 de Amazon FSx File Gateway: licencia de terceros.

Límites y cuotas de Amazon FSx File Gateway

Cuotas para los sistemas de FSx archivos de Amazon

La siguiente tabla muestra los límites y cuotas mínimos y máximos para los sistemas de FSx archivos de Amazon.

Recurso	Límite por sistema de FSx archivos de Amazon
Número máximo de etiquetas	50 etiquetas
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 solicitudes
Capacidad mínima de almacenamiento para sistemas de archivos SSD	32 GiB
Capacidad mínima de almacenamiento para sistemas de archivos HDD	2000 GiB
Capacidad máxima de almacenamiento para sistemas de archivos SSD y HDD	64 TiB
La capacidad de rendimiento mínima	8 MBps
La capacidad de rendimiento máxima	2.048 MBps
Número máximo de FSx archivos compartidos en Amazon	100 000

Tamaños de disco local recomendados para la puerta de enlace

En la siguiente tabla se recomiendan tamaños de almacenamiento AWS Storage Gateway en disco local para cada uno de los componentes de la implementación.

Tipo de gateway	Caché (mínimo)	Caché (máximo)	
FSx Puerta de enlace de archivos	150 GiB	64 TiB	

> **Note**
>
> Puede configurar una o más unidades locales para la memoria caché hasta la capacidad máxima.
> Cuando se agrega caché a una puerta de enlace de archivo de FSx existente, es importante crear nuevos discos en el host virtual (hipervisor o instancia de Amazon EC2). No cambie el tamaño de los discos si se han asignado previamente como caché.

Referencia de la API para Storage Gateway

Además de usar la consola, puede usar la AWS Storage Gateway API para configurar y administrar sus puertas de enlace mediante programación. En esta sección se describen las AWS Storage Gateway operaciones, la firma de solicitudes para la autenticación y la gestión de errores. Para obtener información acerca de las regiones y los puntos de enlace disponibles para Storage Gateway, consulte Puntos de enlace y cuotas de AWS Storage Gateway en la Referencia general de AWS.

> **Note**
>
> También puede utilizarla para AWS SDKs desarrollar aplicaciones con Storage Gateway. La AWS SDKs versión para Java, .NET y PHP incluye la API Storage Gateway subyacente, lo que simplifica las tareas de programación. Para obtener información sobre la descarga de las bibliotecas de SDK, consulte Código de muestra y bibliotecas.

Temas

- AWS Storage Gateway Encabezados de solicitud obligatorios
- Firmar solicitudes
- Respuestas de error
- Acciones de la API de Storage Gateway

AWS Storage Gateway Encabezados de solicitud obligatorios

En esta sección se describen los encabezados obligatorios que debe enviar con cada solicitud POST a AWS Storage Gateway. Puede incluir encabezados HTTP para identificar información clave sobre la solicitud, incluidas la operación que desea invocar, la fecha de la solicitud y la información que indica su autorización como remitente de la solicitud. Los encabezados no distinguen entre mayúsculas y minúsculas y el orden de los encabezados no es importante.

El siguiente ejemplo muestra los encabezados que se utilizan en la ActivateGatewayoperación.

```
POST / HTTP/1.1
```

```
Host: storagegateway.us-east-2.amazonaws.com
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120425/us-east-2/
storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target,
 Signature=9cd5a3584d1d67d57e61f120f35102d6b3649066abdd4bf4bbcf05bd9f2f8fe2
x-amz-date: 20120912T120000Z
x-amz-target: StorageGateway_20120630.ActivateGateway
```

Los siguientes son los encabezados que se deben incluir en las solicitudes POST a. AWS Storage Gateway Los encabezados que se muestran a continuación y que comienzan por «x-amz» son encabezados específicos. AWS El resto de los encabezados que se muestran son encabezados comunes utilizados en transacciones HTTP.

Encabezado	Description (Descripción)
`Authorization`	El encabezado de autorización contiene varios datos sobre la solicitud que permiten determinar si la solicitud es una acción válida AWS Storage Gateway para el solicitante. El formato de este encabezado es el siguiente (se han agregado saltos de línea para mejorar la legibilidad): `Authorization: AWS4-HMAC_SHA456 Credentials= YourAccessKey /yyymmdd/region/storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target, Signature= CalculatedSignature` En la sintaxis anterior, se especifican el año YourAccessKey, el mes y el día (aaaammdd), la región y el. CalculatedSignature El formato del encabezado de autorización viene determinado por los requisitos del proceso de firma de la versión 4. AWS Los detalles de la firma se tratan en el tema Firmar solicitudes.
`Content-Type`	`application/x-amz-json-1.1` Utilícelo como tipo de contenido para todas las solicitudes de AWS Storage Gateway. `Content-Type: application/x-amz-json-1.1`

Encabezado	Description (Descripción)
`Host`	Usa el encabezado del host para especificar el AWS Storage Gateway punto final al que envías la solicitud. Por ejemplo, `storagegateway.us-east-2.amazonaws.com` es el punto de conexión de la región Este de EE. UU. (Ohio). Para obtener más información sobre los puntos de enlace disponibles AWS Storage Gateway, consulte AWS Storage Gateway Puntos de enlace y cuotas en el. Referencia general de AWS `Host: storagegateway. region.amazonaws.com`
`x-amz-date`	Debe proporcionar la marca temporal que figura en el encabezado HTTP `Date` del encabezado AWS `x-amz-date` . (Algunas bibliotecas de cliente HTTP no permiten configurar el encabezado `Date`). Cuando hay un `x-amz-date` encabezado, AWS Storage Gateway ignora cualquier `Date` encabezado durante la autenticación de la solicitud. El `x-amz-date` formato debe ser ISO8601 Básico y tener el formato YYYMMDD'T'HHMMSS'Z'. Si se utilizan tanto el encabezado como el encabezado, el `Date` formato del `x-amz-date` encabezado de fecha no tiene por qué serlo. ISO8601 `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`
`x-amz-target`	Este encabezado especifica la versión de la API y la operación que se está solicitando. Los valores de encabezado de destino se forman concatenando la versión de la API con el nombre de la API y están en el siguiente formato. `x-amz-target: StorageGateway_ APIversion .operationName` El valor OperationName (por ejemplo, "ActivateGateway«) se encuentra en la lista de API,. Referencia de la API para Storage Gateway

Firmar solicitudes

Storage Gateway requiere que se firmen todas las solicitudes enviadas para autenticarlas. Para firmar una solicitud, se calcula una firma digital mediante una función hash criptográfica. Un hash criptográfico es una función que devuelve un valor hash único basado en la entrada. La entrada a la función hash incluye el texto de la solicitud y la clave de acceso secreta. La función hash devuelve un valor hash que se incluye en la solicitud como la firma. La firma forma parte del encabezado de la `Authorization` de la solicitud.

Tras recibir la solicitud, Storage Gateway recalcula la firma utilizando la misma función hash y los datos especificados para firmar la solicitud. Si la firma resultante coincide con la firma de la solicitud, Storage Gateway procesa la solicitud. De lo contrario, la solicitud se rechaza.

Storage Gateway admite la autenticación mediante AWS Signature Version 4. El proceso para calcular una firma se puede dividir en tres tareas:

- Tarea 1: Creación de una solicitud canónica

  Reorganice la solicitud HTTP en formato canónico. Es preciso utilizar un formato canónico, ya que Storage Gateway utiliza el mismo formato canónico cuando recalcula una firma para compararla con la que se ha enviado.

- Tarea 2: Creación de una cadena para firmar

  Crear una cadena que se utilizará como uno de los valores de entrada de la función hash criptográfica. La cadena, denominada cadena para firmar, es una concatenación del nombre del algoritmo hash, la fecha de la solicitud, una cadena de ámbito de credenciales y la solicitud en formato canónico de la tarea anterior. La cadena del ámbito de credenciales es una concatenación de fecha, región e información del servicio.

- Tarea 3: Crear una firma

  Cree una firma para su solicitud mediante una función hash criptográfica que acepte dos cadenas de entrada: la cadena para firmar y una clave derivada. La clave derivada se calcula empezando por la clave de acceso secreta y utilizando la cadena del ámbito de las credenciales para crear una serie de códigos de autenticación de mensajes basados en Hash ()HMACs.

Ejemplo de cálculo de firma

En el siguiente ejemplo se presentan los detalles de la creación de una firma para ListGateways. Puede utilizar el ejemplo como referencia para comprobar su método de cálculo de firmas.

El ejemplo supone lo siguiente:

- La marca temporal de la solicitud es "Mon, 10 Sep 2012 00:00:00" GMT.
- El punto de conexión es la región Este de EE. UU. (Ohio).

La sintaxis general de la solicitud (incluido el cuerpo JSON) es:

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
x-amz-Date: 20120910T000000Z
Authorization: SignatureToBeCalculated
Content-type: application/x-amz-json-1.1
x-amz-target: StorageGateway_20120630.ListGateways
{}
```

El formato canónico de la solicitud calculado para Tarea 1: Creación de una solicitud canónica es:

```
POST
/

content-type:application/x-amz-json-1.1
host:storagegateway.us-east-2.amazonaws.com
x-amz-date:20120910T000000Z
x-amz-target:StorageGateway_20120630.ListGateways

content-type;host;x-amz-date;x-amz-target
44136fa355b3678a1146ad16f7e8649e94fb4fc21fe77e8310c060f61caaff8a
```

La última línea de la solicitud canónica es el hash del cuerpo de la solicitud. Además, observe que la tercera línea de la solicitud canónica está vacía. Esto se debe a que no hay parámetros de consulta para esta API (ni para ningún Storage Gateway APIs).

La cadena para firmar de Tarea 2: Creación de una cadena para firmar es:

```
AWS4-HMAC-SHA256
20120910T000000Z
20120910/us-east-2/storagegateway/aws4_request
92c0effa6f9224ac752ca179a04cecbede3038b0959666a8160ab452c9e51b3e
```

La primera línea de la cadena para firmar es el algoritmo, la segunda es la marca temporal, la tercera es el ámbito de credenciales y la última es el hash de la solicitud canónica de la tarea 1.

En Tarea 3: Crear una firma, la clave derivada se pude representar como sigue:

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey,"20120910"),"us-
east-2"),"storagegateway"),"aws4_request")
```

Si se utiliza la clave de acceso secreta, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY, la firma calculada es:

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

El último paso consiste en construir el encabezado `Authorization`. Para la clave de acceso de demostración AKIAIOSFODNN7EXAMPLE, el encabezado (al que se han agregado saltos de línea para que resulte más legible) es el siguiente:

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120910/us-east-2/
storagegateway/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

Respuestas de error

Temas

- Excepciones
- Códigos de error de operación
- Respuestas de error

En esta sección se proporciona información de referencia sobre AWS Storage Gateway los errores. Estos errores se representan mediante una excepción de error y un código de

error de operación. Por ejemplo, cualquier respuesta de la API devuelve la excepción de error `InvalidSignatureException` si hay un problema con la firma de la solicitud. Sin embargo, el código de error de la operación `ActivationKeyInvalid` se devuelve solo para la ActivateGatewayAPI.

Según el tipo de error, Storage Gateway puede devolver solamente una excepción o puede devolver una excepción y un código de error de operación. Ejemplos de respuestas de error se muestran en Respuestas de error.

Excepciones

En la siguiente tabla se enumeran las excepciones AWS Storage Gateway de la API. Cuando una AWS Storage Gateway operación devuelve una respuesta de error, el cuerpo de la respuesta contiene una de estas excepciones. Las excepciones `InternalServerError` e `InvalidGatewayRequestException` devuelven uno de los códigos de mensaje Códigos de error de operación de los códigos de error de operación que proporcionan el código de error de operación específico.

Excepción	Mensaje	Código de estado HTTP
`IncompleteSignatureException`	La firma especificada está incompleta.	400: solicitud maligna
`InternalFailure`	El procesamiento de la solicitud ha fallado debido a un error o una excepción desconocidos.	500 Error de servidor interno
`InternalServerError`	Uno de los mensajes de código de error de operaciónCódigos de error de operación.	500 Error de servidor interno
`InvalidAction`	La acción u operación solicitada no es válida.	400: solicitud maligna
`InvalidClientTokenId`	El certificado X.509 o la ID de clave de AWS acceso proporcionados no existen en nuestros registros.	403: prohibido

Excepción	Mensaje	Código de estado HTTP
`InvalidGatewayRequestException`	Uno de los mensajes de código de error de operación de Códigos de error de operación.	400: solicitud maligna
`InvalidSignatureException`	La firma de solicitud que calculamos no coincide con la firma que proporcionó. Compruebe su clave de AWS acceso y su método de firma.	400: solicitud maligna
`MissingAction`	Falta un parámetro de operación o acción en la solicitud.	400: solicitud maligna
`MissingAuthenticationToken`	La solicitud debe contener un identificador de clave de AWS acceso válido (registrado) o un certificado X.509.	403: prohibido
`RequestExpired`	La solicitud es posterior a la fecha de vencimiento o la fecha de la solicitud (con un margen de 15) o la fecha de la solicitud ocurre más de 15 minutos en el futuro.	400: solicitud maligna
`SerializationException`	Se ha producido un error durante la serialización. Compruebe que la carga útil de JSON esté bien formada.	400: solicitud maligna
`ServiceUnavailable`	La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.	503 Service Unavailable
`SubscriptionRequiredException`	El identificador de clave de AWS acceso necesita una suscripción al servicio.	400: solicitud maligna
`ThrottlingException`	Tasa superada.	400: solicitud maligna

Excepción	Mensaje	Código de estado HTTP
`TooManyRequests`	Demasiadas solicitudes.	429 Demasiadas solicitudes
`UnknownOperationException`	Se ha especificado una operación desconocida. Las operaciones válidas se muestran en Acciones de la API de Storage Gateway.	400: solicitud maligna
`UnrecognizedClientException`	El token de seguridad incluido en la solicitud no es válido.	400: solicitud maligna
`ValidationException`	El valor de un parámetro de entrada es incorrecto o está fuera del intervalo .	400: solicitud maligna

Códigos de error de operación

En la siguiente tabla se muestra el mapeo entre los códigos de error de AWS Storage Gateway operación y los códigos APIs que pueden devolverse. Todos los códigos de error de operación se devuelven con una o dos excepciones generales, `InternalServerError` e `InvalidGatewayRequestException` que se describen en Excepciones.

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
`ActivationKeyExpired`	La clave de activación especificada ha vencido.	ActivateGateway
`ActivationKeyInvalid`	La clave de activación especificada no es válida.	ActivateGateway

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
`ActivationKeyNotFound`	La clave de activación especificada no se ha encontrado.	ActivateGateway
`BandwidthThrottleScheduleNotFound`	La limitación de ancho de banda especificada no se ha encontrado.	DeleteBandwidthRateLimit
`CannotExportSnapshot`	La snapshot especificada no se puede exportar.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`InitiatorNotFound`	El iniciador especificado no se ha encontrado.	DeleteChapCredentials
`DiskAlreadyAllocated`	El disco especificado ya está asignado.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
`DiskDoesNotExist`	El disco especificado no existe.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
`DiskSizeNotGigAligned`	El disco especificado no está alineado en gigabytes.	CreateStorediSCSIVolume

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
`DiskSizeGreaterThanVolumeMaxSize`	El tamaño de disco especificada es mayor que el tamaño del volumen máximo.	CreateStorediSCSIVolume
`DiskSizeLessThanVolumeSize`	El tamaño de disco especificada es menor que el tamaño del volumen.	CreateStorediSCSIVolume
`DuplicateCertificateInfo`	La información de certificado especificada es un duplicado.	ActivateGateway
FileSystemAssociationEndpointConfigurationConflict	La configuración de punto de conexión final de la asociación de sistema de archivos entra en conflicto con la configuración especificada.	AssociateFileSystem
FileSystemAssociationEndpointIpAddressAlreadyInUse	La dirección IP del punto de conexión especificada ya está en uso.	AssociateFileSystem
FileSystemAssociationEndpointIpAddressMissing	Falta la dirección IP del punto de conexión de la asociación del sistema de archivos.	AssociateFileSystem

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
FileSystemAssociationNotFound	No se ha encontrado la asociación de sistema de archivos especific ada.	UpdateFileSystemAssociation DisassociateFileSystem DescribeFileSystemAssociations
FileSystemNotFound	No se ha encontrado el sistema de archivos especificado.	AssociateFileSystem

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
`GatewayInternalError`	Se produjo un error interno de la gateway.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
`GatewayNotConnected`	La gateway especificada no está conectada.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
`GatewayNotFound`	La gateway especificada no se ha encontrado.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
		ListLocalDisks ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
`GatewayProxyNetworkConnectionBusy`	La conexión de red proxy de la gateway especificada está ocupada.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
`InternalError`	Se ha producido un error interno.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
`InvalidParameters`	La solicitud especificada contiene parámetros no válidos.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
`LocalStorageLimitExceeded`	El límite de almacenamiento local se ha superado.	AddCache AddUploadBuffer AddWorkingStorage
`LunInvalid`	El valor de LUN especificado no es válido.	CreateStorediSCSIVolume

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
`MaximumVolumeCountExceeded`	El número de volúmenes máximo se ha superado.	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes
`NetworkConfigurationChanged`	La configuración de red de la gateway ha cambiado.	CreateCachediSCSIVolume CreateStorediSCSIVolume

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
`NotSupported`	La operación especificada no es compatible.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
`OutdatedGateway`	La gateway especific ada está obsoleta.	ActivateGateway
`SnapshotInProgress Exception`	La snapshot especific ada está en curso.	DeleteVolume
`SnapshotIdInvalid`	La snapshot especific ada no es válida.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`StagingAreaFull`	El espacio provisional está lleno.	CreateCachediSCSIVolume CreateStorediSCSIVolume

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
`TargetAlreadyExists`	El destino especificado ya existe.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`TargetInvalid`	El destino especificado no es válido.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials UpdateChapCredentials
`TargetNotFound`	El destino especificado no se ha encontrado.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials DeleteVolume UpdateChapCredentials

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
`UnsupportedOperationForGatewayType`	La operación especificada no es válida para el tipo de gateway.	AddCache AddWorkingStorage CreateCachediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteSnapshotSchedule DescribeCache DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
`VolumeAlreadyExists`	El volumen especificado ya existe.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`VolumeIdInvalid`	El volumen especificado no es válido.	DeleteVolume
`VolumeInUse`	El volumen especificado ya se está usando.	DeleteVolume

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
`VolumeNotFound`	El volumen especificado no se ha encontrado.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint DeleteVolume DescribeCachediSCSIVolumes DescribeSnapshotSchedule DescribeStorediSCSIVolumes UpdateSnapshotSchedule
`VolumeNotReady`	El volumen especificado no está listo.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

Respuestas de error

Cuando se produce un error, la información de encabezado de la respuesta contiene:

- Tipo de contenido: application/ -1.1 x-amz-json
- Un código de estado HTTP `4xx` o `5xx` adecuado

El cuerpo de una respuesta de error contiene información sobre el error que se ha producido. El siguiente ejemplo de respuesta de error muestra la sintaxis de salida de los elementos de respuesta comunes a todas las respuestas de error.

```
{
    "__type": "String",
    "message": "String",
    "error":
        { "errorCode": "String",
```

```
          "errorDetails": "String"
        }
}
```

En la tabla siguiente se explican los campos de respuesta de error JSON que se muestran en la sintaxis anterior.

__type

Una de las excepciones de Excepciones.

Tipo: cadena

error

Contiene detalles del error específicos de la API. En los errores generales (es decir, no específicos de ninguna API), esta información de error no se muestra.

Tipo: recopilación

errorCode

Uno de los códigos de error de operación .

Tipo: cadena

errorDetails

Este campo no se utiliza en la versión actual de la API.

Tipo: cadena

message

Uno de los mensajes de código de error de operación.

Tipo: cadena

Ejemplos de respuestas de error

Si utilizas la DescribeStoredi SCSIVolumes API y especificas una entrada de solicitud de ARN de puerta de enlace que no existe, se devuelve el siguiente cuerpo de JSON.

```
{
```

```
  "__type": "InvalidGatewayRequestException",
  "message": "The specified volume was not found.",
  "error": {
    "errorCode": "VolumeNotFound"
  }
}
```

El siguiente cuerpo JSON se devuelve si Storage Gateway calcula una firma que no coincida con la firma enviada con una solicitud.

```
{
  "__type": "InvalidSignatureException",
  "message": "The request signature we calculated does not match the signature you
 provided."
}
```

Acciones de la API de Storage Gateway

Para ver una lista completa de las operaciones de Storage Gateway, consulte Acciones en la Referencia de la API de AWS Storage Gateway .

Historial de documentos de la Guía del usuario de Amazon FSx File Gateway

En la siguiente tabla se describen los cambios importantes en cada versión de la Guía del usuario posteriores a abril de 2018. Para recibir notificaciones sobre los cambios en esta documentación, puede suscribirse a una fuente RSS.

Cambio	Descripción	Fecha
Aviso de cambio de disponibilidad para FSx File Gateway	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.	28 de octubre de 2024
Aviso de cambio de disponibilidad para FSx File Gateway	AWS Storage Gateway de FSx File Gateway dejará de estar disponible para nuevos clientes a partir del 28 de octubre del 24 de octubre. Para utilizar el servicio, debe registrarse antes de esa fecha. 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.	26 de septiembre de 2024

Se ha agregado la opción de activar o desactivar las actualizaciones de mantenimiento	Storage Gateway recibe actualizaciones de mantenimiento periódicas que pueden incluir actualizaciones del sistema operativo y del software, correcciones para mejorar la estabilidad, el rendimiento y la seguridad, y acceso a nuevas características. Ahora puede configurar un ajuste para activar o desactivar estas actualizaciones para cada puerta de enlace individual en la implementación. Para obtener más información, consulte . AWS Storage Gateway	6 de junio de 2024
CloudWatch Alarmas recomendadas actualizadas	La CloudWatch `HealthNotifications` alarma ahora se aplica a todos los tipos de puertas de enlace y plataformas host, y se recomienda su uso. Los ajustes de configuración recomendados también se han actualizado para `HealthNotifications` y `AvailabilityNotifications` . Para obtener más información, consulte Comprensión de CloudWatch las alarmas.	2 de octubre de 2023

Se agregaron consejos para la GatewayClockOutOfSync solución	La sección Solución de problemas: problemas de File Gateway ahora incluye pautas de solución de problemas para ayudar a diagnosticar los problemas que pueden surgir si el reloj del sistema de puerta de enlace no está sincronizado con la hora del servidor AWS Storage Gateway. Para obtener más información, consulte Error: GatewayClockOutOfSync.	19 de octubre de 2022
Se han agregado consejos para la solución de problemas relacionados con la unión a un dominio de Active Directory	La sección Solución de problemas: problemas con la puerta de enlace de archivo ahora incluye pautas de solución de problemas para ayudar a diagnosticar los problemas que puedan surgir al intentar unir la puerta de enlace a un dominio de Active Directory. Para obtener más información, consulte Solución de problemas: problemas con el dominio de Active Directory.	19 de octubre de 2022

Actualización de procedimientos de creación de puerta de enlace	El procedimiento para la creación de una puerta de enlace nueva se ha actualizado para reflejar los cambios en la consola de Storage Gateway. Para obtener más información, consulte Crear y activar una puerta de enlace de archivo de Amazon S3.	12 de octubre de 2021
Compatibilidad con varios sistemas de archivos	Amazon FSx File Gateway ahora admite hasta cinco sistemas de FSx archivos de Amazon adjuntos. Para obtener más información, consulte Adjuntar un sistema de archivos de Amazon FSx for Windows File Server.	7 de julio de 2021

Soporte de cuotas FSx de almacenamiento de software de Amazon	Amazon FSx File Gateway ahora admite cuotas de almacenamiento flexible (que le avisan cuando los usuarios sobrepasan sus límites de datos) al escribir en sistemas de FSx archivos adjuntos de Amazon donde están configuradas las cuotas de almacenamiento. No se admiten las cuotas rígidas (que imponen límites de datos mediante la denegación del acceso de escritura). Las cuotas flexibles funcionan para todos los usuarios, excepto para el usuario FSx administr ador de Amazon. Para obtener más información sobre cómo configurar las cuotas de almacenamiento, consulte Cuotas de almacenamiento en la Guía del usuario de Amazon FSx para Windows File Server.	7 de julio de 2021

Nueva guía	Además del File Gateway original (ahora conocido como Amazon S3 File Gateway), Storage Gateway ofrece Amazon FSx File Gateway (FSx File Gateway). FSx File Gateway proporciona una latencia baja y un acceso eficiente a la nube FSx para compartir archivos del servidor de archivos de Windows desde sus instalaciones locales. Para obtener más información, consulte ¿Qué es Amazon FSx File Gateway?	27 de abril de 2021
Conformidad con FedRAMP	Storage Gateway ahora es compatible con FedRAMP. Para obtener más informaci ón, consulte Validación de conformidad para Storage Gateway.	24 de noviembre de 2020
Migración de una puerta de enlace de archivo	La puerta de enlace de archivo ahora proporciona un proceso documentado para reemplaza r una puerta de enlace de archivo existente por una nueva. Para obtener más información, consulte Sustituci ón de una puerta de enlace de archivo por una puerta de enlace de archivo nueva.	30 de octubre de 2020

El rendimiento de lectura de la caché fría de la puerta de enlace de archivo se ha cuadruplicado	La puerta de enlace de almacenamiento ha multiplicado por 4 el rendimiento de lectura de la caché fría. Para obtener más información, consulte Directrices de rendimiento para puertas de enlace de archivo.	31 de agosto de 2020
Pedir el dispositivo de hardware a través de la consola	Ahora puede solicitar el dispositivo de hardware a través de la consola. AWS Storage Gateway Para obtener más información, consulte Uso del dispositivo de hardware de AWS Storage Gateway.	12 de agosto de 2020
Support for Federal Information Processing Standard (FIPS) en nuevas regiones AWS	Ahora puede activar una puerta de enlace con puntos de conexión FIPS en las regiones Este de EE. UU. (Ohio), Este de EE. UU. (Norte de Virginia), Oeste de EE. UU. (Norte de California), Oeste de EE. UU. (Oregón) y Canadá (centro). Para obtener más información, consulte Puntos de conexión y cuotas de AWS Storage Gateway en la Referencia general de AWS.	31 de julio de 2020

El almacenamiento en caché local de la puerta de enlace de archivo se ha cuadruplicado	Storage Gateway ahora admite una caché local de hasta 64 TB para la puerta de enlace de archivo, lo que mejora el rendimiento de las aplicaciones en las instalaciones al proporcionar acceso de baja latencia a conjuntos de datos de trabajo más grandes. Para obtener más información, consulte Tamaños de disco local recomendados para la puerta de enlace en la Guía del usuario de Storage Gateway.	7 de julio de 2020
Vea CloudWatch las alarmas de Amazon en la consola Storage Gateway	Ahora puede ver CloudWatch las alarmas en la consola Storage Gateway. Para obtener más información, consulte Descripción de CloudWatch las alarmas.	29 mayo de 2020
Compatibilidad con los puntos de enlace del estándar federal de procesamiento de información (FIPS)	Ahora puede activar una puerta de enlace con puntos de enlace de FIPS en las regiones AWS GovCloud (US) . Para elegir un punto de conexión de FIPS para una puerta de enlace de archivo, consulte Selección de un punto de conexión de servicio.	22 de mayo de 2020

Nuevas AWS regiones	Storage Gateway ya está disponible en las regiones de África (Ciudad del Cabo) y Europa (Milán). Para obtener más información, consulte Puntos de conexión y cuotas de AWS Storage Gateway en la Referencia general de AWS.	7 de mayo de 2020
Compatibilidad con la clase de almacenamiento S3 Intelligent-Tiering	Storage Gateway ahora admite la clase de almacenamiento S3 Intelligent-Tiering. La clase de almacenamiento S3 Intelligent-Tiering optimiza los costos de almacenamiento mediante el desplazamiento automático de los datos a la capa de acceso de almacenamiento más rentable, sin que afecte al rendimiento ni se produzca sobrecarga operativa. Para obtener más información, consulte Clase de almacenamiento para optimizar automáticamente los objetos a los que se obtiene acceso de forma frecuente e infrecuente en la Guía del usuario de Amazon Simple Storage Service.	30 de abril de 2020

Nueva AWS región	Storage Gateway ya está disponible en la región AWS GovCloud (EE. UU. Este). Para obtener más información, consulte Puntos de enlace y cuotas de AWS Storage Gateway en la Referencia general de AWS.	12 de marzo de 2020
Compatibilidad con hiperviso r de máquinas virtuales de Linux basadas en el kernel (KVM)	Storage Gateway ahora permite implementar una puerta de enlace en las instalaciones en la plataform a de virtualización Microsoft Hyper-V. Las puerta de enlaces implementadas en KVM tienen la misma funcional idad y características que las puerta de enlaces en las instalaciones existentes. Para obtener más informaci ón, consulte Hipervisores compatibles y requisitos de host en la Guía del usuario de Storage Gateway.	4 de febrero de 2020

Support para VMware vSphere High Availability	Storage Gateway ahora admite la alta disponibilidad para ayudar VMware a proteger las cargas de trabajo de almacenamiento contra fallas de hardware, hipervisor o red. Para obtener más información, consulte Uso de VMware vSphere High Availability con Storage Gateway en la Guía del usuario de Storage Gateway. Esta versión también incluye mejoras de rendimiento. Para obtener más información, consulte Rendimiento en la Guía del usuario de Storage Gateway.	20 de noviembre de 2019
Support para Amazon CloudWatch Logs	Ahora puede configurar File Gateways con Amazon CloudWatch Log Groups para recibir notificaciones sobre los errores y el estado de su puerta de enlace y sus recursos. Para obtener más información, consulte Cómo recibir notificaciones sobre el estado y los errores de Gateway con Amazon CloudWatch Log Groups en la Guía del usuario de Storage Gateway.	4 de septiembre de 2019

New Región de AWS	Storage Gateway ya está disponible en la región Asia Pacífico (Hong Kong). Para obtener más información, consulte Puntos de enlace y cuotas de AWS Storage Gateway en la Referencia general de AWS.	14 de agosto de 2019
New Región de AWS	Storage Gateway ya está disponible en la región Medio Oriente (Baréin). Para obtener más información, consulte Puntos de enlace y cuotas de AWS Storage Gateway en la Referencia general de AWS.	29 de julio de 2019
Posibilidad de activar una puerta de enlace en una nube privada virtual (VPC)	Ahora puede activar una puerta de enlace en una VPC. Puede crear una conexión privada entre su dispositivo de software local y una infraestructura de almacenamiento basada en la nube. Para obtener más información, consulte Activación de una puerta de enlace en una nube virtual privada.	20 de junio de 2019

Compatibilidad de la puerta de enlace de archivo con la autorización basada en etiquetas	La puerta de enlace de archivo ahora es compatible con la autorización basada en etiquetas. Puede controlar el acceso a los recursos de la puerta de enlace de archivo basándose en las etiquetas de esos recursos. También puede controlar el acceso basándose en las etiquetas que se pueden pasar en una condición de solicitud de IAM. Para obtener más informaci ón, consulte Control de acceso a los recursos de gateway de archivos.	4 de marzo de 2019

Disponibilidad del dispositivo de hardware AWS Storage Gateway en Europa	El dispositivo de hardware AWS Storage Gateway ya está disponible en Europa. Para obtener más información, consulte Regiones de dispositivo de hardware de AWS Storage Gateway en la Referencia general de AWS. Además, ahora puede aumentar el almacenamiento utilizable en el dispositivo de hardware Storage Gateway de 5 TB a 12 TB y reemplazar la tarjeta de red de cobre instalada por una tarjeta de red de fibra óptica de 10 gigabits. AWS Para obtener más información, consulte Configuración del dispositivo de hardware.	25 de febrero de 2019
Soporte para AWS Storage Gateway Hardware Appliance	El dispositivo de hardware AWS Storage Gateway incluye el software Storage Gateway preinstalado en un servidor de terceros. Puede administrar el dispositivo desde la Consola de administración de AWS. El dispositivo puede alojar puertas de enlace de archivos, cintas y volúmenes. Para obtener más información, consulte Uso del dispositivo de hardware de Storage Gateway.	18 de septiembre de 2018

Actualizaciones anteriores

En la siguiente tabla, se describen los cambios importantes de cada versión de la Guía del usuario de AWS Storage Gateway anteriores a mayo de 2018.

Cambio	Descripción	Fecha de modificación
¿Nuevo Región de AWS	La puerta de enlace de cinta ahora está disponible en la región Asia Pacífico (Singapur). Para obtener información detallada, consulta Regiones de AWS compatibles con Storage Gateway.	3 de abril de 2018
¿Nuevo Región de AWS	Storage Gateway ya está disponible en la región Europa (París). Para obtener información detallada, consulta Regiones de AWS compatibles con Storage Gateway.	18 de diciembre de 2017
Support for VMware ESXi Hypervisor versión 6.5	AWS Storage Gateway ahora es compatible con la versión 6.5 de VMware ESXi Hypervisor. Esta se suma a las versiones 4.1, 5.0, 5.1, 5.5 y 6.0. Para obtener más información, consulte Hipervisores compatibles y requisitos de host.	13 de septiembre de 2017
Compatibilidad de la puerta de enlace de archivo con el hipervisor Microsoft Hyper-V	A partir de ahora, se puede implementar una puerta de enlace de archivo en un hipervisor Microsoft Hyper-V. Para obtener información, consulte Hipervisores compatibles y requisitos de host.	22 de junio de 2017
Nuevo Región de AWS	Storage Gateway ya está disponible en la región Asia-Pacífico (Bombay). Para obtener información detallada , consulta Regiones de AWS compatibles con Storage Gateway.	02 de mayo de 2017
Compatibilidad con las puertas de	AWS Storage Gateway ahora ofrece la posibilidad de implementar una puerta de enlace de archivos en Amazon EC2. Puede lanzar una puerta de enlace	08 de febrero de 2017

Cambio	Descripción	Fecha de modificación
enlace de archivo en Amazon EC2	de archivo en Amazon EC2 mediante la imagen de máquina de Amazon (AMI) de Storage Gateway que está disponible como AMI de la comunidad. Para obtener información sobre cómo crear una puerta de enlace de archivo e implementarla en una instancia EC2, consulte Crear y activar un Amazon FSx File Gateway. Para obtener información sobre cómo lanzar una AMI de puerta de enlace de archivo, consulte Implemente un host Amazon EC2 predeterminado para File Gateway FSx. Además, la puerta de enlace de archivo admite la configuración de proxy HTTP. Para obtener más información, consulte Direccionamiento de la puerta de enlace implementada en Amazon EC2 a través de un proxy HTTP.	
¿Nuevo Región de AWS	Storage Gateway ya está disponible en la región de Europa (Londres). Para obtener información detallada , consulta Regiones de AWS compatibles con Storage Gateway.	13 de diciembre de 2016
Nuevo Región de AWS	Storage Gateway ya está disponible en la región Canadá (centro). Para obtener información detallada, consulta Regiones de AWS compatibles con Storage Gateway.	08 de diciembre de 2016

Cambio	Descripción	Fecha de modificación
Compatibilidad con la puerta de enlace de archivos	Además de puerta de enlace de volumen y puerta de enlace de cinta, Storage Gateway ahora ofrece puerta de enlace de archivo. La puerta de enlace de archivo combina un servicio y dispositivo de software virtual, lo que le permite almacenar y recuperar objetos en Amazon S3 a través de protocolos de archivo estándar del sector como Network File System (NFS). La puerta de enlace proporciona acceso a objetos de Amazon S3 como archivos en un punto de montaje NFS.	29 de noviembre de 2016