Guía del usuario de Amazon S3 File Gateway

AWS Storage Gateway

Versión de API 2013-06-30

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

AWS Storage Gateway: Guía del usuario de Amazon S3 File Gateway

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

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

Table of Contents

¿Qué es Amazon S3 File Gateway? ... 1
Cómo funciona S3 File Gateway ... 2
Cómo empezar con AWS Storage Gateway ... 6
Inscribirse en Amazon Web Services ... 6
Creación de un usuario de IAM con privilegios de administrador ... 7
Accediendo AWS Storage Gateway ... 9
Regiones de AWS compatibles con Storage Gateway ... 9
Requisitos de configuración de File Gateway ... 11
Requisitos previos ... 11
Requisitos de hardware y almacenamiento ... 12
Requisitos de hardware para instalaciones locales VMs ... 12
Requisitos para los tipos de EC2 instancias de Amazon ... 12
Requisitos de almacenamiento ... 14
Requisitos de red y firewall ... 15
Requisitos de los puertos ... 15
Requisitos de red y firewall para el dispositivo de hardware ... 35
Permisos de acceso de gateway a través de firewalls y routers ... 38
Configuración de grupos de seguridad ... 42
Hipervisores compatibles y requisitos de host ... 42
Clientes NFS y SMB compatibles con File Gateway ... 43
Operaciones del sistema de archivos compatibles ... 44
Administración de discos locales ... 45
Cálculo de la cantidad de almacenamiento en disco local ... 45
Añadir almacenamiento en caché ... 47
Uso de almacenamiento efímero con puertas de enlace EC2 ... 48
Uso del dispositivo de hardware ... 50
Configuración del dispositivo de hardware ... 51
Instalación física del dispositivo de hardware ... 53
Acceso a la consola del dispositivo de hardware ... 55
Configuración de los parámetros de red del dispositivo de hardware ... 56
Activación del dispositivo de hardware ... 58
Creación de una puerta de enlace en el dispositivo de hardware ... 59
Configuración de una dirección IP de puerta de enlace en el dispositivo de hardware ... 60
Eliminación del software de puerta de enlace del dispositivo de hardware ... 63

Eliminación del dispositivo de hardware 64
Creación de la puerta de enlace 66
Descripción general: activación de una puerta de enlace 66
Configuración de una puerta de enlace 66
Connect to AWS 67
Revisión y activación 67
Descripción general: configuración de la puerta de enlace 67
Descripción general: recursos de almacenamiento 67
Cree una pasarela de archivos S3 68
Configuración de una pasarela de archivos Amazon S3 68
Conecte su Amazon S3 File Gateway a AWS 69
Revise la configuración y active su Amazon S3 File Gateway 71
Configure su Amazon S3 File Gateway 71
Activación de una puerta de enlace en una VPC 74
Crear un punto final de VPC para Storage Gateway 75
Creación de un recurso compartido de archivos 77
Evite costes imprevistos 78
Cifre los objetos almacenados por File Gateway 79
Crear un recurso compartido de archivos NFS 80
Cree un recurso compartido de archivos NFS con la configuración predeterminada 81
Cree un recurso compartido de archivos NFS con una configuración personalizada 87
Crear un recurso compartido de archivos SMB 95
Cree un recurso compartido de archivos SMB con la configuración predeterminada 95
Cree un recurso compartido de archivos SMB con una configuración personalizada 103
Montaje y uso del recurso compartido de archivos 114
Monte su recurso compartido de archivos NFS en su cliente 114
Monta tu recurso compartido de archivos SMB en tu cliente 116
Uso de archivos compartidos en depósitos con objetos preexistentes 120
Pruebe su S3 File Gateway 121
Administración de su Amazon S3 File Gateway 123
Edite la información básica de la pasarela 124
Otorgar acceso y permisos 125
Conceder acceso a un bucket de S3 126
Prevención de la sustitución confusa entre servicios 130
Uso de un recurso compartido de archivos para el acceso entre cuentas 131
Eliminar un archivo compartido 133

Edición de la configuración SMB de la pasarela ... 134
Establezca el nivel de seguridad de la pasarela ... 135
Configure la autenticación de Active Directory ... 137
Proporcione acceso como invitado ... 139
Configure los grupos locales ... 140
Configura la visibilidad de los archivos compartidos ... 141
Edita la configuración de uso compartido de archivos SMB ... 142
Limite el acceso a los archivos compartidos SMB ... 144
Cambie el método de cifrado del recurso compartido de archivos ... 145
Edita la configuración de uso compartido de archivos NFS ... 146
Edite los valores predeterminados de los metadatos de los archivos compartidos de NFS ... 149
Limite el acceso a los archivos compartidos de NFS ... 150
Actualización de la caché de objetos del bucket de Amazon S3 ... 151
Configure un programa de actualización automática de la memoria caché mediante la consola Storage Gateway ... 152
Configura un programa de actualización de caché automático AWS Lambda con una CloudWatch regla de Amazon ... 153
Realice una actualización manual de la memoria caché mediante la consola Storage Gateway ... 157
Realice una actualización manual de la caché mediante la API Storage Gateway ... 157
Usar Bloqueo de objetos de S3 ... 159
Estado del uso compartido de archivos ... 159
Estado de la pasarela ... 161
Administración del ancho de banda ... 161
Edite el bandwidth-rate-limit horario ... 163
Usando el AWS SDK para Java ... 164
Usando el AWS SDK para .NET ... 167
Usando el AWS Tools for Windows PowerShell ... 169
Supervisión de Storage Gateway ... 171
Comprensión de CloudWatch las alarmas ... 172
Cree CloudWatch las alarmas recomendadas ... 173
Crea una CloudWatch alarma personalizada ... 174
Supervisión de su puerta de enlace de archivos S3: ... 176
Obtener los registros de estado de de S3 File Gateway ... 177
Uso de CloudWatch las métricas de Amazon ... 179
Recibir notificaciones sobre las operaciones con archivos ... 181

Información acerca de las métricas de gateway 189
Descripción de las métricas de uso compartido de archivos 196
Descripción de los registros de auditoría de S3 FSx File Gateway 199
Cree un informe de caché 205
Administre los informes de caché 208
Comprensión de los informes de caché 210
Mantenimiento de su puerta de enlace 213
Administración de actualizaciones de puertas de enlace 213
Frecuencia de actualización y comportamiento esperado 214
Activación o desactivación de las actualizaciones de mantenimiento 215
Modificación del programa de periodos de mantenimiento de la puerta de enlace 216
Aplicación de una actualización manualmente 217
Realización de tareas de mantenimiento con la consola local 218
Acceso a la consola local de la puerta de enlace 219
Realizar tareas en la consola local de la máquina virtual 222
Realizar tareas en la consola EC2 local 239
Apagar la máquina virtual de puerta de enlace 247
Sustituir la puerta de enlace de archivos de S3 existente por una nueva instancia 247
Método 1: migrar el disco caché y el ID de puerta de enlace a la instancia de reemplazo 250
Método 2: reemplazar la instancia por un disco caché vacío y un nuevo ID de puerta de enlace 253
Eliminación de la puerta de enlace y eliminación de los recursos 255
Eliminación de la puerta de enlace mediante la consola de Storage Gateway 255
Rendimiento y optimización 258
Guía básica de rendimiento para S3 File Gateway FSx 258
Rendimiento de S3 File Gateway en clientes Linux 259
Rendimiento de File Gateway en clientes Windows 261
Guía de rendimiento para pasarelas con varios archivos compartidos 263
Maximizar el rendimiento de S3 File Gateway 265
Implemente su puerta de enlace en la misma ubicación que sus clientes 265
Reduzca los cuellos de botella causados por la lentitud de los discos 266
Ajuste la asignación de recursos de la máquina virtual para los discos de CPU, RAM y caché 266
Ajusta el nivel de seguridad de las pequeñas y medianas empresas 268
Utilice varios subprocesos y clientes para paralelizar las operaciones de escritura 269
Desactive la actualización automática de la memoria caché 271

Aumente el número de subprocesos de carga de Amazon S3 272
Aumente la configuración de tiempo de espera de SMB 273
Active el bloqueo oportunista para las aplicaciones compatibles 273
Ajuste la capacidad de la puerta de enlace en función del tamaño del conjunto de archivos de trabajo 274
Implemente varias puertas de enlace para cargas de trabajo más grandes 275
Optimización de S3 File Gateway para las copias de seguridad de bases de datos de SQL Server 276
Implemente su puerta de enlace en la misma ubicación que sus servidores SQL 276
Reduzca los cuellos de botella causados por la lentitud de los discos 277
Ajuste la asignación de recursos de la máquina virtual S3 File Gateway para los discos de CPU, RAM y caché 277
Mejore el rendimiento de los clientes SMB ajustando el nivel de seguridad de su S3 File Gateway 279
Mejore el rendimiento de los clientes SMB dividiendo las copias de seguridad de SQL en varios archivos 280
Evite errores al copiar archivos de gran tamaño aumentando la configuración de tiempo de espera de SMB 281
Aumente el número de subprocesos de carga de Amazon S3 282
Desactive la actualización automática de la memoria caché 282
Implemente varias puertas de enlace para soportar la carga de trabajo 283
Recursos adicionales para las cargas de trabajo de respaldo de bases de datos 284
Seguridad 285
Protección de los datos 285
Cifrado de datos 286
Identity and Access Management 287
Público 288
Autenticación con identidades 289
Administración de acceso mediante políticas 292
Cómo funciona AWS Storage Gateway con IAM 295
Ejemplos de políticas basadas en identidades 302
Solución de problemas 305
Uso de etiquetas para controlar el acceso a los recursos de 308
Se utiliza ACLs para el acceso a archivos compartidos en SMB 310
Validación de conformidad 315
Resiliencia 315

Seguridad de la infraestructura 316
AWS Prácticas recomendadas de seguridad 317
Registro y supervisión 317
Información sobre Storage Gateway en CloudTrail 318
Descripción de las entradas de los archivos de registro de Storage Gateway 319
Solución de problemas 322
Solución de problemas: problemas sin conexión de puerta de enlace 323
Comprobación del firewall o el proxy asociados 323
Comprobación para una inspección continua de SSL o de paquetes exhaustiva del tráfico de la puerta de enlace 323
Compruebe la métrica IOWait porcentual tras un reinicio o una actualización de software ... 324
Comprobación de si hay un corte de energía o un error de hardware en el host del hipervisor 324
Comprobación de si hay problemas con un disco de caché asociado 324
Solución de problemas: problemas con Active Directory 325
Confirme que la puerta de enlace puede llegar al controlador de dominio mediante la ejecución de una prueba de ping 325
Compruebe las opciones de DHCP configuradas para la VPC de su instancia de Amazon Gateway EC2 326
Confirme que la puerta de enlace puede resolver el dominio ejecutando una consulta de búsqueda 326
Compruebe la configuración y las funciones del controlador de dominio 328
Comprueba que la puerta de enlace esté unida al controlador de dominio más cercano 328
Confirme que Active Directory cree nuevos objetos informáticos en la unidad organizativa (OU) predeterminada 328
Comprueba los registros de eventos de tu controlador de dominio 329
Solución de problemas: problemas de activación de la puerta de enlace 329
Resolución de errores al activar la puerta de enlace mediante un punto de conexión público 330
Resolución de errores al activar la puerta de enlace mediante un punto de conexión de VPC de Amazon 333
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 337
Solución de problemas: problemas con la puerta de enlace local 338
Solución de problemas: abrir puertos NFS 343
Activa el Soporte acceso para ayudar a solucionar los problemas de tu puerta de enlace 344

Solución de problemas: problemas de configuración de Microsoft Hyper-V 345
Solución de problemas: problemas con Amazon EC2 Gateway 349
La puerta de enlace no se ha activado poco tiempo después 349
No puedes encontrar la instancia de EC2 puerta de enlace en la lista de instancias 350
Conéctate a tu Amazon EC2 Gateway mediante la consola serie 350
Activar el Soporte acceso para ayudar a solucionar los problemas de la puerta de enlace ... 350
Solución de problemas: problemas con los dispositivos de hardware 353
Cómo determinar la dirección IP del servicio 353
Cómo restablecer la configuración de fábrica 354
Cómo realizar un reinicio remoto 354
Cómo obtener soporte para iDRAC de Dell 354
Cómo encontrar el número de serie del dispositivo hardware 354
Cómo obtener soporte para el dispositivo de hardware 355
Solución de problemas: problemas con File Gateway 355
Error: 1344 (0x00000540) 356
Error: GatewayClockOutOfSync 356
Error: InaccessibleStorageClass 357
Error: InvalidObjectState 357
Error: ObjectMissing 358
Error: RoleTrustRelationshipInvalid 359
Error: S3 AccessDenied 359
Error: DroppedNotifications 360
Notificación: HardReboot 361
Notificación: reinicio 361
Solución de problemas: abrir puertos NFS 343
Solución de problemas con CloudWatch las métricas 362
Solución de problemas: problemas con el uso compartido de archivos 365
El archivo compartido está bloqueado en el estado DE CREACIÓN 366
No puedes crear un recurso compartido de archivos 367
Los archivos compartidos SMB no permiten varios métodos de acceso diferentes 367
Varios archivos compartidos no pueden escribir en el bucket de S3 mapeado 367
Notificación de un grupo de registros eliminado cuando se utilizan registros de auditoría 367
No se pueden cargar archivos en el bucket de S3 368
No puedo cambiar el cifrado predeterminado a SSE-KMS 368
Los cambios realizados directamente en un bucket de S3 con el control de versiones de objetos activado pueden afectar a lo que veas en tu recurso compartido de archivos 369

Al escribir en un bucket de S3 con el control de versiones activado, Amazon S3 File Gateway puede crear varias versiones de los objetos de Amazon S3 370
Los cambios en un bucket de S3 no se reflejan en Storage Gateway 371
Los permisos de ACL no funcionan como se esperaba 372
El rendimiento de la puerta de enlace disminuyó después de una operación recursiva 372
Notificaciones de estado de alta disponibilidad 373
Solución de problemas: problemas de alta disponibilidad 373
Notificaciones de estado 373
Métricas 375
Prácticas recomendadas 376
Recuperación de los datos 376
Recuperación de un cierre inesperado de una VM 377
Recuperación de datos a partir de un disco de la caché que no funciona correctamente 377
Recuperación de datos de un centro de datos inaccesible 377
Gestión de cargas multiparte 378
Descomprimir archivos comprimidos 378
Copiar datos de Windows Server 379
Tamaño del disco de caché 379
Varios depósitos y recursos compartidos de archivos 380
Limpie los recursos innecesarios 381
Recursos adicionales 383
Configuración del host 384
Implemente un EC2 host de Amazon predeterminado para File Gateway 384
Implemente un EC2 host Amazon personalizado para File Gateway 387
Modificar las opciones de metadatos de las EC2 instancias de Amazon 391
Sincronización de la hora de la máquina virtual con la hora del host KVM de Hyper-V o Linux 392
Sincronice la hora de la máquina virtual con la hora del host VMware 393
Configuración de adaptadores de red para la puerta de enlace 394
Uso de Storage Gateway con VMware HA 398
Obtener la clave de activación 403
Linux (curl) 404
Linux (bash/zsh) 404
Microsoft Windows PowerShell 405
Mediante la consola local 406
Compatibilidad con los atributos de los archivos 406

Usando AWS Direct Connect 407
Permisos de Active Directory 408
Obtención de la dirección IP de la puerta de enlace 409
Obtener una dirección IP de un EC2 host de Amazon 409
Comprensión de los recursos y los recursos IDs 411
Trabajando con un recurso IDs 411
Etiquetado de recursos 412
Trabajo con etiquetas 413
Componentes de código abierto 414
Componentes de código abierto para Storage Gateway 415
Componentes de código abierto para Amazon S3 File Gateway 415
Cuotas 415
Cuotas para compartir archivos 415
Tamaños de disco local recomendados para la puerta de enlace 418
Uso de clases de almacenamiento 419
Uso de clases de almacenamiento con un File Gateway 420
Uso de la clase de almacenamiento GLACIER con File Gateway 425
Uso de los controladores CSI de Kubernetes 425
Trabajar con controladores CSI para pequeñas y medianas empresas 426
Trabajando con controladores CSI de NFS 431
Módulo Terraform 435
referencia de la API 437
Encabezados de solicitud obligatorios 437
Firmar solicitudes 440
Ejemplo de cálculo de firma 441
Respuestas de error 442
Excepciones 443
Códigos de error de operación 445
Respuestas de error 466
Acciones 468
Historial de documentos 469
Actualizaciones anteriores 489
Notas de la versión 494
..... dxiii

¿Qué es Amazon S3 File Gateway?

Amazon S3 File Gateway: Amazon S3 File Gateway admite una interfaz de archivos en Amazon Simple Storage Service (Amazon S3) y combina un servicio y un dispositivo de software virtual. Con esta combinación, puede almacenar y recuperar objetos en Amazon S3 mediante protocolos de archivos estándares del sector, como Network File System (NFS) y Server Message Block (SMB). La puerta de enlace se implementa en su entorno local como una máquina virtual (VM) que se ejecuta en VMware ESXi Microsoft Hyper-V o una máquina virtual basada en el núcleo de Linux (KVM), o como un dispositivo de hardware que solicita a su distribuidor preferido. También puede implementar la máquina virtual Storage Gateway en VMware Cloud on AWS o como AMI en Amazon EC2. La gateway proporciona acceso a los objetos de S3 como archivos o puntos de montaje de recursos compartidos de archivos. Con una puerta de enlace de archivos S3, puede hacer lo siguiente:

- Puede almacenar y recuperar archivos directamente mediante NFS versión 3 o el protocolo 4.1.
- Puede almacenar y recuperar archivos directamente mediante el protocolo de sistema de archivos SMB versión 2 y 3.
- Puede acceder a sus datos directamente en Amazon S3 desde cualquier aplicación o servicio AWS en la nube.
- Puede administrar sus datos de S3 mediante políticas de ciclo de vida, replicación entre regiones y control de versiones. Puede pensar en un S3 File Gateway como un montaje de sistema de archivos en Amazon S3.

Una puerta de enlace de archivos S3 simplifica el almacenamiento de archivos en Amazon S3, se integra en las aplicaciones existentes mediante protocolos de sistemas de archivos estándares del sector y proporciona una alternativa rentable al almacenamiento local. También proporciona acceso de baja latencia a los datos a través de caché local transparente. Una puerta de enlace de archivos S3 gestiona la transferencia de datos hacia y desde AWS ella, protege las aplicaciones de la congestión de la red, optimiza y transmite los datos en paralelo y gestiona el consumo de ancho de banda.

S3 File Gateway se integra con otros AWS servicios, por ejemplo:

- Administración de acceso común mediante AWS Identity and Access Management (IAM)
- Cifrado mediante AWS Key Management Service ()AWS KMS
- Monitorización mediante Amazon CloudWatch (CloudWatch)

- Auditoría mediante AWS CloudTrail (CloudTrail)
- Operaciones con AWS Management Console y AWS Command Line Interface (AWS CLI)
- Administración de costos y facturación

En esta documentación, encontrará una sección de introducción que abarca la información de configuración común para todas las gateways y secciones de configuración específicas de gateways. La sección de introducción muestra cómo implementar, activar y configurar almacenamiento para una gateway. La sección de administración muestra cómo administrar la gateway y los recursos:

- proporciona instrucciones sobre cómo crear y usar una puerta de enlace de archivos S3. Le muestra cómo crear un recurso compartido de archivos, asignar su unidad a un bucket de Amazon S3 y cargar archivos y carpetas a Amazon S3.

- describe cómo realizar tareas de administración para todos los tipos de puertas de enlace y recursos.

En esta guía, aprenderá principalmente a trabajar con las operaciones de la gateway mediante el uso de la AWS Management Console. Si desea realizar estas operaciones mediante programación, consulte la referencia de la API de AWS Storage Gateway.

Cómo funciona Amazon S3 File Gateway

Para usar una puerta de enlace de archivos S3, comience por descargar una imagen de máquina virtual para la puerta de enlace. A continuación, active la puerta de enlace desde AWS Management Console o a través de la API Storage Gateway. También puede crear una puerta de enlace de archivos S3 con una EC2 imagen de Amazon.

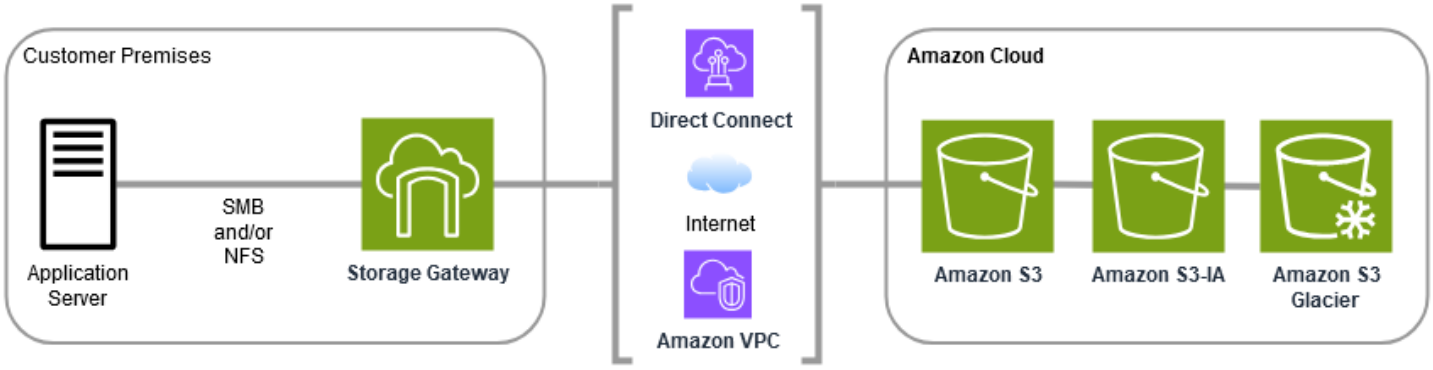
Tras activar S3 File Gateway, debe crear y configurar el recurso compartido de archivos y asociarlo a su depósito de Amazon Simple Storage Service (Amazon S3). De este modo, los clientes podrán acceder al recurso compartido mediante el protocolo Network File System (NFS) o Server Message Block (SMB). Los archivos escritos en un recurso compartido de archivos se convierten en objetos en Amazon S3, con la ruta como clave. Hay un one-to-one mapeo entre los archivos y los objetos, y la puerta de enlace actualiza de forma asíncrona los objetos de Amazon S3 a medida que usted cambia los archivos. Los objetos existentes en el bucket de Amazon S3 aparecen como archivos en el sistema de archivos y la clave pasa a ser la ruta. Los objetos se cifran con claves de cifrado del

lado del servidor (SSE-S3) de Amazon S3. Todas las transferencias de datos se realizan a través de HTTPS.

Al enviar solicitudes de carga de datos HTTPS a Amazon S3, File Gateway rellena el MD5 encabezado Content- con la MD5 suma de verificación de los datos que se están cargando. El uso de este encabezado provoca que Amazon S3 devuelva un error en caso de que no coincida la MD5 suma de comprobación calculada por Amazon S3 y el valor recibido de File Gateway. Si se devuelve un error de este tipo, File Gateway vuelve a enviar la solicitud.

El servicio optimiza la transferencia de datos entre la puerta de enlace y AWS utiliza cargas paralelas multiparte o descargas de rango de bytes, para aprovechar mejor el ancho de banda disponible. La caché local se mantiene para proporcionar un acceso de baja latencia a los datos a los que se ha accedido recientemente y reducir los gastos de salida de datos. CloudWatch las métricas proporcionan información sobre el uso de los recursos en la máquina virtual y la transferencia de datos hacia y desde AWS ella. CloudTrail rastrea todas las llamadas a la API.

Con el almacenamiento de S3 File Gateway, puede realizar tareas como transferir cargas de trabajo en la nube a Amazon S3, realizar copias de seguridad y archivar, organizar en niveles y migrar los datos de almacenamiento a la nube. AWS El siguiente diagrama proporciona una descripción general de la implementación del almacenamiento de archivos para Storage Gateway.



S3 File Gateway convierte los archivos en objetos S3 al cargar archivos en Amazon S3. La interacción entre las operaciones de archivos que se realizan con los archivos compartidos en S3 File Gateway y los objetos de S3 requiere que se consideren detenidamente determinadas operaciones al realizar conversiones entre archivos y objetos.

Las operaciones de archivo habituales modifican los metadatos de los archivos, lo que provoca la eliminación del objeto S3 actual y la creación de un nuevo objeto S3. En la siguiente tabla se muestran ejemplos de operaciones con archivos y su impacto en los objetos de S3.

Funcionamiento de archivos	Impacto en un objeto S3	Implicación de la clase de almacenamiento
Cambiar el nombre del archivo	Sustituye el objeto S3 existente y crea un nuevo objeto S3 para cada archivo	Se pueden aplicar tarifas de eliminación anticipada y de recuperación
Cambie el nombre de la carpeta	Sustituye todos los objetos S3 existentes y crea nuevos objetos S3 para cada carpeta y archivos de la estructura de carpetas	Se pueden aplicar tarifas de eliminación anticipada y de recuperación
Cambie los permisos file/folder	Sustituye el objeto S3 existente y crea un nuevo objeto S3 para cada archivo o carpeta	Se pueden aplicar tarifas de eliminación anticipada y de recuperación
Cambiar file/folder de propietario	Sustituye el objeto S3 existente y crea un nuevo objeto S3 para cada archivo o carpeta	Se pueden aplicar tarifas de eliminación anticipada y de recuperación
Añadir a un archivo	Sustituye el objeto S3 existente y crea un nuevo objeto S3 para cada archivo	Se pueden aplicar tarifas de eliminación anticipada y de recuperación

Cuando un cliente NFS o SMB escribe un archivo en S3 File Gateway, File Gateway carga los datos del archivo a Amazon S3 seguidos de sus metadatos (propietarios, marcas de tiempo, etc.). Al cargar los datos del archivo, se crea un objeto S3 y, al cargar los metadatos del archivo, se actualizan los metadatos del objeto S3. Este proceso crea otra versión del objeto, lo que da como resultado dos versiones de un objeto. Si el control de versiones de S3 está activado, se almacenarán ambas versiones.

Cuando un cliente NFS o SMB modifica un archivo en S3 File Gateway después de haberlo cargado en Amazon S3, S3 File Gateway carga los datos nuevos o modificados en lugar de cargar todo el

archivo. La modificación del archivo da como resultado la creación de una nueva versión del objeto S3.

Cuando la puerta de enlace de archivos de S3 carga archivos más grandes, es posible que tenga que cargar partes más pequeñas del archivo antes de que el cliente termine de escribir en la puerta de enlace de archivos de S3. Esto se debe, entre otras razones, a la liberación de espacio en la memoria caché o a una alta tasa de escrituras en un recurso compartido de archivos. Esto puede provocar varias versiones de un objeto en el bucket de S3.

Debe supervisar su depósito de S3 para determinar cuántas versiones de un objeto existen antes de configurar políticas de ciclo de vida para mover los objetos a diferentes clases de almacenamiento. Debe configurar la caducidad del ciclo de vida de las versiones anteriores a fin de minimizar la cantidad de versiones que tiene para un objeto en su depósito de S3. El uso de la replicación en la misma región (SRR) o la replicación entre regiones (CRR) entre depósitos de S3 aumentará el almacenamiento utilizado.

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 el. 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 suscribirte a una Cuenta de AWS

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

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

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

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

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 desees lanzar EC2 instancias de Amazon para alojar tus AWS Storage Gateway dispositivos en o Región de AWS en Europa para estar más cerca de tus usuarios europeos o para

cumplir con los requisitos legales. Tú Cuenta de AWS determinas qué regiones compatibles con un servicio específico están disponibles para que las utilices.

- 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 Storage Gateway: para ver las regiones compatibles que puede utilizar con el dispositivo de hardware, consulte las regiones del dispositivo de AWS Storage Gateway hardware en Referencia general de AWS.

Requisitos de configuración de File Gateway

A menos que se indique lo contrario, los siguientes requisitos son comunes a todos los tipos de File Gateway en AWS Storage Gateway. La configuración debe cumplir los requisitos de 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 NFS y SMB compatibles con File Gateway
- Operaciones de sistema de archivos compatibles con File Gateway
- Administrar los discos locales de su puerta de enlace

Requisitos previos

Antes de configurar Amazon S3 File Gateway (S3 File Gateway), debe cumplir los siguientes requisitos previos:

- 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 permisos de las cuentas de servicio de Active Directory Requisitos de permisos de las Directory.
- Asegúrese de que haya suficiente ancho de banda de 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 vaya 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 AWS 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 su puerta de enlace pueda resolver el nombre de su 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 requeridas para la puerta de enlace y la cantidad mínima de espacio en disco que se debe asignar al almacenamiento requerido.

Para obtener información sobre las prácticas recomendadas para el rendimiento de File Gateway, consulteGuía básica de rendimiento para S3 File Gateway FSx .

Requisitos de hardware para aplicaciones locales VMs

Al implementar la puerta de enlace de forma local, asegúrese de que el hardware subyacente en el que se implementa la máquina virtual (VM) de la puerta de enlace pueda dedicar los siguientes recursos mínimos:

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

Para obtener más información, consulte Maximizar el rendimiento de S3 File Gateway. Para obtener información acerca de cómo afecta el hardware al rendimiento de la MV de la gateway, consulte Cuotas para compartir archivos.

Requisitos para los tipos de EC2 instancias de Amazon

Al implementar la puerta de enlace en Amazon Elastic Compute Cloud (Amazon EC2), el tamaño de la instancia debe ser como mínimo **`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.

Se recomienda para los tipos de puerta de enlace de archivos

- Familia de instancias de uso general: tipo de instancia m4, m5, m6 o m7. Elija el tamaño de instancia xlarge o superior para cumplir con los requisitos de RAM y procesador Storage Gateway.
- Familia de instancias optimizadas para computación: tipos de instancias c4, c5, c6 o c7. Elija el tamaño de instancia 2xlarge o superior para cumplir con los requisitos de RAM y procesador Storage Gateway.
- Familia de instancias optimizada para memoria: tipos de instancias r3, r5, r6 o r7. Elija el tamaño de instancia xlarge o superior para cumplir con los requisitos de RAM y procesador Storage Gateway.
- Familia de instancias optimizada para el almacenamiento: tipos de instancias i3, i4 o i7. Elija el tamaño de instancia xlarge o superior para cumplir con los requisitos de RAM y procesador Storage Gateway.

> **Note**
>
> Cuando lanzas tu puerta de enlace en Amazon EC2 y el tipo de instancia que eliges admite el almacenamiento efímero, los discos se muestran automáticamente. Para obtener más información sobre el almacenamiento de EC2 instancias de Amazon, consulta Almacenamiento de instancias en la Guía del EC2 usuario de Amazon.
> Las escrituras de aplicaciones se almacenan en la memoria caché de forma sincrónica y, a continuación, se cargan de forma asíncrona en un almacenamiento duradero de Amazon S3. Si se pierde el almacenamiento efímero porque una instancia se detiene antes de que se complete la carga, se pueden perder los datos que aún se encuentran en la memoria caché y que aún no se han escrito en Amazon Simple Storage Service (Amazon S3). Antes de detener la instancia que aloja la puerta de enlace, asegúrese de que la `CachePercentDirty` CloudWatch métrica lo sea. `0` Para obtener información sobre el almacenamiento efímero, consulte Uso de almacenamiento efímero con puertas de enlace

EC2 . Para obtener información sobre las métricas de monitoreo de Storage Gateway, consulteSupervisión de su puerta de enlace de archivos S3: .
Si tiene más de 5 millones de objetos en su bucket de S3 y utiliza un volumen EBS gp2, se requiere un volumen EBS raíz mínimo de 350 GiB para que su gateway tenga un rendimiento aceptable durante la puesta en marcha. Las instancias de Amazon EC2 File Gateway recién creadas utilizan volúmenes raíz gp3 de forma predeterminada, que no tienen este requisito. Para obtener información sobre cómo aumentar el tamaño del volumen, consulte Modificación de un volumen de EBS mediante volúmenes elásticos (consola).

Requisitos de almacenamiento

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

Tipo de puerta de enlace	Caché (mínimo)	Caché (máximo)			
Gateway de archivos	150 GiB	64 TiB			

Note

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

Para obtener información acerca de las cuotas de gateway, consulte Cuotas para compartir archivos.

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, puedes implementar tu puerta de enlace en Amazon EC2 o usar otros tipos de implementación (incluida la implementación local) con políticas de seguridad de red que restrinjan los rangos de direcciones AWS IP. 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 su instancia de Amazon EC2 Gateway

Requisitos de los puertos

S3 File Gateway requiere la entrada de puertos específicos 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 clientes NFS o SMB, puntos finales de VPC o Microsoft Active Directory.

Para S3 File Gateway, solo necesita usar Microsoft Active Directory cuando desee permitir que los usuarios del dominio accedan a un recurso compartido de archivos del bloque de mensajes del servidor (SMB). Puede unir su File Gateway a cualquier dominio válido de Microsoft Windows (que se pueda resolver mediante DNS).

También puede utilizarla AWS 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 la creación de un conjunto de opciones de DHCP, consulte Crear un conjunto de opciones de DHCP en la Guía de administración.AWS Directory Service

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

Requisitos de puerto para S3 File Gateway

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
Navegadc web	El navegado web	VM de Storage Gateway	TCP HTTP	80	✓	✓	✓	La utilizan los sistemas locales para obtener la clave de activació n de Storage Gateway. El puerto 80 solo se

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
								utiliza durante la activación de un dispositivo de Storage Gateway. La máquina virtual de Storage Gateway no requiere que el puerto 80 sea accesible públicamente. El nivel de acceso exigido al puerto 80 depende de la configuración de la

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
								red. Si activa la puerta de enlace desde la consola de administración de Storage Gateway, el host desde el que se conecta a la consola debe tener acceso al puerto 80 de la puerta de enlace.

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
Navegadc web	VM de Storage Gateway	AWS	TCP HTTPS	443	✓	✓	✓	AWS Consola de administración (todas las demás operaciones)
DNS	VM de Storage Gateway	Servidor DNS (Domain Name Service)	DNS TCP Y UDP	53	✓	✓	✓	Se utiliza para la comunicación entre una máquina virtual Storage Gateway y el servidor DNS para la resolución de nombres IP.

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
NTP	VM de Storage Gateway	Servidor de Network Time Protocol (NTP)	TCP Y UDP (NTP)	123	✓	✓	✓	Lo utilizan los sistemas locales para sincronizar la hora de la máquina virtual 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 obligatorio para las pasarelas 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 finales de soporte, consulte puntos Soporte finales.
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 *Necesario solo cuando se utilizan puntos finales de VPC
VPC	VM de Storage Gateway	AWS	TCP HTTPS	1026		✓	✓*	Punto final del plano de control *Necesario solo cuando se utilizan puntos finales 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) *Necesario solo cuando se utilizan puntos finales de VPC
VPC	VM de Storage Gateway	AWS	TCP HTTPS	1028		✓	✓*	Punto final proxy *Necesario solo cuando se utilizan puntos finales 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 *Necesario solo cuando se utilizan puntos finales de VPC
VPC	VM de Storage Gateway	AWS	TCP HTTPS	2222		✓	✓*	Canal de soporte SSH para VPCe *Necesario solo para abrir un canal de soporte cuando se utilizan puntos finales 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 *Necesario solo cuando se utilizan puntos finales de VPC

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
Cliente de recurso compartido de archivos	Cliente SMB	VM de Storage Gateway	TCP o UDP SMBv3	445	✓	✓	✓*	Servicio de sesión de transferencia de datos para compartir archivos. Sustituye a los puertos 137-139 de Microsoft Windows NT y versiones posteriores. *Necesario únicamente para pequeñas y medianas empresas.

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
Microsoft Active Directory	VM de Storage Gateway	Servidor de Active Directory	UDP NetBIOS	137	✓	✓	✓*	Servicio de nombres *Necesario únicamente para. SMBv1
Microsoft Active Directory	VM de Storage Gateway	Servidor de Active Directory	UDP NetBIOS	138	✓	✓	✓*	Servicio de datagramas *Necesario únicamente para. SMBv1

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
Microsoft Active Directory	VM de Storage Gateway	Servidor de Active Directory	TCP Y UDP LDAP	389	✓	✓	✓*	Conexión de cliente del Agente del Sistema de Directorios (DSA) *Necesaria únicamente para pequeñas y medianas empresas.
Microsoft Active Directory	VM de Storage Gateway	Servidor de Active Directory	Kerberos TCP y UDP	88	✓	✓	✓*	Kerberos *Necesario únicamente para pequeñas y medianas empresas.

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
Microsoft Active Directory	VM de Storage Gateway	Servidor de Active Directory	Mapeador de Environment/Endpuntos de computación distribuida TCP (DCE/EMAP)	135	✓	✓	✓*	RPC *Necesario únicamente para pequeñas y medianas empresas.
Cliente de recurso compartido de archivos	Cliente NFS	VM de Storage Gateway	Datos TCP o UDP NFSv3	111	✓	✓	✓*	Transferencia de datos para compartir archivos (solo para NFS v3) *Necesario únicamente para NFS.

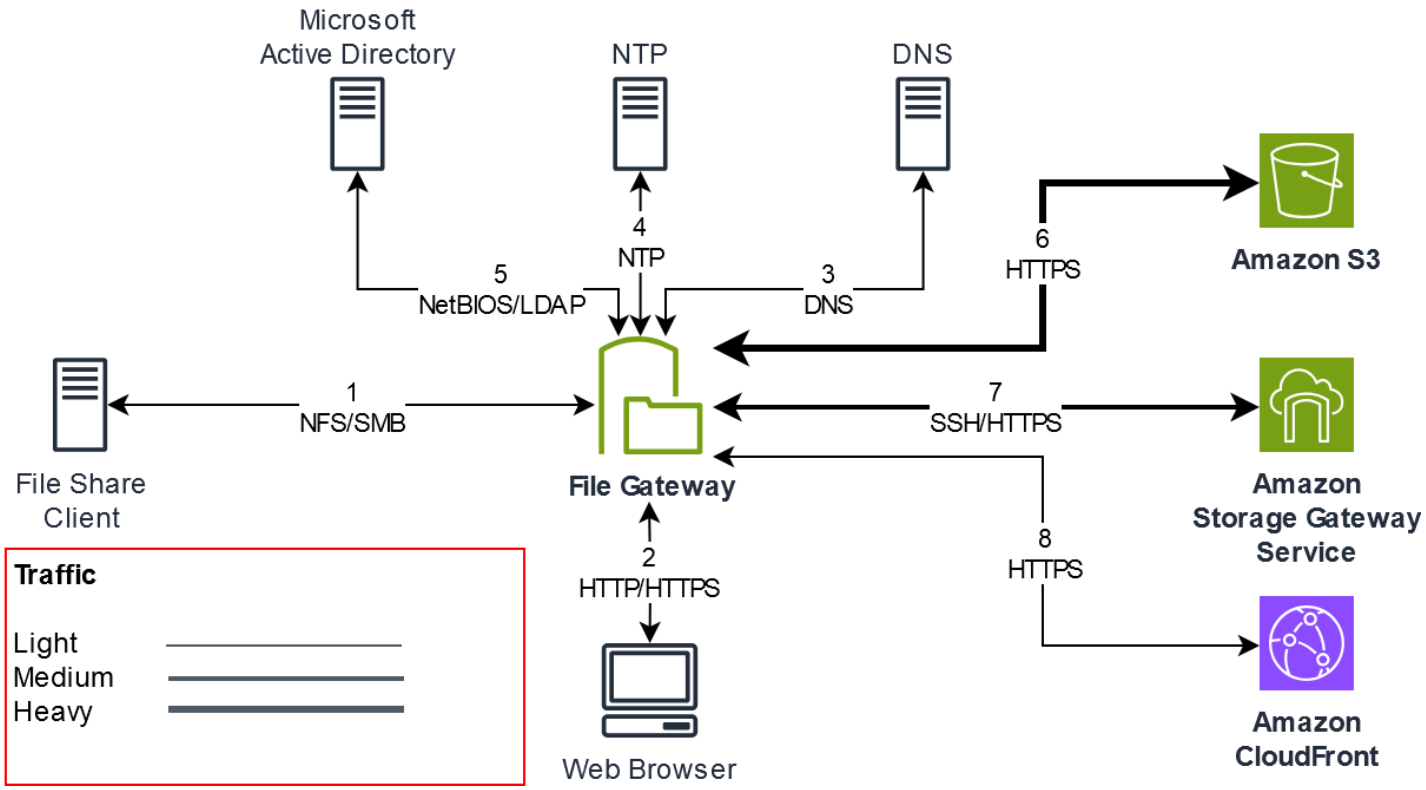
Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
Cliente de recurso compartido de archivos	Cliente NFS	VM de Storage Gateway	TCP o UDP NFS	2049	✓	✓	✓*	Transferencia de datos para compartir archivos *Necesario únicamente para NFS v3 y v4.
Cliente de recurso compartido de archivos	Cliente NFS	VM de Storage Gateway	TCP o UDP NFSv3	20048	✓	✓	✓*	Transferencia de datos para compartir archivos *Necesario únicamente para NFSv3

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
Cliente de recurso compartido de archivos	Cliente NFS	VM de Storage Gateway	TCP o UDP NFSv3	8750	✓	✓	✓*	Cuota de compartición de archivos *Necesaria únicamente para NFSv3
Cliente de recurso compartido de archivos	Cliente para pequeñas y medianas empresas	VM de Storage Gateway	TCP o UDP SMBv2	139	✓	✓	✓*	Servicio de sesión de transferencia de datos para compartir archivos *Necesario únicamente para pequeñas y medianas empresas

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
Amazon S3	VM de Storage Gateway	Puntos de enlace del servicio Amazon S3	TCP HTTPS	443	✓	✓	✓	Para la comunicación entre la máquina virtual Storage Gateway y el punto final del AWS servicio. Para obtener información sobre los puntos finales del servicio, consulte Permitir el acceso a AWS Storage Gateway a través de firewalls

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
								y enrutadores.

La siguiente ilustración muestra el flujo de tráfico de red para una implementación básica de S3 File Gateway.



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:

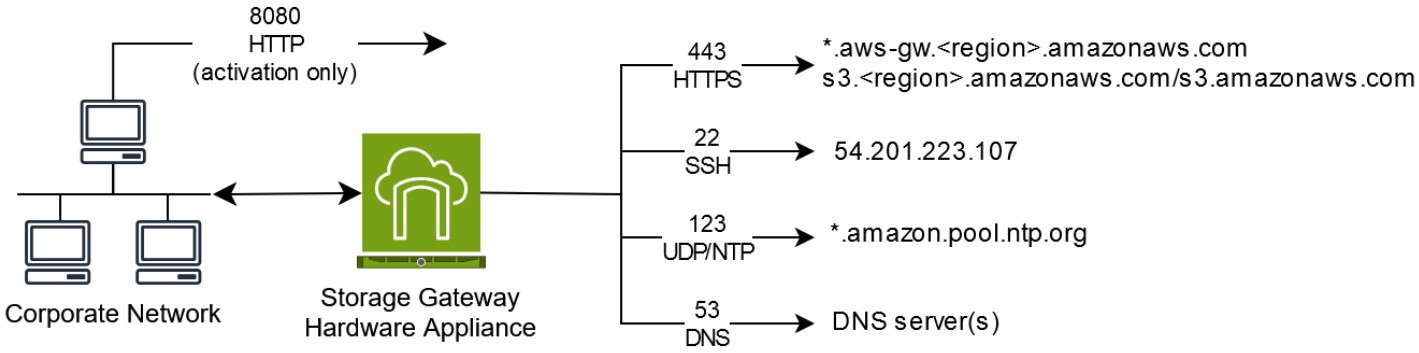
- Acceso a Internet: una conexión de red permanente a Internet a través de cualquier interfaz de red del servidor.
- Servicios DNS: servicios DNS para la comunicación entre el dispositivo de hardware y el servidor DNS.

- Sincronización horaria: se debe poder acceder a un servicio horario de Amazon NTP configurado automáticamente.
- Dirección IP: una IPv4 dirección estática o de DHCP asignada. 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	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

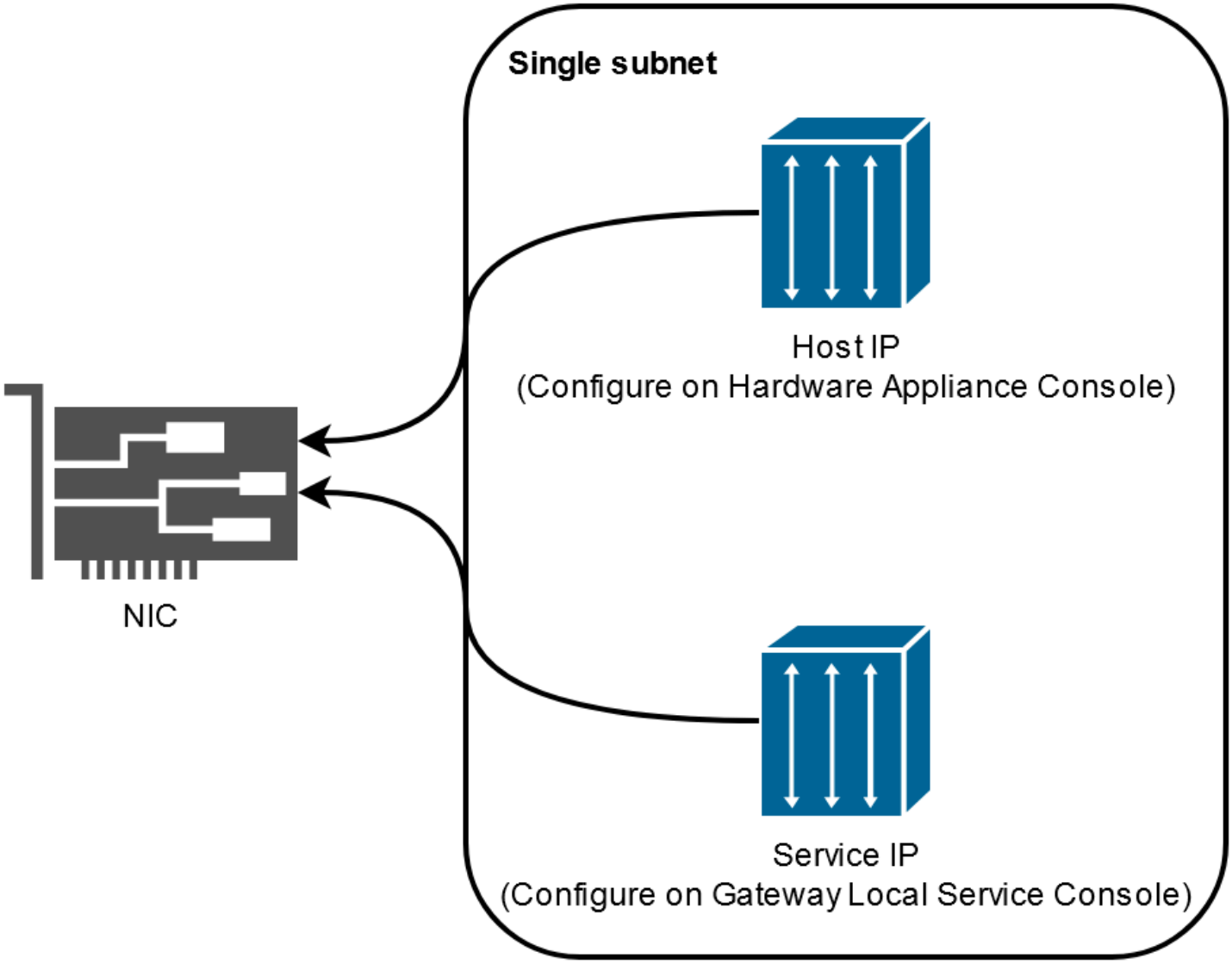
Protocolo	Puerto	Dirección	Origen	Destino	Uso
UDP/NTP	123	Salida	Dispositivo de hardware	`*.amazon.pool.ntp.org`	Sincronización horaria
HTTPS	443	Salida	Dispositivo de hardware	`*.amazonaws.com`	Transferencia de datos
HTTP	8080	Entrada	AWS	Dispositivo de hardware	Activación (solo brevemente)

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 sobre la activación y configuración de un dispositivo de hardware, consulteUso 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 para poder comunicarse con ellos. AWS 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 utilizar un asterisco (*) en lugar de *amzn-s3-demo-bucket* para crear una entrada comodín en las reglas del firewall, lo que 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`

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
```

Todas las pasarelas requieren los siguientes puntos finales de servicio para las operaciones de la ruta de control (`anon-cp`,`client-cp`,`proxy-app`) y la 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
```

Puntos de enlace del servicio Amazon S3

Amazon S3 File Gateway requiere los siguientes tres tipos de puntos de enlace para conectarse al servicio Amazon S3:

Punto final del servicio Amazon S3

> **Note**
>
> Solo para este punto final, no lo sustituya `s3-fips` por `s3` despliegues compatibles con FIPS.

```
s3.amazonaws.com
```

Puntos de enlace regionales de Amazon S3

```
s3.region.amazonaws.com
```

El siguiente ejemplo muestra un punto de enlace regional de Amazon S3 en la región EE.UU. Este (Ohio) (`us-east-2`).

```
s3.us-east-2.amazonaws.com
```

El siguiente ejemplo muestra un punto de enlace regional Amazon S3 compatible con FIPS en la región EE.UU. Oeste (Norte de California) (). `us-west-1`

```
s3-fips.us-west-1.amazonaws.com
```

Los siguientes ejemplos muestran los puntos de enlace regionales de Amazon S3 que utilizan las AWS GovCloud (US) regiones:

```
s3-fips.us-gov-west-1.amazonaws.com (AWS GovCloud (US-West) Region (FIPS))
s3-fips.us-gov-east-1.amazonaws.com (AWS GovCloud (US-East) Region (FIPS))
```

```
s3.us-gov-west-1.amazonaws.com (AWS GovCloud (US-West) Region (Standard))
s3.us-gov-east-1.amazonaws.com (AWS GovCloud (US-East) Region (Standard))
```

> **Note**
>
> Si su puerta de enlace no puede determinar Región de AWS dónde se encuentra su bucket de Amazon S3, este punto de enlace de servicio se establece de forma predeterminada. `s3.us-east-1.amazonaws.com` Le recomendamos que permita el acceso a la región EE.UU. Este (Norte de Virginia) (`us-east-1`) además de la región en la Regiones de AWS que esté activada su puerta de enlace y donde se encuentre su bucket de Amazon S3.

Puntos de enlace de bucket de Amazon S3

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

El siguiente ejemplo muestra un punto final de bucket de Amazon S3 para un bucket denominado `amzn-s3-demo-bucket` en la región EE.UU. Este (Ohio) (`us-east-2`).

```
amzn-s3-demo-bucket.s3.us-east-2.amazonaws.com
```

En el siguiente ejemplo, se muestra un punto final de bucket de Amazon S3 compatible con FIPS para un bucket denominado `amzn-s3-demo-bucket1` en la región AWS GovCloud (EE. UU. Este) (). `us-gov-east-1`

```
amzn-s3-demo-bucket1.s3-fips.us-gov-east-1.amazonaws.com
```

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:

```
0.amazon.pool.ntp.org
1.amazon.pool.ntp.org
2.amazon.pool.ntp.org
3.amazon.pool.ntp.org
```

- Para obtener una lista completa de AWS las regiones y puntos de enlace de AWS servicio compatibles que puede usar con Storage Gateway, consulte los AWS Storage Gateway puntos de enlace y las cuotas en. Referencia general de AWS

- Para obtener una lista de AWS las regiones compatibles que puede usar con el dispositivo de hardware, consulte Regiones del dispositivo de hardware Storage Gateway en Referencia general de AWS.

Configuración de grupos de seguridad para su instancia de Amazon EC2 Gateway

En AWS Storage Gateway, un grupo de seguridad controla el tráfico a tu instancia de Amazon EC2 Gateway. 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 necesitas permitir que las instancias se conecten a la puerta de enlace desde fuera de su grupo de seguridad, te recomendamos que permitas las conexiones solo en el puerto 80 (para la activación).
- Si quieres activar tu puerta de enlace desde un EC2 host de Amazon ajeno al grupo de seguridad de la puerta de enlace, permite 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 Quieres ayudar Soporte a solucionar los problemas de tu Amazon Gateway EC2 .

Para obtener más información acerca de los puertos que se deben abrir para la gateway, consulte Requisitos de los puertos.

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 EC2 instancia de Amazon.

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.
- Microsoft Hyper-V Hypervisor (2012 R2, 2016, 2019 o 2022): hay una versión gratuita independiente de Hyper-V disponible en el Centro de descarga de Microsoft. 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.
- EC2 Instancia de Amazon: Storage Gateway proporciona una imagen de máquina de Amazon (AMI) que contiene la imagen de máquina virtual de la puerta de enlace. Para obtener información sobre cómo implementar una puerta de enlace en Amazon EC2, consulteImplemente un EC2 host de Amazon predeterminado para S3 File Gateway.
- Dispositivo de hardware Storage Gateway: Storage Gateway proporciona un dispositivo de hardware físico como opción de implementación local para ubicaciones con una infraestructura de máquinas virtuales limitada.

> **Note**
>
> Storage Gateway no admite la recuperación de una puerta de enlace de una máquina virtual que se creó a partir de una instantánea o un clon de otra máquina virtual de puerta de enlace o de su Amazon EC2 AMI. 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 NFS y SMB compatibles con File Gateway

File Gateway admite los siguientes clientes:

Versión del sistema operativo	Versión del núcleo	Protocolos admitidos
Amazon Linux 2023	6.1 LTS	NFSv4.1, NFSv3
Amazon Linux 2	5,10 LITROS	NFSv4.1, NFSv3
RHEL 9	5.14	NFSv4.1, NFSv3
ARHEL 8.10	4.18	NFSv4.1, NFSv3
USO 15	6.4	NFSv4.1, NFSv3
Ubuntu 24.04 LTS	6.8 LTS	NFSv4.1, NFSv3
Ubuntu 22.04 LTS	5,15 LITROS	NFSv4.1, NFSv3
Microsoft Windows Server 2025		SMBv2, SMBv3, NFSv3
Microsoft Windows Server 2022		SMBv2, SMBv3, NFSv3
Microsoft Windows 11		SMBv2, SMBv3, NFSv3
Microsoft Windows 10		SMBv2, SMBv3, NFSv3

> **Note**
>
> El cifrado del bloque de mensajes del servidor (SMB) requiere clientes que admitan los dialectos SMB v3.

Operaciones de sistema de archivos compatibles con File Gateway

El cliente de NFS o SMB puede escribir, leer, eliminar y truncar archivos. Cuando los clientes envían escrituras a AWS Storage Gateway, estas escriben en la caché local de forma sincrónica. A continuación, escribe en Amazon S3 de forma asíncrona a través de transferencias optimizadas. Las lecturas se sirven primero a través de la caché local. Si los datos no están disponibles, se recuperan a través de S3 como caché de lectura previa.

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 objetos de Amazon S3. Los directorios se administran como objetos de carpeta en S3, con la misma sintaxis que en la consola de Amazon S3.

Las operaciones HTTP como, por ejemplo, `GET`, `PUT`, `UPDATE` y `DELETE` pueden modificar los archivos de un recurso compartido de archivos. Estas operaciones se ajustan a las funciones atómicas de creación, lectura, actualización y eliminación (CRUD).

Administrar los discos locales de su puerta de enlace

La máquina virtual (VM) de la gateway utiliza los discos locales que se le asignan on-premise para almacenamiento en búfer y permanente. Una puerta de enlace de archivos que cree en una EC2 instancia de Amazon utilizará los 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 que usted asigna para proporcionar un acceso de baja latencia a los datos a los que ha accedido recientemente. El almacenamiento en caché actúa como un almacén duradero local para los datos pendientes de carga en Amazon S3 . Las puertas de enlace de archivos requieren al menos un disco de 150 GiB para usarlo como caché. Tras la configuración y el despliegue iniciales de la puerta de enlace, puede añadir más discos para el almacenamiento en caché a medida que aumente la demanda de carga de trabajo. Esta sección contiene los siguientes temas, que describen los conceptos y procedimientos relacionados con la administración de discos locales.

Temas

- Cálculo de la cantidad de almacenamiento en disco local- Aprenda a determinar la cantidad y el tamaño de los discos de caché locales que desea asignar a su File Gateway.
- Configuración de almacenamiento en caché adicional- Aprenda a aumentar la capacidad de almacenamiento en caché de su File Gateway a medida que cambien las necesidades de su aplicación.
- Uso de almacenamiento efímero con puertas de enlace EC2 - Aprenda a evitar la pérdida de datos al utilizar un almacenamiento en disco efímero con File Gateway.

Cálculo de la cantidad de almacenamiento en disco local

Al implementar una puerta de enlace de S3, tenga en cuenta la cantidad de memoria caché que desea asignar. S3 File Gateway FSx 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 S3 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 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 agregar disco caché a la puerta de enlace (hasta las cuotas actuales de S3 File Gateway), pero no puede reducir la memoria caché de una puerta de enlace determinada. Puede realizar un análisis básico del conjunto de datos para determinar la cantidad correcta de memoria caché en disco, pero no hay forma de determinar exactamente cuántos datos están «calientes» y deben almacenarse localmente, en lugar de «fríos» y se pueden agrupar en la nube. Las cargas de trabajo cambian con el tiempo, y File Gateway de S3 proporciona flexibilidad y elasticidad en función de la cantidad de recursos que se pueden consumir. La cantidad de memoria caché siempre se puede aumentar, por lo que empezar de a poco y aumentarla según sea necesario suele ser el enfoque más rentable.

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 usarlo como almacenamiento en caché), tiene la opción de 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 el almacenamiento en caché. Un almacén de datos que esté respaldado por un solo disco físico subyacente puede provocar un rendimiento deficiente en algunas situaciones cuando se utiliza para respaldar ambos tipos de 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 cambien las necesidades de su 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**
>
> Al añadir memoria caché a una puerta de enlace existente, debe crear nuevos discos en el hipervisor del host de la puerta de enlace o en la EC2 instancia de Amazon. No elimines ni cambies el tamaño de los discos existentes que ya se hayan asignado como caché.

Para configurar un almacenamiento en caché adicional para su puerta de enlace

1. Aprovisione uno o más discos nuevos en el hipervisor del host de la puerta de enlace o en la EC2 instancia de Amazon. Para obtener información sobre cómo aprovisionar un disco en un hipervisor, consulte el manual de usuario del hipervisor. Para obtener información sobre el aprovisionamiento de volúmenes de Amazon EBS para una EC2 instancia de Amazon, consulte los 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 el almacenamiento en caché.
6. En la sección Configurar el almacenamiento en caché, identifica los discos que aprovisionaste. Si no ve los discos, seleccione el icono de actualización para actualizar la lista. Para cada disco, selecciona Caché en el menú desplegable Asignado a.

> **Note**
>
> La memoria caché es la única opción disponible para asignar discos en una puerta de enlace de archivos.

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

Uso de almacenamiento efímero con puertas de enlace EC2

En esta sección, se describen los pasos que tendrá que seguir para evitar la pérdida de datos al seleccionar un disco efímero como almacenamiento para la memoria caché de la gateway.

Los discos efímeros proporcionan almacenamiento temporal a nivel de bloque para tu instancia de Amazon. EC2 Los discos efímeros son ideales para el almacenamiento temporal de datos que cambian con frecuencia, como los datos en el almacenamiento en caché de una puerta de enlace. Cuando lanzas tu gateway con una EC2 Amazon Machine Image y el tipo de instancia que selecciones admite el almacenamiento efímero, los discos efímeros se muestran automáticamente. Puede seleccionar uno de los discos para almacenar los datos de la memoria caché de la puerta de enlace. Para obtener más información, consulta la tienda de EC2 instancias de Amazon en la Guía del EC2 usuario de Amazon.

Si la EC2 instancia de Amazon 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 Amazon S3 FSx . Puede evitar esta pérdida de datos siguiendo los pasos que se indican antes de reiniciar o detener la EC2 instancia que aloja la puerta de enlace.

> **Important**
>
> Si detiene e inicia una EC2 puerta de enlace de Amazon que utiliza almacenamiento efímero, la puerta de enlace quedará desconectada 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 instancia nueva EC2 .

Los pasos del siguiente procedimiento son específicos de las pasarelas de archivos.

Para evitar la pérdida de datos en las puertas de enlace de archivos que utilizan discos efímeros

1. Detenga todos los procesos que se escriben en Amazon S3.
2. Suscríbase para recibir notificaciones de CloudWatch Events. Para obtener información, consulte Recibir notificaciones sobre las operaciones con archivos.
3. Llame a la NotifyWhenUploaded API para recibir una notificación cuando los datos escritos, hasta que se haya perdido el almacenamiento efímero, se hayan almacenado de forma duradera en Amazon S3.
4. Espere a que la API se complete y hasta que reciba un ID de notificación.

   Recibe un CloudWatch evento con el mismo identificador de notificación.
5. Compruebe que la métrica `CachePercentDirty` del recurso compartido de archivos es 0. Esto confirma que todos sus datos se han escrito en Amazon S3. Para obtener información acerca de las métricas de recursos compartidos de archivos, consulte Descripción de las métricas de uso compartido de archivos.
6. Ahora puede reiniciar o detener el File Gateway sin correr el riesgo de perder ningún dato.

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.

Para 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 en el dispositivo de hardware se configuran de la misma manera que en VMware ESXi Microsoft Hyper-V, la máquina virtual basada en el núcleo de Linux (KVM) o Amazon. EC2

Como 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:

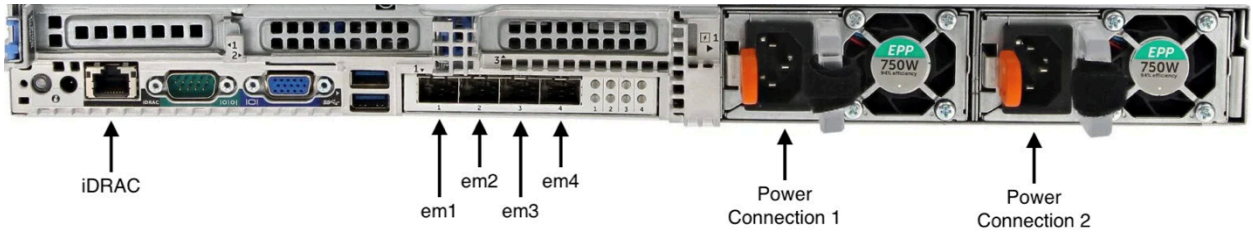
- Cables de alimentación: se necesita uno pero se recomienda tener dos.
- Cableado de red compatible (según la tarjeta de interfaz de red [NIC] que se incluya en el dispositivo de hardware). DAC de cobre Twinax, módulo óptico SFP+ (compatible con Intel) o transceptor de cobre SFP a Base-T.
- Un teclado 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 y el iDRAC.
una parte trasera del dispositivo de hardware con etiquetas de conectores de red y alimentación.

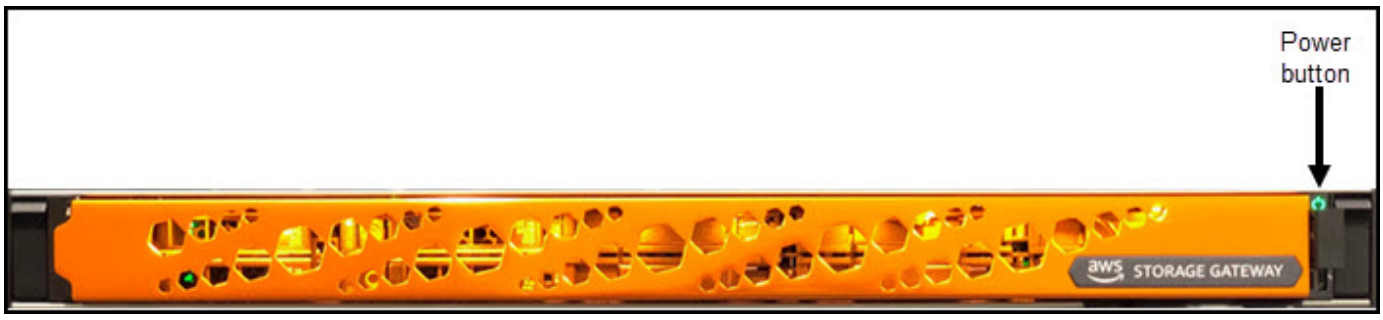


una parte trasera del dispositivo de hardware con etiquetas de conectores de red y alimentación.

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.

Para establecer 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 .

     Ingrese 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.

Para 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.

Para 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 AWS Management Console 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.

Para 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 Configuración de la contraseña de la consola local desde la consola 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.

Para salir de la consola local de la gateway

- 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 S3 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.

Eliminar una gateway 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 las instalaciones.

Para 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 EC2 instancia de Amazon en su entorno de AWS 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 y activación de una puerta de enlace de archivo de Amazon S3

En esta sección, encontrará instrucciones sobre cómo crear, implementar y activar una pasarela de archivos en AWS Storage Gateway.

Temas

- Configuración de una pasarela de archivos Amazon S3
- Conecte su Amazon S3 File Gateway a AWS
- Revise la configuración y active su Amazon S3 File Gateway
- Configure su Amazon S3 File Gateway

Configuración de una pasarela de archivos Amazon S3

Para configurar una nueva puerta de enlace de archivos S3

1. Abra AWS Management Console at https://console.aws.amazon.com/storagegateway/home/ y elija el Región de AWS lugar donde desea crear su 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. Una vez creada la puerta de enlace, puede buscar este nombre para encontrarla en las páginas de la lista de la AWS Storage Gateway consola.

    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 S3 File Gateway.
5. En la sección Opciones de plataforma, haga lo siguiente:

    a. En Plataforma host, elija la plataforma en la que desee implementar la puerta de enlace. A continuación, siga las instrucciones específicas de la plataforma que aparecen 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.
- KVM de Linux: descargue, implemente y configure la máquina virtual de puerta de enlace mediante una máquina virtual basada en el núcleo de Linux (KVM).
- Amazon EC2: configura y lanza una EC2 instancia de Amazon para alojar tu puerta de enlace.
- Dispositivo de hardware: solicite un dispositivo de hardware físico dedicado AWS para alojar su puerta de enlace.

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

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

Conecte su Amazon S3 File Gateway a AWS

Para conectar un nuevo S3 File Gateway a AWS

1. Si aún no lo ha hecho, complete el procedimiento descrito en Configurar una pasarela de archivos Amazon S3. Cuando haya terminado, seleccione Siguiente para abrir la AWS página Conectar a en la AWS Storage Gateway consola.
2. 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 su 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.

     Puedes obtener la dirección IP de la puerta de enlace iniciando sesión en la consola local de la puerta de enlace desde tu cliente hipervisor o copiándola desde la página de detalles de tu EC2 instancia de Amazon. Para obtener más información, consulteObtención de la dirección IP de la puerta de enlace».

- Clave de activación: proporcione la clave de activación de su 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 su puerta de enlace no está disponible, elija esta opción.

3. 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 final con FIPS habilitado para especificar si la conexión debe cumplir con 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 punto final compatible con FIPS. Para obtener más información, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.
     > El punto final del servicio FIPS solo está disponible en algunas regiones. 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 enlace de VPC existente eligiendo su ID de punto de enlace de VPC en la lista desplegable. También puede proporcionar el nombre o la dirección IP del sistema de nombres de dominio (DNS) del punto final de la VPC.

     > **Note**
     >
     > Para especificar un punto de enlace de VPC que pertenezca a Cuenta de AWS otro que no sea el que está utilizando actualmente para crear la puerta de enlace, debe proporcionar su nombre DNS o su dirección IP.

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

Revise la configuración y active su Amazon S3 File Gateway

Para revisar la configuración y activar un nuevo S3 File Gateway

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

   - Configuración de una pasarela de archivos Amazon S3
   - Conecte su Amazon S3 File Gateway a AWS

   Cuando haya terminado, seleccione Siguiente para abrir la página de revisión y activación en la AWS Storage Gateway consola.
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 S3 File Gateway

Para realizar la configuración por primera vez en una nueva puerta de enlace de archivos S3

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

   - Configuración de una pasarela de archivos Amazon S3
   - Conecte su Amazon S3 File Gateway a AWS
   - Revise la configuración y active su Amazon S3 File Gateway

   Cuando haya terminado, seleccione Siguiente para abrir la página de configuración de la puerta de enlace en la AWS Storage Gateway consola.

2. En la sección Configurar almacenamiento, usa 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 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

   - Cree una alarma personalizada: configure una nueva CloudWatch alarma para que le notifique 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 reciba CloudWatch notificaciones sobre las métricas de su pasarela.

5. (Opcional) En la sección Etiquetas, selecciona Añadir nueva etiqueta y, a continuación, introduce un par clave-valor que distinga entre mayúsculas y minúsculas para ayudarte a buscar y filtrar tu puerta de enlace en las páginas de listas de la consola. 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 probar la configuración de alta disponibilidad de su puerta de enlace en cualquier momento. La verificación tarda unos minutos y reinicia la máquina virtual (VM) Storage Gateway.

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

   Para comprobar el estado de la nueva puerta de enlace, búsquelo en la página de información general de la puerta de enlace de la AWS Storage Gateway consola.

Ahora que ha creado su puerta de enlace, debe crear un recurso compartido de archivos para que pueda utilizarlo. Para obtener instrucciones, consulte Crear un recurso compartido de archivos.

Activar 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 enlace de VPC para Storage Gateway, cree un punto de enlace de VPC para Storage Gateway y obtenga el ID del y activar la puerta de enlace. Para obtener más información, consulte Connect your Amazon S3 File Gateway to AWS a.

Para configurar su puerta de enlace de archivos de S3 para transferir datos a través de la VPC, debe crear un punto de enlace de VPC independiente para Amazon S3 y, a continuación, especificar este punto de enlace de VPC al crear recursos compartidos de archivos para la puerta de enlace.

> **Note**
>
> Debe activar la puerta de enlace en la misma región en la que creó el punto de enlace de VPC para Storage Gateway, y el almacenamiento de Amazon S3 que configure para el uso compartido de archivos debe estar en la misma región en la que creó el punto de enlace de VPC para Amazon S3.

Crear un punto final de VPC para Storage Gateway

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

Para crear un punto de conexión de VPC para Storage Gateway

1. Inicie sesión en la consola de Amazon VPC AWS Management Console 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 Service Name (Nombre de servicio), seleccione `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 Enable Private DNS Name (Habilitar nombre de DNS privado) 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. Elija 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. Su nombre de DNS debe tener un aspecto similar al del siguiente ejemplo: `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

Ahora que tiene un punto final de VPC, puede crear y activar su puerta de enlace. Para obtener más información, consulte Crear y activar un Amazon S3 File Gateway .

Para obtener información sobre cómo obtener una clave de activación, consulte Obtener una clave de activación para su puerta de enlace .

> **Important**
>
> Para configurar su puerta de enlace de archivos de S3 para transferir datos a través de la VPC, debe crear un punto de enlace de VPC independiente para Amazon S3 y, a continuación, especificar este punto de enlace de VPC al crear recursos compartidos de archivos para la puerta de enlace.
> Para ello, siga los mismos pasos que se muestran arriba, pero elija `com.amazonaws.region.s3` el nombre del servicio y, a continuación, seleccione la tabla de rutas a la que desee asociar el punto de enlace de S3 en lugar del grupo. subnet/security Para obtener instrucciones, consulte Crear un punto final de puerta de enlace.

Creación de un recurso compartido de archivos

En esta sección, encontrará instrucciones sobre cómo crear un recurso compartido de archivos al que se pueda acceder mediante el protocolo del Sistema de archivos de red (NFS) o el protocolo del bloque de mensajes del servidor (SMB).

Al crear un recurso compartido NFS, cualquier persona que tenga acceso al servidor NFS podrá acceder al recurso compartido de archivos NFS de forma predeterminada. Puede limitar el acceso a los clientes por dirección IP.

Al crear un recurso compartido de archivos SMB, puede utilizar uno de los tres modos de autenticación:

- Un recurso compartido de archivos con acceso mediante Microsoft Active Directory (AD). Cualquier usuario autenticado de Microsoft AD obtiene acceso a este tipo de recurso compartido de archivos.
- Un recurso compartido de archivos SMB con acceso limitado. Solo se permite el acceso a determinados usuarios y grupos del dominio que especifique (a través de una lista de permitidos). También se puede denegar el acceso a los usuarios y grupos (mediante una lista de denegación).
- Un recurso compartido de archivos SMB con acceso de invitado. Cualquier usuario que pueda proporcionar la contraseña de invitado tiene acceso a este recurso compartido de archivos.

> **Note**
>
> Los recursos compartidos de archivos que se exportan a través de la puerta de enlace para recursos compartidos de archivos NFS admiten permisos POSIX. En el caso de los archivos compartidos SMB, puede utilizar las listas de control de acceso (ACLs) para gestionar los permisos de los archivos y carpetas de su recurso compartido de archivos. Para obtener más información, consulte Uso de Windows ACLs para limitar el acceso a los archivos compartidos en pequeñas y medianas empresas.

Una pasarela de archivos puede alojar uno o más recursos compartidos de archivos de distintos tipos. Puede tener varios recursos compartidos de archivos NFS y SMB en una puerta de enlace de archivos.

> **Important**
>
> Para crear un recurso compartido de archivos, una pasarela de archivos requiere que active AWS Security Token Service ()AWS STS. Si AWS STS no está activado en el Región de AWS lugar donde creó su puerta de enlace de archivos, actívela. Para obtener información sobre cómo activarlo AWS STS, consulte Activación y desactivación AWS Security Token Service en una AWS región en la Guía del AWS Identity and Access Management usuario.

Temas

- Evitar costes imprevistos al cargar los datos de la pasarela
- Cifre los objetos almacenados por File Gateway en Amazon S3
- Crear un recurso compartido de archivos NFS
- Crear un recurso compartido de archivos SMB

Evitar costes imprevistos al cargar los datos de la pasarela

Cuando un cliente NFS escribe un archivo en File Gateway, File Gateway carga los datos del archivo en Amazon S3 seguidos de sus metadatos. Al cargar los datos del archivo, se crea un objeto S3 y, al cargar los metadatos del archivo, se actualizan los metadatos del objeto S3. Este proceso crea una versión adicional del objeto. Si el control de versiones de S3 está activado, se almacenan ambas versiones.

Si cambias los metadatos de un archivo que está almacenado en tu File Gateway, se crea un nuevo objeto de S3 que reemplaza al objeto de S3 existente. Este comportamiento es diferente al de editar un archivo en un sistema de archivos, donde la edición de un archivo no implica la creación de un archivo nuevo. Pruebe todas las operaciones de archivos que planea usar con AWS Storage Gateway para comprender cómo interactúa cada operación de archivo con el almacenamiento de Amazon S3.

Considere detenidamente el uso del control de versiones de S3 y la replicación entre regiones (CRR) en Amazon S3 cuando cargue datos desde su File Gateway. Al cargar archivos desde File Gateway a Amazon S3 cuando el control de versiones de S3 está activado, se obtienen al menos dos versiones de un objeto de S3.

Determinados flujos de trabajo que implican archivos de gran tamaño y patrones de escritura de archivos, como la carga de archivos que se realiza en varios pasos, pueden aumentar el número

de versiones de objetos de S3 almacenadas. Si la caché de File Gateway necesita liberar espacio debido a las altas velocidades de escritura de archivos, es posible que se creen varias versiones de objetos de S3. Estos escenarios aumentan el almacenamiento en S3 si el control de versiones en S3 está activado y aumentan los costes de transferencia asociados a la CRR. Pruebe todas las operaciones de archivos que planea usar con Storage Gateway para comprender cómo interactúa cada operación de archivo con el almacenamiento de Amazon S3.

El uso de la utilidad Rsync con su File Gateway da como resultado la creación de archivos temporales en la memoria caché y la creación de objetos S3 temporales en Amazon S3. Esta situación se traduce en gastos de eliminación anticipada en la clase de almacenamiento S3 Standard-Infrequent Access (S3 Standard-IA).

Cifre los objetos almacenados por File Gateway en Amazon S3

S3 File Gateway admite los siguientes métodos de cifrado del lado del servidor para los datos que almacena en Amazon S3:

- SSE-S3: de forma predeterminada, todos los objetos nuevos cargados en los buckets de Amazon S3 utilizan el cifrado del lado del servidor con claves administradas de Amazon S3. Para obtener más información, consulte Uso del cifrado del lado del servidor con claves administradas de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.
- SSE-KMS: puede configurar su recurso compartido de archivos para que utilice el cifrado del lado del servidor con claves administradas (). AWS Key Management Service AWS KMS AWS KMS es un servicio que combina hardware y software seguros y de alta disponibilidad para proporcionar un sistema de administración de claves adaptado a la nube. Para obtener más información, consulte ¿Qué es el servicio de administración de AWS claves? en la Guía para AWS Key Management Service desarrolladores.
- DSSE-KMS: el cifrado de doble capa del lado del servidor con AWS KMS claves aplica dos capas de cifrado a los objetos cuando se cargan en Amazon S3. Esto ayuda a cumplir con los estándares de conformidad para el cifrado multicapa. Para obtener más información, consulte Uso del cifrado de doble capa del lado del servidor con AWS KMS claves en la Guía del usuario de Amazon Simple Storage Service.

> **Note**
>
> El uso del DSSE-KMS y las claves conlleva cargos adicionales. AWS KMS Para más información, consulte Precios de AWS KMS.

Puede especificar un método de cifrado al crear un nuevo recurso compartido de archivos mediante la consola Storage Gateway o la API Storage Gateway. Para conocer los procedimientos de la consola, consulte Cree un recurso compartido de archivos NFS con una configuración personalizada oCree un recurso compartido de archivos SMB con una configuración personalizada. Para obtener información sobre los comandos de API correspondientes, consulte Create NFSFile Share o Create SMBFile Share en la referencia de la API AWS de Storage Gateway.

También puede actualizar la configuración de cifrado de un recurso compartido de archivos existente mediante la consola Storage Gateway o la API Storage Gateway. Para ver el procedimiento de la consola, consulteCambia el método de cifrado del lado del servidor para un recurso compartido de archivos existente. Para obtener información sobre los comandos de API correspondientes, consulte Update NFSFile Share o Update SMBFile Share en la referencia de la API AWS de Storage Gateway.

> **Note**
>
> Tras actualizar el método de cifrado, la puerta de enlace utilizará el nuevo método para todos los objetos nuevos que cree en Amazon S3 y para cualquier objeto almacenado que actualice o modifique en el futuro. Los objetos Amazon S3 existentes solo recibirán el nuevo método de cifrado si la puerta de enlace los actualiza o modifica.

> **Important**
>
> Asegúrese de que el recurso compartido de archivos utilice el mismo tipo de cifrado que el bucket de Amazon S3 en el que almacena los datos.
> Si configura su puerta de enlace de archivos para utilizar SSE-KMS o DSSE-KMS para el cifrado, debe añadir manualmente los `kms:DescribeKey` permisos`kms:Encrypt`, `kms:Decrypt` `kms:ReEncrypt*` `kms:GenerateDataKey`, y a la función de IAM asociada al recurso compartido de archivos. Para obtener más información, consulte Uso de políticas basadas en la identidad (políticas de IAM) para Storage Gateway.

Crear un recurso compartido de archivos NFS

El protocolo Network File System (NFS) es un protocolo de intercambio de archivos con estado para sistemas basados en UNIX. Cuando un cliente con NFS y un servidor NFS se comunican, el cliente

solicita un archivo o directorio al servidor mediante llamadas a procedimientos remotos (RPC). El servidor verifica que el archivo o directorio esté disponible y que el cliente tenga los permisos de acceso necesarios. A continuación, el servidor monta el archivo o directorio de forma remota en el cliente y comparte el acceso a través de una conexión virtual. Para las operaciones del cliente, NFS hace que el uso del archivo del servidor remoto sea similar al acceso a un archivo local.

> **Note**
>
> El protocolo NFS admite un máximo de 16 grupos por usuario. Los usuarios pueden tener problemas para montar los recursos compartidos de archivos NFS si pertenecen a más de 16 grupos. Para evitar problemas de montaje, asegúrese de que los usuarios sean miembros de 16 grupos o menos al acceder a los recursos compartidos de archivos NFS.

En los temas siguientes se explican varios métodos para crear un recurso compartido de archivos NFS para su puerta de enlace de archivos:

Contenido

- Cree un recurso compartido de archivos NFS con la configuración predeterminada
  - Parámetros de configuración predeterminados para los recursos compartidos de archivos NFS
- Cree un recurso compartido de archivos NFS con una configuración personalizada

Cree un recurso compartido de archivos NFS con la configuración predeterminada

En esta sección se explica cómo crear un nuevo recurso compartido de archivos del Sistema de archivos de red (NFS) utilizando los ajustes predeterminados preconfigurados. Utilice este método para implementaciones básicas, uso personal, pruebas o como una forma de implementar rápidamente varios recursos compartidos de archivos que desee editar y personalizar más adelante. Para obtener una lista de los ajustes predeterminados de los recursos compartidos de archivos que cree mediante este procedimiento, consulte los valores de configuración predeterminados de los recursos compartidos de archivos NFS. Si necesita un control más detallado o desea utilizar una configuración avanzada para el recurso compartido de archivos, consulte Crear un recurso compartido de archivos NFS mediante una configuración personalizada.

> **Note**
>
> Si necesita conectar su recurso compartido de archivos a Amazon S3 a través de una Nube Privada Virtual (VPC), debe seguir el procedimiento de configuración personalizado. No puedes editar la configuración de VPC de un recurso compartido de archivos después de crearlo.

> **Important**
>
> El uso del control de versiones de S3, la replicación entre regiones o la utilidad Rsync al cargar datos desde una puerta de enlace de archivos puede tener importantes repercusiones económicas. Para obtener más información, consulte Evitar costes imprevistos al cargar datos desde File Gateway.

Para crear un recurso compartido de archivos NFS con la configuración predeterminada:

1. Abra la consola AWS Storage Gateway en https://console.aws.amazon.com/storagegateway/casa/ y seleccione Archivos compartidos en el panel de navegación izquierdo.
2. Elija Create file share (Crear recurso compartido de archivos).
3. Para Gateway, elija su Amazon S3 File Gateway de la lista.
4. Para el protocolo de uso compartido de archivos, elija NFS.
5. Para el bucket S3, realice una de las siguientes acciones:

   - Elija un bucket de Amazon S3 existente en su cuenta en la lista desplegable.
   - Elija un depósito de otra cuenta de la lista desplegable y, a continuación, introduzca el nombre del depósito en Nombre del depósito multicuenta.
   - Seleccione Crear nuevo depósito de S3 y, a continuación, elija la Región de AWS ubicación del punto de conexión de Amazon S3 para su nuevo depósito e introduzca un nombre de depósito de S3 único. Elija Crear depósito de S3 cuando haya terminado.

     Para obtener información sobre cómo crear un depósito nuevo, consulta ¿Cómo se crea un depósito de S3? en la Guía del usuario de Amazon S3.

> **Note**
>
> S3 File Gateway no admite buckets de Amazon S3 con puntos (.) en el nombre del bucket.
> Asegúrese de que el nombre de su bucket cumpla con las normas de denominación de bucket de Amazon S3. Para obtener más información, consulte Reglas para nombrar buckets en la Guía del usuario de Amazon Simple Storage Service.

6. Revisa los ajustes en Configuración predeterminada y, a continuación, selecciona Crear recurso compartido de archivos para crear tu nuevo recurso compartido de archivos NFS con la configuración predeterminada.

Una vez creado el recurso compartido de archivos NFS, puede ver sus ajustes de configuración en la consola AWS Storage Gateway, en la pestaña Detalles del recurso compartido de archivos. Para obtener información sobre cómo montar el recurso compartido de archivos, consulte Montar el recurso compartido de archivos NFS en el cliente.

Parámetros de configuración predeterminados para los recursos compartidos de archivos NFS

Los siguientes ajustes se aplican a todos los nuevos recursos compartidos de archivos NFS que cree con la configuración predeterminada. Tras crear un recurso compartido de archivos, puede seleccionarlo en la página Recursos compartidos de archivos de la consola AWS Storage Gateway para ver los detalles de su configuración.

> **Important**
>
> La configuración predeterminada del recurso compartido de archivos de NFS proporciona permisos de acceso y control total de los archivos al propietario del depósito de S3 asignado al recurso compartido de archivos, incluso si el depósito pertenece a una cuenta diferente AWS . Para obtener más información sobre cómo usar el recurso compartido de archivos para acceder a los objetos de un bucket que es propiedad de otra cuenta, consulte. Uso de un recurso compartido de archivos para el acceso entre cuentas

Opción	Valor predeterminado	Notas
Ubicación de Amazon S3	El recurso compartido de archivos se conecta directamente al bucket de Amazon S3 y tiene el mismo nombre que el bucket. Su puerta de enlace utiliza este depósito para almacenar y recuperar archivos.	El nombre no incluye un prefijo.
AWS PrivateLink para S3	El recurso compartido de archivos no se conecta a Amazon S3 a través de un punto de enlace de interfaz en su nube privada virtual (VPC).	
Notificación de carga de archivos	Desactivado	
Clase de almacenamiento para objetos nuevos	Estándar Amazon S3	Esto le permite almacenar los datos de objetos a los que accede con frecuencia de forma redundante en varias zonas de disponibilidad separadas geográficamente. Para obtener más información sobre la clase Amazon S3 Standard de almacenamiento, consulte Clases de almacenamiento para objetos a los que se accede con frecuencia en la Guía del usuario de Amazon Simple Storage Service.

Opción	Valor predeterminado	Notas
Cifrado	Cifrado del lado del servidor con claves administradas por S3 (SSE-S3)	Todos los objetos de Amazon S3 que suba, actualice o modifique su S3 File Gateway se cifran de forma predeterminada con un cifrado del lado del servidor mediante claves gestionadas de Amazon S3.
Metadatos de objetos	Adivina el tipo MIME	Esto permite a Storage Gateway adivinar el tipo de extensión multipropósito de correo de Internet (MIME) para los objetos cargados en función de las extensiones de archivo. Esta opción requiere que las listas de control de acceso (ACLs) estén activadas para el bucket de Amazon S3 asociado a tu recurso compartido de archivos. Si ACLs son desactivado, el recurso compartido de archivos no puede acceder al bucket de Amazon S3 y permanece en el estado No disponible indefinidamente.
Habilitar los pagos del solicitante	Desactivado	Para obtener más información, consulte Buckets de pago por solicitante.

Opción	Valor predeterminado	Notas
Registros de auditoría	Desactivado	El registro en un Amazon CloudWatch grupo está desactivado de forma predeterminada.
Acceda a su bucket de S3	Cree un nuevo rol de IAM	La opción predeterminada permite a File Gateway crear un nuevo rol de IAM y acceder política en su nombre. Se permite el acceso a todos los clientes NFS. Para obtener información sobre los compatibles Clientes NFS, consulteClientes NFS y SMB compatibles con File Gateway.
Opciones de montaje	• Nivel de squash: calabaza de raíz • Exportar como: lectura-e scritura	El valor predeterminado del nivel Squash significa que acceso para el control remoto el superusuario (raíz) se asigna al identificador de usuario (UID) (65534) y al identificador de grupo (GID) (65534).
Valores predeterminados de los metadatos de los archivos	• Permisos de directorio: 0777 • Permisos de archivos: 0666 • Identificador de usuario (UID): 65534 • Identificador de grupo (GID): 65534	

Cree un recurso compartido de archivos NFS con una configuración personalizada

Utilice el siguiente procedimiento para crear un recurso compartido de archivos del Sistema de archivos de red (NFS) con una configuración personalizada. Para crear un recurso compartido de archivos NFS con los valores de configuración predeterminados, consulte Crear un recurso compartido de archivos NFS con la configuración predeterminada.

> **Important**
>
> El uso del control de versiones de S3, la replicación entre regiones o la utilidad Rsync al cargar datos desde una puerta de enlace de archivos puede tener importantes implicaciones económicas. Para obtener más información, consulte Evitar costes imprevistos al cargar datos desde File Gateway.

Para crear un recurso compartido de archivos NFS con una configuración personalizada

1. Abra la consola AWS Storage Gateway en https://console.aws.amazon.com/storagegateway/casa/ y seleccione Archivos compartidos en el panel de navegación izquierdo.
2. Elija Create file share (Crear recurso compartido de archivos).
3. Seleccione Personalizar la configuración. Por ahora, puede ignorar los demás campos de esta página. En los pasos siguientes, se le pedirá que configure los ajustes de puerta de enlace, protocolo y almacenamiento.
4. En el caso de Gateway, elija Amazon S3 File Gateway para su nuevo recurso compartido de archivos en la lista desplegable.
5. Para el grupo de CloudWatch registros, elija una de las siguientes opciones de la lista desplegable:

   - Para desactivar el registro de este recurso compartido de archivos, selecciona Desactivar el registro.
   - Para crear automáticamente un nuevo grupo de registros para este recurso compartido de archivos, elija Created by Storage Gateway.
   - Para enviar notificaciones de estado y recursos de este recurso compartido de archivos a un grupo de registros existente, elija el grupo deseado de la lista.

Para obtener más información sobre los registros de auditoría, consulte Descripción de los registros de auditoría de S3 File Gateway.

6. (Opcional) En Etiquetas: opcional, seleccione Añadir nueva etiqueta e introduzca una clave y un valor para el recurso compartido de archivos.

   Una etiqueta es un par clave-valor que distingue entre mayúsculas y minúsculas y que le ayuda a clasificar los recursos de Storage Gateway. Agregar etiquetas puede facilitar el filtrado y la búsqueda de los archivos compartidos. Puedes repetir este paso para añadir hasta 50 etiquetas.

   Elija Siguiente cuando haya terminado.

7. En el caso del bucket S3, realice una de las siguientes acciones para especificar dónde almacenará y recuperará los archivos el recurso compartido:

   - Para conectar el recurso compartido de archivos directamente a un bucket de S3 existente en su cuenta de Amazon Web Services, elija el nombre del bucket en la lista desplegable.
   - Para conectar el recurso compartido de archivos a un depósito de S3 existente que sea propiedad de una cuenta de Amazon Web Services distinta de la que utilizaste para crear el recurso compartido de archivos, selecciona Un depósito de otra cuenta en la lista desplegable e introduce el nombre del depósito entre cuentas.
   - Para conectar el recurso compartido de archivos a un nuevo depósito de S3, seleccione Crear un nuevo depósito de S3 y, a continuación, elija la región en la que se encuentra el punto de conexión de Amazon S3 para su nuevo depósito e introduzca un nombre de depósito de S3 único. Selecciona Crear depósito de S3 cuando hayas terminado. Para obtener más información sobre la creación de depósitos nuevos, consulta ¿Cómo se crea un depósito de S3? en la Guía del usuario de Amazon S3.
   - Para conectar el recurso compartido de archivos a un bucket de S3 mediante un nombre de punto de acceso, elija el nombre del punto de acceso Amazon S3 en la lista desplegable y, a continuación, introduzca el nombre del punto de acceso. Si necesita crear un nuevo punto de acceso, puede elegir Crear un punto de acceso S3. Para obtener más instrucciones, consulte Creación de un punto de acceso en la Guía del usuario de Amazon S3. Para obtener más información sobre los puntos de acceso, consulte Administrar el acceso a los datos con puntos de acceso de Amazon S3 y Delegar el control de acceso a los puntos de acceso en la Guía del usuario de Amazon S3.
   - Para conectar el recurso compartido de archivos a un bucket de S3 mediante un alias de punto de acceso, elija el alias del punto de acceso de Amazon S3 en la lista desplegable y,

a continuación, introduzca el alias del punto de acceso. Si necesita crear un nuevo punto de acceso, puede elegir Crear un punto de acceso S3. Para obtener más instrucciones, consulte Creación de un punto de acceso en la Guía del usuario de Amazon S3. Para obtener más información sobre los alias de puntos de acceso, consulte Uso de un alias tipo bucket para su punto de acceso en la Guía del usuario de Amazon S3.

> **Note**
>
> Cada recurso compartido de archivos solo se puede conectar a un bucket de S3, pero varios recursos compartidos de archivos se pueden conectar al mismo bucket. Si conecta más de un recurso compartido de archivos al mismo depósito, debe configurar cada recurso compartido de archivos para que utilice un prefijo de depósito de S3 único y que no se superponga para evitar read/write conflictos.
>
> S3 File Gateway no admite buckets de Amazon S3 con puntos (`.`) en el nombre del bucket.
>
> Asegúrese de que el nombre de su bucket cumpla con las normas de denominación de bucket de Amazon S3. Para obtener más información, consulte Reglas para nombrar buckets en la Guía del usuario de Amazon Simple Storage Service.

8. (Opcional) Para el prefijo de bucket de S3, introduzca un prefijo para que el recurso compartido de archivos se aplique a los objetos que cree en Amazon S3. Los prefijos son una forma de organizar los datos en S3, de forma similar a los directorios de las estructuras de archivos tradicionales. Para obtener más información, consulte Organizar objetos mediante prefijos en la Guía del usuario de Amazon S3.

> **Note**
>
> - Si conecta más de un recurso compartido de archivos al mismo depósito, debe configurar cada recurso compartido de archivos para que utilice un prefijo único que no se superponga a fin de evitar conflictos. read/write
> - El prefijo debe terminar con una barra diagonal: (/).
> - Una vez creado el recurso compartido de archivos, el prefijo no se puede modificar ni eliminar.

9. En el Región de AWS caso de la región, selecciona la ubicación del punto final de S3 para tu bucket en la lista desplegable. Este campo aparece solo cuando se especifica un punto de acceso o un depósito en otra cuenta para el depósito de S3.
10. En Clase de almacenamiento para objetos nuevos, elija una clase de almacenamiento de la lista desplegable. Para obtener más información sobre las clases de almacenamiento, consulte Uso de clases de almacenamiento con una puerta de enlace de archivos.
11. En el caso del rol de IAM, realice una de las siguientes acciones para configurar un rol de IAM para su recurso compartido de archivos:

    - Para crear automáticamente una nueva función de IAM con los permisos necesarios para que el recurso compartido de archivos funcione correctamente, seleccione Created by Storage Gateway en la lista desplegable.
    - Para usar un rol de IAM existente, elija el nombre del rol en la lista desplegable.
    - Para crear un nuevo rol de IAM, elija Crear un rol. Para obtener más instrucciones, consulte Crear un rol para delegar permisos a un AWS servicio en la Guía del AWS Identity and Access Management usuario.

    Para obtener más información sobre cómo las funciones de IAM controlan el acceso entre el recurso compartido de archivos y el bucket de S3, consulte Otorgar acceso a un bucket de Amazon S3.
12. Para el enlace privado, haga lo siguiente solo si necesita configurar el recurso compartido de archivos para que se comunique con él AWS mediante un punto final privado en una Nube Privada Virtual (VPC). De lo contrario, omita este paso. Para obtener más información, consulte ¿Qué es? AWS PrivateLink en la AWS PrivateLink Guía.

    a. Seleccione Usar punto final de VPC.

    b. Para identificar el punto final de la VPC mediante, realice una de las siguientes acciones:

        - Seleccione el ID de punto de conexión de VPC y, a continuación, elija el punto de conexión que desee utilizar en la lista desplegable de puntos de conexión de VPC.
        - Selecciona el nombre de DNS y, a continuación, introduce el nombre de DNS del punto de conexión que quieres usar.
13. Para el cifrado, elija el tipo de cifrado del lado del servidor que el recurso compartido de archivos utilizará para los datos que almacene en Amazon S3:

- Para usar el cifrado del lado del servidor gestionado con Amazon S3 (SSE-S3), elija S3 Managed Keys (SSE-S3).

  Para obtener más información, consulte Uso del cifrado del lado del servidor con claves administradas de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

- Para usar el cifrado del lado del servidor administrado con el Servicio de administración de AWS claves (SSE-KMS), elija claves administradas por KMS (SSE-KMS). Para la clave de KMS principal, elige una clave de AWS KMS existente o selecciona Crear una nueva clave de KMS para crear una nueva clave de KMS en la consola del Servicio de administración de claves (). AWS AWS KMS

  Para obtener más información AWS KMS, consulte ¿Qué es el servicio de administración de AWS claves? en la Guía para AWS Key Management Service desarrolladores.

- Para usar el cifrado de doble capa del lado del servidor administrado con el Servicio de administración de AWS claves (DSSE-KMS), elija el cifrado de doble capa del lado del servidor con claves (DSSE-KMS). AWS Key Management Service Para la clave KMS principal, elija una clave AWS KMS existente o elija Crear una nueva clave KMS para crear una nueva clave KMS en la consola del Servicio de administración de claves (). AWS AWS KMS

  Para obtener más información sobre DSSE-KMS, consulte Uso del cifrado de doble capa del lado del servidor con claves AWS KMS en la Guía del usuario de Amazon Simple Storage Service.

  > **Note**
  >
  > El uso del DSSE-KMS y las claves conlleva cargos adicionales. AWS KMS Para más información, consulte Precios de AWS KMS.
  > Para especificar una AWS KMS clave con un alias que no aparezca en la lista o para usar una AWS KMS clave de otra AWS cuenta, debe usar la. AWS Command Line Interface No se admiten las claves KMS asimétricas. Para obtener más información, consulte Create NFSFile Share in the AWS Storage Gateway API Reference.

> **Important**
>
> Asegúrese de que el recurso compartido de archivos utilice el mismo tipo de cifrado que el bucket de Amazon S3 en el que almacena los datos.

14. Para los tipos MIME de Guess, seleccione el tipo MIME de medios de Guess para permitir que Storage Gateway adivine el tipo de medio de los objetos cargados en función de sus extensiones de archivo.
15. En Nombre del recurso compartido de archivos, introduzca un nombre para el recurso compartido de archivos.

> **Note**
>
> Un nombre de recurso compartido de archivos NFS válido solo puede contener los siguientes caracteres: a `A` - `zZ`, `0` -9, - `-.`, y `_`.

16. En Cargar eventos, seleccione Registrar un evento cuando la puerta de enlace cargue correctamente un archivo si quiere que la puerta de enlace registre los eventos de CloudWatch registro cuando suba correctamente los archivos a Amazon S3. El retraso de la notificación controla el retraso mínimo entre la operación de escritura más reciente del cliente y la generación de la notificación de `ObjectUploaded` registro. Como los clientes pueden realizar muchas escrituras pequeñas en los archivos en poco tiempo, recomendamos configurar este parámetro durante el mayor tiempo posible para evitar generar varias notificaciones para el mismo archivo de forma rápida y sucesiva. Para obtener más información, consulte Recibir una notificación de carga de archivos.

> **Note**
>
> Esta configuración no afecta a la hora de carga del objeto a S3, solo a la hora de la notificación.
> Esta configuración no pretende especificar la hora exacta a la que se enviará la notificación. En algunos casos, es posible que la pasarela requiera un tiempo de retraso superior al especificado para generar y enviar las notificaciones.

Elija Siguiente cuando haya terminado.

17.

18. Para el protocolo de uso compartido de archivos, elija NFS.

19. Para el acceso de cliente, realice una de las siguientes acciones para especificar qué clientes NFS pueden acceder a su recurso compartido de archivos:

    - Para aceptar todas las conexiones de clientes entrantes, seleccione Todos los clientes NFS.
    - Para aceptar conexiones de clientes entrantes solo desde direcciones IP específicas, seleccione Clientes NFS específicos y, a continuación, elija Agregar un cliente. En Clientes permitidos, especifique una dirección IP válida o un bloque CIDR desde el que aceptar las conexiones. Si necesita especificar direcciones IP adicionales, elija Agregar otro cliente.

    > **Note**
    >
    > Le recomendamos configurar la limitación del acceso a su recurso compartido de archivos mediante la opción Clientes NFS específicos. Si no lo hace, cualquier cliente de la red puede montarlo en el recurso compartido de archivos.

20. En Tipo de acceso, seleccione una de las siguientes opciones:

    - Para permitir que los clientes lean y escriban archivos en el recurso compartido de archivos, seleccione Lectura/Escritura.
    - Para permitir que los clientes lean los archivos pero no escriban en el recurso compartido de archivos, seleccione Solo lectura.

    > **Note**
    >
    > En el caso de los recursos compartidos de archivos que están montados en un cliente de Microsoft Windows, si selecciona Solo lectura, es posible que aparezca un mensaje sobre un error inesperado que le impide crear la carpeta. Puede hacer caso omiso del mensaje.

21. Para el nivel de acceso, elija una de las siguientes opciones:

    - Root squash (default) (Agrupación en raíz) (predeterminado): el acceso del superusuario remoto (raíz) se asigna al UID (65534) y al GID (65534).
    - All squash (Agrupación para todos): el acceso de todos los usuarios se asigna al ID de usuario (UID) (65534) y al ID de grupo (GID) (65534).

- No root squash (Sin agrupación en raíz): el superusuario remoto (raíz) recibe acceso como usuario raíz.

22. (Opcional) Para actualizar la caché automáticamente desde S3, seleccione Establecer intervalo de actualización de la caché y, a continuación, establezca el tiempo en minutos o días para actualizar la caché del recurso compartido de archivos mediante Time To Live (TTL). TTL es el tiempo transcurrido desde la última actualización. Una vez transcurrido el intervalo TTL, al acceder a un directorio, File Gateway actualiza el contenido de ese directorio desde el bucket de Amazon S3.

    > **Note**
    >
    > Establecer este valor en menos de 30 minutos puede afectar negativamente al rendimiento de la puerta de enlace en situaciones en las que se crean o eliminan con frecuencia grandes cantidades de objetos de Amazon S3.

23. En los valores predeterminados de los metadatos de los archivos, seleccione Cambiar los metadatos predeterminados de los objetos de S3 que su puerta de enlace no haya creado ni modificado si desea que la puerta de enlace aplique los metadatos de los archivos (incluidos los permisos de Unix) a los objetos preexistentes que descubra en su bucket de S3. Especifique los permisos del directorio, los permisos de los archivos, el ID de usuario y el ID de grupo que desee aplicar en los campos correspondientes.
24. Para la propiedad y los permisos de los archivos, seleccione Otorgar al propietario del bucket de S3 la propiedad total de los archivos creados por la puerta de enlace, incluidos los permisos de lectura, escritura, edición y eliminación si desea que la AWS cuenta propietaria del bucket de S3 tenga el control total de todos los objetos escritos en el bucket por su recurso compartido de archivos.

    Selecciona Siguiente cuando termines.
25. Revise la configuración del recurso compartido de archivos. Seleccione Editar para modificar la configuración de cualquier sección que desee cambiar. Cuando termine, elija Create (Crear).

Una vez creado el recurso compartido de archivos NFS, puede ver sus ajustes de configuración en la consola AWS Storage Gateway, en la pestaña Detalles del recurso compartido de archivos. Para obtener instrucciones sobre cómo montar el recurso compartido de archivos, consulte Montar el recurso compartido de archivos NFS en el cliente.

Crear un recurso compartido de archivos SMB

El protocolo Server Message Block (SMB) está profundamente integrado en el conjunto de productos de Microsoft Windows y sigue siendo el protocolo de intercambio de archivos predeterminado para los sistemas operativos Windows. El proceso de comunicación cliente-servidor es similar al de NFS en un nivel alto, pero hay diferencias en algunos detalles y mecanismos operativos. Por ejemplo, en SMB, los sistemas de archivos no están montados en el cliente SMB local. En su lugar, se accede a un recurso compartido de red alojado en el servidor SMB a través de una ruta de red.

En los temas de esta sección se explican varios métodos para crear un recurso compartido de archivos SMB para su puerta de enlace de archivos.

Contenido

- Cree un recurso compartido de archivos SMB con la configuración predeterminada
  - Parámetros de configuración predeterminados para los recursos compartidos de archivos SMB
- Cree un recurso compartido de archivos SMB con una configuración personalizada

Cree un recurso compartido de archivos SMB con la configuración predeterminada

En esta sección se explica cómo crear un nuevo recurso compartido de archivos del bloque de mensajes del servidor (SMB) utilizando los ajustes predeterminados preconfigurados. Utilice este método para despliegues básicos, uso personal, pruebas o como una forma de implementar rápidamente varios recursos compartidos de archivos que desee editar y personalizar más adelante. Para obtener una lista de los ajustes predeterminados de los recursos compartidos de archivos que se crean mediante este procedimiento, consulte Valores de configuración predeterminados para los recursos compartidos de archivos SMB. Si necesita un control más detallado o desea utilizar una configuración avanzada para el recurso compartido de archivos, consulte Crear un recurso compartido de archivos SMB con una configuración personalizada.

> **Note**
>
> Si necesita conectar su recurso compartido de archivos a Amazon S3 a través de una Nube Privada Virtual (VPC), debe seguir el procedimiento de configuración personalizado. No puedes editar la configuración de VPC de un recurso compartido de archivos después de crearlo.

> **Important**
>
> El uso del control de versiones de S3, la replicación entre regiones o la utilidad Rsync al cargar datos desde una puerta de enlace de archivos puede tener importantes repercusiones económicas. Para obtener más información, consulte Evitar costes imprevistos al cargar datos desde File Gateway.

Requisitos previos

Antes de crear el recurso compartido de archivos, haga lo siguiente:

- Configure los ajustes de seguridad SMB para su File Gateway. Para obtener instrucciones, consulte Configurar un nivel de seguridad para la puerta de enlace.
- Configure Microsoft Active Directory o el acceso de invitado para la autenticación. Para obtener instrucciones, consulte Uso de Active Directory para autenticar usuarios o Proporcionar acceso de invitado al recurso compartido de archivos.
- Asegúrese de que los puertos necesarios estén abiertos en su grupo de seguridad. Para obtener más información, consulte Requisitos de puertos.

Para crear un recurso compartido de archivos SMB con la configuración predeterminada:

1. Abra la consola AWS Storage Gateway en https://console.aws.amazon.com/storagegateway/casa/ y seleccione Archivos compartidos en el panel de navegación izquierdo.
2. Elija Create file share (Crear recurso compartido de archivos).
3. Para Gateway, elija Amazon S3 File Gateway en la lista desplegable.
4. Para el protocolo de uso compartido de archivos, elija SMB.
5. Para el bucket S3, realice una de las siguientes acciones:
   - Elija un bucket de Amazon S3 existente en su cuenta en la lista desplegable.
   - Selecciona un depósito en otra cuenta de la lista desplegable y, a continuación, introduce el nombre del depósito en Nombre del depósito entre cuentas.
   - Seleccione Crear nuevo depósito de S3 y, a continuación, elija la Región de AWS ubicación del punto de conexión de Amazon S3 para su nuevo depósito e introduzca un nombre de depósito de S3 único. Elija Crear depósito de S3 cuando haya terminado.

Para obtener información sobre cómo crear un depósito nuevo, consulta ¿Cómo se crea un depósito de S3? en la Guía del usuario de Amazon S3.

> **Note**
>
> S3 File Gateway no admite buckets de Amazon S3 con puntos (`.`) en el nombre del bucket.
> Asegúrese de que el nombre de su bucket cumpla con las normas de denominación de bucket de Amazon S3. Para obtener más información, consulte Reglas para nombrar buckets en la Guía del usuario de Amazon Simple Storage Service.

6. Autenticación de usuario: elige el método de autenticación que quieres usar de la lista desplegable:

   - Para usar su Microsoft Active Directory corporativo o AWS Managed Microsoft AD para autenticar el acceso de los usuarios a su recurso compartido de archivos SMB, elija Active Directory. Para usar este método, la puerta de enlace debe estar unida a un dominio. Para obtener más información, consulte Uso de Active Directory para autenticar usuarios.

     > **Note**
     >
     > Para AWS Managed Microsoft AD utilizarla con una EC2 puerta de enlace de Amazon, debe crear la EC2 instancia de Amazon en la misma VPC que la AWS Managed Microsoft AD, añadir el grupo de `_workspaceMembers` seguridad a la EC2 instancia de Amazon y unirse al dominio de AD con las credenciales de administrador de. AWS Managed Microsoft AD
     > Para obtener más información al respecto AWS Managed Microsoft AD, consulte la Guía de AWS Directory Service administración.
     > Para obtener más información sobre Amazon EC2, consulte la documentación de Amazon Elastic Compute Cloud.

   Si el estado de unión indica que su puerta de enlace ya está unida a un dominio de Active Directory, continúe con el siguiente paso. De lo contrario, realice lo siguiente:

   1. Elija Configurar.

2. En Dominio, introduzca el nombre del dominio de Active Directory al que desee que se una la puerta de enlace.
3. Introduzca el nombre de usuario y la contraseña que utilizará la puerta de enlace para unirse al dominio.
4. (Opcional) En el caso de la unidad organizativa (OU), introduzca la OU designada que Active Directory utiliza para los nuevos objetos informáticos.
5. (Opcional) Para los controladores de dominio (DC), introduzca el nombre del DC a través del cual la puerta de enlace se conectará a Active Directory. Puede dejar este campo en blanco para permitir que DNS seleccione automáticamente un DC.
6. Elija Unirse a Active Directory.

> **Note**
>
> Al unirse a un dominio, se crea una cuenta de Active Directory en el contenedor predeterminado (que no es una unidad organizativa) con el ID de 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, debe crear esta cuenta con antelación.
> Si su entorno de Active Directory tiene una unidad organizativa designada para los nuevos objetos informáticos, debe especificarla al unirse al dominio.

- Para conceder acceso protegido por contraseña a cualquier persona que proporcione la contraseña de invitado que usted configure, elija Acceso de invitado. No es necesario que File Gateway forme parte de un dominio de Microsoft Active Directory para utilizar este método. Elija Configurar para especificar la contraseña de invitado y, a continuación, seleccione Guardar.

7. Revise los ajustes en Configuración predeterminada y, a continuación, seleccione Crear recurso compartido de archivos para crear su nuevo recurso compartido de archivos SMB con la configuración predeterminada.

Una vez creado el recurso compartido de archivos SMB, puede ver sus ajustes de configuración en la consola AWS Storage Gateway, en la pestaña Detalles del recurso compartido de archivos. Para obtener información sobre cómo montar el recurso compartido de archivos, consulte Montar el recurso compartido de archivos SMB en el cliente.

Parámetros de configuración predeterminados para los recursos compartidos de archivos SMB

La siguiente configuración se aplica a todos los nuevos recursos compartidos de archivos SMB que cree con la configuración predeterminada. Tras crear un recurso compartido de archivos, puede seleccionarlo en la página Recursos compartidos de archivos de la consola AWS Storage Gateway para ver los detalles de su configuración.

> **Important**
>
> La configuración predeterminada para compartir archivos SMB proporciona control total de los archivos y permisos de acceso al propietario del bucket de S3 que está asignado al recurso compartido de archivos, incluso si el bucket es propiedad de una cuenta diferente de Amazon Web Services. Para obtener más información sobre cómo usar el recurso compartido de archivos para acceder a los objetos de un bucket que es propiedad de otra cuenta, consulte Uso de un recurso compartido de archivos para el acceso entre cuentas.

Opción	Valor predeterminado	Notas
Ubicación de Amazon S3	El recurso compartido de archivos se conecta directamente al bucket de Amazon S3 y tiene el mismo nombre que el bucket. Su puerta de enlace utiliza este depósito para almacenar y recuperar archivos.	El nombre no incluye un prefijo.
AWS PrivateLink para S3	El recurso compartido de archivos no se conecta a Amazon S3 a través de un punto de enlace de interfaz en su nube privada virtual (VPC).	
Notificación de carga de archivos	Desactivado	

Opción	Valor predeterminado	Notas
Clase de almacenamiento para objetos nuevos	Amazon S3 Standard	Esto le permite almacenar los datos de objetos a los que se accede con frecuencia de forma redundante en varias zonas de disponibilidad separadas geográficamente. Para obtener más información sobre la clase Amazon S3 Standard de almacenamiento, consulte Clases de almacenamiento para objetos a los que se accede con frecuencia en la Guía del usuario de Amazon Simple Storage Service.
Cifrado	Cifrado del lado del servidor con claves administradas por S3 (SSE-S3)	Todos los objetos de Amazon S3 que suba, actualice o modifique su S3 File Gateway se cifran de forma predeterminada con un cifrado del lado del servidor mediante claves gestionadas de Amazon S3.

Opción	Valor predeterminado	Notas
Metadatos de objetos	Adivina el tipo MIME	Esto permite a Storage Gateway adivinar el tipo de extensión multipropósito de correo de Internet (MIME) para los objetos cargados en función de las extensiones de archivo. Esta opción requiere que las listas de control de acceso (ACLs) estén activadas en el bucket de Amazon S3 asociado al recurso compartid o de archivos. Si lo ACLs son desactivado, el recurso compartido de archivos no puede acceder al bucket de Amazon S3 y permanece en el estado No disponible indefinid amente.
Enumeración basada en el acceso	No está activado	Todos los usuarios pueden ver los archivos y las carpetas del recurso compartido durante la enumeración de directori os. La enumeración basada en el acceso es un sistema que filtra la enumeración de archivos y carpetas de un recurso compartido de archivos SMB en función del acceso al recurso compartido listas de control (ACLs).

Opción	Valor predeterminado	Notas
Habilitar los pagos del solicitante	Desactivado	Para obtener más información, consulte Buckets de pago por solicitante.
Bloqueo oportunista	Activado	Esto permite que el archivo compartido utilice el bloqueo oportunista para optimizar la estrategia de almacenamiento en búfer de archivos. En la mayoría de los casos, la activación del bloqueo oportunista mejora rendimien to, particularmente en lo que respecta al contexto de Windows menús.
Registros de auditoría	Desactivado	El registro en un Amazon CloudWatch grupo está desactivado de forma predeterminada.
Defina la sensibilidad entre mayúsculas	Desactivado	Esto permite al cliente controlar la distinción entre mayúsculas y minúsculas.
Acceda a su bucket de S3	Cree un nuevo rol de IAM	La opción predeterminada permite a File Gateway crear un nuevo rol de IAM y acceder política en su nombre.

Cree un recurso compartido de archivos SMB con una configuración personalizada

Utilice el siguiente procedimiento para crear un recurso compartido de archivos del bloque de mensajes del servidor (SMB) con una configuración personalizada. Para crear un recurso compartido de archivos SMB con los valores de configuración predeterminados, consulte Crear un recurso compartido de archivos SMB con la configuración predeterminada.

> **Important**
>
> El uso del control de versiones de S3, la replicación entre regiones o la utilidad Rsync al cargar datos desde una puerta de enlace de archivos puede tener importantes implicaciones económicas. Para obtener más información, consulte Evitar costes imprevistos al cargar datos desde File Gateway.

Requisitos previos

Antes de crear el recurso compartido de archivos, haga lo siguiente:

- Configure los ajustes de seguridad SMB para su File Gateway. Para obtener instrucciones, consulte Configurar un nivel de seguridad para la puerta de enlace.
- Configure Microsoft Active Directory o el acceso de invitado para la autenticación. Para obtener instrucciones, consulte Uso de Active Directory para autenticar usuarios o Proporcionar acceso de invitado al recurso compartido de archivos.
- Asegúrese de que los puertos necesarios estén abiertos en su grupo de seguridad. Para obtener más información, consulte Requisitos de puertos.

Para crear un recurso compartido de archivos SMB con una configuración personalizada

1. Abra la consola AWS Storage Gateway en https://console.aws.amazon.com/storagegateway/casa/ y seleccione Archivos compartidos en el panel de navegación izquierdo.
2. Elija Create file share (Crear recurso compartido de archivos).
3. Seleccione Personalizar la configuración. Por ahora, puede ignorar los demás campos de esta página. En los pasos siguientes, se le pedirá que configure los ajustes de puerta de enlace, protocolo y almacenamiento.
4. Para Gateway, elija Amazon S3 File Gateway en la lista desplegable.

5. Para el grupo de CloudWatch registros, elija una de las siguientes opciones de la lista desplegable:

   - Para desactivar el registro de este recurso compartido de archivos, selecciona Desactivar el registro.
   - Para crear automáticamente un nuevo grupo de registros para este recurso compartido de archivos, elija Created by Storage Gateway.
   - Para enviar notificaciones de estado y recursos de este recurso compartido de archivos a un grupo de registros existente, elija el grupo deseado de la lista.

   Para obtener más información sobre los registros de auditoría, consulte Descripción de los registros de auditoría de S3 File Gateway.

6. (Opcional) En Etiquetas: opcional, seleccione Añadir nueva etiqueta e introduzca una clave y un valor para el recurso compartido de archivos. Una etiqueta es un par clave-valor que distingue entre mayúsculas y minúsculas y que le ayuda a clasificar los recursos de Storage Gateway. Agregar etiquetas puede facilitar el filtrado y la búsqueda del recurso compartido de archivos. Puedes repetir este paso para añadir hasta 50 etiquetas.

   Elija Siguiente cuando haya terminado.

7. En el caso del bucket S3, realice una de las siguientes acciones para especificar dónde almacenar y recuperar los archivos:

   - Para conectar el recurso compartido de archivos directamente a un bucket de S3 existente en su cuenta de Amazon Web Services, elija el nombre del bucket en la lista desplegable.
   - Para conectar el recurso compartido de archivos a un depósito de S3 existente que sea propiedad de una cuenta de Amazon Web Services distinta de la que está utilizando para crear el recurso compartido de archivos, elija Un depósito de otra cuenta en la lista desplegable e introduzca el nombre del depósito multicuenta.
   - Para conectar el recurso compartido de archivos a un nuevo depósito de S3, seleccione Crear un nuevo depósito de S3 y, a continuación, elija la región en la que se encuentra el punto de conexión de Amazon S3 para su nuevo depósito e introduzca un nombre de depósito de S3 único. Selecciona Crear depósito de S3 cuando hayas terminado. Para obtener más información sobre la creación de depósitos nuevos, consulta ¿Cómo se crea un depósito de S3? en la Guía del usuario de Amazon S3.
   - Para conectar el recurso compartido de archivos a un bucket de S3 mediante un nombre de punto de acceso, elija el nombre del punto de acceso Amazon S3 en la lista desplegable y, a

continuación, introduzca el nombre del punto de acceso. Si necesita crear un nuevo punto de acceso, puede elegir Crear un punto de acceso S3. Para obtener más instrucciones, consulte Creación de un punto de acceso en la Guía del usuario de Amazon S3. Para obtener más información sobre los puntos de acceso, consulte Administrar el acceso a los datos con puntos de acceso de Amazon S3 y Delegar el control de acceso a los puntos de acceso en la Guía del usuario de Amazon S3.

- Para conectar el recurso compartido de archivos a un bucket de S3 mediante un alias de punto de acceso, elija el alias del punto de acceso de Amazon S3 en la lista desplegable y, a continuación, introduzca el alias del punto de acceso. Si necesita crear un nuevo punto de acceso, puede elegir Crear un punto de acceso S3. Para obtener más instrucciones, consulte Creación de un punto de acceso en la Guía del usuario de Amazon S3. Para obtener más información sobre los alias de puntos de acceso, consulte Uso de un alias tipo bucket para su punto de acceso en la Guía del usuario de Amazon S3.

> **Note**
>
> Cada recurso compartido de archivos solo se puede conectar a un bucket de S3, pero varios recursos compartidos de archivos se pueden conectar al mismo bucket. Si conecta más de un recurso compartido de archivos al mismo depósito, debe configurar cada recurso compartido de archivos para que utilice un prefijo de depósito de S3 único y que no se superponga para evitar read/write conflictos.
> S3 File Gateway no admite buckets de Amazon S3 con puntos (`.`) en el nombre del bucket.
> Asegúrese de que el nombre de su bucket cumpla con las normas de denominación de bucket de Amazon S3. Para obtener más información, consulte Reglas para nombrar buckets en la Guía del usuario de Amazon Simple Storage Service.

8. (Opcional) Para el prefijo de bucket de S3, introduzca un prefijo para que el recurso compartido de archivos se aplique a los objetos que cree en Amazon S3. Los prefijos son una forma de organizar los datos en S3, de forma similar a los directorios de las estructuras de archivos tradicionales. Para obtener más información, consulte Organizar objetos mediante prefijos en la Guía del usuario de Amazon S3.

> **Note**
>
> - Si conecta más de un recurso compartido de archivos al mismo depósito, debe configurar cada recurso compartido de archivos para que utilice un prefijo único que no se superponga a fin de evitar conflictos. read/write
> - El prefijo debe terminar con una barra diagonal: (/).
> - Una vez creado el recurso compartido de archivos, el prefijo no se puede modificar ni eliminar.

9. En el Región de AWS caso de la región, selecciona la ubicación del punto final de S3 para tu bucket en la lista desplegable. Este campo aparece solo cuando se especifica un punto de acceso o un depósito en otra cuenta para el depósito de S3.
10. En Clase de almacenamiento para objetos nuevos, elija una clase de almacenamiento de la lista desplegable. Para obtener más información sobre las clases de almacenamiento, consulte Uso de clases de almacenamiento con una puerta de enlace de archivos.
11. En el caso del rol de IAM, realice una de las siguientes acciones para configurar un rol de IAM para su recurso compartido de archivos:

    - Para crear automáticamente una nueva función de IAM con los permisos necesarios para que el recurso compartido de archivos funcione correctamente, seleccione Created by Storage Gateway en la lista desplegable.
    - Para usar un rol de IAM existente, elija el nombre del rol en la lista desplegable.
    - Para crear un nuevo rol de IAM, elija Crear un rol. Para obtener más instrucciones, consulte Crear un rol para delegar permisos a un AWS servicio en la Guía del AWS Identity and Access Management usuario.

    Para obtener más información sobre cómo las funciones de IAM controlan el acceso entre el recurso compartido de archivos y el bucket de S3, consulte Otorgar acceso a un bucket de Amazon S3.
12. En el caso del enlace privado, haga lo siguiente solo si necesita configurar el recurso compartido de archivos para que se comunique con él AWS mediante un punto de conexión privado en una Nube Privada Virtual (VPC). De lo contrario, omita este paso. Para obtener más información, consulte ¿Qué es? AWS PrivateLink en la AWS PrivateLink Guía.

a. Seleccione Usar punto final de VPC.

b. Para identificar el punto final de la VPC mediante, realice una de las siguientes acciones:

- Seleccione el ID de punto de conexión de VPC y, a continuación, elija el punto de conexión que desee utilizar en la lista desplegable de puntos de conexión de VPC.
- Selecciona el nombre de DNS y, a continuación, introduce el nombre de DNS del punto de conexión que quieres usar.

13. Para el cifrado, elija el tipo de claves de cifrado que se van a utilizar para cifrar los objetos que File Gateway almacena en Amazon S3:

- Para usar el cifrado del lado del servidor gestionado con Amazon S3 (SSE-S3), elija S3 Managed Keys (SSE-S3).

  Para obtener más información, consulte Uso del cifrado del lado del servidor con claves administradas de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

- Para usar el cifrado del lado del servidor administrado con el Servicio de administración de AWS claves (SSE-KMS), elija claves administradas por KMS (SSE-KMS). Para la clave KMS principal, elige una clave AWS KMS existente o selecciona Crear una nueva clave KMS para crear una nueva clave KMS en la consola del Servicio de administración de claves (). AWS AWS KMS

  Para obtener más información AWS KMS, consulte ¿Qué es el Servicio de administración de AWS claves? en la Guía para AWS Key Management Service desarrolladores.

- Para usar el cifrado de doble capa del lado del servidor administrado con el Servicio de administración de AWS claves (DSSE-KMS), elija el cifrado de doble capa del lado del servidor con claves (DSSE-KMS). AWS Key Management Service Para la clave KMS principal, elija una clave AWS KMS existente o elija Crear una nueva clave KMS para crear una nueva clave KMS en la consola del Servicio de administración de claves (). AWS AWS KMS

  Para obtener más información sobre DSSE-KMS, consulte Uso del cifrado de doble capa del lado del servidor con claves AWS KMS en la Guía del usuario de Amazon Simple Storage Service.

> **Note**
>
> El uso del DSSE-KMS y las claves conlleva cargos adicionales. AWS KMS Para más información, consulte Precios de AWS KMS.
> Para especificar una AWS KMS clave con un alias que no aparezca en la lista o para usar una AWS KMS clave de otra AWS cuenta, debe usar la. AWS Command Line Interface No se admiten las claves KMS asimétricas. Para obtener más información, consulte Create SMBFile Share in the AWS Storage Gateway API Reference.

> **Important**
>
> Asegúrese de que el recurso compartido de archivos utilice el mismo tipo de cifrado que el bucket de Amazon S3 en el que almacena los datos.

14. Para los tipos MIME de Guess, seleccione el tipo MIME de medios de Guess para permitir que Storage Gateway adivine el tipo de extensión multipropósito de correo de Internet (MIME) de los objetos cargados en función de sus extensiones de archivo.
15. En Nombre del recurso compartido de archivos, introduzca un nombre para el recurso compartido de archivos.

> **Note**
>
> Un nombre de archivo compartido SMB válido no puede contener los siguientes caracteres:`[,,],#,;,<,,>,:,",\,/,, | ? *+`, o caracteres de control ASCII. `1-31`

16. En Cargar eventos, seleccione Registrar un evento cuando la puerta de enlace cargue correctamente un archivo si quiere que la puerta de enlace registre los eventos de CloudWatch registro cuando suba correctamente los archivos a Amazon S3. El retraso de la notificación controla el retraso entre la operación de escritura más reciente del cliente y la generación de la notificación de `ObjectUploaded` registro. Como los clientes pueden realizar muchas escrituras pequeñas en los archivos en poco tiempo, recomendamos configurar este parámetro durante el mayor tiempo posible para evitar generar varias notificaciones para el mismo archivo en rápida sucesión. Para obtener más información, consulte Recibir una notificación de carga de archivos.

> **Note**
>
> Esta configuración no afecta a la hora de carga del objeto a S3, solo a la hora de la notificación.
> Esta configuración no pretende especificar la hora exacta a la que se enviará la notificación. En algunos casos, es posible que la pasarela requiera un tiempo de retraso superior al especificado para generar y enviar las notificaciones.

Elija Siguiente cuando haya terminado.

17. Para el protocolo de uso compartido de archivos, elija SMB.
18. Para la autenticación de usuarios, elija el método de autenticación que desee utilizar en la lista desplegable:

    - Para usar su Microsoft Active Directory corporativo o AWS Managed Microsoft AD para autenticar el acceso de los usuarios a su recurso compartido de archivos SMB, elija Active Directory. Para usar este método, la puerta de enlace debe estar unida a un dominio. Para obtener más información, consulte Uso de Active Directory para autenticar usuarios.

      > **Note**
      >
      > Para AWS Managed Microsoft AD utilizarla con una EC2 puerta de enlace de Amazon, debe crear la EC2 instancia de Amazon en la misma VPC que la AWS Managed Microsoft AD, añadir el grupo de `_workspaceMembers` seguridad a la EC2 instancia de Amazon y unirse al dominio de AD con las credenciales de administrador de. AWS Managed Microsoft AD
      > Para obtener más información al respecto AWS Managed Microsoft AD, consulte la Guía de AWS Directory Service administración.
      > Para obtener más información sobre Amazon EC2, consulte la documentación de Amazon Elastic Compute Cloud.

    Si el estado de unión indica que su puerta de enlace ya está unida a un dominio de Active Directory, continúe con el siguiente paso. De lo contrario, realice lo siguiente:

    1. Elija Configurar.

2. En Dominio, introduzca el nombre del dominio de Active Directory al que desea que se una la puerta de enlace.
3. Introduzca el nombre de usuario y la contraseña que utilizará la puerta de enlace para unirse al dominio.
4. (Opcional) En el caso de la unidad organizativa (OU), introduzca la OU designada que Active Directory utiliza para los nuevos objetos informáticos.
5. (Opcional) Para los controladores de dominio (DC), introduzca el nombre del DC a través del cual la puerta de enlace se conectará a Active Directory. Puede dejar este campo en blanco para permitir que DNS seleccione automáticamente un DC.
6. Elija Unirse a Active Directory.

> **Note**
>
> Al unirse a un dominio, se crea una cuenta de Active Directory en el contenedor predeterminado (que no es una unidad organizativa) y se utiliza el ID de puerta de enlace de la puerta de enlace como nombre de la 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, debe crear esta cuenta con antelación.
> Si su entorno de Active Directory tiene una unidad organizativa designada para los nuevos objetos informáticos, debe especificarla al unirse al dominio.

- Para conceder acceso protegido por contraseña a cualquier persona que proporcione la contraseña de invitado que usted configure, elija Acceso de invitado. No es necesario que File Gateway forme parte de un dominio de Microsoft Active Directory para utilizar este método. Elija Configurar para especificar la contraseña de invitado y, a continuación, seleccione Guardar.

19. Para el acceso de usuario, realice una de las siguientes acciones para especificar qué clientes SMB pueden acceder a su recurso compartido de archivos:

    - Para conceder acceso a todos los usuarios que se hayan autenticado correctamente a través de Active Directory, seleccione Todos los usuarios autenticados por AD.
    - Para permitir o denegar el acceso a usuarios o grupos específicos, elija Usuarios o grupos específicos autenticados por AD y, a continuación, haga lo siguiente:
        - En Usuarios y grupos permitidos, elija Agregar usuario permitido o Agregar grupo permitido e introduzca un usuario o grupo de Active Directory al que desee permitir el acceso a los

archivos compartidos. Repita este proceso para permitir tantos usuarios y grupos como sea necesario

- En el caso de los usuarios y grupos denegados, elija Agregar usuario denegado o Agregar grupo denegado e introduzca un usuario o grupo de Active Directory al que desee denegar el acceso al recurso compartido de archivos. Repita este proceso para denegar tantos usuarios y grupos como sea necesario.

> **Note**
>
> La sección Acceso a archivos compartidos de usuarios y grupos solo aparece si la autenticación de usuario está configurada en Active Directory.
> Al especificar usuarios o grupos, no incluya el dominio. El nombre de dominio está implícito en la pertenencia de la puerta de enlace al Active Directory específico al que está unida.

20. (Opcional) Para los usuarios administradores, introduzca una lista separada por comas de los usuarios y grupos de Active Directory. Los usuarios administradores reciben privilegios para actualizar las listas de control de acceso (ACLs) en todos los archivos y carpetas del recurso compartido de archivos. Los grupos deben llevar el prefijo del @ carácter, por ejemplo,`@group1`.
21. Para el tipo de acceso, seleccione una de las siguientes opciones:

    - Para permitir que los clientes lean y escriban archivos en el recurso compartido de archivos, seleccione Lectura/Escritura.
    - Para permitir que los clientes lean los archivos pero no escriban en el recurso compartido de archivos, seleccione Solo lectura.

    > **Note**
    >
    > En el caso de los recursos compartidos de archivos que están montados en un cliente de Microsoft Windows, si selecciona Solo lectura, es posible que aparezca un mensaje sobre un error inesperado que le impide crear la carpeta. Puede hacer caso omiso del mensaje.

22. En Control de acceso a archivos y directorios, seleccione una de las siguientes opciones:

    - Para establecer permisos detallados en los archivos y carpetas de su recurso compartido de archivos SMB, seleccione Lista de control de acceso de Windows. Para obtener más

información, consulte Uso de Microsoft Windows ACLs para controlar el acceso a un recurso compartido de archivos SMB.

- Para usar los permisos POSIX para controlar el acceso a los archivos y directorios que se almacenan en el recurso compartido de archivos SMB, seleccione los permisos POSIX.

23. Para la enumeración basada en el acceso, realice una de las siguientes acciones:

    - Para que los archivos y las carpetas del recurso compartido sean visibles solo para los usuarios con acceso de lectura, seleccione Ocultar archivos y directorios en los que el usuario no tenga permiso.
    - Para que todos los usuarios puedan ver los archivos y las carpetas del recurso compartido durante la enumeración de directorios, no active la casilla de verificación.

    > **Note**
    >
    > La enumeración basada en el acceso es un sistema que filtra la enumeración de archivos y carpetas de un recurso compartido de archivos SMB en función de las listas de control de acceso del recurso compartido (). ACLs

24. Para ver las opciones de acceso a los archivos, seleccione una de las siguientes opciones:

    - Para optimizar la estrategia de almacenamiento en búfer de archivos del recurso compartido mediante el bloqueo oportunista, seleccione Bloqueo oportunista. En la mayoría de los casos, la activación del bloqueo oportunista mejora el rendimiento, especialmente en lo que respecta a los menús contextuales de Windows.
    - Para permitir que la puerta de enlace, y no el cliente SMB, controle la distinción entre mayúsculas y minúsculas en los nombres de los archivos, seleccione Forzar la distinción entre mayúsculas y minúsculas.
    - Para desactivar ambos ajustes, selecciona Ninguno.

    > **Note**
    >
    > Para evitar conflictos de acceso a los archivos, estas configuraciones se excluyen mutuamente y no se pueden activar al mismo tiempo.

25. (Opcional) Para actualizar la caché automáticamente desde S3, seleccione Establecer intervalo de actualización de la caché y, a continuación, establezca el tiempo en minutos o días para

actualizar la caché del recurso compartido de archivos mediante Time To Live (TTL). TTL es el tiempo transcurrido desde la última actualización. Una vez transcurrido el intervalo TTL, al acceder a un directorio, File Gateway actualiza el contenido de ese directorio desde el bucket de Amazon S3.

> **Note**
>
> Establecer este valor en menos de 30 minutos puede afectar negativamente al rendimiento de la puerta de enlace en situaciones en las que se crean o eliminan con frecuencia grandes cantidades de objetos de Amazon S3.

26. Para la propiedad y los permisos de los archivos, seleccione Otorgar al propietario del bucket de S3 la propiedad total de los archivos creados por la puerta de enlace, incluidos los permisos de lectura, escritura, edición y eliminación si desea que la AWS cuenta propietaria del bucket de S3 tenga el control total de todos los objetos que el recurso compartido de archivos escribe en el bucket.

    Selecciona Siguiente cuando termines.

27. Revise la configuración del recurso compartido de archivos. Seleccione Editar para modificar la configuración de cualquier sección que desee cambiar. Cuando termine, elija Create (Crear).

Una vez creado el recurso compartido de archivos SMB, puede ver sus ajustes de configuración en la consola AWS Storage Gateway, en la pestaña Detalles del recurso compartido de archivos. Para obtener instrucciones sobre cómo montar el recurso compartido de archivos, consulte Montar el recurso compartido de archivos SMB en el cliente.

Montaje y uso del recurso compartido de archivos

En los temas de esta sección se proporcionan instrucciones sobre cómo montar el recurso compartido de archivos en el cliente, utilizar el recurso compartido de archivos, probar la puerta de enlace de archivos y limpiar los recursos que ya no se necesitan, como las puertas de enlace, las EC2 instancias de Amazon o las instalaciones locales VMs que pueda crear con fines de prueba. Para obtener más información sobre los clientes de Network File System (NFS) y Service Message Block (SMB) compatibles, consulte. Clientes NFS y SMB compatibles con File Gateway

> **Note**
>
> AWS Management Console También proporciona ejemplos de comandos que puede utilizar para montar su recurso compartido de archivos.

Temas

- Monte su recurso compartido de archivos NFS en su cliente- Aprenda a montar su recurso compartido de archivos NFS en una unidad de su cliente y a asignarlo a su bucket de Amazon S3.
- Monta tu recurso compartido de archivos SMB en tu cliente- Aprenda a montar su recurso compartido de archivos SMB y a asignarlo a una unidad a la que pueda acceder su cliente.
- Uso de archivos compartidos en depósitos con objetos preexistentes- Aprenda a exportar un recurso compartido de archivos a un bucket de Amazon S3 con objetos creados fuera de File Gateway mediante NFS o SMB.
- Pruebe su S3 File Gateway- Aprenda a probar su puerta de enlace copiando archivos y carpetas a la unidad mapeada y verificando que aparecen automáticamente en su bucket de Amazon S3.

Monte su recurso compartido de archivos NFS en su cliente

Utilice el siguiente procedimiento para montar el recurso compartido de archivos NFS en una unidad de su cliente y asignarlo a su bucket de Amazon S3.

Para montar un recurso compartido de archivos y asignarlo a un bucket de Amazon S3

1. Si está utilizando un cliente de Microsoft Windows, le recomendamos que cree un recurso compartido de archivos SMB y acceda a él mediante un cliente de SMB que ya esté instalado en un cliente de Windows. Si utiliza NFS, active Servicios para NFS en Windows.
2. Monte el recurso compartido de archivos NFS:

   - Para los clientes de Linux, escriba el siguiente comando en el símbolo del sistema.

     sudo mount -t nfs -o nolock,hard *[GatewayVMIPAddress]*:/*[FileShareName]* *[ClientMountPath]*

   - Para los clientes de Windows, escriba el siguiente comando en la línea de comandos (cmd.exe).

     mount -o nolock -o mtype=hard *[GatewayVMIPAddress]*:/*[FileShareName]* *[WindowsDriveLetter]*

   Por ejemplo, supongamos que en un cliente Windows la dirección IP de la máquina virtual es 123.123.1.2 y el nombre del archivo compartido es. `test-fileshare` Suponga también que desea asignar la unidad T. En este caso, el comando será similar al siguiente.

   mount -o nolock -o mtype=hard 123.123.1.2:/test-fileshare T:

   > **Note**
   >
   > Cuando monte recursos compartidos de archivos, tenga en cuenta lo siguiente:
   >
   > - De forma predeterminada, Windows usa un montaje flexible para los recursos compartidos de NFS. Los montajes flexibles agotan el tiempo de espera más fácilmente cuando se producen problemas de conexión. Recomendamos utilizar un montaje duro para cargas de trabajo críticas, ya que los montajes rígidos son más seguros y conservan mejor los datos. Para usar un montaje duro, asegúrese de que el comando utilice el `-o mtype=hard` conmutador.
   > - S3 File Gateway no admite el bloqueo de archivos NFS. Utilice siempre la `-o nolock` opción de desactivar el bloqueo de archivos al montar recursos compartidos de archivos NFS.
   > - Es posible que se dé un caso en el que una carpeta y un objeto existan en un bucket de Amazon S3 y tengan el mismo nombre. En este caso, si el nombre del objeto no

contiene una barra al final, solo la carpeta estará visible en una puerta de enlace de archivos. Por ejemplo, si un depósito contiene un objeto con el nombre `test` o `test/` y una carpeta con el nombre`test/test1`, solo `test/` y `test/test1` están visibles en una puerta de enlace de archivos.

- Puede que sea preciso volver a montar el recurso compartido de archivos después de reiniciar el cliente.
- Si está utilizando clientes de Windows, compruebe sus opciones de `mount` después del montaje ejecutando el comando `mount` sin indicar ninguna opción. La respuesta debe confirmar que el recurso compartido de archivos se ha montado utilizando las últimas opciones que indicó. También debe confirmar que no está utilizando entradas antiguas almacenadas en caché, que tardan al menos 60 segundos en borrarse.

Paso siguiente

Pruebe su S3 File Gateway

Monta tu recurso compartido de archivos SMB en tu cliente

Utilice los siguientes procedimientos para montar el recurso compartido de archivos SMB y asignarlo a una unidad accesible para el cliente. La sección File Gateway de la consola muestra los comandos de montaje compatibles que puede utilizar para los clientes SMB. A continuación, puede encontrar algunas opciones adicionales para probar.

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

- Símbolo del sistema (`cmdkey`y`net use`): utilice el símbolo del sistema para montar el recurso compartido de archivos. Guarde sus credenciales con los `/savecred` conmutadores y`cmdkey`, a continuación, monte la unidad `net use` e `/persistent:yes` inclúyalos si desea que la conexión persista después de que se reinicie el sistema. Los comandos específicos que utilice variarán en función de si desea montar la unidad para el acceso a Microsoft Active Directory (AD) o para el acceso de un usuario invitado. A continuación se proporcionan algunos ejemplos.
- Explorador de archivos (unidad de red de mapas): utilice el Explorador de archivos de Windows para montar el recurso compartido de archivos. Configure los ajustes para especificar si desea que la conexión persista después de que se reinicie el sistema y solicite las credenciales de red.

- PowerShell script: cree un PowerShell script personalizado para montar su recurso compartido de archivos. En función de los parámetros que especifique en el script, la conexión puede ser persistente después de que se reinicie el sistema y el recurso compartido puede estar visible o invisible para el sistema operativo mientras está montado.

> **Note**
>
> Si es un usuario de Microsoft AD, 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.
> Si es un usuario invitado, asegúrese de tener la contraseña del usuario invitado antes de intentar montar el recurso compartido de archivos.

Para montar el recurso compartido de archivos SMB para los usuarios autorizados de Microsoft AD mediante la línea de comandos:

1. Asegúrese de que el usuario de Microsoft AD tiene los permisos necesarios para el recurso compartido de archivos SMB antes de montarlo en el sistema del usuario.
2. Introduzca lo siguiente en la línea de comandos para montar el recurso compartido de archivos:

   ```
   net use WindowsDriveLetter: \\GatewayIPAddress\FileShareName /
   persistent:yes
   ```

Para montar el recurso compartido de archivos SMB con una combinación de credenciales de inicio de sesión específica mediante la línea de comandos:

1. Asegúrese de que el usuario tenga acceso al recurso compartido de archivos SMB antes de montarlo en el sistema.
2. Introduzca lo siguiente en la línea de comandos para guardar las credenciales de usuario en el Administrador de credenciales de Windows:

   ```
   cmdkey /add:GatewayIPAddress /user:DomainName\UserName /pass:Password
   ```
3. Introduzca lo siguiente en la línea de comandos para montar el recurso compartido de archivos:

   ```
   net use WindowsDriveLetter: \\GatewayIPAddress\FileShareName /
   persistent:yes /savecred
   ```

Para montar el recurso compartido de archivos SMB para los usuarios invitados mediante la línea de comandos:

1. Asegúrese de tener la contraseña del usuario invitado antes de montar el recurso compartido de archivos.
2. Escriba lo siguiente en la línea de comandos para guardar las credenciales de invitado en el Administrador de credenciales de Windows:

   ```
   cmdkey /add:GatewayIPAddress /user:DomainName\smbguest /pass:Password
   ```

3. Escriba lo siguiente en la línea de comandos.

   ```
   net use WindowsDriveLetter: \\$GatewayIPAddress\$Path /user:$Gateway
   ID\smbguest /persistent:yes /savecred
   ```

> **Note**
>
> Cuando monte recursos compartidos de archivos, tenga en cuenta lo siguiente:
>
> - Es posible que se dé un caso en el que una carpeta y un objeto existan en un bucket de Amazon S3 y tengan el mismo nombre. En este caso, si el nombre del objeto no contiene una barra al final, solo la carpeta estará visible en una puerta de enlace de archivos. Por ejemplo, si un depósito contiene un objeto con el nombre `test` o `test/` y una carpeta con el nombre`test/test1`, solo `test/` y `test/test1` están visibles en una puerta de enlace de archivos.
> - A menos que configure la conexión del recurso compartido de archivos para guardar las credenciales de usuario y conservarlas durante los reinicios del sistema, es posible que tenga que volver a montar el recurso compartido de archivos cada vez que reinicie el sistema cliente.

Para 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 Search Windows o pulse **`Win+E`**.
2. En el panel de navegación, elija Este PC. A continuación, en la pestaña Ordenador, selecciona Map Network Drive.

3. En el cuadro de diálogo Map Network Drive, elija una letra de unidad en Drive.
4. En Folder, escriba ***[File Gateway IP]**[SMB File Share Name]*** o elija Browse 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 Connect using different credentials si desea que el usuario introduzca las credenciales de inicio de sesión de Microsoft AD o la contraseña del usuario de la cuenta de invitado.
7. Elija Finish para finalizar el punto de montaje.

> **Note**
>
> Todos los archivos o directorios que comiencen con un punto (`.`) se marcarán ocultos en Windows. Para que estos archivos y directorios estén visibles, debe seleccionar la casilla de verificación Elementos ocultos en la pestaña Ver del Explorador de archivos de Windows.

Puede editar la configuración del recurso compartido de archivos, modificar los usuarios y grupos a los que se permite o deniega el acceso, y cambiar la contraseña de acceso de invitado desde la consola de administración de Storage Gateway. También puede actualizar los datos de la memoria caché del recurso compartido de archivos y eliminar un recurso compartido de archivos desde la consola.

Para modificar las propiedades del recurso compartido de archivos SMB

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. En el panel de navegación, elija File Shares.
3. En la página File Share, seleccione la casilla situada junto al recurso compartido de archivos SMB que desea modificar.
4. En Actions, elija la acción que desea:

   - Elija Edit file share settings para modificar el acceso compartido.
   - Seleccione Editar allowed/denied usuarios para añadir o eliminar usuarios y grupos y, a continuación, escriba los usuarios y grupos permitidos y denegados en los cuadros Usuarios permitidos, Usuarios denegados, Grupos permitidos y Grupos denegados. Utilice los botones Add Entry para crear nuevos derechos de acceso y el botón (X) para eliminar el acceso.

> **Note**
>
> Los grupos deben llevar el prefijo del @ carácter. Los formatos aceptables incluyen:`DOMAIN\User1`, `user1@group1`, y`@DOMAIN\group1`.

5. Cuando haya terminado, elija Save.

   Al introducir los usuarios y grupos permitidos, se crea una lista de usuarios permitidos. Sin una lista de permitidos, todos los usuarios autenticados de Microsoft AD pueden acceder al recurso compartido de archivos SMB. Los usuarios y grupos que estén marcados como denegados se añadirán a una lista de denegaciones y no podrán acceder al recurso compartido de archivos SMB. En los casos en que un usuario o grupo se encuentra tanto en la lista de denegación como en la lista de permitidos, la lista de denegación tiene prioridad.

   Puede activar las listas de control de acceso (ACLs) en su recurso compartido de archivos SMB. Para obtener información sobre cómo activarlas ACLs, consulteUso de Windows ACLs para limitar el acceso a los archivos compartidos en pequeñas y medianas empresas.

Paso siguiente

Pruebe su S3 File Gateway

Uso de archivos compartidos en depósitos con objetos preexistentes

Puede exportar un recurso compartido de archivos a un bucket de Amazon S3 con objetos creados fuera de File Gateway mediante NFS o SMB. Los objetos del bucket creados fuera de la gateway se muestran como archivos en el sistema de archivos NFS o SMB cuando los clientes del sistema de archivos tienen acceso a ellos. En el recurso compartido de archivos, se utilizan el acceso y los permisos POSIX (Portable Operating System Interface) estándar. Cuando vuelve a escribir archivos en un bucket de Amazon S3, los archivos asumen las propiedades y los derechos de acceso que les ha otorgado.

Se pueden cargar objetos en un bucket de S3 en cualquier momento. Para que el recurso compartido de archivos muestre estos objetos que se acaban de añadir como archivos, primero es necesario actualizar el bucket de S3. Para obtener más información, consulte the section called “Actualización de la caché de objetos del bucket de Amazon S3”.

> **Note**
>
> No recomendamos tener varios escritores para un bucket de Amazon S3. Si es así, asegúrese de leer la sección «¿Puedo tener varios grabadores en mi bucket de Amazon S3?» en las Preguntas frecuentes sobre Storage Gateway.

Para asignar los valores predeterminados de los metadatos para los objetos a los que se ha tenido acceso mediante NFS, consulte Edición de los valores predeterminados de los metadatos en Administración de su Amazon S3 File Gateway.

En el caso de las pequeñas y medianas empresas, puede exportar un recurso compartido mediante Microsoft AD o mediante el acceso de invitado a un bucket de Amazon S3 con objetos preexistentes. Los objetos exportados a través de un recurso compartido de archivos SMB heredan los propietarios y los permisos de POSIX del directorio principal situado en el nivel inmediatamente superior. Para los objetos de la carpeta raíz, se heredan las listas de control de acceso (ACL) raíz. Para la ACL raíz, el propietario es `smbguest` y los permisos de los archivos son 666, y los de los directorios son 777. Esto se aplica a todas las formas de acceso autenticado (Microsoft AD y de invitado)

Pruebe su S3 File Gateway

Utilice el siguiente procedimiento para probar su puerta de enlace copiando archivos y carpetas en la unidad mapeada y verificando que aparecen automáticamente en su bucket de Amazon S3.

Para cargar archivos desde su cliente de Windows a Amazon S3

1. En el cliente Windows, vaya a la unidad en la que montó el recurso compartido de archivos. El nombre de la unidad va precedido del nombre del bucket de S3.
2. Copie archivos o una carpeta en la unidad.
3. En la consola de administración de Amazon S3, navegue hasta el bucket asignado. Debería ver los archivos y las carpetas que copió en el bucket de Amazon S3 que especificó.

   Puede ver el recurso compartido de archivos que creó en la pestaña Archivos compartidos de la consola de administración AWS de Storage Gateway.

El cliente de NFS o SMB puede escribir, leer, eliminar, renombrar y truncar archivos.

> **Note**
>
> Las pasarelas de archivos no admiten la creación de enlaces físicos o simbólicos en un recurso compartido de archivos.

Tenga en cuenta los siguientes puntos sobre cómo funcionan las pasarelas de archivos con S3:

- Las lecturas se entregan desde una caché de lectura previa. En otras palabras, si los datos no están disponibles, se obtienen de S3 y se añaden a la caché.
- Las escrituras se envían a S3 a través de cargas multiparte optimizadas mediante una caché de retroescritura.
- Las lecturas y escrituras se optimizan de tal forma que solamente se transfieren a través de la red las partes solicitadas o modificadas.
- Las eliminaciones quitan los objetos de S3.
- Los directorios se administran como objetos de carpeta en S3, con la misma sintaxis que en la consola de Amazon S3. A los directorios vacíos se les puede cambiar el nombre.
- El rendimiento del funcionamiento del sistema de archivos recursivo (por ejemplo, `ls -l`) depende del número de objetos del bucket.

Administración de su Amazon S3 File Gateway

Los temas de esta sección proporcionan información sobre cómo administrar los recursos de Amazon S3 File Gateway. La administración de puertas de enlace incluye la concesión de permisos para que su puerta de enlace acceda a los recursos compartidos de archivos y a los buckets de Amazon S3, la edición de la información y la configuración de las puertas de enlace y los recursos compartidos de archivos, la eliminación de archivos compartidos, la actualización de los objetos en caché y la comprensión de los indicadores del estado operativo de las puertas de enlace y los recursos compartidos de archivos.

Temas

- Edite la información básica de la pasarela- Aprenda a 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.
- Otorgar acceso y permisos- Aprenda a utilizar las funciones de IAM para proporcionar a su puerta de enlace permisos de acceso para los buckets de Amazon S3 y los puntos de enlace de Amazon VPC, evitar determinados problemas de seguridad y conectar los archivos compartidos a los buckets de todas las cuentas. AWS
- Eliminar un archivo compartido- Aprenda a eliminar un archivo compartido mediante la consola Storage Gateway.
- Edición de la configuración SMB de la pasarela- Aprenda a editar la configuración de SMB a nivel de puerta de enlace que controla la estrategia de seguridad, la autenticación de Active Directory, el acceso de invitados, los permisos de los grupos locales y la visibilidad de los archivos compartidos de archivos SMB en una puerta de enlace.
- Edita la configuración de uso compartido de archivos SMB- Aprenda a editar los ajustes para configurar el nombre, el registro, la actualización de la caché, la clase de almacenamiento, la exportación de archivos y mucho más para un recurso compartido de archivos SMB.
- Limite el acceso a los archivos compartidos SMB- Aprenda a añadir usuarios o grupos permitidos o denegados para limitar el acceso a su recurso compartido de archivos SMB.
- Edita la configuración de uso compartido de archivos NFS- Aprenda a editar los ajustes para configurar el nombre, el registro, la actualización de la caché, la clase de almacenamiento, la exportación de archivos y mucho más para un recurso compartido de archivos NFS.

- Edite los valores predeterminados de los metadatos de los archivos compartidos de NFS- Aprenda a editar los valores de metadatos predeterminados que incluyen los permisos de Unix para los archivos y carpetas de los recursos compartidos de archivos NFS.
- Limite el acceso a los archivos compartidos de NFS- Aprenda a limitar el acceso a los clientes desde direcciones IP o rangos de IP específicos para su recurso compartido de archivos NFS.
- Actualización de la caché de objetos del bucket de Amazon S3- Aprenda a actualizar la caché de objetos del bucket de S3 para un recurso compartido de archivos y a configurar un programa para actualizar la caché automáticamente.
- Usar Bloqueo de objetos de S3- Obtenga información sobre cómo funciona Amazon S3 File Gateway con la función S3 Object Lock.
- Estado del uso compartido de archivos- Aprenda a ver e interpretar el estado de los archivos compartidos.
- Estado de la pasarela- Aprenda a ver e interpretar el estado de la puerta de enlace.
- Administración del ancho de banda de su Amazon S3 File Gateway- Aprenda a limitar el rendimiento de carga desde su puerta de enlace AWS para controlar la cantidad de ancho de banda de red que utiliza la puerta de enlace.

Edite la información básica de una pasarela de archivos S3

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.

Para 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.

Otorgar acceso y permisos para compartimentos y depósitos de archivos

Una vez que su puerta de enlace de archivos S3 esté activada y en funcionamiento, podrá añadir recursos compartidos de archivos adicionales y conceder acceso a los depósitos de Amazon S3, incluidos los depósitos situados en zonas Cuentas de AWS distintas de sus puertas de enlace y recursos compartidos de archivos. En las siguientes secciones, se describe cómo utilizar las funciones de IAM para proporcionar a su puerta de enlace permisos de acceso para los buckets de Amazon S3 y los puntos de enlace de VPC, evitar determinados problemas de seguridad y conectar los recursos compartidos de archivos a los buckets cruzados. Cuentas de AWS

Para obtener información sobre cómo crear un nuevo recurso compartido de archivos, consulte. Creación de un recurso compartido de archivos

Esta sección contiene los siguientes temas, que proporcionan información adicional sobre cómo conceder acceso y permisos para los recursos compartidos de archivos y los buckets de Amazon S3:

Temas

- Concesión de acceso a un bucket de Amazon S3- Aprenda a conceder acceso a su File Gateway para cargar archivos en su bucket de Amazon S3 y realizar acciones en cualquier punto de acceso o punto de enlace de Amazon Virtual Private Cloud (Amazon VPC) que utilice para conectarse al bucket.
- Prevención de la sustitución confusa entre servicios- Aprenda a evitar un problema de seguridad común en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción.
- Uso de un recurso compartido de archivos para el acceso entre cuentas- Aprenda a conceder acceso a una cuenta de Amazon Web Services y a los usuarios de esa cuenta para que accedan a los recursos que pertenecen a otra cuenta de Amazon Web Services.

Concesión de acceso a un bucket de Amazon S3

Al crear un recurso compartido de archivos, su File Gateway necesita acceso para cargar archivos en su bucket de Amazon S3 y para realizar acciones en cualquier punto de acceso o punto final de nube privada virtual (VPC) que utilice para conectarse al bucket. Para conceder este acceso, su File Gateway asume una función AWS Identity and Access Management (IAM) asociada a una política de IAM que concede este acceso.

El rol requiere esta política de IAM y una relación de confianza de Security Token Service (STS). La política determina qué acciones puede realizar el rol. Además, su bucket de S3 y cualquier punto de acceso o punto de enlace de VPC asociado deben tener una política de acceso que permita al rol de IAM acceder a ellos.

Puede crear el rol y la política de acceso usted mismo, o File Gateway puede crearlos por usted. Si File Gateway crea la política por usted, la política contendrá una lista de acciones de S3. Para obtener información sobre las funciones y los permisos, consulte Crear una función para delegar permisos a una Servicio de AWS en la Guía del usuario de IAM.

El siguiente ejemplo es una política de confianza que permite a File Gateway asumir una función de IAM.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "storagegateway.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Important

Storage Gateway puede asumir las funciones de servicio existentes que se transfieren mediante la acción de `iam:PassRole` política, pero no admite las políticas de IAM que utilizan la clave de `iam:PassedToService` contexto 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: transfiere 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

Si no quiere que File Gateway cree una política en su nombre, puede crear su propia política y adjuntarla a su recurso compartido de archivos. Para obtener más información acerca de cómo hacerlo, consulte Creación de un recurso compartido de archivos.

El siguiente ejemplo de política permite a File Gateway realizar todas las acciones de Amazon S3 enumeradas en la política. La primera parte de la declaración permite que todas las acciones que se muestran se realicen en el bucket de S3 denominado `amzn-s3-demo-bucket`. La segunda parte permite las acciones que se muestran en todos los objetos de `amzn-s3-demo-bucket`.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:GetAccelerateConfiguration",
                "s3:GetBucketLocation",
                "s3:GetBucketVersioning",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:ListBucketMultipartUploads"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectVersion",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Effect": "Allow"
        }
    ]
}
```

El siguiente ejemplo de política es similar a la anterior, pero permite a File Gateway realizar las acciones necesarias para acceder a un bucket a través de un punto de acceso.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectVersion",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:us-east-1:111122223333:accesspoint/
TestAccessPointName/*",
            "Effect": "Allow"
        }
    ]
}
```

> **Note**
>
> Si necesita conectar su recurso compartido de archivos a un bucket de S3 a través de un punto de enlace de VPC, consulte las políticas de puntos de conexión para Amazon S3 en la Guía del AWS PrivateLink usuario.

> **Note**
>
> En el caso de los depósitos cifrados, el recurso compartido de archivos debe usar la clave de la cuenta del bucket de S3 de destino.

> **Note**
>
> Si su puerta de enlace de archivos utiliza SSE-KMS o DSSE-KMS para el cifrado, asegúrese de que la función de IAM asociada al recurso compartido de archivos incluya los permisos KMS:Encrypt, KMS:Decrypt, kms: *, kms: y kms:. ReEncrypt GenerateDataKey DescribeKey Para obtener más información, consulte Uso de políticas basadas en la identidad (políticas de IAM) para Storage Gateway.

Prevención de la sustitución confusa entre servicios

El problema de la sustitución confusa es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación de identidad entre servicios puede provocar el confuso problema de un diputado. La suplantación entre servicios puedes producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio que lleva a cabo las llamadas se puedes manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente de una manera en la que no debe tener permiso para acceder. Para evitarlo, AWS proporciona herramientas que lo ayudan a proteger sus datos para todos los servicios con entidades principales de servicio a las que se les ha dado acceso a los recursos de su cuenta.

Se recomienda utilizar las claves de contexto de condición `aws:SourceAccount`global `aws:SourceArn`y las claves de contexto en las políticas de recursos para limitar los permisos que se AWS Storage Gateway otorgan a otro servicio al recurso. Si se utilizan ambas claves contextuales de condición global, el valor `aws:SourceAccount` y la cuenta del valor `aws:SourceArn` deben utilizar el mismo ID de cuenta cuando se utilicen en la misma declaración de política.

El valor de `aws:SourceArn` debe ser el ARN del Storage Gateway al que está asociado el recurso compartido de archivos.

La forma más eficaz de protegerse contra el problema de la sustitución confusa es utilizar la clave de contexto de condición global de `aws:SourceArn` con el ARN completo del recurso. Si no conoce el ARN completo del recurso o si especifica varios recursos, utiliza la clave de condición de contexto global `aws:SourceArn` con comodines (*) para las partes desconocidas del ARN. Por ejemplo, `arn:aws:`*`servicename`*`::`*`123456789012`*`:*`.

El siguiente ejemplo muestra cómo se pueden utilizar las claves de contexto de condición `aws:SourceAccount` global `aws:SourceArn` y las claves de contexto de Storage Gateway para evitar el confuso problema de los adjuntos.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "storagegateway.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:storagegateway:us-east-1:123456789012:gateway/
sgw-712345DA"
        }
      }
    }
  ]
}
```

Uso de un recurso compartido de archivos para el acceso entre cuentas

El acceso entre cuentas se produce cuando una cuenta de Amazon Web Services y los usuarios de esa cuenta tienen acceso a los recursos que pertenecen a otra cuenta de Amazon Web Services. Con File Gateways, puede utilizar un recurso compartido de archivos de una cuenta de Amazon Web Services para acceder a los objetos de un bucket de Amazon S3 que pertenezca a otra cuenta de Amazon Web Services.

Para usar un recurso compartido de archivos propiedad de una cuenta de Amazon Web Services para acceder a un bucket de S3 en otra cuenta de Amazon Web Services

1. Asegúrese de que el propietario del bucket de S3 haya concedido a su cuenta de Amazon Web Services acceso al bucket de S3 al que necesita acceder y a los objetos de ese bucket. Para obtener información sobre cómo conceder este acceso, consulte el Ejemplo 2: El propietario de un bucket concede permisos de bucket para varias cuentas en la Guía del usuario de Amazon Simple Storage Service. Para obtener una lista de los permisos necesarios, consulte Concesión de acceso a un bucket de Amazon S3.

2. Asegúrese de que el rol de IAM que utiliza el recurso compartido de archivos para obtener acceso al bucket de S3 incluya permisos para operaciones como `s3:GetObjectAcl` y `s3:PutObjectAcl`. Asegúrese también de que el rol de IAM incluya una política de confianza que permita a su cuenta para adoptar dicho rol. Para ver un ejemplo de esta política de confianza, consulte Concesión de acceso a un bucket de Amazon S3.

   Si el recurso compartido de archivos utiliza un rol existente para obtener acceso al bucket de S3, se deben incluir permisos para las operaciones `s3:GetObjectAcl` y `s3:PutObjectAcl`. El rol también necesita una política de confianza que permita a su cuenta asumir este rol. Para ver un ejemplo de esta política de confianza, consulte Concesión de acceso a un bucket de Amazon S3.
3. Elija los archivos Gateway a los que pueda acceder el propietario del bucket de S3 al crear el recurso compartido de archivos o al editar la configuración de uso compartido de archivos en el hogar. https://console.aws.amazon.com/storagegateway/

Una vez que haya creado o actualizado el recurso compartido de archivos para el acceso entre cuentas y lo haya montado localmente, recomendamos encarecidamente que pruebe la configuración. Puede hacerlo mostrando el contenido del directorio o escribiendo archivos de prueba y asegurándose de que los archivos aparecen como objetos en el bucket de S3.

> **Important**
>
> Asegúrese de configurar las políticas correctamente para conceder acceso entre cuentas a la cuenta utilizada por el recurso compartido de archivos. Si no lo hace, las actualizaciones de los archivos a través de sus aplicaciones locales no se propagarán al bucket de Amazon S3 con el que esté trabajando.

Recursos

Para obtener más información sobre políticas de acceso y listas de control de acceso, consulte los siguientes temas:

Directrices para usar las opciones de política de acceso disponibles en la Guía del usuario de Amazon Simple Storage Service

Información general sobre la lista de control de acceso (ACL) en la Guía del usuario de Amazon Simple Storage Service

Eliminar un archivo compartido

Si ya no necesita un recurso compartido de archivos, puede eliminarlo de la consola Storage Gateway. Al eliminar un recurso compartido de archivos, la puerta de enlace se separa del depósito de Amazon S3 al que se asigna el recurso compartido de archivos. Sin embargo, el bucket de S3 y su contenido no se eliminan.

Si la gateway está cargando datos en un bucket de S3 en el momento de eliminar un recurso compartido de archivos, el proceso de eliminación no se completa hasta que todos los datos se hayan cargado. El recurso compartido de archivos estará en estado DELETING hasta que los datos se hayan cargado por completo.

Si no desea esperar a que los datos estén totalmente cargados, consulte el procedimiento para eliminar un recurso compartido de archivos de manera forzada que se explica más adelante en este tema.

Para eliminar un recurso compartido de archivos

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Seleccione Recursos compartidos de archivos y, a continuación, seleccione uno o más recursos compartidos de archivos para eliminarlos.
3. En ActionsAPI (Acciones), elija Delete file share (Eliminar recurso compartido de archivos). Aparece el cuadro de diálogo de confirmación.
4. Compruebe que desea eliminar los archivos compartidos especificados, escriba la palabra eliminar en el cuadro de confirmación y seleccione Eliminar.

En algunos casos, es posible que no quiera esperar hasta que todos los datos escritos en archivos del recurso compartido de archivos Network File System (NFS) se carguen antes de eliminar dicho recurso. Por ejemplo, es posible que desee descartar intencionadamente los datos que se escribieron pero que aún no se han cargado, o es posible que el depósito de Amazon S3 que respalda el archivo compartido ya se haya eliminado, lo que significa que ya no es posible cargar los datos especificados.

En estos casos, puede eliminar por la fuerza el recurso compartido de archivos mediante la operación AWS Management Console o la API. `DeleteFileShare` Esta operación detiene el proceso de carga de datos. Cuando concluya este procedimiento, el recurso compartido de archivos pasa al estado FORCE_DELETING. Para eliminar por la fuerza un recurso compartido de archivos mediante la consola Storage Gateway, consulte el procedimiento siguiente.

Para eliminar un recurso compartido de archivos de manera forzada

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. En la página de lista de archivos compartidos, seleccione el recurso compartido de archivos que ha marcado para su eliminación en el procedimiento anterior para ver sus detalles. Transcurridos unos segundos, aparecerá un mensaje de notificación de eliminación en la pestaña Detalles.
3. En el mensaje que aparece en la pestaña Detalles, compruebe el ID del archivo compartido que desea eliminar por la fuerza, active la casilla de confirmación y elija Forzar la eliminación ahora.

> **Note**
>
> La eliminación forzada no se puede deshacer.
> Al eliminar por la fuerza un archivo compartido, es posible que algunos archivos transferidos parcialmente procedentes de cargas múltiples permanezcan en Amazon S3, donde pueden incurrir en gastos de almacenamiento. Recomendamos configurar una regla del ciclo de vida de los buckets de Amazon S3 para eliminar estas partes del archivo automáticamente. Para obtener más información, consulte Prácticas recomendadas: gestión de cargas de varias partes.

También puedes usar la operación de la DeleteFileShareAPI para eliminar por la fuerza el recurso compartido de archivos. La eliminación de un archivo compartido mediante la API requiere el permiso de la política de `storagegateway:DeleteFileShare` IAM.

Editar la configuración SMB de una puerta de enlace

La configuración de SMB a nivel de puerta de enlace permite configurar la estrategia de seguridad, la autenticación de Active Directory, el acceso de invitados, los permisos de los grupos locales y la visibilidad de los archivos compartidos de archivos SMB de una puerta de enlace.

Para editar la configuración de SMB a nivel de puerta de enlace

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Elija Gateways y, a continuación, elija la puerta de enlace en la que desee editar la configuración de SMB.
3. En el menú desplegable Acciones, selecciona Editar la configuración de SMB y, a continuación, selecciona la configuración que deseas editar.

Esta sección contiene los siguientes temas, que proporcionan información y procedimientos adicionales relacionados con la configuración de cada uno de los ajustes SMB individuales de su puerta de enlace.

Temas

- Establezca el nivel de seguridad de la pasarela- Aprenda a establecer un nivel de seguridad para especificar los requisitos de conexión, como la firma y el cifrado del bloque de mensajes del servidor (SMB), y si se deben permitir las conexiones desde clientes SMB de la versión 1.
- Configure la autenticación de Active Directory- Aprenda a configurar su Active Directory corporativo o Microsoft AD AWS administrado para el acceso autenticado por el usuario a su recurso compartido de archivos SMB.
- Proporcione acceso como invitado- Aprenda a configurar su puerta de enlace para permitir el acceso de invitados a cualquier usuario que proporcione el nombre de usuario y la contraseña correctos de la cuenta de invitado.
- Configure los grupos locales- Aprenda a configurar grupos locales para conceder a los usuarios de Active Directory permisos especiales para compartir archivos.
- Configura la visibilidad de los archivos compartidos- Aprenda a especificar si los recursos compartidos de una puerta de enlace están visibles al publicar los recursos compartidos para los usuarios.

Establezca un nivel de seguridad para su puerta de enlace

Al utilizar una puerta de enlace de archivos S3, puede especificar un nivel de seguridad para la puerta de enlace. Al especificar este nivel de seguridad, puede establecer si su puerta de enlace debe requerir la firma del bloque de mensajes del servidor (SMB) o el cifrado SMB, o si desea permitir la versión 1 de SMB.

Para configurar el nivel de seguridad

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Elija Gateways y, a continuación, elija la puerta de enlace en la que desee editar la configuración de SMB.
3. En el menú desplegable Acciones, selecciona Editar la configuración de SMB y, a continuación, selecciona la 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, consulta la sección SMBSecurityEstrategia de actualización en la referencia de la AWS Storage Gateway API.
> Un nivel de estrategia de seguridad más alto puede afectar al rendimiento de la puerta de enlace.

- Imponer el AES256 cifrado: si elige esta opción, S3 File Gateway solo permite las conexiones desde SMBv3 clientes que utilicen algoritmos de cifrado AES de 256 bits. No se permiten los algoritmos de 128 bits. Esta opción se recomienda para entornos que manejan datos confidenciales. Funciona con todos los clientes SMB actuales de Microsoft Windows.
- Imponer el cifrado: si elige esta opción, S3 File Gateway solo permite las conexiones desde SMBv3 clientes que tengan el cifrado activado. Se permiten algoritmos de 256 y 128 bits. Esta opción se recomienda para entornos que manejan datos confidenciales. Funciona con todos los clientes SMB actuales de Microsoft Windows.
- Forzar la firma: si elige esta opción, S3 File Gateway solo permite conexiones desde SMBv2 SMBv3 clientes que tengan activada la firma. Esta opción funciona con todos los clientes SMB actuales de Microsoft Windows.
- Negociado por el cliente: si elige esta opción, las solicitudes se establecen en función de lo negociado por el cliente. Esta opción es recomendable cuando desea maximizar la compatibilidad con distintos clientes de su entorno.

> **Note**
>
> Para las gateway activadas antes del 20 de junio de 2019 el nivel de seguridad predeterminado esClient negotiated (negociado con el cliente).
> Para las gateway activadas el 20 de junio de 2019 y posteriormente, el nivel de seguridad predeterminado es Enforce encryption (Activar cifrado).

5. Seleccione Save.

Use Active Directory para autenticar a los usuarios

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

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

También puede activar las listas de control de acceso (ACLs) en su recurso compartido de archivos SMB. Para obtener información sobre cómo activarlas ACLs, consulteUso de Windows ACLs para limitar el acceso a los archivos compartidos en pequeñas y medianas empresas.

Para activar la autenticación de Active Directory

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Elija Gateways y, a continuación, elija la puerta de enlace en la que desee editar la configuración de SMB.
3. En el menú desplegable Acciones, elija Editar la configuración de SMB y, a continuación, elija la configuración de Active Directory.
4. En Nombre de dominio, introduzca el nombre del dominio de Active Directory al que desee que se una a 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 Requisitos de permiso de la Directory.
> Al unirse a un dominio, se crea una cuenta de equipo de Active Directory en el contenedor de equipos predeterminado (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 informáticos, 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 el campo Usuario de dominio y Contraseña de 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 la unidad organizativa (OU), introduzca la OU designada que Active Directory utilizará para los nuevos objetos informáticos.
7. (Opcional) En el caso de 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 DC.
8. Seleccione Save changes (Guardar cambios).

Para limitar el acceso a los recursos compartidos de archivos a determinados usuarios y grupos de AD

1. En la consola Storage Gateway, elija el recurso compartido de archivos al que desee limitar el acceso.
2. En el menú desplegable Acciones, seleccione Editar la configuración de acceso a los archivos compartidos.

3. En la sección Acceso a archivos compartidos de usuarios y grupos, selecciona tu configuración.

   En Usuarios y grupos permitidos, selecciona Añadir usuario permitido o Añadir grupo permitido e introduce un usuario o grupo de AD al que quieras permitir el acceso a los archivos compartidos. Repite este proceso para permitir tantos usuarios y grupos como sea necesario.

   En el caso de los usuarios y grupos denegados, seleccione Añadir usuario denegado o Añadir grupo denegado e introduzca un usuario o grupo de AD al que desee denegar el acceso a los archivos compartidos. Repita este proceso para denegar tantos usuarios y grupos como sea necesario.

   > **Note**
   >
   > La sección Acceso a archivos compartidos de usuarios y grupos solo aparece si se selecciona Active Directory.
   > Los grupos deben llevar el prefijo del @ carácter. Los formatos aceptables incluyen:`DOMAIN\User1`, `user1@group1`, y`@DOMAIN\group1`.
   > Si configura listas de usuarios y grupos permitidos y denegados, Windows ACLs no concederá ningún acceso que invalide esas listas.
   > Las listas de usuarios y grupos permitidos y denegados se evalúan previamente ACLs y controlan qué usuarios pueden montar el recurso compartido de archivos o acceder a él.
   > Si se incluye algún usuario o grupo en la lista de permitidos, la lista se considera activa y solo esos usuarios pueden montar el recurso compartido de archivos.
   > Una vez que un usuario haya montado un recurso compartido de archivos, ofrezca una protección más detallada que ACLs controle a qué archivos o carpetas específicos puede acceder el usuario. Para obtener más información, consulte Activar Windows ACLs en un nuevo recurso compartido de archivos SMB.

4. Cuando termine de añadir entradas, elija Save (Guardar).

Proporcione acceso como invitado a su recurso compartido de archivos

Puede configurar su S3 File Gateway para permitir el acceso como invitado a cualquier usuario que pueda proporcionar el nombre de usuario y la contraseña correctos de la cuenta de invitado. Si desea que este sea el único método mediante el cual los usuarios puedan acceder a la puerta de enlace de archivos, no necesita unir la puerta de enlace a un dominio de Microsoft Active Directory. También puede usar este método de acceso como invitado para crear recursos compartidos de

archivos en una puerta de enlace de archivos de S3 que sea miembro de un dominio de Active Directory.

Al configurar un recurso compartido de archivos para que utilice el método de autenticación de acceso de invitado, el nombre de usuario de acceso de invitado es`smbguest`. Antes de poder crear un recurso compartido de archivos mediante el acceso de invitado, debe cambiar la contraseña predeterminada del `smbguest` usuario.

Puede utilizar el siguiente procedimiento para cambiar la contraseña del usuario invitado`smbguest`.

Para cambiar la contraseña de acceso de invitado

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Seleccione Puertas de enlace en el panel de navegación situado en la parte izquierda de la página de la consola y, a continuación, elija el nombre de la puerta de enlace a la que desea proporcionar acceso como invitado.
3. En el menú desplegable Acciones, seleccione Editar la configuración de SMB y, a continuación, elija la configuración de acceso como invitado.
4. En Contraseña de invitado, introduce la contraseña de acceso de invitado que deseas configurar y, a continuación, selecciona Guardar cambios.

Configura grupos locales para tu puerta de enlace

La configuración del grupo local le permite conceder a los usuarios o grupos de Active Directory permisos especiales para los recursos compartidos de archivos SMB de su puerta de enlace.

Puede usar la configuración del grupo local para asignar permisos de administrador de Gateway. Los administradores de Gateway pueden usar el complemento Carpetas compartidas de Microsoft Management Console para forzar el cierre de los archivos que están abiertos y bloqueados.

> **Note**
>
> Debe agregar al menos un usuario o grupo de administradores de la puerta de enlace para poder unir la puerta de enlace a un dominio de Active Directory.

Para asignar administradores de Gateway

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

2. Elija Gateways y, a continuación, elija la puerta de enlace en la que desee editar la configuración de SMB.
3. En el menú desplegable Acciones, selecciona Editar la configuración de SMB y, a continuación, selecciona la configuración del grupo local.
4. En la sección de configuración del grupo local, selecciona tu configuración. Esta sección solo aparece para los archivos compartidos que utilizan Active Directory.

   En el caso de los administradores de Gateway, añada los usuarios y grupos de Active Directory a los que desee conceder permisos de administrador de Gateway locales. Agregue un usuario o grupo por línea, incluido el nombre de dominio. Por ejemplo, **`corp\Domain Admins`**. Para crear líneas adicionales, elija Agregar nuevo administrador de Gateway.

   > **Note**
   >
   > Al editar Gateway Admins, se desconectan y vuelven a conectar todos los archivos compartidos SMB.

5. Seleccione Guardar cambios y, a continuación, pulse Continuar para confirmar el mensaje de advertencia que aparece.

Configura la visibilidad de los archivos compartidos

La visibilidad de los archivos compartidos controla si los recursos compartidos de una pasarela están visibles al enumerarlos para los usuarios, por ejemplo, en una vista de red o en una lista de navegación. Si los archivos compartidos de una puerta de enlace están visibles, los clientes pueden descubrirlos fácilmente mediante un explorador de archivos si conocen la dirección IP o el nombre DNS de la puerta de enlace. Si los recursos compartidos de archivos no están visibles, los clientes deben conocer el nombre del recurso compartido de archivos además de la IP o el nombre DNS de la puerta de enlace para poder detectarlos.

> **Note**
>
> Esta configuración no es un método eficaz para proteger el acceso a los archivos compartidos de su implementación. Por motivos de seguridad, recomendamos configurar los permisos para limitar el acceso a usuarios y grupos específicos. Para obtener instrucciones, consulte Limitar el acceso de usuarios y grupos a su recurso compartido de archivos SMB.

Para configurar la visibilidad de los archivos compartidos

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Elija Gateways y, a continuación, elija la puerta de enlace en la que desee editar la configuración de SMB.
3. En el menú desplegable Acciones, selecciona Editar la configuración de SMB y, a continuación, selecciona la configuración de visibilidad para compartir archivos.
4. En el estado de visibilidad, active la casilla de verificación si desea que los recursos compartidos de esta puerta de enlace aparezcan cuando la puerta de enlace muestre los recursos compartidos a los usuarios. Mantenga la casilla desactivada si no desea que los recursos compartidos de esta puerta de enlace aparezcan cuando la puerta de enlace muestre los recursos compartidos a los usuarios.

Edite la configuración de su recurso compartido de archivos SMB

Puedes editar los siguientes ajustes para un recurso compartido de archivos SMB existente:

- Nombre del recurso compartido de archivos: elija un nombre para el recurso compartido de archivos
- Registros de auditoría: activa o desactiva los registros de auditoría
- Lista de grupos de registros existentes: elija un grupo de registros existente para los registros de auditoría
- Tiempo de actualización de la caché de archivos que no es Gateway: especifique el intervalo en el que se debe actualizar la memoria caché del recurso compartido de archivos

> **Note**
>
> Establecer este valor en menos de 30 minutos puede afectar negativamente al rendimiento de la puerta de enlace en situaciones en las que se crean o eliminan con frecuencia grandes cantidades de objetos de Amazon S3.

- Tiempo de finalización de los eventos de carga: especifique el número de segundos que debe esperar después del último momento en el que un cliente escribió en un archivo antes de generar una `ObjectUploaded` notificación
- Clase de almacenamiento para objetos nuevos: elija una clase de almacenamiento para utilizarla en los nuevos objetos creados en su bucket de Amazon S3

- Adivina el tipo MIME: elige si quieres que Storage Gateway adivine el tipo MIME de los objetos cargados en función de las extensiones de archivo
- Archivos de puerta de enlace accesibles para el propietario del bucket de S3: elija si desea que los archivos de la puerta de enlace sean accesibles para la AWS cuenta propietaria del bucket de Amazon S3 que está vinculado al recurso compartido de archivos
- Habilite los pagos por parte del solicitante: elija si desea que las cuentas que lean o soliciten datos del recurso compartido de archivos paguen los cargos de acceso, en lugar de hacerlo el propietario del depósito
- Exportar como: elija si los archivos se exportarán en estado de lectura/escritura o de solo lectura
- El acceso a los archivos y directorios se controla mediante: elija si desea utilizar los permisos de Windows ACLs o POSIX para controlar el acceso a los archivos y directorios
- Bloqueo oportunista (oplock): elija si desea permitir que el recurso compartido de archivos utilice el bloqueo oportunista para optimizar la estrategia de almacenamiento en búfer de archivos
- Utilice la distinción entre mayúsculas y minúsculas: elija si el cliente o la puerta de enlace controlarán la distinción entre mayúsculas y minúsculas en los nombres de archivos y directorios
- Enumeración de archivos y directorios basada en el acceso: elija si desea que los archivos y carpetas del recurso compartido estén visibles para todos los usuarios durante la enumeración de directorios o solo para los usuarios con acceso de lectura

> **Note**
>
> No puede editar un recurso compartido de archivos existente para que apunte a un nuevo depósito o punto de acceso, ni modificar la configuración del punto final de la VPC. Puede configurar esos ajustes solo al crear un nuevo recurso compartido de archivos.

Para editar la configuración del recurso compartido de archivos

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Elija File shares (Recursos compartidos de archivos) y, a continuación, seleccione el recurso compartido de archivos que desee actualizar.
3. En Actions, elija Edit file share settings.
4. Edita cualquier configuración que desees cambiar.
5. Seleccione Save.

Limite el acceso de usuarios y grupos a su recurso compartido de archivos SMB

Recomendamos agregar usuarios o grupos permitidos o denegados para limitar el acceso a su recurso compartido de archivos. Si no lo haces, el recurso compartido de archivos estará disponible para todos los usuarios autenticados.

Para editar la configuración de acceso a SMB

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Seleccione Recursos compartidos de archivos y, a continuación, elija el recurso compartido de archivos SMB que desee editar.
3. En Acciones, selecciona Editar la configuración de acceso a los archivos compartidos.
4. En la sección Acceso a archivos compartidos de usuarios y grupos, selecciona tu configuración.

   En Usuarios y grupos permitidos, selecciona Añadir usuario permitido o Añadir grupo permitido e introduce un usuario o grupo de AD al que quieras permitir el acceso a los archivos compartidos. Repite este proceso para permitir tantos usuarios y grupos como sea necesario. Se denegará el acceso a los usuarios y grupos que no figuren en la lista de usuarios y grupos permitidos.

   En el caso de los usuarios y grupos denegados, seleccione Añadir usuario denegado o Añadir grupo denegado e introduzca un usuario o grupo de AD al que desee denegar el acceso a los archivos compartidos. Repita este proceso para denegar tantos usuarios y grupos como sea necesario. Si la lista de usuarios y grupos permitidos está vacía, se concederá el acceso a todos los usuarios que no estén incluidos en la lista de usuarios y grupos denegados.

   > **Note**
   >
   > Escriba solo el nombre de usuario o grupo de AD. El nombre del dominio se deduce de la pertenencia de la gateway al AD específico al que se ha unido la gateway.
   > Si no especificas ningún usuario o grupo permitido o denegado, cualquier usuario de AD autenticado podrá exportar el recurso compartido de archivos.

Cambia el método de cifrado del lado del servidor para un recurso compartido de archivos existente

El siguiente procedimiento describe cómo cambiar el método de cifrado del lado del servidor para un recurso compartido de archivos NFS o SMB existente mediante la consola Storage Gateway. Para realizar esta acción mediante la API de Storage Gateway, consulte Update NFSFile Share o Update SMBFile Share en la referencia de la API AWS de Storage Gateway.

> **Note**
>
> Al actualizar el método de cifrado, se aplica el nuevo método a los objetos existentes almacenados en los buckets de Amazon S3 tras la actualización.
> Si configura su puerta de enlace de archivos para utilizar SSE-KMS para el cifrado, debe añadir manualmente los `kms:DescribeKey` permisos`kms:Encrypt`,, `kms:Decrypt` `kms:ReEncrypt*` `kms:GenerateDataKey`, y a la función de IAM asociada al recurso compartido de archivos. Para obtener más información, consulte Uso de políticas basadas en la identidad (políticas de IAM) para Storage Gateway.

Para cambiar el método de cifrado del lado del servidor para un recurso compartido de archivos NFS o SMB

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Seleccione Recursos compartidos de archivos y, a continuación, elija el recurso compartido de archivos para el que desee cambiar el método de cifrado.
3. En Acciones, elija Editar el cifrado de los archivos compartidos.
4. En Cifrado, elija el tipo de cifrado que quiere usar para los archivos en reposo en Amazon S3:
   - Para usar el cifrado del lado del servidor gestionado con Amazon S3 (SSE-S3), elija S3 Managed Keys (SSE-S3). Para obtener más información, consulte Uso del cifrado del lado del servidor con claves administradas de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.
   - Para usar el cifrado del lado del servidor administrado con el Servicio de administración de AWS claves (SSE-KMS), elija claves administradas por KMS (SSE-KMS). Para la clave de KMS principal, elige una clave de AWS KMS existente o selecciona Crear una nueva clave

de KMS para crear una nueva clave de KMS en la consola del Servicio de administración de claves (). AWS AWS KMS

Para obtener más información AWS KMS, consulte ¿Qué es el servicio de administración de AWS claves? en la Guía para AWS Key Management Service desarrolladores.

- Para usar el cifrado de doble capa del lado del servidor administrado con el Servicio de administración de AWS claves (DSSE-KMS), elija el cifrado de doble capa del lado del servidor con claves (DSSE-KMS). AWS Key Management Service Para la clave KMS principal, elija una clave AWS KMS existente o elija Crear una nueva clave KMS para crear una nueva clave KMS en la consola del Servicio de administración de claves (). AWS AWS KMS

  Para obtener más información sobre DSSE-KMS, consulte Uso del cifrado de doble capa del lado del servidor con claves AWS KMS en la Guía del usuario de Amazon Simple Storage Service.

  > **Note**
  >
  > El uso del DSSE-KMS y las claves conlleva cargos adicionales. AWS KMS Para más información, consulte Precios de AWS KMS.
  > Para especificar una AWS KMS clave con un alias que no aparezca en la lista o para usar una AWS KMS clave de otra AWS cuenta, debe usar la. AWS Command Line Interface No se admiten las claves KMS asimétricas. Para obtener más información, consulte Create SMBFile Share in the AWS Storage Gateway API Reference.

5. Cuando haya finalizado, elija Guardar cambios.

Edite la configuración de su recurso compartido de archivos NFS

Utilice el siguiente procedimiento para editar la configuración de un recurso compartido de archivos NFS existente después de crearlo.

> **Note**
>
> No puede editar un recurso compartido de archivos existente para que apunte a un nuevo depósito o punto de acceso, ni modificar la configuración del punto final de la VPC. Puede configurar esos ajustes solo al crear un nuevo recurso compartido de archivos.

Para editar la configuración del recurso compartido de archivos

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Elija File shares (Recursos compartidos de archivos) y, a continuación, seleccione el recurso compartido de archivos que desee actualizar.
3. En Actions, elija Edit file share settings.
4. En Nombre del recurso compartido de archivos, introduzca un nombre para el recurso compartido de archivos.
5. Para los registros de auditoría, seleccione una de las siguientes opciones:

   - Para crear un nuevo grupo de registros para este recurso compartido de archivos, elija Crear un nuevo grupo de registros.
   - Para enviar notificaciones de estado y recursos de este recurso compartido de archivos a un grupo de registros existente, elija Usar un grupo de registros existente y, a continuación, elija el grupo deseado de la lista.
   - Para desactivar el registro de este recurso compartido de archivos, seleccione Desactivar el registro.

   Para obtener más información sobre los registros de auditoría, consulte Descripción de los registros de auditoría de S3 File Gateway.
6. Para el tiempo de actualización de la caché de archivos que no sea de Gateway, seleccione Establecer intervalo de actualización y, a continuación, establezca el tiempo en minutos o días para actualizar la caché del recurso compartido de archivos mediante Time To Live (TTL). TTL es el tiempo transcurrido desde la última actualización. Una vez transcurrido el intervalo TTL, al acceder a un directorio, File Gateway actualiza el contenido de ese directorio desde el bucket de Amazon S3.

   > **Note**
   >
   > Establecer este valor en menos de 30 minutos puede afectar negativamente al rendimiento de la puerta de enlace en situaciones en las que se crean o eliminan con frecuencia grandes cantidades de objetos de Amazon S3.
7. En Tiempo de estabilización de los eventos de carga, seleccione Establecer tiempo de estabilización y, a continuación, introduzca el tiempo de estabilización en segundos. El tiempo de estabilización controla el retraso mínimo entre la operación de escritura más reciente del

cliente y la generación de la notificación de `ObjectUploaded` registro. Como los clientes pueden realizar muchas operaciones pequeñas de escritura en archivos en poco tiempo, recomendamos configurar este parámetro durante el mayor tiempo posible para evitar generar varias notificaciones para el mismo archivo de forma rápida y sucesiva. Para obtener más información, consulte Recibir una notificación de carga de archivos.

8. En Clase de almacenamiento para objetos nuevos, selecciona una clase de almacenamiento de la lista desplegable. Para obtener más información sobre las clases de almacenamiento, consulte Uso de clases de almacenamiento con una puerta de enlace de archivos.
9. En Metadatos de objetos, haga lo siguiente:

   a. Seleccione Adivina el tipo MIME si quiere permitir que Storage Gateway adivine el tipo de soporte de los objetos cargados en función de sus extensiones de archivo.

   b. Seleccione los archivos de puerta de enlace a los que pueda acceder el propietario del depósito de S3 si desea que la AWS cuenta propietaria del depósito de S3 sea la propietaria total de los archivos creados por la puerta de enlace, incluidos los permisos de lectura, escritura, edición y eliminación.
10. Seleccione Habilitar que el solicitante pague si quiere que el solicitante del archivo, y no el propietario del bucket, pague el costo de la solicitud de datos y la descarga del bucket de S3.
11.
12. Para el nivel de acceso, elige una de las siguientes opciones:

    - Root squash (default) (Agrupación en raíz) (predeterminado): el acceso del superusuario remoto (raíz) se asigna al UID (65534) y al GID (65534).
    - All squash (Agrupación para todos): el acceso de todos los usuarios se asigna al ID de usuario (UID) (65534) y al ID de grupo (GID) (65534).
    - No root squash (Sin agrupación en raíz): el superusuario remoto (raíz) recibe acceso como usuario raíz.
13. En Exportar como, seleccione una de las siguientes opciones:

    - Para permitir que los clientes lean y escriban archivos en el recurso compartido de archivos, seleccione Lectura/Escritura.
    - Para permitir que los clientes lean los archivos pero no escriban en el recurso compartido de archivos, seleccione Solo lectura.

> **Note**
>
> En el caso de los recursos compartidos de archivos que están montados en un cliente de Microsoft Windows, si selecciona Solo lectura, es posible que aparezca un mensaje sobre un error inesperado que le impide crear la carpeta. Puede hacer caso omiso del mensaje.

14. Cuando haya terminado de editar la configuración, seleccione Guardar cambios.

Edite los metadatos predeterminados de su recurso compartido de archivos NFS

Si no establece los valores de metadatos para los archivos o directorios del bucket, su S3 File Gateway establece los valores de metadatos predeterminados. Estos valores incluyen los permisos de Unix para los archivos y las carpetas. Puede editar los valores predeterminados de los metadatos en la consola Storage Gateway.

Cuando su S3 File Gateway almacena archivos y carpetas en Amazon S3, los permisos de archivos de Unix se almacenan en metadatos de objetos. Cuando la puerta de enlace de archivos de S3 descubre objetos que no estaban almacenados en la puerta de enlace de archivos de S3, se les asignan los permisos de archivo Unix predeterminados. Los permisos de Unix predeterminados se muestran en la tabla siguiente.

Metadatos	Descripción
Permisos de directorio	El modo de directorio de Unix en formato "nnnn". Por ejemplo, "0666" representa el modo de acceso para todos los directori os contenidos en el recurso compartido de archivos. El valor predeterminado es 0777.
Permisos de archivos	El modo de archivo de Unix en formato "nnnn". Por ejemplo, "0666" representa el modo de archivos contenidos en el recurso compartido de archivos. El valor predeterminado es 0666.

Metadatos	Descripción
ID de usuario	ID del propietario predeterminado de los archivos contenidos en el recurso compartido de archivos. El valor predeterminado es 65534.
ID de grupo	ID del grupo predeterminado del recurso compartido de archivos. El valor predeterm inado es 65534.

Para editar los valores predeterminados de los metadatos

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Elija File shares (Recursos compartidos de archivos) y, a continuación, seleccione el recurso compartido de archivos que desee actualizar.
3. En Actions (Acciones), elija Edit file metadata defaults (Editar valores predeterminados de los metadatos de archivo).
4. En el cuadro de diálogo Edit file metadata defaults (Editar valores predeterminados de los metadatos de archivo), indique la información de los metadatos y elija Save (Guardar).

Limite el acceso de los clientes a su recurso compartido de archivos NFS

Se recomienda editar la configuración de acceso del cliente NFS para definir una lista de direcciones IP de cliente o rangos de bloques CIDR específicos para los clientes NFS que pueden conectarse a su recurso compartido de archivos NFS. Si decide no limitar el acceso, cualquier cliente de la red podrá montarlo en su recurso compartido de archivos.

Para limitar el acceso de los clientes a su recurso compartido de archivos NFS

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Seleccione Recursos compartidos de archivos en el panel de navegación situado en la parte izquierda de la página de la consola y, a continuación, elija el ID del recurso compartido de archivos NFS que desee editar.

3. En el menú desplegable Acciones, selecciona Editar la configuración de acceso a los archivos compartidos.

   La sección Objeto de acceso muestra una lista de direcciones IP y bloques de CIDR que actualmente pueden conectarse al recurso compartido de archivos NFS. Si el acceso no está limitado actualmente, verá una entrada en la sección Clientes permitidos para el bloque CIDR 0.0.0.0/0, que indica que todas las direcciones posibles pueden conectarse. IPv4
4. En Clientes permitidos, a la derecha del bloque CIDR 0.0.0.0/0, selecciona Eliminar.
5. Elija Agregar cliente y, a continuación, proporcione una dirección IP o un rango de direcciones en notación CIDR para los clientes que desee permitir.
6. Repita el paso anterior para agregar más direcciones IP o rangos según sea necesario. Si comete un error o necesita revocar el acceso, puede seleccionar Eliminar a la derecha de la dirección IP o el rango que desee eliminar de la lista.
7. Cuando haya finalizado, elija Guardar cambios.

Actualización de la caché de objetos del bucket de Amazon S3

A medida que su cliente NFS o SMB realiza operaciones en el sistema de archivos, su puerta de enlace mantiene un inventario de los objetos de la caché de objetos de Amazon S3 asociados a su recurso compartido de archivos. Su puerta de enlace utiliza este inventario en caché para reducir la latencia y la frecuencia de las solicitudes de Amazon S3. Esta operación no importa archivos al almacenamiento en caché de S3 File Gateway. Solo actualiza el inventario en caché para reflejar los cambios en el inventario de los objetos de la caché de objetos de Amazon S3.

Para actualizar la caché de objetos del bucket de S3 de su recurso compartido de archivos, seleccione el método que mejor se adapte a su caso de uso de la siguiente lista y, a continuación, complete el procedimiento correspondiente que se indica a continuación.

> **Note**
>
> Independientemente del método que utilice, al publicar un directorio por primera vez, se inicializa, lo que provoca que la puerta de enlace muestre el contenido de metadatos del directorio desde Amazon S3. El tiempo necesario para inicializar un directorio es proporcional al número de entradas de ese directorio.

Temas

- Configure un programa de actualización automática de la memoria caché mediante la consola Storage Gateway
- Configura un programa de actualización de caché automático AWS Lambda con una CloudWatch regla de Amazon
- Realice una actualización manual de la memoria caché mediante la consola Storage Gateway
- Realice una actualización manual de la caché mediante la API Storage Gateway

Configure un programa de actualización automática de la memoria caché mediante la consola Storage Gateway

El siguiente procedimiento configura un programa de actualización automática de la caché en función del valor de tiempo de vida (TTL) que especifique. Antes de configurar un programa de actualización de la caché basado en TTL, tenga en cuenta lo siguiente:

- El TTL se mide como el tiempo transcurrido desde la última actualización de la caché de un directorio determinado.
- La actualización de la caché basada en TTL solo se produce cuando se accede a un directorio determinado después de que haya expirado el período de TTL especificado.
- La actualización no es recursiva. Solo se produce en los directorios específicos a los que se accede.
- La actualización implica costes de la API de Amazon S3 únicamente en los directorios que no se han sincronizado desde la caducidad del TTL.
  - Los directorios solo se sincronizan si se accede a ellos mediante una actividad de NFS o SMB.
  - La sincronización no se produce con más frecuencia que el período TTL que especifique.
- Se recomienda configurar la actualización de la caché basada en TTL solo si actualiza con frecuencia el contenido de su bucket de Amazon S3 directamente, fuera del flujo de trabajo entre la puerta de enlace y el bucket de Amazon S3.
- Las operaciones de NFS y SMB que accedan a directorios caducados se TTLs bloquearán mientras la puerta de enlace actualiza el contenido del directorio.

> **Note**
>
> Dado que la actualización de la memoria caché puede bloquear las operaciones de acceso a los directorios, recomendamos configurar el período TTL más largo que resulte práctico para su implementación.

Para configurar un programa de actualización automática de la memoria caché mediante la consola Storage Gateway

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Seleccione Recursos compartidos de archivos.
3. Elija el recurso compartido de archivos para el que desee configurar el programa de actualización.
4. En Actions, elija Edit file share settings.
5. Para actualizar la caché automáticamente desde S3, seleccione la casilla de verificación y configure el tiempo en días, horas y minutos para actualizar la caché del recurso compartido de archivos mediante Time To Live (TTL). TTL es el tiempo transcurrido desde la última actualización, tras el cual el acceso al directorio haría que File Gateway actualizara primero el contenido de ese directorio desde el bucket de Amazon S3.
6. Seleccione Save changes (Guardar cambios).

Configura un programa de actualización de caché automático AWS Lambda con una CloudWatch regla de Amazon

Para configurar un programa de actualización de caché automático AWS Lambda mediante una CloudWatch regla de Amazon

1. Identifique el bucket de S3 que utiliza S3 File Gateway.
2. Compruebe que la sección de eventos esté en blanco. Se rellena automáticamente más adelante.
3. Cree un rol de IAM y permita Trust Relationship for Lambda`lambda.amazonaws.com`.
4. Utilice la siguiente política.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "StorageGatewayPermissions",
            "Effect": "Allow",
            "Action": "storagegateway:RefreshCache",
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchLogsPermissions",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:CreateLogGroup",
                "logs:PutLogEvents"
            ],
            "Resource": "*"
        }
    ]
}
```

5. Cree una función Lambda desde la consola de Lambda.
6. Utilice la siguiente función para la tarea de Lambda.

```
import json
import boto3
client = boto3.client('storagegateway')
def lambda_handler(event, context):
    print(event)
    response = client.refresh_cache(
        FileShareARN='arn:aws:storagegateway:ap-southeast-2:672406474878:share/
share-E51FBS9C'
    )
    print(response)
    return 'Your FileShare cache has been refreshed'
```

7. En el rol de ejecución, elija el rol de IAM que creó.

8. Opcional: añada un activador para Amazon S3 y seleccione el evento ObjectCreatedo ObjectRemoved.

> **Note**
>
> `RefreshCache`debe completar un proceso antes de iniciar otro. Al crear o eliminar muchos objetos de un depósito, es posible que el rendimiento disminuya. Por lo tanto, no recomendamos utilizar activadores de S3. En su lugar, usa la CloudWatch regla de Amazon que se describe a continuación.

9. Crea una CloudWatch regla en la CloudWatch consola y añade un horario. Por lo general, recomendamos una tarifa fija de 30 minutos. Sin embargo, puede utilizar de 1 a 2 horas en un depósito S3 grande.
10. Añade un nuevo desencadenante para CloudWatch los eventos y elige la regla que acabas de crear.
11. Guarde la configuración de Lambda. Seleccione Probar.
12. Elija S3 PUT y personalice la prueba según sus necesidades.
13. La prueba debería tener éxito. De lo contrario, modifique el JSON según sus requisitos y vuelva a realizar la prueba.
14. Abra la consola Amazon S3 y compruebe que el evento que creó y el ARN de la función Lambda estén presentes.
15. Cargue un objeto a su bucket de S3 mediante la consola de Amazon S3 o el AWS CLI.

    La CloudWatch consola genera un CloudWatch resultado similar al siguiente.

```
{
    u'Records': [
        {u'eventVersion': u'2.0', u'eventTime': u'2018-09-10T01:03:59.217Z',
 u'requestParameters': {u'sourceIPAddress': u'MY-IP-ADDRESS'},
        u's3': {u'configurationId': u'95a51e1c-999f-485a-b994-9f830f84769f',
 u'object': {u'sequencer': u'00549CC2BF34D47AED', u'key': u'new/filename.jpeg'},
        u'bucket': {u'arn': u'arn:aws:s3:::amzn-s3-demo-bucket', u'name':
 u'MY-GATEWAY-NAME', u'ownerIdentity': {u'principalId': u'A3OKNBZ72HVPP9'}},
 u's3SchemaVersion': u'1.0'},
        u'responseElements': {u'x-amz-id-2':
 u'76tiugjhvjfyriugiug87t890nefevbck0iA3rPU9I/s4NY9uXwtRL75tCyxasgsdgfsq+IhvAg5M=',
 u'x-amz-request-id': u'651C2D4101D31593'},
```

```
        u'awsRegion': u'MY-REGION', u'eventName': u'ObjectCreated:PUT',
 u'userIdentity': {u'principalId': u'AWS:AROAI5LQR5JHFHDFHDFHJ:MY-USERNAME'},
 u'eventSource': u'aws:s3'}
    ]
}
```

La invocación a Lambda proporciona un resultado similar al siguiente.

```
{
    u'FileShareARN': u'arn:aws:storagegateway:REGION:ACCOUNT-ID:share/MY-SHARE-
ID',
        'ResponseMetadata': {'RetryAttempts': 0, 'HTTPStatusCode': 200,
 'RequestId': '6663236a-b495-11e8-946a-bf44f413b71f',
            'HTTPHeaders': {'x-amzn-requestid': '6663236a-b495-11e8-946a-
bf44f413b71f', 'date': 'Mon, 10 Sep 2018 01:03:59 GMT',
                'content-length': '90', 'content-type': 'application/x-amz-
json-1.1'
        }
    }
}
```

El recurso compartido de NFS montado en el cliente reflejará esta actualización.

> **Note**
>
> En el caso de las cachés que actualizan la creación o eliminación de objetos grandes en depósitos grandes con millones de objetos, las actualizaciones pueden tardar horas.

16. Elimine el objeto manualmente mediante la consola Amazon S3 o AWS CLI.
17. Vea el recurso compartido de NFS montado en su cliente. Compruebe que el objeto ha desaparecido (porque la caché se ha actualizado).
18. Revisa tus CloudWatch registros para ver el registro de tu eliminación junto con el evento`ObjectRemoved:Delete`.

```
{
    u'account': u'MY-ACCOUNT-ID', u'region': u'MY-REGION', u'detail': {}, u'detail-
type': u'Scheduled Event', u'source': u'aws.events',
    u'version': u'0', u'time': u'2018-09-10T03:42:06Z', u'id':
 u'6468ef77-4db8-0200-82f0-04e16a8c2bdb',
    u'resources': [u'arn:aws:events:REGION:MY-ACCOUNT-ID:rule/FGw-RefreshCache-CW']
```

```
}
```

> **Note**
>
> En el caso de los trabajos temporales o las tareas programadas, tu evento de CloudWatch registro es`u'detail-type': u'Scheduled Event'`.

Realice una actualización manual de la memoria caché mediante la consola Storage Gateway

Para realizar una actualización manual de la caché mediante la consola Storage Gateway

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Seleccione Recursos compartidos de archivos y, a continuación, elija el recurso compartido de archivos para el que desee realizar la actualización.
3. En Actions (Acciones), elija Refresh cache (Actualizar caché).

   El tiempo que tarda el proceso de actualización depende del número de objetos almacenados en la memoria caché de la gateway y del número de objetos que se han añadido o eliminado del bucket de S3.

Realice una actualización manual de la caché mediante la API Storage Gateway

El siguiente procedimiento realiza una actualización manual de la caché mediante la API Storage Gateway. Antes de realizar una actualización de la caché basada en la API, tenga en cuenta lo siguiente:

- Puede especificar una actualización recursiva o no recursiva.
- Una actualización recursiva consume más recursos y es más cara.
- La actualización incurre en costes de la API de Amazon S3 únicamente en los directorios que pase como argumentos en la solicitud y en los descendientes de esos directorios si especifica una actualización recursiva.
- La actualización se ejecuta simultáneamente con otras operaciones mientras la puerta de enlace está en uso.

  - Por lo general, las operaciones de NFS y SMB no se bloquean durante las actualizaciones, a menos que haya una actualización activa para el directorio al que se accede mediante la operación.
  - La puerta de enlace no puede determinar si el contenido actual de la caché está obsoleto y lo utiliza para las operaciones de NFS y SMB, independientemente de si está actualizado.
  - Dado que una actualización de la caché utiliza recursos de hardware virtual de la puerta de enlace, el rendimiento de la puerta de enlace podría verse afectado negativamente mientras la actualización esté en curso.
- Se recomienda realizar una actualización de la caché basada en API solo si actualiza el contenido del bucket de Amazon S3 directamente, fuera del flujo de trabajo entre la puerta de enlace y el bucket de Amazon S3.

> **Note**
>
> Si conoce los directorios específicos en los que va a actualizar el contenido de Amazon S3 fuera del flujo de trabajo de la puerta de enlace, le recomendamos que especifique estos directorios en su solicitud de actualización basada en API para reducir los costes de la API de Amazon S3 y el impacto en el rendimiento de la puerta de enlace.

Para realizar una actualización manual de la caché mediante la API Storage Gateway

- Envíe una solicitud HTTP POST para invocar la `RefreshCache` operación con los parámetros que desee a través de la API Storage Gateway. Para obtener más información, consulte la referencia RefreshCachede la API AWS de Storage Gateway.

> **Note**
>
> El envío de la `RefreshCache` solicitud solo inicia la operación de actualización de la caché. El hecho de que finalice la actualización de la caché no significa necesariamente que haya finalizado la actualización del archivo. Para determinar que la operación de actualización archivos ha finalizado antes de comprobar si hay archivos nuevos en el recurso compartido de archivos de la gateway, utilice la notificación `refresh-complete`. Para ello, puedes suscribirte para recibir notificaciones a través de un CloudWatch evento de Amazon. Para obtener más información, consulte Recibir notificaciones sobre las operaciones con archivos.

Uso de S3 Object Lock con Amazon S3 File Gateway

Amazon S3 File Gateway admite el acceso a buckets S3 que tienen activado Amazon S3 Object Lock. Amazon S3 Object Lock le permite almacenar objetos mediante un modelo WORM (Write Once Read Many). Al utilizar Amazon S3 Object Lock, puede impedir que un objeto de su bucket de S3 se elimine o sobrescriba. Amazon S3 Object Lock funciona junto con el control de versiones de objetos para proteger sus datos.

Si activa Amazon S3 Object Lock, podrá seguir modificando el objeto. Por ejemplo, se puede escribir, eliminar o cambiar su nombre a través de un archivo compartido en una puerta de enlace de archivos de S3. Al modificar un objeto de esta manera, S3 File Gateway coloca una nueva versión del objeto sin que ello afecte a la versión anterior (es decir, al objeto bloqueado).

Por ejemplo, si utiliza la interfaz NFS o SMB de S3 File Gateway para eliminar un archivo y el objeto de S3 correspondiente está bloqueado, la puerta de enlace coloca un marcador de eliminación de S3 como la siguiente versión del objeto y deja la versión original del objeto en su lugar. Del mismo modo, si una puerta de enlace de archivos de S3 modifica el contenido o los metadatos de un objeto bloqueado, se carga una nueva versión del objeto con los cambios, pero la versión bloqueada original del objeto permanece inalterada.

Para obtener más información sobre Amazon S3 Object Lock, consulte Bloquear objetos mediante S3 Object Lock en la Guía del usuario de Amazon Simple Storage Service.

Descripción del estado de los archivos compartidos

Puede ver el estado de un archivo compartido de un vistazo consultando su estado. Si el estado indica que el recurso compartido de archivos funciona con normalidad, no es necesario que realices ninguna acción. Si el estado indica que hay un problema, puedes investigar para determinar si es necesario tomar medidas.

Puede ver el estado de un recurso compartido de archivos en la consola Storage Gateway, en la columna Estado. Un recurso compartido 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, qué significan y si es necesario tomar alguna medida.

Estado	Significado
DISPONIBLE	El recurso compartido de archivos está configurado correctamente y se encuentra disponible para su uso. Este es el estado estándar de un recurso compartido de archivos que funciona correctamente.
CREAR	El recurso compartido de archivos aún no se ha creado completamente y no está listo para usarse. El estado CREATING es transitorio. No hay que hacer nada más. Si el recurso compartido de archivos se bloquea en este estado, probablemente se deba a que la máquina virtual de la puerta de enlace perdió la conexión con ella AWS.
ACTUALIZANDO	La configuración del recurso compartido de archivos se está actualiza ndo actualmente. El estado de ACTUALIZACIÓN es transitorio. No hay que hacer nada más. Si un recurso compartido 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 recurso compartido de archivos. El recurso compartido 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	Se está eliminando de forma forzada el recurso compartido de archivos. El archivo compartido se elimina inmediatamente y los datos no se cargan en él AWS. El estado FORCE_DELETING es transitorio y no se requiere ninguna acción.
UNAVAILABLE	El recurso compartido de archivos se encuentra en mal estado. Es necesario tomar medidas. Algunas causas posibles incluyen errores en la política de roles o la asignación a un bucket de Amazon S3 que no existe. Cuando se resuelva el problema que provocó el mal estado, el archivo compartido volverá al estado DISPONIBLE.

Entender el estado de la pasarela

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. La mayoría de las veces, el estado indica que la puerta de enlace funciona con normalidad y que no es necesaria ninguna acción por su parte. En ocasiones, el estado indica algún problema; en este caso, podría o no ser preciso que intervenga.

Puede ver el estado de cada gateway de su implementación en la página Gateways de la consola 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 normalmente tiene un estado de`RUNNING`.

En la siguiente tabla, puede encontrar una descripción del estado de cada puerta de enlace y si debe actuar en función de ese estado. Una puerta de enlace debe estar en `RUNNING` estado todo el tiempo que esté en uso o la mayor parte del tiempo.

Estado	Significado
`RUNNING`	La puerta de enlace está configurada correctamente y está disponible para su uso.
`OFFLINE`	Es posible que la puerta de enlace esté en un `OFFLINE` estado determinado por uno o varios de los siguientes motivos: • 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 un disco caché asociado que está desconect ado, se ha modificado o ha fallado.

Administración del ancho de banda de su Amazon S3 File Gateway

Puede limitar el rendimiento de carga desde su puerta de enlace AWS para controlar la cantidad de ancho de banda de red que utiliza la puerta de enlace. De forma predeterminada, una puerta de enlace activada no tiene límites de carga o descarga.

Puede configurar una bandwidth-rate-limit programación mediante el AWS Management Console kit de desarrollo de AWS software (SDK) o la AWS Storage Gateway API (consulte la referencia de UpdateBandwidthRateLimitSchedulela API AWS de Storage Gateway). Mediante un programa de límites de velocidad de ancho de banda, puede configurar los límites para que cambien automáticamente a lo largo del día o de la semana. Para obtener más información, consulte Vea y edite la bandwidth-rate-limit programación de su gateway mediante la consola Storage Gateway.

Puede supervisar el rendimiento de carga de su pasarela mediante la `CloudBytesUploaded` métrica de la pestaña Monitorización de la consola de Storage Gateway o en Amazon CloudWatch.

> **Note**
>
> Los límites de velocidad de ancho de banda se aplican únicamente a las cargas de archivos de Storage Gateway. Otras operaciones de puerta de enlace no se ven afectadas.
> La limitación de la velocidad del ancho de banda funciona equilibrando el rendimiento de todos los archivos que se están cargando, con un promedio de cada segundo. Si bien es posible que las cargas superen brevemente el límite de velocidad de ancho de banda durante un microsegundo o milisegundo determinado, esto no suele provocar picos importantes durante periodos de tiempo más prolongados.
> Actualmente, el tipo Amazon FSx File Gateway no admite la configuración de límites y horarios de velocidad de ancho de banda.

Temas

- Vea y edite la bandwidth-rate-limit programación de su gateway mediante la consola Storage Gateway
- Actualización de los límites de ancho de banda de la puerta de enlace mediante AWS SDK para Java
- Actualización de los límites de ancho de banda de Gateway mediante AWS SDK para .NET
- Actualización de los límites de ancho de banda de Gateway mediante AWS Tools for Windows PowerShell

Vea y edite la bandwidth-rate-limit programación de su gateway mediante la consola Storage Gateway

En esta sección, se describe cómo ver y editar la programación de límite de velocidad de ancho de banda de su puerta de enlace.

Para ver y editar la programación de límite de velocidad de ancho de banda

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. En el panel de navegación izquierdo, elija Puertas de enlace y, a continuación, elija la puerta de enlace que desee administrar.
3. En Acciones, elija Editar programación de límite de velocidad de ancho de banda.

   La bandwidth-rate-limit programación actual de la puerta de enlace se muestra en la página Editar la programación del límite de velocidad de ancho de banda. De forma predeterminada, una nueva puerta de enlace no tiene límites de velocidad de ancho de banda definidos.
4. (Opcional) Seleccione Añadir un nuevo límite de velocidad de ancho de banda para añadir un nuevo intervalo configurable a la programación. Para cada intervalo que añada, introduzca la siguiente información:

   - Velocidad de carga: introduzca el límite de velocidad de carga, en megabits por segundo (Mbps). El valor mínimo es de 100 Mbps.
   - Días de la semana: seleccione el día o los días de cada semana en los que desee que se aplique el intervalo. Puede aplicar el intervalo los días laborables (de lunes a viernes), los fines de semana (sábado y domingo), todos los días de la semana o un día específico de la semana. Para aplicar el límite de ancho de banda de manera uniforme y constante todos los días y en todo momento, elija Sin programación.
   - Hora de inicio: introduzca la hora de inicio del intervalo de ancho de banda, utilizando el formato HH:MM y la diferencia de zona horaria con respecto a UTC para su puerta de enlace.

     > **Note**
     >
     > bandwidth-rate-limitEl intervalo comienza al principio del minuto que especifique aquí.

   - Hora de finalización: introduzca la hora de finalización del intervalo de ancho de banda, utilizando el formato HH:MM y el desfase de zona horaria con respecto a GMT para su puerta de enlace.

> **Important**
>
> El bandwidth-rate-limit intervalo finaliza al final del minuto especificado aquí. Para programar un intervalo que finalice al final de una hora, introduzca **59**.
> Para programar intervalos continuos consecutivos, con transferencia al principio de la hora, sin interrupción entre los intervalos, introduzca **59** para el minuto final del primer intervalo. Introduzca **00** para el minuto de inicio del siguiente intervalo.

5. (Opcional) Repita el paso anterior según sea necesario hasta completar la bandwidth-rate-limit programación. Si necesita eliminar un intervalo de la programación, elija Eliminar.

> **Important**
>
> Bandwidth-rate-limitlos intervalos no se pueden superponer. La hora de inicio de un intervalo debe producirse después de la hora de finalización del intervalo anterior y antes de la hora de inicio del intervalo siguiente.

6. Cuando haya finalizado, elija Guardar cambios.

Actualización de los límites de ancho de banda de la puerta de enlace mediante AWS SDK para Java

Al actualizar los límites de la velocidad de ancho de banda mediante programación, puede ajustar estos límites automáticamente durante un período de tiempo, por ejemplo, mediante tareas programadas. En el siguiente ejemplo se ilustra cómo actualizar los límites de velocidad del ancho de banda de una puerta de enlace mediante AWS SDK para Java. Para utilizar el código del ejemplo, debe haberse familiarizado con la ejecución de aplicaciones de la consola de Java. Para obtener más información, consulte Introducción en la Guía para desarrolladores de AWS SDK para Java .

Example : Actualización de los límites de ancho de banda de Gateway mediante AWS SDK para Java

El siguiente ejemplo de código Java actualiza los límites de velocidad del ancho de banda de una puerta de enlace. Para usar este código de ejemplo, debe proporcionar el punto de enlace del servicio, el nombre de recurso de Amazon (ARN) de su puerta de enlace y el límite de carga. Para obtener una lista de los puntos de conexión de servicio de AWS con los que puede utilizar Storage

Gateway, consulte Puntos de enlace y cuotas de AWS Storage Gateway en la Referencia general de AWS.

```
   import java.io.IOException;

   import com.amazonaws.AmazonClientException;
   import com.amazonaws.auth.PropertiesCredentials;
   import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
   import com.amazonaws.services.storagegateway.model.
UpdateBandwidthRateLimitScheduleRequest;
   import com.amazonaws.services.storagegateway.model.
UpdateBandwidthRateLimitScheduleReturn;

   import java.util.Arrays;
   import java.util.Collections;
   import java.util.List;

   public class UpdateBandwidthExample {

       public static AWSStorageGatewayClient sgClient;

       // The gatewayARN
       public static String gatewayARN = "*** provide gateway ARN ***";

       // The endpoint
       static String serviceURL = "https://storagegateway.us-east-1.amazonaws.com";

       // Rates
       static long uploadRate = 100 * 1024 * 1024;  // Bits per second, minimum 100
Megabits/second

       public static void main(String[] args) throws IOException {

           // Create a Storage Gateway client
           sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(

UpdateBandwidthExample.class.getResourceAsStream("AwsCredentials.properties")));
           sgClient.setEndpoint(serviceURL);

           UpdateBandwidth(gatewayARN, uploadRate, null); // download rate not
supported by S3 File Gateways

       }
```

```
       private static void UpdateBandwidth(String gatewayArn, long uploadRate, long
downloadRate) {
           try
           {
               BandwidthRateLimit bandwidthRateLimit = new
BandwidthRateLimit(downloadRate, uploadRate);
               BandwidthRateLimitInterval noScheduleInterval = new
BandwidthRateLimitInterval()
                   .withBandwidthRateLimit(bandwidthRateLimit)
                   .withDaysOfWeek(Arrays.asList(1, 2, 3, 4, 5, 6, 0))
                   .withStartHourOfDay(0)
                   .withStartMinuteOfHour(0)
                   .withEndHourOfDay(23)
                   .withEndMinuteOfHour(59);
               UpdateBandwidthRateLimitScheduleRequest
updateBandwidthRateLimitScheduleRequest =
                   new UpdateBandwidthRateLimitScheduleRequest()
                   .withGatewayARN(gatewayArn)
                   .with
BandwidthRateLimitIntervals(Collections.singletonList(noScheduleInterval));

               UpdateBandwidthRateLimitScheduleReturn
updateBandwidthRateLimitScheuduleResponse =
sgClient.UpdateBandwidthRateLimitSchedule(updateBandwidthRateLimitScheduleRequest);

               String returnGatewayARN =
updateBandwidthRateLimitScheuduleResponse.getGatewayARN();
               System.out.println("Updated the bandwidth rate limits of " +
returnGatewayARN);
               System.out.println("Upload bandwidth limit = " + uploadRate + " bits
per second");
           }
           catch (AmazonClientException ex)
           {
               System.err.println("Error updating gateway bandwith.\n" +
ex.toString());
           }
       }
   }
```

Actualización de los límites de ancho de banda de Gateway mediante AWS SDK para .NET

Al actualizar los límites de la velocidad de ancho de banda mediante programación, puede ajustar estos límites automáticamente durante un período de tiempo, por ejemplo, mediante tareas programadas. El siguiente ejemplo muestra cómo actualizar los límites de ancho de banda de una puerta de enlace mediante el kit de desarrollo de software (SDK) para.NET. AWS Para utilizar el código del ejemplo, debe haberse familiarizado con la ejecución de aplicaciones de la consola de .NET. Para obtener más información, consulte Introducción en la Guía para desarrolladores de AWS SDK para .NET .

Example : Actualización de los límites de ancho de banda de la puerta de enlace mediante el AWS SDK para .NET

El siguiente ejemplo de código C# actualiza los límites de velocidad del ancho de banda de una puerta de enlace. Para usar este código de ejemplo, debe proporcionar el punto de enlace del servicio, el nombre de recurso de Amazon (ARN) de su puerta de enlace y el límite de carga. Para obtener una lista de los puntos de conexión de servicio de AWS con los que puede utilizar Storage Gateway, consulte Puntos de enlace y cuotas de AWS Storage Gateway en la Referencia general de AWS.

```
    using System;
    using System.Collections.Generic;
    using System.Linq;
    using System.Text;
    using Amazon.StorageGateway;
    using Amazon.StorageGateway.Model;

    namespace AWSStorageGateway
    {
        class UpdateBandwidthExample
        {
            static AmazonStorageGatewayClient sgClient;
            static AmazonStorageGatewayConfig sgConfig;

            // The gatewayARN
            public static String gatewayARN = "*** provide gateway ARN ***";

            // The endpoint
            static String serviceURL = "https://storagegateway.us-
east-1.amazonaws.com";
```

```
            // Rates
            static long uploadRate = 100 * 1024 * 1024;  // Bits per second, minimum
100 Megabits/second

            public static void Main(string[] args)
            {
                // Create a Storage Gateway client
                sgConfig = new AmazonStorageGatewayConfig();
                sgConfig.ServiceURL = serviceURL;
                sgClient = new AmazonStorageGatewayClient(sgConfig);

                UpdateBandwidth(gatewayARN, uploadRate, null);

                Console.WriteLine("\nTo continue, press Enter.");
                Console.Read();
            }

            public static void UpdateBandwidth(string gatewayARN, long uploadRate, long
downloadRate)
            {
                try
                {
                   BandwidthRateLimit bandwidthRateLimit = new
BandwidthRateLimit(downloadRate, uploadRate);
                    BandwidthRateLimitInterval noScheduleInterval = new
BandwidthRateLimitInterval()
                     .withBandwidthRateLimit(bandwidthRateLimit)
                     .withDaysOfWeek(Arrays.asList(1, 2, 3, 4, 5, 6, 0))
                     .withStartHourOfDay(0)
                     .withStartMinuteOfHour(0)
                     .withEndHourOfDay(23)
                     .withEndMinuteOfHour(59);
                   List <BandwidthRateLimitInterval> bandwidthRateLimitIntervals = new
List<BandwidthRateLimitInterval>();
                   bandwidthRateLimitIntervals.Add(noScheduleInterval);
                   UpdateBandwidthRateLimitScheduleRequest
updateBandwidthRateLimitScheduleRequest =
                     new UpdateBandwidthRateLimitScheduleRequest()
                        .withGatewayARN(gatewayARN)
                        .with BandwidthRateLimitIntervals(bandwidthRateLimitIntervals);
```

```
                    UpdateBandwidthRateLimitScheduleReturn
updateBandwidthRateLimitScheuduleResponse =
sgClient.UpdateBandwidthRateLimitSchedule(updateBandwidthRateLimitScheduleRequest);
                    String returnGatewayARN =
updateBandwidthRateLimitScheuduleResponse.GatewayARN;
                    Console.WriteLine("Updated the bandwidth rate limits of " +
returnGatewayARN);
                    Console.WriteLine("Upload bandwidth limit = " + uploadRate + " bits
per second");
                }
                catch (AmazonStorageGatewayException ex)
                {
                    Console.WriteLine("Error updating gateway bandwith.\n" +
ex.ToString());
                }
            }
        }
    }
```

Actualización de los límites de ancho de banda de Gateway mediante AWS Tools for Windows PowerShell

Al actualizar los límites de la velocidad de ancho de banda mediante programación, puede ajustar estos límites automáticamente durante un período de tiempo, por ejemplo, mediante tareas programadas. En el siguiente ejemplo se ilustra cómo actualizar los límites de velocidad del ancho de banda de una puerta de enlace mediante AWS Tools for Windows PowerShell. Para usar el código de ejemplo, debe estar familiarizado con la ejecución de un script. PowerShell Para obtener más información, consulte la introducción de la Guía del usuario de Herramientas de AWS para PowerShell .

Example : Actualización de los límites de ancho de banda de Gateway mediante el AWS Tools for Windows PowerShell

El siguiente ejemplo de PowerShell script actualiza los límites de ancho de banda de una puerta de enlace. Para usar este script de ejemplo, debe proporcionar el nombre de recurso de Amazon (ARN) de su puerta de enlace y el límite de carga.

```
    <#
    .DESCRIPTION
        Update Gateway bandwidth limits schedule
```

```
    .NOTES
        PREREQUISITES:
        1) AWS Tools for PowerShell from https://aws.amazon.com/powershell/
        2) Credentials and region stored in session using Initialize-AWSDefault.
        For more info, see https://docs.aws.amazon.com/powershell/latest/userguide/
specifying-your-aws-credentials.html


    .EXAMPLE
        powershell.exe .\SG_UpdateBandwidth.ps1
    #>

    $UploadBandwidthRate = 100 * 1024 * 1024
    $gatewayARN = "*** provide gateway ARN ***"

    $bandwidthRateLimitInterval = New-Object
 Amazon.StorageGateway.Model.BandwidthRateLimitInterval
    $bandwidthRateLimitInterval.StartHourOfDay = 0
    $bandwidthRateLimitInterval.StartMinuteOfHour = 0
    $bandwidthRateLimitInterval.EndHourOfDay = 23
    $bandwidthRateLimitInterval.EndMinuteOfHour = 59
    $bandwidthRateLimitInterval.DaysOfWeek = 0,1,2,3,4,5,6
    $bandwidthRateLimitInterval.AverageUploadRateLimitInBitsPerSec =
 $UploadBandwidthRate

    #Update Bandwidth Rate Limits
    Update-SGBandwidthRateLimitSchedule -GatewayARN $gatewayARN `
                                        -BandwidthRateLimitInterval
 @($bandwidthRateLimitInterval)

    $schedule =  Get-SGBandwidthRateLimitSchedule -GatewayARN $gatewayARN

    Write-Output("`nGateway: " + $gatewayARN);
    Write-Output("`nNew bandwidth throttle schedule: " +
 $schedule.BandwidthRateLimitIntervals.AverageUploadRateLimitInBitsPerSec)
```

Supervisión de Storage Gateway

En los temas de esta sección se describe 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. Al usar estas métricas, puede acceder a la información histórica y obtener una mejor perspectiva del rendimiento de sus 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 archivos S3: - 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 S3 File Gateway , consulte Descripción de las métricas de la puerta de enlace Comprensión de las métricas de la puerta de de uso compartido de archivos Descripción de las métricas . 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 las 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 pueden cargar: `FilesFailingUpload` >= 1 para 1 punto de datos en 5 minutos
- No se pueden compartir archivos: `FileSharesUnavailable` >= 1 para 1 punto de datos en 5 minutos
- Notificaciones de salud: `HealthNotifications` >= 1 por 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 alarma adicional: CloudWatch

- Notificaciones de disponibilidad: `AvailabilityNotifications` >= 1 por 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 de CloudWatch alarma.

Estado	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, consulte Configurar Amazon S3 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 de detalles de la puerta de enlace, seleccione 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 de ALARMA cuando la métrica supera el umbral durante un número específico de períodos 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 de valores «normal» 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 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.
   - 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 archivos S3:

Puede monitorizar su puerta de enlace de archivos S3 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 de S3 File Gateway con CloudWatch grupos de registros
- Uso de CloudWatch las métricas de Amazon
- Recibir notificaciones sobre las operaciones con archivos
- Información acerca de las métricas de gateway
- Descripción de las métricas de uso compartido de archivos
- Descripción de los registros de auditoría de S3 FSx File Gateway

Obtener los registros de estado de de S3 File Gateway con CloudWatch grupos de registros

Puede usar Amazon CloudWatch Logs para obtener información sobre el estado de su puerta de enlace de archivos S3 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 supervisar su puerta de enlace y recibir una notificación cuando su S3 File Gateway no pueda cargar archivos en un bucket de Amazon S3. Puede configurar el grupo al activar la puerta de enlace o después de que la puerta de enlace esté activada y en funcionamiento. Para obtener información sobre cómo configurar un grupo de CloudWatch registros al activar una puerta de enlace, consulteConfigure su Amazon S3 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.

El siguiente es un ejemplo de un error registrado por una puerta de enlace de archivos de S3.

```
{
    "severity": "ERROR",
    "bucket": "bucket-smb-share2",
    "roleArn": "arn:aws:iam::123456789012:role/amzn-s3-demo-bucket",
```

```
    "source": "share-E1A2B34C",
    "type": "InaccessibleStorageClass",
    "operation": "S3Upload",
    "key": "myFolder/myFile.text",
    "gateway": "sgw-B1D123D4",
    "timestamp": "1565740862516"
}
```

Este error significa que S3 File Gateway no puede cargar el objeto `myFolder/myFile.text` en Amazon S3 porque ha pasado de la clase de almacenamiento Amazon S3 Standard a la clase de almacenamiento S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive.

En el registro del estado de la gateway anterior, estos elementos especifican una información determinada:

- `source: share-E1A2B34C` indica el recurso compartido de archivos que ha detectado este error.
- `"type": "InaccessibleStorageClass"` indica el tipo de error que se ha producido. En este caso, este error se produjo cuando la puerta de enlace intentaba cargar el objeto especificado en Amazon S3 o leerlo desde Amazon S3. Sin embargo, en este caso, el objeto ha pasado a Amazon S3 Glacier. El valor de `"type"` puede ser cualquier error que encuentre S3 File Gateway. Para obtener una lista de posibles errores, consulte Solución de problemas: problemas con File Gateway
- `"operation": "S3Upload"`indica que este error se produjo cuando la puerta de enlace intentaba cargar este objeto en S3.
- `"key": "myFolder/myFile.text"` indica el objeto que ha provocado el fallo.
- `gateway": "sgw-B1D123D4`indica la puerta de enlace de archivos S3 que detectó este error.
- `"timestamp": "1565740862516"`indica la hora en que se produjo el error.

Para obtener información sobre cómo solucionar los errores que pueda reportar S3 File Gateway , consulteSolución de problemas: problemas con File Gateway.

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 S3 File Gateway FSx

1. Inicie sesión en la consola Storage Gateway de su https://console.aws.amazon.com/storagegateway/casa AWS Management Console 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, elija Editar la información de la puerta de enlace.
4. En Elija cómo configurar el grupo de registros, 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 S3 mediante la API AWS Management Console 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 utilizar la `Gateway Metrics` vista para seleccionar las 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	Descripción
`AWS/StorageGateway`	`GatewayId` , `GatewayName`	Estas dimensiones filtran datos de métricas que describen aspectos de la gateway. 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

Recibir notificaciones sobre las operaciones con archivos

Storage Gateway puede iniciar los siguientes CloudWatch eventos una vez finalizadas las operaciones con los archivos:

- Puede recibir una notificación cuando la puerta de enlace finalice la carga asíncrona de sus archivos desde el recurso compartido de archivos a Amazon S3. Utilice el `NotificationPolicy` parámetro para solicitar una notificación de carga de archivos. Esto envía una notificación por cada carga de archivos completada a Amazon S3. Para obtener más información, consulte Recibir una notificación de carga de archivos.
- Puede recibir una notificación cuando la puerta de enlace finalice la carga asíncrona de su conjunto de archivos de trabajo desde el recurso compartido de archivos a Amazon S3. Utilice la operación de NotifyWhenUploadedAPI para solicitar una notificación de carga de un conjunto de archivos en funcionamiento. Esto envía una notificación cuando todos los archivos del conjunto de archivos de trabajo se han cargado en Amazon S3. Para obtener más información, consulte Obteniendo una notificación de carga de un conjunto de archivos en funcionamiento.
- Puede recibir una notificación cuando la gateway termine de actualizar la caché para el bucket de S3. Cuando invoque la RefreshCacheoperación a través de la consola o la API de Storage Gateway, suscríbase a la notificación cuando se complete la operación. Para obtener más información, consulte Recibir una notificación de actualización de la caché.

Cuando finalice la operación de archivo que solicitó, Storage Gateway le enviará una notificación a través de CloudWatch Events. Puede configurar CloudWatch Events para enviar la notificación a través de destinos de eventos como Amazon SNS, Amazon SQS o una función. AWS Lambda Por ejemplo, puede configurar un destino de Amazon SNS para enviar la notificación a los consumidores de Amazon SNS, como un correo electrónico o un mensaje de texto. Para obtener información sobre CloudWatch los eventos, consulte ¿Qué son los eventos? CloudWatch

Para configurar la notificación de CloudWatch eventos

1. Cree un destino, como un tema de Amazon SNS o una función Lambda, para invocarlo cuando se produzca el evento que solicitó en Storage Gateway.
2. Cree una regla en la consola de CloudWatch eventos para invocar los destinos en función de un evento en Storage Gateway.
3. En la regla, cree un patrón de eventos para el tipo de evento. La notificación que se envía cuando el evento coincide con este patrón de reglas.

4. Seleccione el destino y configure los ajustes.

El siguiente ejemplo muestra una regla que inicia el tipo de evento especificado en la puerta de enlace especificada y en la AWS región especificada. Por ejemplo, puede especificar `Storage Gateway File Upload Event` como tipo de evento.

```
{
   "source":[
      "aws.storagegateway"
   ],
   "resources":[
      "arn:aws:storagegateway:AWS Region:account-id
                :gateway/gateway-id"
   ],
   "detail-type":[
      "Event type"
   ]
}
```

Para obtener información sobre cómo utilizar las reglas de CloudWatch eventos, consulte Crear una regla de CloudWatch eventos que se active en un evento en la Guía del usuario de Amazon CloudWatch Events.

Recibir una notificación de carga de archivos

Hay dos casos de uso en los que puedes usar la notificación de carga de archivos:

- Para automatizar el procesamiento en la nube de los archivos que se cargan, puede llamar al `NotificationPolicy` parámetro y obtener un ID de notificación. La notificación que se produce cuando se cargan los archivos tiene el mismo ID de notificación que la API devolvió. Si asigna este ID de notificación para hacer un seguimiento de la lista de archivos que está cargando, podrá iniciar el procesamiento del archivo que se ha cargado AWS cuando se genere el evento con el mismo ID.
- Para los casos de uso de distribución de contenido, puede tener dos puertas de enlace de archivos de S3 que se asignen al mismo bucket de Amazon S3. El cliente de compartición de archivos de Gateway1 podría subir nuevos archivos a Amazon S3, y los clientes de compartición de archivos de Gateway2 leen los archivos. Los archivos se cargan en Amazon S3, pero Gateway2 no los ve porque utiliza una versión de los archivos en caché local de Amazon S3. Para que los archivos estén visibles en Gateway2, puede usar el `NotificationPolicy` parámetro para

solicitar una notificación de carga de archivos a Gateway1 para que le notifique cuando finalice la carga del archivo. A continuación, puede usar CloudWatch Events para emitir automáticamente una RefreshCachesolicitud para compartir archivos en Gateway2. Cuando se complete la RefreshCachesolicitud, el nuevo archivo estará visible en Gateway2.

Example Ejemplo: notificación de carga de archivos

En el siguiente ejemplo, se muestra una notificación de carga de archivos que se te envía CloudWatch cuando el evento coincide con la regla que has creado. Esta notificación está en formato JSON. Puede configurar esta notificación para que se entregue al destino en un mensaje de texto. El valor de `detail-type` es `Storage Gateway Object Upload Event`.

```
{
    "version": "0",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway Object Upload Event",
    "source": "aws.storagegateway",
    "account": "123456789012",
    "time": "2020-11-05T12:34:56Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:storagegateway:us-east-1:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-1:123456789011:gateway/sgw-712345DA",
        "arn:aws:s3:::do-not-delete-bucket"
    ],
    "detail": {
        "object-size": 1024,
        "modification-time": "2020-01-05T12:30:00Z",
        "object-key": "my-file.txt",
        "event-type": "object-upload-complete",
        "prefix": "prefix/",
        "bucket-name": "amzn-s3-demo-bucket",
    }
}
```

Nombres de los campos	Descripción
versión	Versión actual de la política de IAM.
id	ID que identifica la política de IAM.

Nombres de los campos	Descripción
detail-type	Descripción del evento que inició la notificación que se envió.
origen	El AWS servicio que es el origen de la solicitud y la notificación.
inscrita	El ID de la AWS cuenta desde la que se generaron la solicitud y la notificación.
hora	Cuándo se realizó la solicitud de carga de archivos a Amazon S3.
region	La AWS región desde la que se enviaron la solicitud y la notificación.
recursos	Los recursos de Storage Gateway a los que se aplica la política.
tamaño del objeto	El tamaño del objeto en bytes.
tiempo de modificación	La hora en que el cliente modificó el archivo.
clave de objeto	La ruta al archivo .
event-type	Los CloudWatch eventos que iniciaron la notificación.
prefix	El nombre del prefijo del bucket de S3.
bucket-name	Nombre del bucket de S3.

Obteniendo una notificación de carga de un conjunto de archivos en funcionamiento

Hay dos casos de uso en los que puede utilizar la notificación de carga de un conjunto de archivos en funcionamiento:

- Para automatizar el procesamiento en la nube de los archivos que se cargan, puedes llamar a la `NotifyWhenUploaded` API y obtener un ID de notificación. La notificación que se produce

cuando se carga el conjunto de archivos de trabajo tiene el mismo ID de notificación que el devuelto por la API. Si asigna este ID de notificación para hacer un seguimiento de la lista de archivos que está cargando, podrá iniciar el procesamiento del conjunto de archivos de trabajo que se cargan AWS cuando se genere el evento con el mismo ID.

- Para los casos de uso de distribución de contenido, puede tener dos puertas de enlace de archivos de S3 que se asignen al mismo bucket de Amazon S3. El cliente de compartición de archivos de Gateway1 puede cargar nuevos archivos en Amazon S3, y los clientes de compartición de archivos de Gateway2 leen los archivos. Los archivos se cargan en Amazon S3, pero Gateway2 no los ve porque utiliza una versión de los archivos en caché local de S3. Para que los archivos estén visibles en Gateway2, utilice la operación de NotifyWhenUploadedAPI para solicitar una notificación de carga de archivos a Gateway1, para que le notifique cuando finalice la carga del conjunto de archivos en funcionamiento. A continuación, puede utilizar los CloudWatch eventos para emitir automáticamente una RefreshCachesolicitud para compartir archivos en Gateway2. Cuando se complete la RefreshCachesolicitud, los nuevos archivos estarán visibles en Gateway2. Esta operación no importa archivos al almacenamiento en caché de la puerta de enlace. Solo actualiza el inventario en caché para reflejar los cambios en el inventario de los objetos del depósito de S3.

Example Ejemplo: notificación de carga de un conjunto de archivos de trabajo

El siguiente ejemplo muestra una notificación de carga de un conjunto de archivos en funcionamiento que se le envía CloudWatch cuando el evento coincide con la regla que ha creado. Esta notificación está en formato JSON. Puede configurar esta notificación para que se entregue al destino en un mensaje de texto. El valor de `detail-type` es `Storage Gateway File Upload Event`.

```
{
    "version": "2012-10-17",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway File Upload Event",
    "source": "aws.storagegateway",
    "account": "123456789012",
    "time": "2017-11-06T21:34:42Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:storagegateway:us-east-2:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-2:123456789011:gateway/sgw-712345DA"
    ],
    "detail": {
        "event-type": "upload-complete",
```

```
        "notification-id": "11b3106b-a18a-4890-9d47-a1a755ef5e47",
        "request-received": "2018-02-06T21:34:42Z",
        "completed": "2018-02-06T21:34:53Z"
    }
}
```

Nombres de los campos	Descripción
versión	Versión actual de la política de IAM.
id	ID que identifica la política de IAM.
detail-type	Una descripción del evento que inició la notificación que se envió.
origen	El AWS servicio que es el origen de la solicitud y la notificación.
inscrita	El ID de la AWS cuenta desde la que se generaron la solicitud y la notificación.
hora	Cuándo se realizó la solicitud de carga de archivos a Amazon S3.
region	La AWS región desde la que se enviaron la solicitud y la notificación.
recursos	Los recursos de Storage Gateway a los que se aplica la política.
event-type	Los CloudWatch eventos que iniciaron la notificación.
notification-id	ID generado de forma aleatoria de la notificación que se envió. Este ID tiene el formato UUID. Este es el ID de notificación que se devuelve cuando se llama a `NotifyWhenUploaded` .

Nombres de los campos	Descripción
request-received	Fecha y hora en que la gateway recibió la solicitud `NotifyWhenUploaded` .
completed	Cuando todos los archivos del conjunto de trabajo se cargaron en Amazon S3.

Recibir una notificación de actualización de la caché

Para el caso práctico de notificación de actualización de la caché, puede tener dos puertas de enlace de archivos de S3 que se asignen al mismo depósito de Amazon S3 y el cliente NFS para Gateway1 carga nuevos archivos en el depósito de S3. Los archivos se cargan en Amazon S3, pero no aparecen en Gateway2 hasta que se actualiza la memoria caché. Esto se debe a que Gateway2 utiliza una versión de los archivos en caché local de Amazon S3. Es posible que desee hacer algo con los archivos de Gateway2 una vez que finalice la actualización de la caché. Los archivos grandes pueden tardar un tiempo en aparecer en Gateway2, por lo que es posible que desee recibir una notificación cuando finalice la actualización de la memoria caché. Puede solicitar una notificación de actualización de la caché a Gateway2 para que le avise cuando todos los archivos estén visibles en Gateway2.

Example Ejemplo: notificación de actualización de la caché

En el siguiente ejemplo, se muestra una notificación de actualización de la caché que se le envía CloudWatch cuando el evento coincide con la regla que ha creado. Esta notificación está en formato JSON. Puede configurar esta notificación para que se entregue al destino en un mensaje de texto. El valor de `detail-type` es `Storage Gateway Refresh Cache Event`.

```
{
    "version": "2012-10-17",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway Refresh Cache Event",
    "source": "aws.storagegateway",
    "account": "209870788375",
    "time": "2017-11-06T21:34:42Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:storagegateway:us-east-2:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-2:123456789011:gateway/sgw-712345DA"
```

```
    ],
    "detail": {
        "event-type": "refresh-complete",
        "notification-id": "1c14106b-a18a-4890-9d47-a1a755ef5e47",
        "started": "2018-02-06T21:34:42Z",
        "completed": "2018-02-06T21:34:53Z",
        "folderList": [
            "/"
        ]
    }
}
```

Nombres de los campos	Descripción
versión	Versión actual de la política de IAM.
id	ID que identifica la política de IAM.
detail-type	Una descripción del tipo de evento que inició la notificación que se envió.
origen	El AWS servicio que es el origen de la solicitud y la notificación.
inscrita	El ID de la AWS cuenta desde la que se generaron la solicitud y la notificación.
hora	Fecha y hora en que se realizó la solicitud de actualización de los archivos del conjunto de trabajo.
region	La AWS región desde la que se enviaron la solicitud y la notificación.
recursos	Los recursos de Storage Gateway a los que se aplica la política.
event-type	Los CloudWatch eventos que iniciaron la notificación.

Nombres de los campos	Descripción
notification-id	ID generado de forma aleatoria de la notificación que se envió. Este ID tiene el formato UUID. Este es el ID de notificación que se devuelve cuando se llama a `RefreshCache` .
a	cuando la puerta de enlace recibió la `RefreshCache` solicitud y se inició la actualización.
completed	Fecha y hora en que finalizó la actualización del conjunto de trabajo.
folderList	Lista separada por comas de las rutas de las carpetas que se actualizaron en la caché. El valor predeterminado es ["/"].

Información acerca de las métricas de gateway

En la siguiente tabla se describen las métricas que cubren las pasarelas de archivos de S3. Cada puerta de enlace tiene un conjunto de métricas asociadas. Algunas métricas específicas de la pasarela tienen el mismo nombre que determinadas métricas. file-share-specific Estas métricas representan los mismos tipos de mediciones, pero se refieren a la puerta de enlace y no al recurso compartido de archivos.

Especifique siempre si desea trabajar con una puerta de enlace o un recurso compartido de archivos cuando trabaje con una métrica concreta. En concreto, al trabajar con métricas de puerta de enlace, debe especificar `Gateway Name` las 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 archivos S3 s.

Métrica	Descripción
`AvailabilityNotifications`	Esta métrica indica la cantidad de notificac iones de estado relacionadas con la disponibi lidad que generó la puerta de enlace en el período del informe. Unidades: recuento
`CacheFileSize`	Esta métrica registra el tamaño de los archivos de la memoria caché de la puerta de enlace. Utilice esta métrica con la `Average` estadística para medir el tamaño medio de un archivo en la memoria caché de la puerta de enlace. Utilice esta métrica con la `Max` estadística para medir el tamaño máximo de un archivo en la memoria caché de la puerta de enlace. Unidades: bytes
`CacheFree`	Esta métrica indica el número de bytes disponibles en la memoria caché de la puerta de enlace. Unidades: bytes
`CacheHitPercent`	Porcentaje de operaciones de lectura de aplicaciones desde la puerta de enlace que se gestionan desde la memoria caché. La muestra se obtiene al final del período de notificación. Cuando no hay operaciones de lectura de aplicaciones desde la puerta de enlace, esta métrica indica el 100 por ciento.

Métrica	Descripción
	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. Utilice esta métrica con la Sum estadística. Lo ideal sería que esta métrica permaneciera baja. Unidad: porcentaje
CachePercentUsed	El porcentaje de la caché de datos utilizado en toda la puerta de enlace. La muestra se obtiene al final del período de notificación. Unidad: porcentaje
CacheUsed	Esta métrica indica el número de bytes utilizado s en la memoria 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 estadísti ca Samples para medir las operaciones de entrada/salida por segundo (IOPS). Unidades: bytes

Métrica	Descripción
`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
`FilesFailingUpload`	Esta métrica registra el número de archivos en los que no se puede cargar. AWS Estos archivos generarán notificaciones de salud que contienen más información sobre el problema. Usa esta métrica con la `Sum` estadística para mostrar el número de archivos en los que no se pueden cargar AWS actualmente. Unidades: recuento
`FileSharesUnavailable`	Esta métrica proporciona el número de archivos compartidos en estas pasarelas que se encuentran en el estado No disponible. Si esta métrica indica que algún archivo compartido no está disponible, 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 muestre un valor distinto de cero. Unidades: recuento

Métrica	Descripción
FilesRenamed	Esta métrica registra el número de archivos a los que se ha cambiado el nombre en el período del informe. Unidades: recuento
HealthNotifications	Esta métrica indica el número de notificaciones de salud generadas por esta pasarela en el período del informe. Unidades: recuento
IndexEvictions	Esta métrica indica el número de archivos cuyos metadatos se eliminaron del índice de metadatos de archivos almacenado en caché 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 de los que se obtuvieron los 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 espera una respuesta del disco local. Unidad: porcentaje

Métrica	Descripción
`MemTotalBytes`	Esta métrica indica la cantidad total de memoria de la puerta de enlace. Unidades: bytes
`MemUsedBytes`	Esta métrica indica la cantidad de memoria utilizada en la puerta de enlace. Unidades: bytes
`NfsSessions`	Esta métrica indica el número de sesiones NFS que están activas en la puerta de enlace. Unidades: recuento
`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
`S3GetObjectRequestTime`	Esta métrica indica el tiempo que tarda la puerta de enlace en completar las solicitudes de obtención de objetos de S3. Unidades: milisegundos

Métrica	Descripción
S3PutObjectRequestTime	Esta métrica indica el tiempo que tarda la puerta de enlace en completar las solicitudes de colocación de objetos de S3. Unidades: milisegundos
S3UploadPartRequestTime	Esta métrica indica el tiempo que tarda la pasarela en completar las solicitudes de carga de piezas en S3. Unidades: milisegundos
SmbV1Sessions	Esta métrica indica el número de SMBv1 sesiones que están activas en la puerta de enlace. Unidades: recuento
SmbV2Sessions	Esta métrica indica el número de SMBv2 sesiones que están activas en la puerta de enlace. Unidades: recuento
SmbV3Sessions	Esta métrica indica el número de SMBv3 sesiones que están activas en la puerta de enlace. Unidades: recuento
TotalCacheSize	Esta métrica indica el tamaño total de la memoria caché. Unidades: bytes

Métrica	Descripción
`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 uso compartido de archivos

A continuación, encontrará información sobre las métricas de Storage Gateway que cubren los recursos compartidos de archivos. Cada recurso compartido de archivos tiene un conjunto de métricas asociado. Algunas de las métricas específicas de los recursos compartidos tienen el mismo nombre que determinadas métricas específicas de gateways. Estas métricas representan el mismo tipo de medidas, pero se asignan al volumen en lugar de al recurso compartido de archivos.

Especifique siempre si desea trabajar con una métrica de gateway o de recurso compartido. En concreto, cuando trabaje con métricas de recurso compartido de archivos, debe especificar el valor de `File share ID` que identifique el recurso compartido 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 usar para obtener información sobre sus recursos compartidos de archivos.

Métrica	Descripción
`CacheHitPercent`	Porcentaje de operaciones de lectura de aplicaciones desde los recursos compartidos de archivos que se sirven desde la memoria caché. La muestra se obtiene al final del período de notificación.

Métrica	Descripción
	Cuando no hay operaciones de lectura de aplicaciones desde el recurso compartido de archivos, esta métrica indica el 100 por ciento. Unidad: porcentaje
`CachePercentDirty`	La contribución del recurso compartido de archivos al porcentaje total de la memoria caché de la puerta de enlace que no se ha conservado de forma persistente. AWS La muestra se obtiene al final del período de notificación. Usa esta métrica con la `Sum` estadística. Lo ideal sería que esta métrica permaneciera baja. **Note** Utilice la `CachePercentDirty` métrica de la puerta de enlace para ver el porcentaje total de la memoria caché de la puerta de enlace que no se ha conservado de forma persistente. AWS Unidad: porcentaje
`CachePercentUsed`	El porcentaje de la caché de datos utilizado en toda la puerta de enlace. La muestra se obtiene al final del período de notificación. Esta métrica específica del uso compartido de archivos muestra el mismo valor que la métrica específic a de la puerta de enlace correspondiente. Unidad: porcentaje

Métrica	Descripción
`CloudBytesUploaded`	El número total de bytes en los que se cargó la puerta de enlace durante el período del informe AWS . 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
`FilesFailingUpload`	Esta métrica registra el número de archivos en los que no se puede cargar. AWS Estos archivos generarán notificaciones de salud que contienen más información sobre el problema. Usa esta métrica con la `Sum` estadística para mostrar el número de archivos en los que no se pueden cargar AWS actualmente. Unidades: recuento

Métrica	Descripción
`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 S3 FSx File Gateway

Los registros de auditoría de Amazon S3 File Gateway (S3 File Gateway) proporcionan detalles sobre el acceso de los usuarios a los archivos y carpetas de un recurso compartido de archivos. Puede usarlos para supervisar las actividades de los usuarios y tomar medidas si se identifican patrones de actividad inapropiados.

Operaciones

En la siguiente tabla se describen las operaciones de acceso a los archivos de registro de auditoría de S3 File Gateway.

Nombre de operación	Definición
Leer datos	Lea el contenido de un archivo.
Escribir datos	Cambia el contenido de un archivo.
Creación	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 archivo de registro de auditoría de S3 File Gateway.

Atributo	Definición
`accessMode`	La configuración de permisos para el objeto.
`accountDomain` (solo para pequeñas y medianas empresas)	El dominio de Directorio Activo (AD) al que pertenece la cuenta del cliente.
`accountName` (solo para pequeñas y medianas empresas)	El nombre de usuario de Active Directory del cliente.
`bucket`	El nombre de bucket de S3.
`clientGid` (solo NFS)	El identificador del grupo de usuarios que acceden al objeto.
`clientUid` (Solo NFS)	El identificador del usuario que accede al objeto.

Atributo	Definición
`ctime`	Hora en la que se modificó el contenido o los metadatos del objeto, establecida por el cliente.
`groupId`	El identificador del grupo propietario del objeto.
`fileSizeInBytes`	El tamaño del archivo en bytes, establecido por el cliente en el momento de la creación del archivo.
`gateway`	El ID de Storage Gateway.
`mtime`	El momento en el que el contenido del objeto fue modificado, establecido por el cliente.
`newObjectName`	La ruta de acceso completa al nuevo objeto después de que se haya cambiado el nombre.
`objectName`	La ruta completa al objeto.
`objectType`	Define si el objeto es un archivo o una carpeta.
`operation`	Nombre de la operación de acceso a objetos.
`ownerId`	Identificador del propietario del objeto.
`securityDescriptor` (solo SMB)	Muestra la lista de control de acceso discrecio nal (DACL) establecida en un objeto, en formato SDDL.
`shareName`	Nombre del recurso compartido al que se está accediendo.
`source`	Identificador del recurso compartido de archivos que se está auditando.
`sourceAddress`	La dirección IP del equipo cliente de recurso compartido de archivos.

Atributo	Definición
`status`	El estado de la operación. Solo se registra el éxito (los errores se registran con la excepción de los errores derivados de la denegación de permisos).
`timestamp`	Hora en la que se produjo la operación en función de la marca temporal del sistema operativo de la puerta de enlace.
`version`	Versión del formato de registro de auditoría.

Atributos registrados por operación

En la siguiente tabla se describen los atributos del registro de auditoría de S3 File Gateway registrados en cada operación de acceso a los archivos.

	Lea los datos	Escribe datos	Creación de una carpeta	Crear archivo	Cambie el nombre del archivo/carpeta	Eliminar archivo/carpeta	Escriba los atributos (cambie solo la ACL o SMB)	Escribir atributos (se muestra)	Escribe atributos (chmod)	Escribe atributos (chgrp)
`access e`			X	X					X	
`accoun main (s SMB)`	X	X	X	X	X	X	X	X	X	X
`accoun me (sol para pequeñ`	X	X	X	X	X	X	X	X	X	X

	Lea los datos	Escribe datos	Creación de una carpeta	Crear archivo	Cambie el nombre del archivo/carpeta	Eliminar archivo/carpeta	Escriba los atributos (cambie solo la ACL o SMB)	Escribir atributos (se muestra)	Escribe atributos (chmod)	Escribe atributos (chgrp)
y mediana empresa										
bucket	X	X	X	X	X	X	X	X	X	X
client (solo NFS)	X	X	X	X	X	X		X	X	X
client (solo NFS)	X	X	X	X	X	X		X	X	X
ctime			X	X						
groupI			X	X						
fileSi nBytes				X						
gatewa	X	X	X	X	X	X	X	X	X	X
mtime			X	X						
newObj Name					X					
object e	X	X	X	X	X	X	X	X	X	X

	Lea los datos	Escribe datos	Creación de una carpeta	Crear archivo	Cambie el nombre del archivo/c arpeta	Eliminar archivo/c arpeta	Escriba los atributos (cambie solo la ACL o SMB)	Escribir atributos (se muestra)	Escribe atributos (chmod)	Escribe atributos (chgrp)
object	X	X	X	X	X	X	X	X	X	X
operat	X	X	X	X	X	X	X	X	X	X
ownerI			X	X				X		
securi escrip (solo para pequeña y mediana empresa							X	X		
shareN	X	X	X	X	X	X	X	X	X	X
source	X	X	X	X	X	X	X	X	X	X
source ress	X	X	X	X	X	X	X	X	X	X
status	X	X	X	X	X	X	X	X	X	X
timest	X	X	X	X	X	X	X	X	X	X

	Lea los datos	Escribe datos	Creación de una carpeta	Crear archivo	Cambie el nombre del archivo/c arpeta	Eliminar archivo/c arpeta	Escriba los atributos (cambie solo la ACL o SMB)	Escribir atributos (se muestra)	Escribe atributos (chmod)	Escribe atributos (chgrp)
`versic`	X	X	X	X	X	X	X	X	X	X

Cree un informe de caché para su S3 File Gateway

S3 File Gateway puede generar un informe de los metadatos de los archivos que se encuentran actualmente en la memoria caché de carga local de un recurso compartido de archivos específico. Puede aplicar filtros y criterios adicionales que determinen qué tipos específicos de archivos en caché aparecen en el informe. Puede utilizar este informe para ayudar a identificar y resolver los problemas de las pasarelas. Por ejemplo, si tiene archivos que no se cargan desde su puerta de enlace a Amazon S3, puede generar un informe en el que se enumeren los archivos específicos que no se cargan y los motivos por los que no se carga. El informe es un archivo CSV que contiene una lista de archivos que coinciden con el conjunto de parámetros de filtro que especifique. El archivo de salida se almacena como un objeto de Amazon S3 en una ubicación de bucket que especifique al configurar el informe. Para crear un informe de caché mediante la AWS Storage Gateway API, consulte la referencia StartCacheReportde la API de Storage Gateway. Para crear un informe de caché en la consola Storage Gateway, utilice el siguiente procedimiento.

Requisitos previos

- Su puerta de enlace debe tener `s3:PutObject` `s3:AbortMultipartUpload` permisos para el depósito de Amazon S3 en el que desea almacenar el informe de caché.
- Actualmente, no hay ningún otro informe de caché en curso sobre el uso compartido de archivos.
- Debe haber menos de 10 informes de caché existentes para el recurso compartido de archivos.
- La puerta de enlace debe estar en línea y conectada a AWS.
- El disco raíz de la puerta de enlace debe tener al menos 20 GB de espacio libre.

Para crear un informe de caché mediante la consola Storage Gateway

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, seleccione Archivos compartidos y, a continuación, elija el recurso compartido de archivos para el que desee crear un informe de caché.
3. En el menú desplegable Acciones, selecciona Crear informe de caché.
4. Para la ubicación de Amazon S3, introduzca el depósito de Amazon S3 y el prefijo de la ubicación en la que desee guardar el objeto de archivo CSV del informe de caché completo en Amazon S3. Para seleccionar el depósito y el prefijo de su almacenamiento Amazon S3 existente, elija Browse S3.
5. Para la función de IAM, realice una de las siguientes acciones para especificar una función de IAM que conceda a File Gateway permisos para generar y almacenar su informe de caché:

   - Para especificar un rol de IAM existente, elija un rol de la lista desplegable.
   - Para crear manualmente un nuevo rol de IAM, seleccione Crear un rol y, a continuación, cree el nuevo rol mediante la consola de IAM.

   > **Note**
   >
   > La función de IAM que especifique debe tener los siguientes permisos para escribir objetos en la ubicación Amazon S3 del depósito de informes y detener las cargas de varias partes en el depósito de informes:
   >
   > - `s3:PutObject`
   > - `s3:AbortMultipartUpload`
   >
   > El rol también debe permitir que el `storagegateway.amazonaws.com` servicio asuma el rol mediante la acción. `sts:AssumeRole`

6. En el caso del filtro de informes, realice una de las siguientes acciones para determinar qué archivos se incluirán en el informe de caché:

   - Para incluir todos los archivos en caché que actualmente no se pueden cargar en Amazon S3, seleccione Todos los archivos no se pueden cargar.

- Para incluir solo los archivos que no se cargan en Amazon S3 por un motivo específico, seleccione Solo motivos específicos de error de carga. A continuación, si se trata de un error, seleccione uno o varios de los siguientes motivos:
  - Clase de almacenamiento inaccesible: la puerta de enlace no puede acceder a la clase de almacenamiento de Amazon S3 en la que está almacenado el objeto. Para obtener más información, consulte Error: InaccessibleStorageClass.
  - Estado del objeto no válido: el estado del archivo de la puerta de enlace no coincide con el estado de Amazon S3. Para obtener más información, consulte Error: InvalidObjectState.
  - Falta el objeto: el objeto se ha eliminado o movido en Amazon S3. Para obtener más información, consulte Error: ObjectMissing.
  - Acceso denegado a S3: la función de IAM de acceso al bucket de Amazon S3 no permite que la puerta de enlace realice la operación de carga. Para obtener más información, consulte Error: S3 AccessDenied.

> **Note**
>
> El indicador de archivos que no se pueden cargar se restablece cada 24 horas y durante el reinicio de la puerta de enlace. Si este informe captura los archivos después del restablecimiento, pero antes de que se vuelvan a marcar, no se indicarán como archivos que no se han cargado correctamente.

7. ¿Para utilizar un punto final de VPC para conectarse a S3? , realice una de las siguientes acciones para especificar cómo se conectará su puerta de enlace al bucket de Amazon S3:

   - Para conectarse directamente sin usar Amazon VPC, elija Connect directly to the bucket.
   - Para buscar una lista de puntos de enlace de Amazon VPC existentes, seleccione Elegir un punto de enlace de VPC y, a continuación, especifique un punto de enlace de la lista desplegable de puntos de enlace de VPC que aparece.
   - Para especificar un punto de enlace de Amazon VPC existente por su nombre de DNS, elija Introducir un nombre de DNS de punto de enlace de VPC y, a continuación, introduzca el nombre de DNS en el campo de nombre de DNS del punto de enlace de VPC que aparece.

> **Note**
>
> Si su recurso compartido de archivos utiliza un punto de enlace de VPC para conectarse a Amazon S3 para realizar operaciones normales, le recomendamos que utilice la misma VPC al configurar el informe de caché. La creación del informe de caché fallará si la puerta de enlace no se puede conectar al bucket de Amazon S3 por algún motivo, incluida una configuración de VPC no válida.

8. (Opcional) En Etiquetas: opcional, selecciona Añadir nueva etiqueta e introduce una clave y un valor para tu informe de caché.

   Una etiqueta es un par clave-valor que distingue entre mayúsculas y minúsculas y que le ayuda a clasificar los recursos de Storage Gateway. Agregar etiquetas puede facilitar el filtrado y la búsqueda del informe de caché. Puede repetir este paso para añadir hasta 50 etiquetas.

9. Elija Crear informe cuando haya terminado.

   Storage Gateway comienza a generar el informe. Puede comprobar el progreso y ver el estado en la pestaña Informes de caché de la página de detalles del archivo compartido.

Vea y gestione los informes de caché de su S3 File Gateway

Los informes de caché muestran los archivos que se encuentran actualmente en la memoria caché local de un recurso compartido de archivos específico, según los filtros y criterios que especifique. Puede ver una lista de los informes de caché existentes para un recurso compartido de archivos específico, comprobar el progreso y el estado de los informes y eliminar los informes que ya no necesite mediante la AWS Storage Gateway API o la consola Storage Gateway.

Para administrar los informes de caché mediante la API, consulte las siguientes secciones de la referencia de la API de Storage Gateway:

- ListCacheReports
- DescribeCacheReport
- CancelCacheReport
- DeleteCacheReport

Para administrar los informes de caché en la consola Storage Gateway, utilice el siguiente procedimiento.

Para administrar los informes de caché mediante la consola Storage Gateway

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, seleccione Archivos compartidos y, a continuación, elija el recurso compartido de archivos para el que desee administrar los informes de caché.
3. En la página de detalles del recurso compartido de archivos, seleccione la pestaña Informes en caché. Esta pestaña muestra los informes de caché existentes para el archivo compartido y proporciona información sobre el estado, el progreso y la ruta del objeto donde se almacena el archivo de informe en Amazon S3.
4. Realice una de las siguientes acciones:

   - Para ver detalles adicionales de un informe específico, como el ARN del informe y las etiquetas asociadas, elija un informe en la columna ID del informe.
   - Para especificar varios informes y gestionarlos simultáneamente, seleccione los informes mediante la columna de casillas de verificación.
5. Para administrar uno o más informes, elija una de las siguientes opciones en el menú desplegable Acciones:

   - Eliminar informe de caché: elimina el registro del informe de caché de la base de datos de Storage Gateway. Elimine los registros de los informes de caché obsoletos para dejar espacio para nuevos informes. Cada recurso compartido de archivos puede tener hasta 10 informes de caché existentes en cualquier momento.

     > **Note**
     >
     > Al eliminar el registro del informe en caché mediante este procedimiento, no se elimina el objeto del archivo de informe de Amazon S3.

   - Cancelar informe: esto cancela un informe que está en curso actualmente. Cancela un informe en curso si cometiste un error durante la configuración del informe o si el informe tarda un tiempo inusualmente largo en completarse. Confirme la cancelación cuando se le solicite.

> **Note**
>
> Los tiempos de finalización pueden variar considerablemente en función del número de archivos en la memoria caché. Por lo general, la mayoría de los informes se completan en 5 minutos.

La consola Storage Gateway muestra un mensaje que indica el resultado de la acción de cancelación o eliminación.

Comprenda la información proporcionada en los informes de caché de S3 File Gateway

Los informes de caché muestran los archivos que se encuentran actualmente en la memoria caché local de un recurso compartido de archivos específico, según los filtros y criterios que especifique. Cada informe de caché incluye la siguiente información:

- Bucket: el bucket o punto de acceso de Amazon S3 que está asociado al recurso compartido de archivos.
- S3 ObjectKey: el objeto de Amazon S3 que almacena los datos y metadatos de este archivo. Este objeto tiene los datos más recientes que se han cargado en S3, pero es posible que falten datos que no se puedan cargar en S3.
- FilePath— La ruta del archivo para la entrada del archivo en la memoria caché de la puerta de enlace. Aquí es donde puede encontrar el archivo al montar y explorar el recurso compartido de archivos.
- RenamedTo— La nueva ruta de un archivo renombrado. Al cambiar el nombre de un archivo de su recurso compartido de archivos, la puerta de enlace debe rastrear las ubicaciones antiguas y nuevas del archivo. Este campo muestra el lugar al que se ha movido el archivo, lo que te ayuda a realizar un seguimiento de las operaciones de cambio de nombre de un archivo, incluso si se le ha cambiado el nombre varias veces. Esta información resulta especialmente útil cuando necesita entender cómo los archivos de su recurso compartido de archivos se corresponden con los objetos de su bucket de Amazon S3.

  El siguiente ejemplo muestra las entradas del informe de caché para un escenario complejo en el que un archivo se sobrescribe directamente en Amazon S3 y, al mismo tiempo, se le cambia el

nombre a través de File Gateway. En este escenario, la puerta de enlace carga el archivo `A.txt` a S3 y, a continuación, desaloja el contenido del archivo para liberar espacio en la memoria caché local. A continuación, el objeto S3 asociado se sobrescribe directamente en S3 (no mediante una acción realizada por la puerta de enlace), lo que se `InvalidObjectState` debe a una discordancia entre el objeto S3 y lo que la puerta de enlace espera. Al mismo tiempo, se cambió el nombre del archivo a través de la puerta de enlace. `A.txt` `B.txt`

Bucket	S3 Objectk	FilePat	Renam	Tipo	IsDirt	IsDataI ty	IsDelet	IsFailin ToUplc	Upload or	SizeInE es	IsWholeFi leInCache
sample ket - iad	A.txt	/B.txt		FILE	TRUE	FALSC	FALSC	TRUE	Invalid(jectSta	4	FALSO
sample ket- iad	A.txt	/A.txt	/B.txt	FILE	TRUE	FALSC	TRUE	FALSC		4	FALSO

- Tipo: indica si la entrada es para un `FILE` o`DIRECTORY`.
- IsDirty— `TRUE` Indica si hay algún tipo de cambio en el archivo que no se haya cargado en Amazon S3. Esto incluye los cambios en los metadatos, como el nombre y read/write los permisos del archivo, incluso si los datos del archivo no han cambiado.
- IsDataDirty— `TRUE` Indica si hay cambios en los datos del archivo que no se han cargado en Amazon S3.
- IsDeleted— Indica `TRUE` si el archivo se ha eliminado de la puerta de enlace. Si un archivo está marcado como eliminado, siempre se marcará como sucio.
- IsFailingToUpload— Informa `TRUE` si hay algún problema al cargar el archivo en Amazon S3. Este estado se restablece cada 24 horas para que la puerta de enlace pueda volver a intentar subirla y comprobar si el problema se ha resuelto. La puerta de enlace rechaza cualquier nueva operación de escritura para un archivo que no se puede cargar. Si la puerta de enlace no tiene todo el archivo en caché, también rechaza las operaciones de lectura.
- UploadError— El error que impide que el archivo se cargue en Amazon S3. Para obtener más información y los pasos recomendados para resolver estos errores, consulte Solución de problemas: problemas con File Gateway.
- SizeInBytes— El tamaño total del archivo.

- IsWholeFileInCache— Indica TRUE si todos los datos del archivo están actualmente almacenados en la memoria caché de la puerta de enlace. Si esto es VERDADERO para un archivo que no se puede cargar en Amazon S3, la puerta de enlace permitirá que se lea el archivo.

Mantenimiento de su puerta de enlace

Mantenimiento de su Amazon S3 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 S3 File Gateway:

Temas

- Administración de actualizaciones de puertas de enlace- Aprenda a activar o desactivar las actualizaciones de mantenimiento y a modificar el cronograma de mantenimiento de su File Gateway.
- Realización de tareas de mantenimiento con la consola local- Aprenda a realizar tareas de mantenimiento mediante la consola local de la puerta de enlace.
- Apagar la máquina virtual de la 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 S3 existente por una nueva instancia- Aprenda a reemplazar su puerta de enlace de archivos S3 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 EC2 instancia de Amazon en la AWS 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 ni modificarla de forma alguna. Si se intenta instalar o actualizar cualquier paquete de software mediante métodos distintos al mecanismo de actualización habitual de la AWS puerta de enlace (por ejemplo, el SSM o las herramientas de hipervisor), es posible que la puerta de enlace no funcione correctamente.

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 funciones.
- Urgente: 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 funciones.

Todas las actualizaciones son acumulativas y actualizan las puertas de enlace a la versión actual cuando se aplican. Para obtener información sobre los cambios específicos incluidos en cada actualización, consulte las notas de la versión del software Gateway Appliance.

Todas las actualizaciones del dispositivo Gateway 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.

Al implementar y activar la puerta de enlace, se establece un cronograma de mantenimiento predeterminado. Puede modificar el calendario de periodos de mantenimiento en cualquier momento. También puedes desactivar las actualizaciones de mantenimiento, pero te recomendamos que las dejes activadas.

> **Note**
>
> Las actualizaciones urgentes se aplicarán de acuerdo con el calendario del período 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 AWS Health Dashboard. Para obtener más información, consulte AWS Health Dashboard. 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 o la EC2 instancia de Amazon 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.

- Realizar 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.
- Realizar tareas en la consola local de Amazon EC2 Gateway- Aprenda a iniciar sesión en la consola local para realizar tareas de configuración básica y avanzada para una EC2 puerta de enlace de Amazon, 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.

Para obtener acceso a la consola local de la gateway 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 ID 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 File Gateway Inicio de sesión en la consola .

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 File Gateway Inicio de sesión en la consola .

   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

Para 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 File Gateway Inicio de sesión en la consola .

   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.

Realizar tareas en la consola local de la máquina virtual

En el caso de una puerta de enlace de archivos implementada localmente, puede realizar las siguientes tareas de mantenimiento mediante 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

- Iniciar sesión en la consola local de File Gateway- Aprenda a iniciar sesión en la consola local, donde puede configurar los ajustes de la red de 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.
- Configurar los ajustes de la red de la puerta de enlace- Aprenda a configurar su puerta de enlace para que utilice DHCP o una dirección IP estática.
- Probar la conexión de red de la puerta de enlace- Aprenda a 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- Aprenda a comprobar los núcleos de CPU virtuales, el tamaño del volumen raíz y la RAM de su puerta de enlace.

- Configuración de un servidor de protocolo de tiempo de red (NTP) para su puerta de enlace- Aprenda a ver y editar las configuraciones del servidor del Network Time Protocol (NTP) y a sincronizar la hora de su 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, conectarse a Soporte ellas y mucho más.

Iniciar sesión en la consola local de File Gateway

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, utilice las credenciales predeterminadas para iniciar sesión. Estas credenciales de inicio de sesión predeterminadas le permiten acceder a los menús en los que puede configurar los ajustes de la red de la puerta de enlace y cambiar la contraseña desde la consola local. AWS Storage Gateway le permite establecer su propia contraseña desde la consola Storage Gateway en lugar de cambiarla desde la consola local. No es necesario que conozca la contraseña predeterminada para establecer una nueva contraseña. Para obtener más información, consulte Configuración de la contraseña de la consola local desde la consola Storage Gateway.

Para iniciar sesión en la consola local de la gateway

- Si es la primera vez que inicia sesión en la consola local, inicie sesión en la máquina virtual con las credenciales predeterminadas. El nombre de usuario y la contraseña predeterminados son `admin` y `password`, respectivamente. De lo contrario, utilice las credenciales para iniciar sesión.

> **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 Configuración de la contraseña de la consola local desde la consola Storage Gateway.

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

Cuando inicie sesión por primera vez en la consola local, inicie sesión en la máquina virtual con las credenciales predeterminadas. Se utilizarán las credenciales predeterminadas para todos los tipos de gateways. El nombre de usuario es `admin` y la contraseña es `password`.

Recomendamos que defina siempre una contraseña nueva inmediatamente después de crear una gateway nueva. Si lo desea, puede configurar esta contraseña desde la AWS Storage Gateway consola en lugar de hacerlo desde la consola local. No es necesario que conozca la contraseña predeterminada para establecer una nueva contraseña.

Para 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 Gateways y, a continuación, elija la gateway 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 predeterminada. Storage Gateway no guarda la contraseña, sino que la transmite de forma segura a la máquina virtual.

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

Configuración de un proxy HTTP

Las pasarelas de archivos admiten la configuración de un proxy HTTP.

> **Note**
>
> La única configuración de proxy que admite File Gateways 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.

Para configurar un proxy HTTP para una puerta de enlace de archivos

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.

Configurar los ajustes de la 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.

Para configurar la gateway 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 y configuración del AWS dispositivo, introduzca el número correspondiente para seleccionar la configuración de red.
3. En el menú de configuración de red, realice una de las siguientes tareas:

Para 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 •

Para llevar a cabo esta tarea	Haga lo siguiente
	Máscara de red • Dirección IP de la gateway • Estado de habilitación de DHCP Utilice los nombres de los adaptadores que aparecen aquí al configurar una dirección IP estática o al configurar el adaptador predeterminado de la puerta de enlace.
Configure el enrutamiento DHCP	Introduzca el número correspondiente para seleccionar Configurar DHCP. Se le pedirá que configure la interfaz de red para utilizar DHCP.

Para 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 Apagar la máquina virtual de la puerta de enlace. Si la puerta de enlace utiliza más de una interfaz de red, debe configurar todas las

Para llevar a cabo esta tarea	Haga lo siguiente
	interfaces activas para que utilicen direcciones IP estáticas o DHCP. 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.

Para 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.
Vea la configuración del nombre de host de su puerta de enlace	Introduzca el número correspondiente para seleccionar Ver la configuración del nombre de host. Se muestran el nombre de host, el modo de adquisición, el dominio y el dominio de Active Directory de la puerta de enlace.

Para 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 Apagar la máquina virtual de la puerta de enlace.
Establecer el adaptador de ruta predeterminada del gateway	Introduzca el número correspondiente para seleccionar Establecer adaptador predeterminado. Se muestran los adaptadores disponibles para la puerta de enlace y se le pide 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.

Para 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.

Para probar la conectividad de red de su 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. Para 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	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	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 de protocolo de tiempo de red (NTP) para su 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 y configuración del AWS dispositivo, introduzca el número correspondiente para seleccionar Administración del tiempo del sistema.
3. En el menú de gestión del tiempo del sistema, introduzca el número correspondiente para realizar una de las siguientes tareas.

Para 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 archivos determina la diferencia horaria con la máquina virtual de la puerta de enlace y la hora del servidor NTP le indica 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

Para 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 instalada VMware ESXi, basta con configurar la hora del host del hipervisor y sincronizar la hora de la máquina virtual con el host para evitar cambios 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 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.

Para 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 de la 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 de la 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, consulta Quieres que AWS Support te ayude a solucionar los problemas de tu EC2 puerta de enlace puerta de enlace.
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.

Realizar tareas en la consola local de Amazon EC2 Gateway

Algunas tareas de mantenimiento requieren que inicie sesión en la consola local cuando ejecute una puerta de enlace implementada en una EC2 instancia de Amazon. 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 Amazon EC2 Gateway- Aprenda a conectarse a la consola local de la puerta de enlace de su EC2 instancia de Amazon e iniciar sesión en ella mediante un cliente Secure Shell (SSH).
- Enrutamiento de su 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 AWS y una puerta de enlace implementada en una EC2 instancia de Amazon.
- Probar la conexión de red de la puerta de enlace- Aprenda a usar la consola local de la puerta de enlace para probar la conectividad de red entre su puerta de enlace y varios recursos de la red.
- Visualización del estado de los recursos de sistema de la puerta de enlace- Aprenda a usar la consola local de la puerta de enlace para comprobar los núcleos de CPU virtuales, el tamaño del volumen raíz y la RAM de la puerta de enlace.
- Ejecución de comandos de Storage Gateway en la consola local de una EC2 puerta de enlace de Amazon- Aprenda a ejecutar los comandos de la consola local para realizar tareas como guardar tablas de enrutamiento Soporte, conectarse y más.
- Configuración de los ajustes de red EC2 de Amazon Gateway- Aprenda a 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 EC2 instancia de Amazon.

Inicio de sesión en la consola local de Amazon EC2 Gateway

Inicia sesión en la consola local de la puerta de enlace de una EC2 instancia de Amazon mediante un cliente Secure Shell (SSH). Para obtener información detallada, consulta Connect to your instance en la Guía del EC2 usuario de Amazon. 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 EC2 claves de Amazon, consulte los pares de EC2 claves de Amazon en la Guía del EC2 usuario de Amazon.

Para iniciar sesión en la consola local de la gateway

1. Conéctate a la EC2 instancia de Amazon mediante SSH e inicia sesión como usuario administrador.
2. Tras iniciar sesión, verá el menú principal Activación y configuración del AWS dispositivo, desde el que podrá realizar diversas tareas.

Para obtener información sobre esta tarea	Consulte este tema
Configurar un proxy HTTP para la gateway	Enrutamiento de su puerta de enlace implementada en Amazon EC2 a través de un proxy HTTP
Configurar la red para la gateway	Configuración de los ajustes de red EC2 de Amazon Gateway
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 de una EC2 puerta de enlace de Amazon

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

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

Enrutamiento de su puerta de enlace implementada en Amazon EC2 a través de un proxy HTTP

Storage Gateway admite 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.

Para 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 Amazon EC2 Gateway.
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.

Para 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 Amazon EC2 Gateway.
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. Para 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	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 se inicia File Gateway, comprueba los núcleos de la CPU virtual, el tamaño del volumen raíz y la RAM. A continuación, 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 su Amazon EC2 File Gateway. Para obtener instrucciones, consulte Inicio de sesión en la consola local de Amazon EC2 Gateway.
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 [FALLO] para indicar el estado del recurso de la siguiente manera:

Mensaje	Descripción
[OK]	El recurso ha superado la comprobación de recursos del sistema.
[WARNING]	El recurso no cumple los requisitos recomendados, pero la puerta de enlace puede seguir funcionando. La consola local de la puerta de

Mensaje	Descripción
	enlace muestra un mensaje que describe 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 que describe los resultados de la comprobación de recursos.

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

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

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

Para 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 Amazon EC2 Gateway.
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.

Comando	Función
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 de la 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 de la 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.

Comando	Función
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 los ajustes de red EC2 de Amazon Gateway

Puede ver y configurar los ajustes de red de su Amazon EC2 File Gateway mediante la consola local de la puerta de enlace.

Para configurar los ajustes de red

1. Inicie sesión en la consola local de su Amazon EC2 File Gateway. Para obtener instrucciones, consulte Inicio de sesión en la consola local de Amazon EC2 Gateway.
2. En el menú principal Activación y configuración del AWS dispositivo, introduzca el número correspondiente para seleccionar la configuración de red.
3. En el menú Activación del AWS dispositivo: configuración de red, introduzca el número correspondiente a la tarea que desee realizar:

   - Editar la 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 la configuración de DNS: la consola local de la puerta de enlace muestra los adaptadores disponibles para los servidores DNS principal y secundario.
   - Configurar el nombre de host: la consola local de la puerta de enlace le pide que elija si la puerta de enlace utilizará el nombre de host estático que especifique o si lo adquirirá automáticamente a través de DCHP o rDNS.

> **Note**
>
> Si decide configurar 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 la configuración del nombre de host: la consola local de la puerta de enlace muestra el nombre de host, el modo de adquisición, el dominio y el dominio de Active Directory de su Amazon File Gateway. EC2

Apagar la máquina virtual de la puerta de enlace

Puede que tenga que apagar la máquina virtual o reiniciarla para realizar tareas de mantenimiento, como aplicar un parche al hipervisor. Apaga la puerta de enlace local VMs mediante la interfaz de hipervisor y las EC2 instancias de Amazon mediante la consola de Amazon EC2 .

> **Important**
>
> Si detiene e inicia una EC2 puerta de enlace de Amazon que utiliza almacenamiento efímero, la puerta de enlace quedará desconectada 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 instancia nueva EC2 .

Sustituir la puerta de enlace de archivos de S3 existente por una nueva instancia

Puede reemplazar una puerta de enlace de archivos S3 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 tengas que hacerlo si quieres mover tu puerta de enlace a una plataforma de alojamiento mejor o a EC2 instancias de Amazon más nuevas, o si deseas actualizar el hardware del servidor subyacente.

Existen dos métodos para reemplazar una pasarela de archivos de S3 existente. En la siguiente tabla se describen las ventajas y desventajas de cada método. Con esta información, seleccione el

método que mejor se adapte a su entorno de puerta de enlace y, a continuación, consulte los pasos del procedimiento en la sección correspondiente que aparece a continuación.

> **Note**
>
> Si necesita iniciar sesión en la consola local de su nuevo Storage Gateway para completar cualquiera de los métodos, el nombre de usuario predeterminado es admin y la contraseña predeterminada es password.

	Método 1: migrar el disco caché y el ID de la puerta de enlace a la instancia de reemplazo	Método 2: reemplazar la instancia por un disco de caché vacío y un nuevo ID de puerta de enlace
Guardar en caché los datos del disco	Se conservan los datos del disco caché. Este método resulta útil si la puerta de enlace tiene un disco caché de gran tamaño o si las aplicaciones son sensibles al retraso provocado por las operaciones de out-of-cache lectura.	Los datos de la caché se descargan de la AWS nube. Este método es óptimo para cargas de trabajo de escritura intensiva, si sus aplicacio nes pueden tolerar el retraso provocado por las lecturas. out-of-cache
Tiempo de inactividad	Su puerta de enlace estará fuera de línea durante una o dos horas durante el proceso de migración.	Los archivos compartidos siempre están disponibles, pero los clientes experimen tarán un breve periodo de inactividad al cambiar de un recurso compartido de archivos a otro durante la transición a la nueva instancia .

	Método 1: migrar el disco caché y el ID de la puerta de enlace a la instancia de reemplazo	Método 2: reemplazar la instancia por un disco de caché vacío y un nuevo ID de puerta de enlace
		Note No se admite la escritura simultáne a en un bucket de Amazon S3 desde dos recursos compartid os de archivos, por lo que todos los clientes deben reasignarse de un recurso compartid o a otro simultáne amente, en lugar de hacerlo de forma gradual.
ID de puerta de enlace	La nueva puerta de enlace hereda el ID de puerta de enlace de la puerta de enlace a la que sustituye.	La puerta de enlace existente y la puerta de enlace de reemplazo tienen una puerta de enlace IDs única e independiente.

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.

Método 1: migrar el disco caché y el ID de puerta de enlace a la instancia de reemplazo

Para migrar el disco caché y el ID de Gateway de S3 a una instancia de reemplazo:

1. Detenga cualquier aplicación que esté grabando en la puerta de enlace de archivos de S3 existente.
2. Compruebe que la `CachePercentDirty` métrica de la pestaña Supervisión de la puerta de enlace de archivos de S3 existente sea`0`.
3. Cierre la puerta de enlace de archivos de S3 existente apagando la máquina virtual (VM) host mediante los controles del hipervisor.

   Para obtener más información sobre cómo cerrar una EC2 instancia de Amazon, consulta Detener e iniciar una instancia en la Guía del EC2 usuario de Amazon.

   Para obtener más información sobre cómo apagar una máquina virtual KVM o Hyper-V VMware, consulte la documentación del hipervisor.
4. Separe todos los discos, incluidos el disco raíz y los discos de caché, de la antigua máquina virtual de puerta de enlace.

   > **Note**
   >
   > Anote el ID de volumen del disco raíz, así como el ID de puerta de enlace asociado a ese disco raíz. Deberá separar este disco del nuevo hipervisor Storage Gateway en un paso posterior.

   Si utiliza una EC2 instancia de Amazon como máquina virtual para su puerta de enlace de archivos S3 , consulte Separar un volumen de Amazon EBS de una instancia de Windows o Separar un volumen de Amazon EBS de una instancia de Linux en la Guía del usuario de Amazon. EC2

   Para obtener información sobre cómo separar discos de una máquina virtual KVM o Hyper-V VMware, consulte la documentación del hipervisor.
5. Cree una nueva instancia de máquina virtual con AWS Storage Gateway hipervisor, pero no la active como puerta de enlace. En un paso posterior, esta nueva máquina virtual asumirá la identidad de la puerta de enlace anterior.

Para obtener más información sobre la creación de una nueva máquina virtual con hipervisor Storage Gateway, consulte Elegir una plataforma de host y descargar la máquina virtual.

> **Note**
>
> No añada discos de caché para la nueva máquina virtual. Esta máquina virtual utilizará los mismos discos de caché que utilizaba la máquina virtual anterior.

6. Configure su nueva máquina virtual Storage Gateway para que utilice la misma configuración de red que la máquina virtual anterior.

   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.

   Si necesita configurar manualmente una dirección IP estática para su máquina virtual de puerta de enlace, consulte Configurar los parámetros de red.

   Si la máquina virtual de puerta de enlace debe usar un proxy Socket Secure versión 5 (SOCKS5) para conectarse a Internet, consulte Enrutar la puerta de enlace implementada EC2 mediante un proxy HTTP.
7. Inicie la nueva máquina virtual Storage Gateway.
8. Conecte los discos que desconectó de la máquina virtual de puerta de enlace anterior a la nueva máquina virtual de puerta de enlace. No separe el disco raíz existente de la nueva máquina virtual de puerta de enlace.

   > **Note**
   >
   > Para que la migración se realice correctamente, todos los discos deben permanecer sin cambios. Cambiar el tamaño del disco u otros valores provoca incoherencias en los metadatos que impiden que la migración se realice correctamente.

9. Inicie el proceso de migración de la puerta de enlace conectándose a la nueva máquina virtual con una URL que utilice el siguiente formato:

   `http://`*`your-VM-IP-address`*`/migrate?gatewayId=`*`your-gateway-ID`*

   Puede usar la misma dirección IP para la nueva máquina virtual de puerta de enlace que usó para la máquina virtual de puerta de enlace anterior. Para usar la misma IP, elimine primero

la puerta de enlace anterior y, a continuación, continúe con el paso 5. La URL debe tener un aspecto similar al del siguiente ejemplo:

http://*198.51.100.123*/migrate?gatewayId=*sgw-12345678*

Usa esta URL desde un navegador o desde la línea de comandos mediante cURL.

Cuando la migración de la puerta de enlace se inicia correctamente, aparece el siguiente mensaje:

```
Successfully imported Storage Gateway information. Please refer to Storage Gateway
 documentation to perform the next steps to complete the migration.
```

10. Espere a que el estado de la puerta de enlace aparezca como En ejecución en la AWS Storage Gateway consola. Según el ancho de banda disponible, esto puede tardar hasta 10 minutos.
11. Detenga la nueva máquina virtual Storage Gateway.
12. Separe el disco raíz de la puerta de enlace anterior, cuyo ID de volumen indicó anteriormente, de la nueva puerta de enlace.
13. Inicie la nueva máquina virtual Storage Gateway.
14. Si la puerta de enlace estaba unida a un dominio de Active Directory, vuelva a unirse al dominio. Para obtener instrucciones, consulte Uso de Active Directory para autenticar usuarios.

> **Note**
>
> Debe completar este paso aunque el estado de la puerta de enlace de archivos de S3 aparezca como Unido.

15. Confirme que sus recursos compartidos estén disponibles en la dirección IP de la nueva máquina virtual de puerta de enlace y, a continuación, elimine la máquina virtual de puerta de enlace anterior.

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

Para obtener más información sobre la eliminación de una EC2 instancia de Amazon, consulta Terminar tu instancia en la Guía del EC2 usuario de Amazon. Para obtener más información

sobre cómo eliminar una máquina virtual KVM o Hyper-V, consulte la documentación del hipervisor. VMware

Método 2: reemplazar la instancia por un disco caché vacío y un nuevo ID de puerta de enlace

Para configurar una instancia de S3 File Gateway de reemplazo con el disco 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 S3 existente. Compruebe que la `CachePercentDirty` métrica de la pestaña Supervisión se encuentra `0` antes de configurar los recursos compartidos 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 S3 y los recursos compartidos de archivos existentes de la siguiente manera:

   a. Guarde la información de configuración de la puerta de enlace para la puerta de enlace de archivos de S3 .

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

   Este comando genera un bloque JSON que contiene metadatos sobre la puerta de enlace, como su nombre, las interfaces de red, la zona horaria configurada y su estado (si la puerta de enlace está en ejecución).

   b. Guarde la configuración del bloque de mensajes del servidor (SMB) de la puerta de enlace de archivos S3 .

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

   Este comando genera un bloque JSON que contiene metadatos sobre el recurso compartido de archivos SMB, como su nombre de dominio, el estado de Microsoft Active Directory, si se ha establecido la contraseña de invitado y el tipo de estrategia de seguridad.

   c.
   - Use el siguiente comando para compartir archivos SMB.

```
aws storagegateway describe-smb-file-shares --file-share-arn-list
 "arn:aws:storagegateway:us-east-2:123456789012:share/share-987A654B"
```

Este comando genera un bloque JSON que contiene metadatos sobre el recurso compartido de archivos SMB, como su nombre, clase de almacenamiento, estado, función de IAM, Amazon Resource Name (ARN), una lista de clientes que pueden acceder a S3 File Gateway y la ruta utilizada por el cliente SMB para identificar el punto de montaje.

- Utilice el siguiente comando para los recursos compartidos de archivos NFS.

```
aws storagegateway  describe-nfs-file-shares --file-share-arn-list
 "arn:aws:storagegateway:us-east-2:123456789012:share/share-321A978B"
```

Este comando genera un bloque JSON que contiene metadatos sobre el recurso compartido de archivos NFS, como su nombre, clase de almacenamiento, estado, ARN del rol de IAM, una lista de clientes que pueden acceder a la puerta de enlace de archivos de S3 y la ruta utilizada por el cliente NFS para identificar el punto de montaje.

3. Cree una nueva puerta de enlace de archivos S3 con los mismos ajustes y la misma configuración que la puerta de enlace anterior. Si es necesario, consulte la información que guardó en el paso 2.
4. Cree nuevos recursos compartidos de archivos para la nueva puerta de enlace con los mismos ajustes y configuración que los recursos compartidos 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 separe sus clientes de los antiguos recursos compartidos de archivos a los nuevos recursos compartidos de archivos 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 S3 , 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 EC2 instancia anterior de Amazon o VM de gateway.

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 de AWS Storage Gateway administración y sus conexiones con el compartidos 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**
>
> En el caso de las puertas de enlace implementadas en una EC2 instancia de Amazon, la instancia seguirá existiendo hasta que la elimines.
> 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.

Para 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**
>
> Ya no paga los cargos de software después de eliminar una puerta de enlace, pero recursos como el bucket de Amazon S3 y EC2 las instancias de Amazon persisten. Puedes eliminar

la EC2 instancia de puerta de enlace de Amazon después de eliminar la puerta de enlace de archivos. Si no necesita los datos de los buckets de Amazon S3 asociados a los archivos compartidos, puede optar por eliminar los buckets de Amazon S3. Para obtener instrucciones, consulte Eliminar un depósito.

Rendimiento y optimización

En esta sección se describen las directrices y las prácticas recomendadas para optimizar el rendimiento de File Gateway.

Temas

- Guía básica de rendimiento para S3 File Gateway FSx
- Guía de rendimiento para pasarelas con varios archivos compartidos
- Maximizar el rendimiento de S3 File Gateway
- Optimización de S3 File Gateway para las copias de seguridad de bases de datos de SQL Server

Guía básica de rendimiento para S3 File Gateway FSx

En esta sección, encontrará instrucciones para el aprovisionamiento de hardware para su máquina virtual S3 File Gateway. Las configuraciones de instancia que se muestran 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 de almacenamiento efímero con puertas de enlace EC2 .
> En el caso de EC2 las instancias de Amazon, si tiene más de 5 millones de objetos en su bucket de S3 y utiliza un volumen SSD de uso general, se necesita un volumen EBS raíz mínimo de 350 GiB para que su gateway tenga un rendimiento aceptable durante la puesta en marcha. Para obtener información sobre cómo aumentar el tamaño del volumen, consulte Modificación de un volumen de EBS mediante volúmenes elásticos (consola).
> El límite de tamaño sugerido para los directorios individuales de los que se conecten a File Gateway es de 10 000 archivos por directorio. Puede usar File Gateway con directorios que tengan más de 10 000 archivos, pero es posible que el rendimiento se vea afectado.

En las tablas siguientes, las operaciones de lectura de visitas a la memoria caché son lecturas de los archivos compartidos que se sirven desde la memoria caché. Las operaciones de lectura errónea de la caché son lecturas de los recursos compartidos de archivos que se sirven desde Amazon S3.

En las siguientes tablas se muestran ejemplos de configuraciones de S3 File Gateway.

Rendimiento de S3 File Gateway en clientes Linux

Ejemplo de configuraciones	Protocolo	Rendimiento de escritura (tamaños de archivo de 1 GB)	Rendimiento de lectura alcanzado por la memoria caché	La memoria caché pierde el rendimiento de lectura
Disco raíz: 80 GB, io1 SSD, 4000 IOPS Disco caché: caché de 512 GiB, io1, 1500 IOPS aprovisionadas Rendimiento mínimo de red: 10 Gbps CPU: 16 CPU virtuales | RAM: 32 GB Se recomienda el protocolo NFS para Linux	NFSv3 - 1 hilo	110 MiB/sec (0,92 Gbps)	590 MiB/sec (4,9 Gbps)	310 MiB/sec (2,6 Gbps)
	NFSv3 - 8 hilos	160 MiB/sec (1,3 Gbps)	590 MiB/sec (4,9 Gbps)	335 MiB/sec (2,8 Gbps)
	NFSv4 - 1 hilo	130 MiB/sec (1,1 Gbps)	590 MiB/sec (4,9 Gbps)	295 MiB/sec (2,5 Gbps)
	NFSv4 - 8 hilos	160 MiB/sec (1,3 Gbps)	590 MiB/sec (4,9 Gbps)	335 MiB/sec (2,8 Gbps)
	SMBV3 - 1 hilo	115 MiB/sec (1,0 Gbps)	325 MiB/sec (2,7 Gbps)	255 MiB/sec (2,1 Gbps)
	SMBV3 - 8 hilos	190 MiB/sec (1,6 Gbps)	590 MiB/sec (4,9 Gbps)	335 MiB/sec (2,8 Gbps)
Dispositivo de hardware de Storage Gateway	NFSv3 - 1 hilo	265 MiB/sec (2,2 Gbps)	590 MiB/sec (4,9 Gbps)	310 MiB/sec (2,6 Gbps)

Ejemplo de configuraciones	Protocolo	Rendimiento de escritura (tamaños de archivo de 1 GB)	Rendimiento de lectura alcanzado por la memoria caché	La memoria caché pierde el rendimiento de lectura
Rendimiento mínimo de red: 10 Gbps	NFSv3 - 8 hilos	385 MiB/sec (3,1 Gbps)	590 MiB/sec (4,9 Gbps)	335 MiB/sec (2,8 Gbps)
	NFSv4 - 1 hilo	310 MiB/sec (2,6 Gbps)	590 MiB/sec (4,9 Gbps)	295 MiB/sec (2,5 Gbps)
	NFSv4 - 8 hilos	385 MiB/sec (3,1 Gbps)	590 MiB/sec (4,9 Gbps)	335 MiB/sec (2,8 Gbps)
	SMBV3 - 1 hilo	275 MiB/sec (2,4 Gbps)	325 MiB/sec (2,7 Gbps)	255 MiB/sec (2,1 Gbps)
	SMBV3 - 8 hilos	455 MiB/sec (3,8 Gbps)	590 MiB/sec (4,9 Gbps)	335 MiB/sec (2,8 Gbps)
Disco raíz: 80 GB, io1 SSD, 4000 IOPS Disco caché: 4 discos caché NVME de 2 TB Rendimiento mínimo de red: 10 Gbps CPU: 32 vCPU | RAM: 24 GB Se recomienda el protocolo NFS para Linux	NFSv3 - 1 hilo	300 MiB/sec (2,5 Gbps)	590 MiB/sec (4,9 Gbps)	325 MiB/sec (2,7 Gbps)
	NFSv3 - 8 hilos	585 MiB/sec (4,9 Gbps)	590 MiB/sec (4,9 Gbps)	580 MiB/sec (4,8 Gbps)
	NFSv4 - 1 hilo	355 MiB/sec (3,0 Gbps)	590 MiB/sec (4,9 Gbps)	340 MiB/sec (2,9 Gbps)
	NFSv4 - 8 hilos	575 MiB/sec (4,8 Gbps)	590 MiB/sec (4,9 Gbps)	575 MiB/sec (4,8 Gbps)
	SMBV3 - 1 hilo	230 MiB/sec (1,9 Gbps)	325 MiB/sec (2,7 Gbps)	245 MiB/sec (2,0 Gbps)
	SMBV3 - 8 hilos	585 MiB/sec (4,9 Gbps)	590 MiB/sec (4,9 Gbps)	580 MiB/sec (4,8 Gbps)

Rendimiento de File Gateway en clientes Windows

Ejemplo de configuraciones	Protocolo	Rendimiento de escritura (tamaños de archivo de 1 GB)	Rendimiento de lectura alcanzado por la memoria caché	La memoria caché pierde el rendimiento de lectura
Disco raíz: 80 GB, io1 SSD, 4000 IOPS Disco caché: caché de 512 GiB, io1, 1500 IOPS aprovisionadas Rendimiento mínimo de red: 10 Gbps CPU: 16 CPU virtuales | RAM: 32 GB Se recomienda el protocolo SMB para Windows	SMBV3 - 1 hilo	150 MiB/sec (1,3 Gbps)	180 MiB/sec (1,5 Gbps)	20 MiB/sec (0,2 Gbps)
	SMBV3 - 8 hilos	190 MiB/sec (1,6 Gbps)	335 MiB/sec (2,8 Gbps)	195 MiB/sec (1,6 Gbps)
	NFSv3 - 1 hilo	95 MiB/sec (0,8 Gbps)	130 MiB/sec (1,1 Gbps)	20 MiB/sec (0,2 Gbps)
	NFSv3 - 8 hilos	190 MiB/sec (1,6 Gbps)	330 MiB/sec (2,8 Gbps)	190 MiB/sec (1,6 Gbps)
Dispositivo de hardware de Storage Gateway Rendimiento mínimo de red: 10 Gbps	SMBV3 - 1 hilo	230 MiB/sec (1,9 Gbps)	255 MiB/sec (2,1 Gbps)	20 MiB/sec (0,2 Gbps)
	SMBV3 - 8 hilos	835 MiB/sec (7,0 Gbps)	475 MiB/sec (4,0 Gbps)	195 MiB/sec (1,6 Gbps)
	NFSv3 - 1 hilo	135 MiB/sec (1,1 Gbps)	185 MiB/sec (1,6 Gbps)	20 MiB/sec (0,2 Gbps)

Ejemplo de configuraciones	Protocolo	Rendimiento de escritura (tamaños de archivo de 1 GB)	Rendimiento de lectura alcanzado por la memoria caché	La memoria caché pierde el rendimiento de lectura
	NFSv3 - 8 hilos	545 MiB/sec (4,6 Gbps)	470 MiB/sec (4,0 Gbps)	190 MiB/sec (1,6 Gbps)
Disco raíz: 80 GB, io1 SSD, 4000 IOPS Disco caché: 4 discos caché NVME de 2 TB Rendimiento mínimo de red: 10 Gbps CPU: 32 vCPU | RAM: 24 GB Se recomienda el protocolo SMB para Windows	SMBV3 - 1 hilo	230 MiB/sec (1,9 Gbps)	265 MiB/sec (2,2 Gbps)	30 MiB/sec (0,3 Gbps)
	SMBV3 - 8 hilos	835 MiB/sec (7,0 Gbps)	780 MiB/sec (6,5 Gbps)	250 MiB/sec (2,1 Gbps)
	NFSv3 - 1 hilo	135 MiB/sec (1.1). Gbps)	220 MiB/sec (1,8 Gbps)	30 MiB/sec (0,3 Gbps)
	NFSv3 - 8 hilos	545 MiB/sec (4,6 Gbps)	570 MiB/sec (4,8 Gbps)	240 MiB/sec (2,0 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.

Guía de rendimiento para pasarelas con varios archivos compartidos

Amazon S3 File Gateway admite la conexión de hasta 50 recursos compartidos de archivos a un único dispositivo Storage Gateway. Al agregar varios recursos compartidos de archivos por puerta de enlace, puede admitir más usuarios y cargas de trabajo y, al mismo tiempo, administrar menos puertas de enlace y recursos de hardware virtual. Además de otros factores, la cantidad de recursos compartidos de archivos gestionados por una puerta de enlace puede afectar al rendimiento de esa puerta de enlace. En esta sección se describe cómo se espera que cambie el rendimiento de las puertas de enlace en función de la cantidad de recursos compartidos de archivos adjuntos y se recomiendan configuraciones de hardware virtual para optimizar el rendimiento de las puertas de enlace que administran varios recursos compartidos.

En general, aumentar el número de recursos compartidos de archivos administrados por un único Storage Gateway puede tener las siguientes consecuencias:

- Aumento del tiempo necesario para reiniciar la puerta de enlace.
- Mayor utilización de los recursos de hardware virtual, como vCPU y RAM.
- Disminución del rendimiento de las operaciones de datos y metadatos si los recursos de hardware virtual se saturan.

En la siguiente tabla se enumeran las configuraciones de hardware virtual recomendadas para las puertas de enlace que administran varios recursos compartidos de archivos:

Recursos compartidos de archivos por puerta de enlace	Configuración de capacidad de puerta de enlace recomendada	Núcleos de vCPU recomendados	RAM recomendada	Tamaño de disco recomendado			
1-10	Pequeña	4 (tipo de EC2 instancia	16 GiB	80 GiB			

Recursos compartidos de archivos por puerta de enlace	Configuración de capacidad de puerta de enlace recomendada	Núcleos de vCPU recomendados	RAM recomendada	Tamaño de disco recomendado			
		m4.xlarge o superior)					
10-20	Medio	8 (tipo de EC2 instancia m4.2xlarge o superior)	32 GiB	160 GiB			
Más de 20	Grande	16 (tipo de EC2 instancia m4.4xlarge o superior)	64 GiB	240 GiB			

Además de las configuraciones de hardware virtual recomendadas anteriormente, recomendamos las siguientes prácticas recomendadas para configurar y mantener los dispositivos Storage Gateway que administran varios recursos compartidos de archivos:

- Tenga en cuenta que la relación entre la cantidad de archivos compartidos y la demanda que se ejerce sobre el hardware virtual de la puerta de enlace no es necesariamente lineal. Algunos recursos compartidos de archivos pueden generar más rendimiento y, por lo tanto, más demanda de hardware que otros. Las recomendaciones de la tabla anterior se basan en las capacidades máximas de hardware y en varios niveles de rendimiento de los recursos compartidos de archivos.

- Si considera que agregar varios recursos compartidos de archivos a una sola puerta de enlace reduce el rendimiento, considere la posibilidad de mover los recursos compartidos de archivos más activos a otras puertas de enlace. En concreto, si se utiliza un recurso compartido de archivos para una very-high-throughput aplicación, considere la posibilidad de crear una puerta de enlace independiente para ese recurso compartido de archivos.
- No recomendamos configurar una puerta de enlace para varias aplicaciones de alto rendimiento y otra para varias aplicaciones de bajo rendimiento. En su lugar, intente distribuir los archivos compartidos de alto y bajo rendimiento de manera uniforme entre las pasarelas para equilibrar la saturación del hardware. Para medir el rendimiento del uso compartido de archivos, utilice las `ReadBytes` métricas y. `WriteBytes` Para obtener más información, consulta Cómo entender las métricas de uso compartido de archivos.

Maximizar el rendimiento de S3 File Gateway

En las siguientes secciones se describen las prácticas recomendadas para maximizar el rendimiento entre sus clientes NFS y SMB, S3 File Gateway y Amazon S3. La orientación que se proporciona en cada sección contribuye 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 Soporte implementaciones de S3 File Gateway. Al implementar y probar estas sugerencias, tenga en cuenta que cada implementación de S3 File Gateway es única, por lo que los resultados pueden variar.

S3 File Gateway proporciona una interfaz de archivos para almacenar y recuperar objetos de Amazon S3 mediante protocolos de archivos NFS o SMB estándares del sector, con un mapeo 1:1 nativo 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 nube AWS como una instancia de Amazon. EC2 S3 File Gateway no está diseñado para sustituir completamente al NAS empresarial. S3 File Gateway emula un sistema de archivos, pero no es un sistema de archivos. 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.

Implemente su puerta de enlace en la misma ubicación que sus clientes

Recomendamos implementar su dispositivo virtual S3 File Gateway en una ubicación física con la menor latencia de red posible entre él y sus clientes NFS o SMB. Al elegir una ubicación para su 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 NFS o SMB.
- S3 File Gateway está diseñado 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 S3 File Gateway implementadas en Amazon EC2, recomendamos mantener la puerta de enlace y los clientes NFS o SMB en el mismo grupo de ubicación. Para obtener más información, consulte Grupos de ubicación para sus EC2 instancias de Amazon en la Guía del usuario de Amazon Elastic Compute Cloud.

Reduzca 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 el disco, tenga en cuenta lo siguiente:

- `IoWaitPercent`indica el porcentaje de tiempo que la CPU espera una respuesta de los discos raíz o de la memoria caché.
- Cuando `IoWaitPercent` es superior al 5 o 10%, suele indicar un cuello de botella en el rendimiento de la puerta de enlace provocado por discos con un rendimiento inferior. 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`.

Ajuste 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 archivos de S3, es importante asignar suficientes recursos a la máquina virtual de la 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 para cargas de trabajo más grandes, recomendamos 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 `UserCpuPercent` métrica. Para obtener más información, consulta Cómo entender las métricas de las puertas de enlace.
- Aumente la RAM asignada a entre 32 y 64 GB.

  > **Note**
  >
  > S3 File Gateway no puede utilizar más de 64 GB de RAM.

- Utilice NVMe un SSD para los discos raíz y el disco caché, y ajuste el tamaño de los discos de caché a fin de ajustarlos 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 virtual a la puerta de enlace, en lugar de utilizar un solo 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 desea implementar 12 TB de caché, puede usar 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

  Además del rendimiento, esto permite una administración más eficiente 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 Decidir la cantidad de almacenamiento en disco local.

Al implementar S3 File Gateway como una EC2 instancia de Amazon, 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 su instancia de S3 File Gateway.
- Para ver los tipos de EC2 instancias de Amazon recomendados para S3 File Gateway, consulta Requisitos para los tipos de EC2 instancias de Amazon.
- Puede cambiar el tipo de EC2 instancia de Amazon que aloja un S3 File Gateway activo. Esto le permite ajustar fácilmente la generación de EC2 hardware y la asignación de recursos de Amazon para encontrar una price-to-performance proporción ideal. Para cambiar el tipo de instancia, usa el siguiente procedimiento en la EC2 consola de Amazon:

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

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

- La price-to-performance proporción de una EC2 instancia de Amazon se refiere a la potencia de cálculo que obtienes por el precio que pagas. Por lo general, EC2 las instancias Amazon 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.

Ajusta el nivel de seguridad de las pequeñas y medianas empresas

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 SMB de la puerta de enlace para especificar cuáles de estas funciones 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.

Al ajustar el nivel de seguridad de las pequeñas y medianas empresas, tenga en cuenta lo siguiente:

- El nivel de seguridad predeterminado de S3 File Gateway es Exigir el cifrado. Esta configuración impone el cifrado y la firma de las conexiones de los clientes SMB a los archivos compartidos 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 S3 File Gateway suele estar limitado a entre 40 y 60 MB/s.
- Si sus requisitos de seguridad le permiten adoptar una postura más relajada, puede cambiar el nivel de seguridad a negociado por 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 SMB de su S3 File Gateway, debe esperar a que el estado del recurso compartido de archivos cambie de Actualizado a Disponible en la consola de Storage Gateway y, a continuación, desconectar y volver a conectar los clientes SMB para que se aplique la nueva configuración.

Utilice varios subprocesos y clientes para paralelizar las operaciones de escritura

Es difícil lograr el máximo rendimiento con una puerta de enlace de archivos de S3 que utilice solo un cliente NFS o SMB para escribir un archivo a la vez, ya que la escritura secuencial desde un único cliente es una operación de un solo subproceso. En su lugar, recomendamos usar varios subprocesos de cada cliente NFS o SMB para escribir varios archivos en paralelo y usar varios clientes NFS o SMB simultáneamente en su S3 File Gateway 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, puede esperar lograr 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 su puerta de enlace. Le recomendamos que experimente con distintos recuentos de subprocesos para encontrar el equilibrio óptimo entre la velocidad y el uso de recursos del sistema para su configuración específica de hardware y red.

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

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

  Para utilizar varios subprocesos con robocopy, añada el `/MT:n` modificador a su comando, donde `n` se 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 evaluación comparativa de almacenamiento, como DISKSPD o FIO. Estas herramientas tienen opciones para ajustar la cantidad de subprocesos, la profundidad de E/S y otros parámetros para adaptarlos a sus requisitos de carga de trabajo específicos.

  DiskSpd permite controlar el número de subprocesos 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`
  - Funciona durante 300 segundos () `-d300`

- Realiza una I/O prueba aleatoria con un 50% de lecturas y un 50% de escrituras (`-r -w50`)
- Utiliza 64 hilos (`-t64`)
- Establece la profundidad de cola en 32 por hilo () `-o32`
- Utiliza un tamaño de bloque de 1 MB () `-b1M`
- Desactiva el almacenamiento en caché de hardware y software () `-h -L`

Para obtener más información, consulte Usar DISKSPD para probar el rendimiento del almacenamiento de cargas de trabajo en el sitio web de Microsoft Learn.

- FIO usa el `numjobs` parámetro para controlar el número de hilos 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 I/O la profundidad en 64 () `--iodepth=64`
- Pruebas en un archivo de 10 GB (`--size=10G`)
- Funciona durante 5 minutos (`--runtime=300`)
- Crea 64 trabajos paralelos (hilos) (`--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 de manual de fio Linux.

-

Desactive la actualización automática de la memoria caché

La función de actualización automática de la caché permite a su S3 File Gateway actualizar sus metadatos automáticamente, lo que puede ayudar a capturar cualquier cambio que los usuarios o las aplicaciones realicen en su 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 de bucket de Amazon S3.

Para optimizar el rendimiento de la puerta de enlace, recomendamos desactivar esta función en las implementaciones en las que todas las lecturas y escrituras del bucket de Amazon S3 se realicen a través de su S3 File Gateway.

Al 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 su implementación escriben ocasionalmente directamente en Amazon S3, le recomendamos configurar el intervalo de tiempo más largo posible entre las actualizaciones, lo que siga siendo práctico para 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 navegar por 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 de 30 días.
- Si decide establecer un intervalo de actualización de la caché muy corto, le recomendamos que pruebe la experiencia de navegación de directorios de sus clientes 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.

Aumente el número de subprocesos de carga de Amazon S3

De forma predeterminada, S3 File Gateway 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 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 las métricas de las pasarelas 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.

Aumente la configuración de tiempo de espera de SMB

Cuando S3 File Gateway copia archivos de gran tamaño a un recurso compartido de archivos SMB, se agota el tiempo de espera de la conexión del cliente SMB tras un período prolongado de tiempo.

Recomendamos ampliar el tiempo de espera de sesión SMB para sus clientes 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 de 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.

Active el bloqueo oportunista para las aplicaciones compatibles

El bloqueo oportunista, o «oplocks», está activado de forma predeterminada para cada nueva puerta de enlace de archivos 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. Recomendamos 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 desactivas el bloqueo oportunista, las aplicaciones que admiten los 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.

Ajuste 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 funciona bien para la mayoría de las cargas de trabajo, incluso si hay 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 funcional de archivos de más de 5 millones, la puerta de enlace tendrá que realizar frecuentes desalojos 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 recientes de Amazon S3.

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

Recomendamos utilizar la acción de la `UpdateGatewayInformation` API para aumentar la capacidad de la puerta de enlace y adaptarla al número de archivos de un 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.

Implemente varias puertas de enlace para cargas de trabajo más grandes

Recomendamos 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 la Guía de rendimiento para puertas de enlace con varios recursos compartidos de archivos.
- Los recursos de cada puerta de enlace de archivos 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 recomendamos crear varios recursos compartidos de archivos que estén mapeados 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 de escritura múltiple, lo que puede provocar problemas de integridad de los datos.

Optimización de S3 File Gateway para las 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 S3 File Gateway, que proporciona una retención 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 costos de los niveles de almacenamiento según sea necesario. Con esta solución, puede reducir la necesidad de aplicaciones de backup empresariales mediante herramientas integradas, como SQL Server Management Studio y Oracle RMAN.

En las siguientes secciones se describen las mejores prácticas para ajustar la implementación de S3 File Gateway a fin de optimizar el rendimiento y ofrecer un soporte rentable para cientos de terabytes de copias de seguridad de bases de datos SQL. La guía que se proporciona en cada sección contribuye 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 Soporte implementaciones de S3 File Gateway. Al implementar y probar estas sugerencias, tenga en cuenta que cada implementación de S3 File Gateway es única, por lo que los resultados pueden variar.

S3 File Gateway proporciona una interfaz de archivos para almacenar y recuperar objetos de Amazon S3 mediante protocolos de archivos NFS o SMB estándares del sector, con un mapeo 1:1 nativo 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 nube AWS como una instancia de Amazon. EC2 S3 File Gateway no está diseñado para sustituir completamente al NAS empresarial. S3 File Gateway emula un sistema de archivos, pero no es un sistema de archivos. 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.

Implemente su puerta de enlace en la misma ubicación que sus servidores SQL

Recomendamos implementar su dispositivo virtual S3 File Gateway en una ubicación física con la menor latencia de red posible entre este y sus servidores SQL. Al elegir una ubicación para su 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 SMB, como los servidores SQL.
- S3 File Gateway está diseñado 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 S3 File Gateway implementadas en Amazon EC2, recomendamos mantener la puerta de enlace y los servidores SQL en el mismo grupo de ubicación. Para obtener más información, consulte Grupos de ubicación para sus EC2 instancias de Amazon en la Guía del usuario de Amazon Elastic Compute Cloud.

Reduzca 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 el disco, tenga en cuenta lo siguiente:

- `IoWaitPercent`indica el porcentaje de tiempo que la CPU espera una respuesta de los discos raíz o de la memoria caché.
- Cuando `IoWaitPercent` es superior al 5 o 10%, suele indicar un cuello de botella en el rendimiento de la puerta de enlace provocado por discos con un rendimiento inferior. 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`.

Ajuste la asignación de recursos de la máquina virtual S3 File Gateway para los discos de CPU, RAM y caché

Al intentar optimizar el rendimiento de la puerta de enlace de archivos de S3, es importante asignar suficientes recursos a la máquina virtual de la 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 para cargas de trabajo más grandes, recomendamos 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 `UserCpuPercent` métrica. Para obtener más información, consulta Cómo entender las métricas de las puertas de enlace.
- Aumente la RAM asignada a entre 32 y 64 GB.

  > **Note**
  >
  > S3 File Gateway no puede utilizar más de 64 GB de RAM.

- Utilice NVMe un SSD para los discos raíz y el disco caché, y ajuste el tamaño de los discos de caché a fin de ajustarlos 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 virtual a la puerta de enlace, en lugar de utilizar un solo 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 desea implementar 12 TB de caché, puede usar 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

  Además del rendimiento, esto permite una administración más eficiente 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 Decidir la cantidad de almacenamiento en disco local.

Al implementar S3 File Gateway como una EC2 instancia de Amazon, 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 su instancia de S3 File Gateway.
- Para ver los tipos de EC2 instancias de Amazon recomendados para S3 File Gateway, consulta Requisitos para los tipos de EC2 instancias de Amazon.
- Puede cambiar el tipo de EC2 instancia de Amazon que aloja un S3 File Gateway activo. Esto le permite ajustar fácilmente la generación de EC2 hardware y la asignación de recursos de Amazon para encontrar una price-to-performance proporción ideal. Para cambiar el tipo de instancia, usa el siguiente procedimiento en la EC2 consola de Amazon:

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

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

- La price-to-performance proporción de una EC2 instancia de Amazon se refiere a la potencia de cálculo que obtienes por el precio que pagas. Por lo general, EC2 las instancias Amazon 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.

Mejore el rendimiento de los clientes SMB ajustando el nivel de seguridad de su S3 File Gateway

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 SMB de la puerta de enlace para especificar cuáles de estas funciones 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.

Al ajustar el nivel de seguridad de las pequeñas y medianas empresas, tenga en cuenta lo siguiente:

- El nivel de seguridad predeterminado de S3 File Gateway es Exigir el cifrado. Esta configuración impone el cifrado y la firma de las conexiones de los clientes SMB a los archivos compartidos 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 S3 File Gateway suele estar limitado a entre 40 y 60 MB/s.
- Si sus requisitos de seguridad le permiten adoptar una postura más relajada, puede cambiar el nivel de seguridad a negociado por 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 SMB de su S3 File Gateway, debe esperar a que el estado del recurso compartido de archivos cambie de Actualizado a Disponible en la consola de Storage Gateway y, a continuación, desconectar y volver a conectar los clientes SMB para que se aplique la nueva configuración.

Mejore el rendimiento de los clientes SMB dividiendo las copias de seguridad de SQL en varios archivos

- Es difícil lograr el máximo rendimiento con una puerta de enlace de archivos 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, recomendamos usar varios subprocesos de cada servidor SQL para escribir varios archivos en paralelo y usar varios servidores SQL simultáneamente en su S3 File Gateway 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 S3 File Gateway. 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 archivos mediante comandos de T-SQL o 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 significativamente la velocidad y la eficiencia del respaldo.

Al configurar las copias de seguridad de un servidor 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:

- Realice 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

Evite errores al copiar archivos de gran tamaño aumentando la configuración de tiempo de espera de SMB

Cuando S3 File Gateway copia archivos de copia de seguridad de SQL de gran tamaño en un recurso compartido de archivos SMB, la conexión del cliente SMB puede agotarse después de un período de tiempo prolongado. Recomendamos ampliar el tiempo de espera de sesión SMB para los clientes 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 de 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.

Aumente el número de subprocesos de carga de Amazon S3

De forma predeterminada, S3 File Gateway 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 los 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 las métricas de las pasarelas 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.

Desactive la actualización automática de la memoria caché

La función de actualización automática de la caché permite a su S3 File Gateway actualizar sus metadatos automáticamente, lo que puede ayudar a capturar cualquier cambio que los usuarios o las aplicaciones realicen en su 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 de bucket de Amazon S3.

Para optimizar el rendimiento de la puerta de enlace, recomendamos desactivar esta función en las implementaciones en las que todas las lecturas y escrituras del bucket de Amazon S3 se realicen a través de su S3 File Gateway.

Al 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 su implementación escriben ocasionalmente directamente en Amazon S3, le recomendamos configurar el intervalo de tiempo más largo posible entre las actualizaciones, lo que siga siendo práctico para 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 navegar por 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 de 30 días.
- Si decide establecer un intervalo de actualización de la caché muy corto, le recomendamos que pruebe la experiencia de navegación de directorios de sus 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.

Implemente 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 múltiples 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 aumentando el número de subprocesos de carga 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 su carga de trabajo de backup de SQL, puede escalar la cantidad de puertas de enlace para cumplir con sus requisitos.

- Recomendamos 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 las cargas de trabajo de respaldo 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
- Realice copias de seguridad de bases de datos de 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
- Mejores prácticas de dimensionamiento de la caché de S3 File Gateway

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 eres responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a 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, consulta las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulta Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con Storage Gateway u otro Servicios de AWS dispositivo mediante la consola AWS CLI, la API o AWS SDKs. Cualquier dato que ingrese en etiquetas o campos de texto de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Cifrado de datos mediante AWS KMS

Storage Gateway utiliza SSL/TLS (Layers/Transport Secure Socket Layer Security) para cifrar los datos que se transfieren entre el dispositivo de puerta de enlace y el AWS almacenamiento. De forma predeterminada, Storage Gateway utiliza claves de cifrado administradas por Amazon S3 (SSE-S3) para cifrar en el servidor todos los datos que almacena en Amazon S3. Tiene la

opción de utilizar la API de Storage Gateway para configurar la puerta de enlace para cifrar los datos almacenados en la nube mediante el cifrado en el lado del servidor con claves de AWS Key Management Service (SSE-KMS).

Cifrado de un recurso compartido de archivos

Puede configurar los recursos compartidos de archivos de su S3 File Gateway para cifrar los objetos almacenados con claves AWS KMS administradas mediante SSE-KMS o DSSE-KMS. Para obtener información sobre los métodos de cifrado para compartir archivos admitidos, consulte Cifrar objetos almacenados por File Gateway en Amazon S3.

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 S3 .
- 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 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 de acceso mediante 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
- Uso de Windows ACLs para limitar el acceso a los archivos compartidos en pequeñas y medianas empresas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que se realice en AWS SGW.

Usuario del servicio: si utiliza el servicio AWS SGW para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más funciones de AWS SGW para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarle a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en SGW AWS , consulte Solución de problemas AWS de identidad y acceso a Storage Gateway.

Administrador de servicios: si está a cargo de los recursos de AWS SGW en su empresa, probablemente tenga acceso completo a AWS SGW. Su trabajo consiste en determinar a qué funciones y recursos de AWS SGW deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su gestionador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar la IAM con AWS SGW, consulte. Cómo funciona AWS Storage Gateway con IAM

Administrador de IAM: si es administrador de IAM, puede que desee obtener más información sobre cómo redactar políticas para administrar el acceso a SGW. AWS Para ver ejemplos de políticas de AWS SGW basadas en la identidad que puede utilizar en IAM, consulte. Ejemplos de políticas basadas en identidad para AWS Storage Gateway

Autenticación con identidades

La autenticación es la forma de iniciar sesión con sus AWS credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (IAM Identity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su gestionador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre la firma de solicitudes, consulte AWS Signature Versión 4 para solicitudes API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Autenticación multifactor AWS en IAM en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utiliza el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulta Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utiliza AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulta ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puedes iniciar sesión como grupo. Puedes usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una persona determinada. Para asumir temporalmente un rol de IAM en el AWS Management Console, puede cambiar de un rol de usuario a uno de IAM (consola). Puedes asumir un rol llamando a una operación de AWS API AWS CLI o usando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulta Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles de federación, consulte Crear un rol para un proveedor de identidad de terceros (federación) en la Guía de usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulta Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulta Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en AWS ellas, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los

permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

- Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
- Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y realizan AWS CLI solicitudes a la AWS API. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte Usar un rol de IAM para conceder permisos a las aplicaciones que se ejecutan en EC2 instancias de Amazon en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utiliza para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para obtener más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso () ACLs

Las listas de control de acceso (ACLs) controlan qué responsables (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios compatibles. AWS WAF ACLs Para obtener más información ACLs, consulte la descripción general de la lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puedes establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): SCPs son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y administrar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una Usuario raíz de la cuenta de AWS. Para obtener más información sobre Organizations SCPs, consulte las políticas de control de servicios en la Guía del AWS Organizations usuario.
- Políticas de control de recursos (RCPs): RCPs son políticas de JSON que puedes usar para establecer los permisos máximos disponibles para los recursos de tus cuentas sin actualizar las políticas de IAM asociadas a cada recurso que poseas. El RCP limita los permisos de los recursos en las cuentas de los miembros y puede afectar a los permisos efectivos de las identidades, incluidos los permisos Usuario raíz de la cuenta de AWS, independientemente de si pertenecen a su organización. Para obtener más información sobre Organizations e RCPs incluir una lista de

Servicios de AWS ese apoyo RCPs, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.

- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona 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
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
ACLs	No

Característica de IAM	AWS Soporte para SGW
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 identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está asociada. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en la identidad para 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 en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política basada en recursos concede acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Cross account resource access in IAM en la Guía del usuario de IAM.

Acciones políticas para 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. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de 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 puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puedes hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utiliza un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de los tipos de 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 puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puedes crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puedes conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulta Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de claves de 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

Soportes 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. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con SGW AWS

Compatibilidad con credenciales temporales: sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluidas las que Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte Cambio de un usuario a un rol de IAM (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Sesiones de acceso directo para AWS SGW

Admite sesiones de acceso directo (FAS): sí

Cuando utiliza un usuario o un rol de IAM para realizar acciones en él AWS, se le considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Roles de servicio de AWS SGW

Compatibilidad 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 Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de la AWS SGW. Edite las funciones de servicio solo cuando AWS SGW le indique cómo hacerlo.

Funciones vinculadas al servicio para SGW AWS

Admite roles vinculados a servicios: 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 puedes 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. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o la AWS API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por 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, consulta las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la

MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de la 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, permite el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la 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 gestionadas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
```

```
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Solución de problemas 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 gestionador 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 el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en 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 administrador. AWS El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

> **Important**
>
> Storage Gateway puede asumir las funciones de servicio existentes que se transfieren mediante la acción de `iam:PassRole` política, pero no admite las políticas de IAM que

utilizan la clave de `iam:PassedToService` contexto 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: transfiere 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

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que respaldan políticas basadas en recursos o listas de control de acceso (ACLs), 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, consulta Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Uso de etiquetas 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. Controlar el 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:account-id:*/*"
        }
    ]
}
```

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 las condiciones de una política de IAM basadas en etiquetas. Por ejemplo, puedes escribir una política que permita o deniegue a un usuario la capacidad de realizar operaciones de API específicas en función de la etiqueta que 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"
            }
         }
      }
   ]
}
```

Uso de Windows ACLs para limitar el acceso a los archivos compartidos en pequeñas y medianas empresas

La puerta de enlace de archivos Amazon S3 admite dos métodos diferentes para controlar el acceso a los archivos y directorios que se almacenan a través de un recurso compartido de archivos SMB: permisos POSIX o Windows. ACLs

En esta sección se describe cómo utilizar las listas de control de acceso (ACLs) de Microsoft Windows en los recursos compartidos de archivos SMB que utilizan Microsoft Active Directory (AD) para la autenticación. Con Windows ACLs, puede establecer permisos detallados en los archivos y carpetas del recurso compartido de archivos SMB.

A continuación se indican algunas características importantes de Windows ACLs en los recursos compartidos de archivos SMB:

- Windows ACLs se selecciona de forma predeterminada para los recursos compartidos de archivos SMB cuando la puerta de enlace de archivos se une a un dominio de Active Directory.
- Cuando ACLs se activan, la información de ACL se conserva en los metadatos del objeto de Amazon S3.
- La puerta de enlace conserva hasta 10 ACLs por archivo o carpeta.
- Cuando se utiliza un recurso compartido de archivos SMB con el acceso ACLs activado a los objetos de S3 creados fuera de la puerta de enlace, los objetos ACLs «heredan» la información de la carpeta principal.

> **Note**
>
> La ACL raíz predeterminada de un recurso compartido de archivos SMB concede acceso completo a todo el mundo, pero es posible cambiar los permisos de la ACL raíz. Puede usar la raíz ACLs para controlar el acceso al recurso compartido de archivos. Puede establecer quién puede montar el recurso compartido de archivos (mapear la unidad) y los permisos que obtiene el usuario de forma recursiva para los archivos y las carpetas del recurso compartido de archivos. Sin embargo, le recomendamos que defina este permiso en la carpeta de nivel superior del bucket de S3 para que se conserve la ACL.

Puede activar Windows ACLs al crear un nuevo recurso compartido de archivos SMB mediante la operación de API Create SMBFile Share. O bien, puede activar Windows ACLs en un recurso compartido de archivos SMB existente mediante la operación de API Update SMBFile Share.

Activar Windows ACLs en un nuevo recurso compartido de archivos SMB

Realice los siguientes pasos para activar Windows ACLs en un nuevo recurso compartido de archivos SMB.

Para activar Windows ACLs al crear un nuevo recurso compartido de archivos SMB

1. Cree una gateway de archivos si todavía no tiene una. Para obtener más información, consulte Creación de la puerta de enlace.

2. Si la gateway no se ha unido a un dominio, añádala a un dominio. Para obtener más información, consulte Uso de Active Directory para autenticar usuarios.
3. Cree un recurso compartido de archivos SMB. Para obtener más información, consulte
4. Active Windows ACLs en el recurso compartido de archivos desde la consola Storage Gateway.

   Para usar la consola Storage Gateway, haga lo siguiente:

   a. Elija el recurso compartido de archivos y elija Edit file share (Editar recurso compartido de archivos).

   b. Para la opción File/directory access controlled by (Acceso de archivo/directorio controlado por) elija Windows Access Control List (Lista de control de acceso de Windows).
5. (Opcional) Agregue un usuario administrador a AdminUsersList, si desea que el usuario administrador tenga privilegios para actualizar todos ACLs los archivos y carpetas del recurso compartido de archivos.

   > **Note**
   >
   > Si ha configurado las listas de usuarios y grupos permitidos y denegados en la configuración del recurso compartido de archivos SMB, no ACLs concederá ningún acceso que invalide esas listas.
   > Las listas de usuarios y grupos permitidos y denegados se evalúan previamente ACLs y controlan qué usuarios pueden montar el recurso compartido de archivos o acceder a él. Si se incluye algún usuario o grupo en la lista de permitidos, la lista se considera activa y solo esos usuarios pueden montar el recurso compartido de archivos.
   > Una vez que un usuario haya montado un recurso compartido de archivos, ofrezca una protección más detallada que ACLs controle a qué archivos o carpetas específicos puede acceder el usuario.
6. Actualice ACLs las carpetas principales de la carpeta raíz. Para ello, utilice el Explorador de archivos de Windows para configurar ACLs las carpetas del recurso compartido de archivos SMB.

   > **Note**
   >
   > Si configura la carpeta raíz ACLs en lugar de la carpeta principal situada debajo de la raíz, los permisos de ACL no se conservan en Amazon S3.

Recomendamos configurarlos ACLs en la carpeta de nivel superior situada debajo de la raíz del recurso compartido de archivos, en lugar de configurarlos ACLs directamente en la raíz del recurso compartido de archivos. Este enfoque conserva la información como metadatos de objetos en Amazon S3.

7. Active la herencia según corresponda.

> **Note**
>
> Puedes activar la herencia en los archivos compartidos creados después del 8 de mayo de 2019.

Si activas la herencia y actualizas los permisos de forma recursiva, Storage Gateway actualiza todos los objetos del bucket de S3. En función del número de objetos del bucket, la actualización puede tardar un tiempo en completarse.

Activación de Windows ACLs en un recurso compartido de archivos SMB existente

Siga los siguientes pasos para activar Windows ACLs en un recurso compartido de archivos SMB existente que tenga permisos POSIX.

Para activar Windows ACLs en un recurso compartido de archivos SMB existente mediante la consola Storage Gateway

1. Elija el recurso compartido de archivos y elija Edit file share (Editar recurso compartido de archivos).
2. Para la opción File/directory access controlled by (Acceso de archivo/directorio controlado por) elija Windows Access Control List (Lista de control de acceso de Windows).
3. Active la herencia según corresponda.

> **Note**
>
> No recomendamos configurarlo ACLs en el nivel raíz, ya que si lo haces y eliminas la puerta de enlace, tendrás que ACLs volver a restablecerla.

Si activas la herencia y actualizas los permisos de forma recursiva, Storage Gateway actualiza todos los objetos del bucket de S3. En función del número de objetos del bucket, la actualización puede tardar un tiempo en completarse.

Limitaciones del uso de Windows ACLs

Tenga en cuenta las siguientes limitaciones cuando utilice Windows ACLs para controlar el acceso a los recursos compartidos de archivos SMB:

- Windows solo ACLs se admite en los recursos compartidos de archivos que utilizan Active Directory para la autenticación cuando se utilizan clientes SMB de Windows para acceder a los recursos compartidos de archivos.
- Las gateways de archivos admiten un máximo de 10 entradas de ACL para cada archivo y directorio.
- Las puertas de enlace de archivos no admiten `Audit Alarm` entradas, que son entradas de la lista de control de acceso al sistema (SACL). Las puertas de enlace de archivos admiten `Allow Deny` entradas, que son entradas de la lista de control de acceso discrecional (DACL).
- Las pasarelas de archivos no admiten los permisos de entrada de control de acceso avanzado (ACE).
- La configuración de la ACL raíz de los recursos compartidos de archivos SMB solo se realiza en la puerta de enlace, y los ajustes se conservan si se actualiza o se reinicia la puerta de enlace.

> **Note**
>
> Si configura la carpeta raíz ACLs en lugar de la carpeta principal situada debajo de la raíz, los permisos de ACL no se conservan en Amazon S3.

Teniendo en cuenta estas condiciones, asegúrese de hacer lo siguiente:

- Si configura varias puertas de enlace para acceder al mismo bucket de Amazon S3, configure la ACL raíz en cada una de las puertas de enlace para mantener la coherencia de los permisos.
- Si eliminas un archivo compartido y lo vuelves a crear en el mismo bucket de Amazon S3, asegúrate de usar el mismo conjunto de root ACLs.

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 e HITRUST CSF.

https://aws.amazon.com/compliance/services-in-scope/ 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: este documento técnico 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— 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 with Storage 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 de 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 los 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 con la implementación de Storage Gateway

A continuación, encontrará información sobre las prácticas recomendadas y la solución de problemas relacionados con las puertas de enlace, las plataformas host, los recursos compartidos de archivos, la alta disponibilidad, la recuperación de datos y la seguridad. 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 con Active Directory- Obtenga información sobre qué hacer si recibe mensajes de error, por ejemplo `NETWORK_ERRORTIMEOUT`, o `ACCESS_DENIED` si intenta unir su File Gateway 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 con la puerta de enlace local- Obtén información sobre los problemas más habituales que puedes encontrar al trabajar con tus puertas de enlace locales y cómo permitir la conexión Soporte a ellas para solucionar problemas.
- Solución de problemas: problemas de 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 Amazon EC2 Gateway- Obtenga información sobre los problemas típicos que puede encontrar al trabajar con pasarelas implementadas en Amazon EC2.
- Solución de problemas: problemas con los dispositivos de hardware- Aprenda a resolver los problemas que puedan surgir con el dispositivo de hardware AWS Storage Gateway.
- Solución de problemas: problemas con File Gateway- 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 con el uso compartido de archivos- Obtenga información sobre las medidas que puede tomar si tiene problemas inesperados con su recurso compartido de archivos.
- Solución de problemas: problemas de alta disponibilidad- Obtenga información sobre qué hacer si tiene problemas con las puertas de enlace que se implementan en un entorno de alta VMware disponibilidad.

Solución de problemas: gateway offline en la consola 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 más 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 Sustitución de la puerta de enlace de archivos S3 existente por una nueva instancia para configurar una nueva puerta de enlace y volver a descargar la información del disco caché desde la AWS nube.

Solución de problemas: problemas al unir la puerta de enlace a Active Directory

Utilice la siguiente información de solución de problemas para determinar qué hacer si recibe mensajes de error como`NETWORK_ERROR`, por ejemplo`TIMEOUT`, o `ACCESS_DENIED` cuando intenta unir su File Gateway a un dominio de Microsoft Active Directory.

Para resolver estos errores, lleve a cabo 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 de hipervisores (VMwareHyper-V o KVM) para las puertas de enlace locales, o mediante ssh para las puertas de enlace de Amazon. EC2
2. Introduzca el número correspondiente para seleccionar Gateway Console y, a continuación, introdúzcalo para ver todos los comandos disponibles. h Para probar la conectividad entre la máquina virtual Storage Gateway y el dominio, ejecute el siguiente comando:

   ```
   nping -d corp.domain.com -p 389 -c 1 -t tcp
   ```

   > **Note**
   >
   > `corp.domain.com`Sustitúyalo por el nombre DNS de su dominio de Active Directory y `389` sustitúyalo por el puerto LDAP de su entorno.
   > Compruebe que ha abierto los puertos necesarios en su firewall.

El siguiente es un ejemplo de una prueba de ping exitosa 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 ni respuesta desde el `corp.domain.com` destino:

```
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 su instancia de Amazon Gateway EC2

Si la puerta de enlace de archivos se ejecuta en una EC2 instancia de Amazon, debe asegurarse de que el conjunto de opciones de DHCP esté correctamente configurado y conectado a la Amazon Virtual Private Cloud (VPC) que contiene la instancia de puerta de enlace. Para obtener más información, consulte Conjuntos de opciones de DHCP en Amazon VPC.

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 excavación:

1. Conéctese a la consola local de la puerta de enlace mediante el software de administración de hipervisores (VMwareHyper-V o KVM) para las puertas de enlace locales, o mediante ssh para las puertas de enlace de Amazon. EC2
2. Introduzca el número correspondiente para seleccionar Gateway Console y, a continuación, introdúzcalo para ver todos los comandos disponibles. h Para comprobar si la puerta de enlace puede resolver el dominio, ejecute el siguiente comando:

   ```
   dig -d corp.domain.com
   ```

   > **Note**
   >
   > `corp.domain.com`Sustitúyalo por el nombre 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 las funciones 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 ordenadores. Para probarlo, intenta unir otros servidores de la misma subred de VPC que la máquina virtual de puerta de enlace al dominio.

Comprueba 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 máximo de tiempo de espera es de 3600 segundos.
> Si recibes errores al ejecutar AWS CLI comandos, asegúrate de usar la versión más reciente AWS CLI .

Confirme que Active Directory cree nuevos objetos informáticos en la unidad organizativa (OU) predeterminada

Asegúrese de que Microsoft Active Directory no tenga ningún objeto de política de grupo que cree nuevos objetos de equipo en cualquier ubicación que no sea la unidad organizativa predeterminada. Para poder unir la puerta de enlace al dominio de Active Directory, debe existir un nuevo objeto informático en la unidad organizativa predeterminada. Algunos entornos de Active Directory están personalizados para que tengan objetos diferentes OUs para los 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. AWS CLI A continuación, especifique la opción para. `--organizational-unit`

> **Note**
>
> El proceso de creación del objeto informático se denomina puesta en escena previa.

Comprueba los registros de eventos de tu controlador de dominio

Si no puedes unirte a la puerta de enlace al dominio después de probar todas las demás comprobaciones y configuraciones descritas en las secciones anteriores, te recomendamos que examines los registros de eventos del controlador de dominio. Comprueba 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 enviadas por 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. En el caso de las puertas de enlace implementadas en una EC2 instancia de Amazon, comprueba 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, puedes usar SSH a 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**
>
> Sustitúyala por *region* la tuya. 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 de administración del tiempo del sistema no está disponible en las pasarelas alojadas en EC2 instancias de Amazon. Para asegurarte de que EC2 las pasarelas de Amazon pueden

sincronizar la hora correctamente, confirma que la EC2 instancia de Amazon se puede conectar a la siguiente lista 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

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 de administración del tiempo del sistema no está disponible en las pasarelas alojadas en EC2 instancias de Amazon. Para asegurarte de que EC2 las pasarelas de Amazon pueden sincronizar la hora correctamente, confirma que la EC2 instancia de Amazon se puede conectar a la siguiente lista 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 local como un proxy Squid en el puerto 3128. En este caso, confirme lo siguiente:

- El grupo de seguridad adjunto al proxy HTTP de 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 Amazon EC2 VPC 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 de 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 con las puertas de enlace locales

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 facilitar la solución de 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 de los hipervisores y VMs, consulte. Configuración de un servidor de protocolo de tiempo de red (NTP) para su 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 su máquina virtual tenga al menos 16 GB de RAM. La asignación de la puerta de enlace falla si hay menos de 16 GB de RAM. Para obtener más información, consulte Requisitos de configuración de File Gateway.

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 AWS 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 Apagar la máquina virtual de la 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 en el cliente de administración del hipervisor y asegúrese de que todas las interfaces que piensa utilizar 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 Configurar los ajustes de la 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.

Solución de problemas: los escaneos de seguridad muestran los puertos NFS abiertos

Algunos puertos NFS están habilitados de forma predeterminada, incluso en las puertas de enlace que solo se utilizan con recursos compartidos de archivos SMB. Si utiliza un software de seguridad de terceros, como Qualys, para escanear la red en la que está instalada su File Gateway, los resultados del análisis podrían indicar que estos puertos NFS abiertos constituyen una posible vulnerabilidad de seguridad. Si solo utiliza la puerta de enlace con archivos compartidos SMB y desea deshabilitar los puertos NFS no utilizados por motivos de seguridad, utilice el siguiente procedimiento:

Para deshabilitar los puertos NFS en una puerta de enlace de archivos:

1. Acceda a la línea de comandos de la consola local de la puerta de enlace mediante el procedimiento descrito enhttps://docs.aws.amazon.com/filegateway/latest/files3/MaintenanceGatewayConsole-fgw.html.
2. Introduzca los siguientes comandos para deshabilitar el tráfico NFS:

```
iptables -I INPUT -p udp -m udp --dport 111 -j DROP
iptables -I INPUT -p udp -m udp --dport 2049 -j DROP
iptables -I INPUT -p udp -m udp --dport 20048 -j DROP
iptables -I INPUT -p tcp -m tcp --dport 111 -j DROP
iptables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
```

```
iptables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
```

3. Introduzca el siguiente comando para confirmar que los puertos NFS bloqueados aparecen en las tablas de IP:

```
iptables -n -L -v --line-numbers
```

Activa el Soporte acceso para ayudar a solucionar los problemas de tu 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. Este acceso se activa a través de la consola local del anfitrión. 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:	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:

Problema	Acción que ejecutar
“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”.	`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 el archivo de [...]: el archivo existe. (0x80070050)”	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
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 compatibl e 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 que está 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 File Gateway.

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 File Gateway.
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 de protocolo de tiempo de red (NTP) para su 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 Amazon EC2 Gateway

En las siguientes secciones, puede encontrar los problemas típicos que puede encontrar al trabajar con su puerta de enlace implementada en Amazon EC2. Para obtener más información sobre la diferencia entre una puerta de enlace local y una puerta de enlace implementada en Amazon EC2, consulteImplemente un EC2 host de Amazon predeterminado para S3 File Gateway.

Para obtener información sobre el uso del almacenamiento efímero, consulte Uso de almacenamiento efímero con puertas de enlace EC2 .

Temas

- La puerta de enlace no se ha activado poco tiempo después
- No puede encontrar su instancia de EC2 gateway en la lista de instancias
- Quieres conectarte a tu instancia de gateway mediante la consola EC2 serie de Amazon
- Quieres ayudar Soporte a solucionar los problemas de tu Amazon Gateway EC2

La puerta de enlace no se ha activado poco tiempo después

Comprueba lo siguiente en la EC2 consola de Amazon:

- El puerto 80 está abierto en el grupo de seguridad que asociaste a la instancia. Para obtener más información sobre cómo añadir una regla de grupo de seguridad, consulte Añadir una regla de grupo de seguridad en la Guía del EC2 usuario de Amazon.
- La instancia de la gateway está marcada como en ejecución. En la EC2 consola de Amazon, el valor State de la instancia debe ser RUNNING.

- Asegúrese de que el tipo de EC2 instancia de Amazon cumpla los requisitos mínimos, tal y como se describe enRequisitos de almacenamiento.

Después de corregir el problema, intente activar la gateway de nuevo. Para ello, abra la consola de Storage Gateway, elija Deploy a new Gateway on Amazon EC2 y vuelva a introducir la dirección IP de la instancia.

No puede encontrar su instancia de EC2 gateway 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.

Quieres conectarte a tu instancia de gateway mediante la consola EC2 serie de Amazon

Puedes usar la consola EC2 serie de Amazon para solucionar problemas de arranque, configuración de red y otros problemas. Para obtener instrucciones y consejos de solución de problemas, consulte Amazon EC2 Serial Console en la Guía del usuario de Amazon Elastic Compute Cloud.

Quieres ayudar Soporte a solucionar los problemas de tu Amazon Gateway 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. Activa este acceso a través de la consola EC2 local de Amazon. Inicia sesión en la consola EC2 local de Amazon a través de un 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 añadir una regla de grupo de seguridad, consulte los grupos de EC2 seguridad de Amazon en la Guía del EC2 usuario de Amazon.

Para permitir la Soporte conexión a su puerta de enlace, primero debe iniciar sesión en la consola local de la EC2 instancia de Amazon, navegar hasta la consola de Storage Gateway y, a continuación, proporcionar el acceso.

Para activar el Soporte acceso a una puerta de enlace implementada en una EC2 instancia de Amazon

1. Inicia sesión en la consola local de tu EC2 instancia de Amazon. Para obtener instrucciones, consulta Connect to your instance en la Guía del EC2 usuario de Amazon.

   Puedes usar el siguiente comando para iniciar sesión en la consola local de la EC2 instancia.

   ```
   ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
   ```

   > **Note**
   >
   > *PRIVATE-KEY*Es el `.pem` archivo que contiene el certificado privado del EC2 key pair que utilizaste para lanzar la EC2 instancia de Amazon. Para obtener más información, consulta Cómo recuperar la clave pública de tu par de claves en la Guía del EC2 usuario de Amazon.
   > *INSTANCE-PUBLIC-DNS-NAME*Es el nombre del Sistema de nombres de dominio (DNS) público de la EC2 instancia de Amazon en la que se ejecuta la puerta de enlace. Para obtener este nombre de DNS público, seleccione la EC2 instancia de Amazon en la EC2 consola 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 (Transmission Control). 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 los dispositivos 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 de AWS Storage Gateway Hardware Appliance 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 File Gateway

Puede configurar su File Gateway para escribir entradas de registro en un grupo de CloudWatch registros de Amazon. Si lo hace, recibirá notificaciones sobre el estado de la puerta de enlace y sobre cualquier error que detecte la puerta de enlace. Puede encontrar información sobre estas notificaciones de error 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: 1344 (0x00000540)
- Error: GatewayClockOutOfSync
- Error: InaccessibleStorageClass

- Error: InvalidObjectState
- Error: ObjectMissing
- Error: RoleTrustRelationshipInvalid
- Error: S3 AccessDenied
- Error: DroppedNotifications
- Notificación: HardReboot
- Notificación: reinicio
- Solución de problemas: los escaneos de seguridad muestran los puertos NFS abiertos
- Solución de problemas: uso de CloudWatch métricas

Error: 1344 (0x00000540)

Al migrar archivos a Amazon S3, es posible que encuentre un error `ERROR 1344 (0x00000540)` si intenta copiar archivos con más de 10 entradas de control de acceso (ACEs) a Amazon S3. Las entradas de control de acceso aparecen en la lista de control de acceso (ACL).

Amazon S3 File Gateway solo puede conservar 10 entradas ACE por archivo o carpeta determinados.

Para resolver un error 1344: copiar la seguridad de NTFS al directorio de destino.

Reduzca el número de entradas en los permisos de Windows para los archivos o carpetas que contengan más de 10 entradas. Un enfoque habitual consiste en crear un grupo que contenga la lista completa de entradas y, a continuación, sustituir la lista de entradas por ese único grupo. Cuando el número de entradas sea inferior a 10, puede volver a intentar copiar los archivos o carpetas a la puerta de enlace.

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 error GatewayClockOutOfSync

- 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 la puerta de enlace y la actualización de la configuración del servidor NTP, consulte Configuración de un servidor de protocolo de tiempo de red (NTP) para la puerta de enlace Configuración de un servidor para la puerta de enlace.

Error: InaccessibleStorageClass

Puede aparecer un `InaccessibleStorageClass` error cuando un objeto se mueve fuera de la clase de almacenamiento estándar de Amazon S3.

Su File Gateway suele encontrar este error cuando intenta cargar un objeto o leer un objeto del bucket de Amazon S3. Por lo general, este error significa que el objeto se ha trasladado a Amazon S3 Glacier y se encuentra en la clase de almacenamiento S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive.

Su S3 File Gateway puede generar un informe de caché que enumere todos los archivos de la memoria caché de la puerta de enlace que actualmente no se pueden cargar en Amazon S3 debido a este error. La información de este informe puede ayudarle Soporte a resolver problemas con la configuración de su gateway, Amazon S3 o IAM. Para obtener más información, consulte Crear un informe de caché.

Para resolver un InaccessibleStorageClass error

- Restaure el objeto de la clase de almacenamiento S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive a su clase de almacenamiento original en S3.

  Si restauras el objeto en el depósito de S3 para corregir un error de carga, el archivo finalmente se cargará. Si restaura el objeto para corregir un error de lectura, el cliente SMB o NFS de File Gateway podrá leer el archivo.

Error: InvalidObjectState

Puede producirse un `InvalidObjectState` error cuando un escritor distinto del File Gateway especificado modifica el archivo especificado en el bucket de Amazon S3 especificado. Como

resultado, el estado del archivo de File Gateway no coincide con el estado de Amazon S3. Se produce un error al cargar el archivo a Amazon S3 o al recuperar el archivo desde Amazon S3.

Su S3 File Gateway puede generar un informe de caché que enumere todos los archivos de la memoria caché de la puerta de enlace que actualmente no se pueden cargar en Amazon S3 debido a este error. La información de este informe puede ayudarle Soporte a resolver problemas con la configuración de su gateway, Amazon S3 o IAM. Para obtener más información, consulte Crear un informe de caché.

Para resolver un InvalidObjectState error

Si la operación que modifica el archivo es `S3Upload` o`S3GetObject`, haga lo siguiente:

1. Guarde la última copia del archivo en el sistema de archivos local de su cliente SMB o NFS (necesitará esta copia del archivo en el paso 4). Si la versión del archivo de Amazon S3 es la más reciente, descargue esa versión. Para ello, puede utilizar la tecla AWS Management Console o AWS CLI.
2. Elimine el archivo en Amazon S3 con la tecla AWS Management Console o AWS CLI.
3. Elimine el archivo de File Gateway con su cliente SMB o NFS.
4. Copie la última versión del archivo que guardó en el paso 1 en Amazon S3 mediante su cliente SMB o NFS. Hágalo a través de su File Gateway.

Error: ObjectMissing

Se puede producir un `ObjectMissing` error cuando un escritor distinto del File Gateway especificado elimina el archivo especificado del bucket de S3. Se produce un error en cualquier carga posterior a Amazon S3 o en las recuperaciones del objeto desde Amazon S3.

Su S3 File Gateway puede generar un informe de caché que enumere todos los archivos de la memoria caché de la puerta de enlace que actualmente no se pueden cargar en Amazon S3 debido a este error. La información de este informe puede ayudarle Soporte a resolver problemas con la configuración de su gateway, Amazon S3 o IAM. Para obtener más información, consulte Crear un informe de caché.

Para resolver un ObjectMissing error

Si la operación que modifica el archivo es `S3Upload` o`S3GetObject`, haga lo siguiente:

1. Guarde la última copia del archivo en el sistema de archivos local de su cliente SMB o NFS (necesitará esta copia del archivo en el paso 3).
2. Elimine el archivo de File Gateway con su cliente SMB o NFS.
3. Copie la última versión del archivo que guardó en el paso 1 con su cliente SMB o NFS. Hágalo a través de su File Gateway.

Error: RoleTrustRelationshipInvalid

Aparece este error cuando la función de IAM de un recurso compartido de archivos tiene una relación de confianza de IAM mal configurada (es decir, la función de IAM no confía en el principal de Storage Gateway mencionado). `storagegateway.amazonaws.com` Como resultado, File Gateway no podría obtener las credenciales para ejecutar ninguna operación en el depósito de S3 que respalda el recurso compartido de archivos.

Para resolver un RoleTrustRelationshipInvalid error

- Utilice la consola de IAM o la API de IAM para incluirlo `storagegateway.amazonaws.com` como principal en el que confíen sus archivos compartidos. IAMrole Para obtener información sobre la función de IAM, consulte el tutorial: delegue el acceso entre AWS cuentas mediante funciones de IAM.

Error: S3 AccessDenied

Puede aparecer un `S3AccessDenied` error para el rol de acceso al bucket AWS Identity and Access Management (IAM) de un recurso compartido de archivos en Amazon S3. En este caso, la función de IAM de acceso al bucket de S3 que se especifica `roleArn` en el error no permite la operación en cuestión. La operación no está permitida debido a los permisos de los objetos del directorio especificados por el prefijo Amazon S3.

Su S3 File Gateway puede generar un informe de caché que enumere todos los archivos de la memoria caché de la puerta de enlace que actualmente no se pueden cargar en Amazon S3 debido a este error. La información de este informe puede ayudarle Soporte a resolver problemas con la configuración de su gateway, Amazon S3 o IAM. Para obtener más información, consulte Crear un informe de caché.

Para resolver un AccessDenied error de S3

- Modifique la política de acceso a Amazon S3 que se adjunta al `roleArn` registro de estado de File Gateway para permitir los permisos para la operación de Amazon S3. Asegúrese de que la política de acceso conceda los permisos de la operación que ha provocado el error. Además, concede los permisos del directorio especificado en el registro para `prefix`. Para obtener información sobre los permisos de Amazon S3, consulte Especificar los permisos en una política en la Guía del usuario de Amazon Simple Storage Service.

  Estas operaciones pueden provocar que se produzca el error `S3AccessDenied`:

  - `S3HeadObject`
  - `S3GetObject`
  - `S3ListObjects`
  - `S3DeleteObject`
  - `S3PutObject`

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 `Root Disk Usage` métrica 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 las instrucciones en la documentación del hipervisor de su máquina virtual.

   Para aumentar el tamaño del disco raíz de EC2 las pasarelas de Amazon, consulte Solicitar modificaciones a sus 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 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: los escaneos de seguridad muestran los puertos NFS abiertos

Algunos puertos NFS están habilitados de forma predeterminada, incluso en las puertas de enlace que solo se utilizan con recursos compartidos de archivos SMB. Si utiliza un software de seguridad de terceros, como Qualys, para escanear la red en la que está instalada su File Gateway, los resultados del análisis podrían indicar que estos puertos NFS abiertos constituyen una posible vulnerabilidad de seguridad. Si solo utiliza la puerta de enlace con archivos compartidos SMB

y desea deshabilitar los puertos NFS no utilizados por motivos de seguridad, utilice el siguiente procedimiento:

Para deshabilitar los puertos NFS en una puerta de enlace de archivos:

1. Acceda a la línea de comandos de la consola local de la puerta de enlace mediante el procedimiento descrito enhttps://docs.aws.amazon.com/filegateway/latest/files3/MaintenanceGatewayConsole-fgw.html.
2. Introduzca los siguientes comandos para deshabilitar el tráfico NFS:

```
iptables -I INPUT -p udp -m udp --dport 111 -j DROP
iptables -I INPUT -p udp -m udp --dport 2049 -j DROP
iptables -I INPUT -p udp -m udp --dport 20048 -j DROP
iptables -I INPUT -p tcp -m tcp --dport 111 -j DROP
iptables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
iptables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
```

3. Introduzca el siguiente comando para confirmar que los puertos NFS bloqueados aparecen en las tablas de IP:

```
iptables -n -L -v --line-numbers
```

Solución de problemas: uso de CloudWatch métricas

A continuación, encontrará información sobre las acciones para abordar los problemas mediante el uso de CloudWatch las métricas de Amazon con Storage Gateway.

Temas

- Tu puerta de enlace reacciona lentamente al navegar por los directorios
- Tu puerta de enlace no responde
- Su puerta de enlace tarda en transferir datos a Amazon S3
- Su puerta de enlace está realizando más operaciones de Amazon S3 de las esperadas
- No ves los archivos en tu bucket de Amazon S3
- El trabajo de copia de seguridad de la puerta de enlace falla o se producen errores al escribir en la puerta de enlace

Tu puerta de enlace reacciona lentamente al navegar por los directorios

Si File Gateway reacciona lentamente al ejecutar el ls comando o al navegar por los directorios, compruebe 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 . Los esfuerzos posteriores para mostrar el contenido de ese directorio deberían realizarse más rápidamente.
- Si la `IndexEviction` métrica es superior a 0, significa que su File Gateway ha alcanzado el límite de lo que puede administrar en su caché en ese momento. En este caso, la puerta de enlace de archivos debe liberar espacio de almacenamiento del directorio al que se ha accedido menos recientemente para incluir 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 segmento de S3 relacionado y las recomendaciones para mejorar el rendimiento en función de su caso de uso.

Tu puerta de enlace no responde

Si File Gateway no responde, haga lo siguiente:

- 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, es posible que la puerta de enlace de archivos se vea obstruida por un disco raíz lento a medida que reconstruye la caché de índices en RAM. Puede solucionar este problema mediante el uso de un disco físico más rápido para el disco raíz.
- Si la `MemUsedBytes` métrica es igual o casi igual a la `MemTotalBytes` métrica, significa que su File Gateway se está quedando sin RAM disponible. Asegúrese de que su puerta de enlace de archivos tenga al menos la RAM mínima requerida. Si ya la tiene, considere la posibilidad de añadir más RAM a su puerta de enlace de archivos en función de su carga de trabajo y 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 su File Gateway.

Su puerta de enlace tarda en transferir datos a Amazon S3

Si su puerta de enlace de archivos tarda en transferir datos a Amazon S3, haga lo siguiente:

- Si la `CachePercentDirty` métrica es 80 o superior, File Gateway escribe los datos en el disco más rápido de lo que puede cargarlos en Amazon S3. Considere aumentar el ancho de banda para cargar archivos desde su puerta de enlace de archivos, añadir uno o más discos de caché o ralentizar las escrituras de los clientes.
- Si la `CachePercentDirty` métrica es baja, `IoWaitPercent` compruébela. Si `IoWaitPercent` es superior a 10, es posible que la velocidad del disco caché local bloquee la puerta de enlace de archivos. Recomendamos 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.
- Si`S3PutObjectRequestTime`, o `S3GetObjectRequestTime` son altos`S3UploadPartRequestTime`, es posible que haya un cuello de botella en la red. Intente analizar la red para comprobar que la puerta de enlace tiene el ancho de banda esperado.

Su puerta de enlace está realizando más operaciones de Amazon S3 de las esperadas

Si su File Gateway realiza más operaciones de Amazon S3 de las esperadas, compruebe la `FilesRenamed` métrica. Las operaciones de cambio de nombre son caras de ejecutar en Amazon S3. Optimice su flujo de trabajo para minimizar la cantidad de operaciones de cambio de nombre.

No ves los archivos en tu bucket de Amazon S3

Si observa que los archivos de la puerta de enlace no se reflejan en el bucket de Amazon S3, compruebe la `FilesFailingUpload` métrica. Si la métrica indica que algunos archivos no se cargan correctamente, comprueba tus notificaciones de estado. Cuando los archivos no se pueden cargar, la pasarela genera una notificación de salud con más detalles sobre el problema.

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 File Gateway falla o se producen errores al escribir en File Gateway, haga lo siguiente:

- Si la `CachePercentDirty` métrica es del 90 por ciento o superior, File Gateway no puede aceptar nuevas escrituras en el disco porque no hay suficiente espacio disponible en la memoria caché. Para ver la rapidez con la que File Gateway se carga en Amazon S3 FSx , consulte la `CloudBytesUploaded` métrica. Compare esa métrica con la `WriteBytes` métrica, que muestra la rapidez con la que el cliente escribe archivos en su File Gateway. Si el cliente SMB escribe en su puerta de enlace de archivos más rápido de lo que puede cargar en Amazon S3 FSx , 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 se produce un error en una copia de un archivo grande, como una tarea de copia de seguridad, pero la `CachePercentDirty` métrica es inferior al 80 por ciento, es posible que su File Gateway esté agotando 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.

  Para NFS, asegúrese de que el cliente se haya montado mediante un montaje rígido en lugar de un montaje blando.

Solución de problemas: problemas con el uso compartido de archivos

A continuación encontrará información sobre las acciones que debe realizar si experimenta problemas inesperados con recursos compartidos de archivos.

Temas

- El archivo compartido está bloqueado en el estado CREATING
- No puedes crear un recurso compartido de archivos
- Los archivos compartidos SMB no permiten varios métodos de acceso diferentes
- Varios archivos compartidos no pueden escribir en el bucket de S3 mapeado

- Notificación de un grupo de registros eliminado cuando se utilizan registros de auditoría
- No puede cargar archivos en su bucket de S3
- No puedo cambiar el cifrado predeterminado para usar SSE-KMS para cifrar los objetos almacenados en mi bucket de S3
- Los cambios realizados directamente en un bucket de S3 con el control de versiones de objetos activado pueden afectar a lo que veas en tu recurso compartido de archivos
- Al escribir en un bucket de S3 con el control de versiones activado, Amazon S3 File Gateway puede crear varias versiones de los objetos de Amazon S3
- Los cambios en un bucket de S3 no se reflejan en Storage Gateway
- Los permisos de ACL no funcionan como se esperaba
- El rendimiento de su puerta de enlace disminuyó después de realizar una operación recursiva

El archivo compartido está bloqueado en el estado CREATING

Cuando el recurso compartido de archivos se está creando, el estado es CREATING. El estado pasa a ser a AVAILABLE una vez que se crea el recurso compartido de archivos. Si el recurso compartido de archivos se bloquea en el estado CREATING, haga lo siguiente:

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. Asegúrese de que el depósito de S3 al que asignó su recurso compartido de archivos existe. Si el bucket no existe, créelo. Después de crear el bucket, el estado del recurso compartido de archivos pasa a ser AVAILABLE. Para obtener información sobre cómo crear un depósito de S3, consulte Crear un depósito en la Guía del usuario de Amazon Simple Storage Service.
3. Asegúrese de que el nombre de su bucket cumpla con las normas de denominación de bucket de Amazon S3. Para obtener más información, consulte Reglas para nombrar buckets en la Guía del usuario de Amazon Simple Storage Service.

   > **Note**
   >
   > S3 File Gateway no admite buckets de Amazon S3 con puntos (`.`) en el nombre del bucket.

4. Asegúrese de que la función de IAM que utilizó para acceder al bucket de S3 tenga los permisos correctos y compruebe que el bucket de S3 aparezca como recurso en la política de IAM. Para obtener más información, consulte Concesión de acceso a un bucket de Amazon S3.

No puedes crear un recurso compartido de archivos

1. Si no puede crear un recurso compartido de archivos porque su recurso compartido de archivos está bloqueado en el estado DE CREACIÓN, compruebe que el depósito de S3 al que lo asignó existe. Para obtener información acerca de cómo hacerlo, consulte El archivo compartido está bloqueado en el estado CREATING, más arriba.
2. Si el depósito de S3 existe, compruebe que AWS Security Token Service esté activado en la región en la que va a crear el recurso compartido de archivos. Si un token de seguridad no está activo, debe activarlo. Para obtener información sobre cómo activar un token mediante AWS Security Token Service, consulte Activación y desactivación del AWS STS en una AWS región en la Guía del usuario de IAM.

Los archivos compartidos SMB no permiten varios métodos de acceso diferentes

Los recursos compartidos de archivos SMB tienen las siguientes restricciones:

1. Cuando el mismo cliente intenta montar un recurso compartido de archivos SMB para el acceso de invitado y para Active Directory, se muestra el siguiente mensaje de error: `Multiple connections to a server or shared resource by the same user, using more than one user name, are not allowed. Disconnect all previous connections to the server or shared resource and try again.`
2. Un usuario de Windows no puede estar conectado a dos recursos compartidos de archivos SMB para el acceso de invitado y es posible que se le desconecte cuando se establezca una nueva conexión de acceso de invitado.
3. Un cliente de Windows no puede montar un recurso compartido de archivos SMB para el acceso de invitado y para Active Directory que se haya exportado por la misma gateway.

Varios archivos compartidos no pueden escribir en el bucket de S3 mapeado

No recomendamos configurar el depósito de S3 para permitir que varios recursos compartidos de archivos escriban en un depósito de S3. Este enfoque puede producir resultados impredecibles.

En su lugar, le recomendamos que solo un recurso compartido de archivos pueda escribir en cada bucket de S3. Puede crear una política de bucket para permitir que únicamente el rol asociado

al recurso compartido de archivos escriba en el bucket. Para obtener más información, consulte Prácticas recomendadas para File Gateway.

Notificación de un grupo de registros eliminado cuando se utilizan registros de auditoría

Si el grupo de registros no existe, el usuario puede seleccionar el enlace del grupo de registros que aparece debajo de ese mensaje para crear un nuevo grupo de registros o usar un grupo de registros existente para usarlo como destino de los registros de auditoría

No puede cargar archivos en su bucket de S3

Si no puede cargar archivos en su bucket de S3, haga lo siguiente:

1. Asegúrese de haber concedido el acceso necesario a Amazon S3 File Gateway para cargar archivos en su bucket de S3. Para obtener más información, consulte Concesión de acceso a un bucket de Amazon S3.
2. Asegúrese de que el rol que creó el bucket tenga permiso para escribir en el bucket de S3. Para obtener más información, consulte las prácticas recomendadas para File Gateway.
3. Si su puerta de enlace de archivos utiliza SSE-KMS o DSSE-KMS para el cifrado, asegúrese de que la función de IAM asociada al recurso compartido de archivos incluya los permisos KMS:Encrypt, KMS:Decrypt, kms: *, kms: y kms:. ReEncrypt GenerateDataKey DescribeKey Para obtener más información, consulte Uso de políticas basadas en la identidad (políticas de IAM) para Storage Gateway.

No puedo cambiar el cifrado predeterminado para usar SSE-KMS para cifrar los objetos almacenados en mi bucket de S3

Si cambia el cifrado predeterminado y establece el SSE-KMS (cifrado del lado del servidor con claves AWS KMS administradas) como el predeterminado para su bucket de S3, los objetos que Amazon S3 File Gateway almacena en el bucket no se cifran con SSE-KMS. De forma predeterminada, una puerta de enlace de archivos de S3 utiliza el cifrado del lado del servidor gestionado con Amazon S3 (SSE-S3) cuando escribe datos en un bucket de S3. Cambiar la configuración predeterminada no cambiará el cifrado automáticamente.

Para cambiar el cifrado y usar SSE-KMS con su propia AWS KMS clave, debe activar el cifrado SSE-KMS. Para ello, debe proporcionar el nombre de recurso de Amazon (ARN) de la clave

de KMS al crear el recurso compartido de archivos. También puede actualizar la configuración de KMS para el recurso compartido de archivos utilizando operación `UpdateNFSFileShare` o `UpdateSMBFileShare` de la API. Esta actualización se aplica a los objetos almacenados en los buckets de S3 después de la actualización. Para obtener más información, consulte Cifrado de datos mediante AWS KMS.

Los cambios realizados directamente en un bucket de S3 con el control de versiones de objetos activado pueden afectar a lo que veas en tu recurso compartido de archivos

Si su bucket de S3 tiene objetos escritos en él por otro cliente, es up-to-date posible que su visión del bucket de S3 no se deba al control de versiones de los objetos del bucket de S3. Actualice siempre la caché antes de examinar los archivos que le interesen.

El control de versiones de objetos es una característica opcional del bucket de S3 que ayuda a proteger los datos al almacenar varias copias del objeto con el mismo nombre. Cada copia tiene un valor de ID independiente, por ejemplo `file1.jpg`: `ID="xxx"` y `file1.jpg`: `ID="yyy"`. La cantidad de objetos con nombres idénticos y su vida útil se controlan mediante las políticas de ciclo de vida de Amazon S3. Para obtener más información sobre estos conceptos de Amazon S3, consulte Uso del control de versiones y la gestión del ciclo de vida de los objetos en la Guía para desarrolladores de Amazon S3.

Cuando se elimina un objeto con control de versiones, ese objeto se marca con un marcador de eliminación pero se conserva. Solo el propietario de un bucket de S3 puede eliminar definitivamente un objeto con el control de versiones activado.

En su puerta de enlace de archivos de S3, los archivos que se muestran son las versiones más recientes de los objetos de un bucket de S3 en el momento en que se obtuvo el objeto o se actualizó la caché. Las pasarelas de archivos de S3 ignoran las versiones anteriores o los objetos marcados para su eliminación. Cuando se lee un archivo, los datos que se leen son de la versión más reciente. Al escribir un archivo en su recurso compartido de archivos, su S3 File Gateway crea una nueva versión de un objeto con nombre asignado con los cambios y esa versión pasa a ser la última versión.

Su puerta de enlace de archivos de S3 sigue leyendo la versión anterior y las actualizaciones que realice se basan en la versión anterior en caso de que se añada una nueva versión al bucket de S3 fuera de su aplicación. Para leer la versión más reciente de un objeto, utilice la acción de la

RefreshCacheAPI o actualice desde la consola, tal y como se describe enActualización de la caché de objetos del bucket de Amazon S3.

> **Important**
>
> No recomendamos que los objetos o archivos se escriban en el bucket S3 de S3 de S3 de S3 desde fuera del recurso compartido de archivos.

Al escribir en un bucket de S3 con el control de versiones activado, Amazon S3 File Gateway puede crear varias versiones de los objetos de Amazon S3

Con el control de versiones de objetos activado, es posible que cree varias versiones de un objeto en Amazon S3 en cada actualización de un archivo desde su cliente NFS o SMB. Estos son algunos escenarios que pueden provocar la creación de varias versiones de un objeto en su bucket de S3:

- Cuando un cliente NFS o SMB modifica un archivo en Amazon S3 File Gateway después de cargarlo en Amazon S3, S3 File Gateway carga los datos nuevos o modificados en lugar de cargar todo el archivo. La modificación del archivo da como resultado la creación de una nueva versión del objeto Amazon S3.
- Cuando un cliente NFS o SMB escribe un archivo en S3 File Gateway, S3 File Gateway carga los datos del archivo en Amazon S3 seguidos de sus metadatos (propietarios, marcas de tiempo, etc.). Al cargar los datos del archivo, se crea un objeto de Amazon S3 y, al cargar los metadatos del archivo, se actualizan los metadatos del objeto de Amazon S3. Este proceso crea otra versión del objeto, lo que da como resultado dos versiones de un objeto.
- Cuando la puerta de enlace de archivos de S3 carga archivos más grandes, es posible que tenga que cargar partes más pequeñas del archivo antes de que el cliente termine de escribir en la puerta de enlace de archivos. Esto se debe, entre otras razones, a liberar espacio en la memoria caché o a una alta tasa de escrituras en un archivo. Esto puede provocar varias versiones de un objeto en el bucket de S3.

Debe supervisar su depósito de S3 para determinar cuántas versiones de un objeto existen antes de configurar políticas de ciclo de vida para mover los objetos a diferentes clases de almacenamiento. Debe configurar la caducidad del ciclo de vida de las versiones anteriores a fin de minimizar la cantidad de versiones que tiene para un objeto en su depósito de S3. El uso de la replicación en

la misma región (SRR) o la replicación entre regiones (CRR) entre depósitos de S3 aumentará el almacenamiento utilizado. Para obtener más información sobre la replicación, consulte Replicación.

> **Important**
>
> No configure la replicación entre depósitos de S3 hasta que sepa cuánto almacenamiento se utiliza cuando se activa el control de versiones de los objetos.

El uso de buckets S3 versionados puede aumentar considerablemente la cantidad de almacenamiento en Amazon S3, ya que cada modificación de un archivo crea una nueva versión del objeto S3. De forma predeterminada, Amazon S3 sigue almacenando todas estas versiones a menos que cree específicamente una política para anular este comportamiento y limitar el número de versiones que se conservan. Si observa un uso de almacenamiento inusualmente elevado con el control de versiones de objetos activado, compruebe que sus políticas de almacenamiento estén configuradas de forma adecuada. Un aumento en el número de respuestas `HTTP 503-slow down` a las solicitudes del navegador también puede indicar la existencia de problemas con el control de versiones de objetos.

Si activa el control de versiones de objetos después de instalar una puerta de enlace de archivos de S3, se conservan todos los objetos únicos (`ID="NULL"`) y podrá verlos todos en el sistema de archivos. A las versiones nuevas de los objetos se les asigna un ID exclusivo (las versiones anteriores se conservan). Basándose en la marca temporal del objeto, solo se puede ver el objeto con control de versiones más reciente en el sistema de archivos de NFS.

Tras activar el control de versiones de objetos, el bucket de S3 no podrá volver a un estado no versionado. Sin embargo, sí que se puede suspender el control de versiones. Al suspender el control de versiones, a los objetos nuevos se les asigna un ID. Si el objeto con el mismo nombre existe con un valor `ID="NULL"`, la versión anterior se sobrescribe. Sin embargo, las versiones que contengan ID que no sean `NULL` se conservan. Las marcas temporales identifican el objeto nuevo como el objeto actual y ese el que aparece en el sistema de archivos de NFS.

Los cambios en un bucket de S3 no se reflejan en Storage Gateway

Storage Gateway actualiza la caché del recurso compartido de archivos automáticamente cuando se escriben archivos en la caché de forma local mediante el recurso compartido de archivos. Sin embargo, Storage Gateway no actualiza automáticamente la memoria caché cuando se carga un archivo directamente en Amazon S3. Al hacerlo, debe realizar una `RefreshCache` operación para

ver los cambios en el recurso compartido de archivos. Si tiene más de un recurso compartido de archivos, debe ejecutar la `RefreshCache` operación en cada recurso compartido de archivos.

Puede actualizar la memoria caché mediante la consola Storage Gateway y AWS Command Line Interface (AWS CLI):

- Para actualizar la caché mediante la consola Storage Gateway, consulte Refrescar objetos en su bucket de Amazon S3.
- Para actualizar la memoria caché mediante AWS CLI:
  1. Ejecute el comando `aws storagegateway list-file-shares`
  2. Copie el número de recurso de Amazon (ARN) del recurso compartido de archivos con la caché que desee actualizar.
  3. Ejecute el `refresh-cache` comando con su ARN como valor para: `--file-share-arn`

     ```
     aws storagegateway refresh-cache --file-share-arn
     arn:aws:storagegateway:eu-west-1:12345678910:share/share-FFDEE12
     ```

Para automatizar la `RefreshCache` operación, consulte ¿Cómo puedo automatizar la RefreshCache operación en Storage Gateway?

Los permisos de ACL no funcionan como se esperaba

Si los permisos de lista de control de acceso (ACL) no funcionan según lo previsto en un recurso compartido de archivos SMB, puede hacer una prueba.

Para ello, en primer lugar, pruebe los permisos en un servidor de archivos de Microsoft Windows o un recurso compartido de archivos de Windows local. A continuación, compare el comportamiento con el del recurso compartido de archivos de la gateway.

El rendimiento de su puerta de enlace disminuyó después de realizar una operación recursiva

En algunos casos, puede realizar una operación recursiva, como cambiar el nombre de un directorio o activar la herencia de una ACL, y forzarla a descender en el árbol. Si lo hace, la puerta de enlace de archivos de S3 aplicará la operación de forma recursiva a todos los objetos del recurso compartido de archivos.

Por ejemplo, supongamos que aplica la herencia a los objetos existentes en un bucket de S3. Su S3 File Gateway aplica la herencia de forma recursiva a todos los objetos del depósito. Este tipo de operaciones pueden provocar la degradación del rendimiento de la gateway.

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 las 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 File Gateway

En esta sección se incluyen los siguientes temas, que proporcionan información sobre las prácticas recomendadas para trabajar con puertas de enlace, recursos compartidos de archivos, depósitos 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 con la implementación de Storage Gateway.

Temas

- Prácticas recomendadas: recuperación de los datos
- Mejores prácticas: gestionar las cargas de varias partes
- Prácticas recomendadas: descomprima los archivos comprimidos localmente antes de copiarlos en una puerta de enlace
- Conserve los atributos del archivo al copiar datos de Windows Server
- Prácticas recomendadas: dimensionar correctamente los discos de caché
- Trabajar con varios recursos compartidos de archivos y buckets de Amazon S3
- Limpie los 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 admite la recuperación de una máquina virtual de puerta de enlace a partir de una instantánea creada por el hipervisor o desde la EC2 Amazon Machine Image (AMI) de Amazon. 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 su puerta de enlace o centro de datos se vuelve inaccesible por algún motivo, puede recuperar los datos en otra puerta de enlace de un centro de datos diferente o recuperarlos en una puerta de enlace alojada en una EC2 instancia de Amazon. Si no tienes acceso a otro centro de datos, te recomendamos crear la puerta de enlace en una EC2 instancia de Amazon. Los pasos que siga dependerán del tipo de gateway cuyos datos intenta recuperar.

Para recuperar datos de una pasarela de archivos situada en un centro de datos inaccesible

En el caso de File Gateway, debe asignar un nuevo de archivos al bucket de Amazon S3 FSx que contiene los datos que desea recuperar.

1. Cree y active un nuevo File Gateway en un EC2 host de Amazon. Para obtener más información, consulte Implemente un EC2 host de Amazon predeterminado para S3 File Gateway.

2. Cree un nuevo en la EC2 pasarela que creó. Para obtener más información, consulte Crear un recurso compartido de archivos .
3. Monte el compartidos en su cliente y asígnelo al bucket S3 FSx que contiene los datos que desea recuperar. Para obtener más información, consulte Montar y usar el recurso compartido de archivos .

Mejores prácticas: gestionar las cargas de varias partes

Al transferir archivos de gran tamaño, S3 File Gateway utiliza la función de carga multiparte de Amazon S3 para dividir los archivos en partes más pequeñas y transferirlos en paralelo para mejorar la eficiencia. Para obtener más información sobre la carga multiparte, consulte Carga y copia de objetos mediante la carga multiparte en la Guía del usuario de Amazon Simple Storage Service.

Si una carga de varias partes no se completa correctamente por algún motivo, la pasarela normalmente detiene la transferencia, elimina cualquier parte del archivo transferida parcialmente de Amazon S3 e intenta realizar la transferencia de nuevo. En raras ocasiones, como cuando un fallo de hardware o red impide que la puerta de enlace se limpie tras una carga multiparte fallida, es posible que partes del archivo parcialmente transferido permanezcan en Amazon S3, donde pueden incurrir en gastos de almacenamiento.

Como práctica recomendada para minimizar los costes de almacenamiento en Amazon S3 derivados de cargas incompletas de varias partes, recomendamos configurar una regla del ciclo de vida de los buckets de Amazon S3 que utilice la acción de la `AbortIncompleteMultipartUpload` API para detener automáticamente las transferencias fallidas y eliminar las partes de archivos asociadas después de un número de días designado. Para obtener instrucciones, consulte Configurar una configuración del ciclo de vida de un bucket para eliminar las cargas multiparte incompletas en la Guía del usuario de Amazon Simple Storage Service.

Prácticas recomendadas: descomprima los archivos comprimidos localmente antes de copiarlos en una puerta de enlace

Si intenta descomprimir un archivo comprimido que contiene miles de archivos mientras está almacenado en la puerta de enlace, es posible que se produzcan retrasos importantes relacionados con el rendimiento. El proceso de descomprimir un archivo que contiene una gran cantidad de archivos en cualquier tipo de recurso compartido de archivos de red implica por sí mismo un alto volumen de input/output operaciones, la manipulación de la caché de metadatos, la sobrecarga de

la red y la latencia. Además, Storage Gateway no puede determinar cuándo se ha terminado de descomprimir cada archivo del archivo y puede empezar a cargar los archivos antes de que finalice el proceso, lo que afecta aún más al rendimiento. Estos problemas se agravan cuando los archivos del archivo son numerosos, pero de tamaño pequeño.

Como práctica recomendada, se recomienda transferir primero los archivos comprimidos desde la puerta de enlace a la máquina local, antes de descomprimirlos. Luego, si es necesario, puedes usar una herramienta como robocopy o rsync para volver a transferir los archivos descomprimidos a la puerta de enlace.

Conserve los atributos del archivo al copiar datos de Windows Server

Es posible copiar archivos a su puerta de enlace de archivos mediante el `copy` comando básico de Microsoft Windows, pero este comando copia solo los datos del archivo de forma predeterminada, omitiendo ciertos atributos del archivo, como los descriptores de seguridad. Si los archivos se copian en la puerta de enlace sin las restricciones de seguridad correspondientes ni la información de la lista de control de acceso discrecional (DACL), es posible que usuarios no autorizados puedan acceder a ellos.

Como práctica recomendada para conservar todos los atributos de los archivos y la información de seguridad al copiar archivos a la puerta de enlace de Microsoft Windows Server, se recomienda utilizar los `xcopy` comandos `robocopy` o, con los `/o` indicadores `/copy:DS` o, respectivamente. Para obtener más información, consulte robocopy y xcopy en la documentación de referencia de comandos de Microsoft Windows Server.

Prácticas recomendadas: dimensionar correctamente los discos de caché

Para obtener el mejor rendimiento, el tamaño total de la memoria caché del disco debe ser lo suficientemente grande como para cubrir el tamaño del conjunto de trabajo activo. En el caso de read/write cargas de trabajo mixtas y con un uso intensivo de lecturas, esto garantiza que se pueda conseguir un alto porcentaje de aciertos de caché en las lecturas, lo cual es deseable. Puede monitorizarlo mediante la `CacheHitPercent` métrica de su S3 File Gateway.

En el caso de cargas de trabajo de escritura intensiva (por ejemplo, para copias de seguridad y archivado), S3 File Gateway almacena en búfer las escrituras entrantes en la memoria caché del

disco antes de copiar estos datos de forma asíncrona a Amazon S3. Debe asegurarse de tener suficiente capacidad de caché para almacenar en búfer los datos escritos. La `CachePercentDirty` métrica proporciona una indicación del porcentaje de la memoria caché del disco que aún no se ha conservado. AWS

Se recomiendan valores bajos `CachePercentDirty` de. Los valores que se acercan constantemente al 100% indican que S3 File Gateway no puede mantener el ritmo del tráfico de escritura entrante. Puede evitarlo aumentando la capacidad de caché en disco aprovisionada o aumentando el ancho de banda de red dedicado disponible desde S3 File Gateway a Amazon S3, o ambas opciones.

Para obtener más información sobre el tamaño del disco caché, consulte las prácticas recomendadas de tamaño de caché de Amazon S3 File Gateway en el canal oficial de Amazon Web Services YouTube .

Trabajar con varios recursos compartidos de archivos y buckets de Amazon S3

Al configurar un único bucket de Amazon S3 para permitir que varias puertas de enlace o recursos compartidos de archivos escriban en él, los resultados pueden ser impredecibles. Puede configurar sus buckets de dos maneras para evitar resultados impredecibles. Elija el método de configuración que mejor se adapte a su caso de uso entre las siguientes opciones:

- Configure los depósitos de S3 para que solo un recurso compartido de archivos pueda escribir en cada depósito. Usa un recurso compartido de archivos diferente para escribir en cada depósito.

  Para ello, cree una política de bucket de S3 que deniegue todas las funciones excepto la que se utiliza para un recurso compartido de archivos específico para colocar o eliminar objetos en el bucket. Adjunta una política similar a cada depósito, especificando un recurso compartido de archivos diferente para escribir en cada depósito.

  El siguiente ejemplo de política deniega los permisos de escritura en el bucket de S3 a todos los roles, excepto al rol que creó el bucket. Las acciones `s3:DeleteObject` y `s3:PutObject` se deniegan a todos los roles excepto a `"TestUser"`. La política es aplicable a todos los objetos del bucket `"arn:aws:s3:::amzn-s3-demo-bucket/*"`.

  JSON

  ```
  {
  ```

```
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyMultiWrite",
         "Effect":"Deny",
         "Principal":"*",
         "Action":[
            "s3:DeleteObject",
            "s3:PutObject"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*",
         "Condition":{
            "StringNotLike":{
               "aws:userid":"TestUser:*"
            }
         }
      }
   ]
}
```

- Si desea que varios recursos compartidos de archivos escriban en el mismo bucket de Amazon S3, debe evitar que los recursos compartidos intenten escribir en los mismos objetos simultáneamente.

  Para ello, configure un prefijo de objeto único e independiente para cada recurso compartido de archivos. Esto significa que cada recurso compartido de archivos solo escribe en los objetos con el prefijo correspondiente y no escribe en los objetos que están asociados a los demás recursos compartidos de archivos de la implementación. El prefijo del objeto se configura en el campo del nombre del prefijo de S3 al crear un nuevo recurso compartido de archivos.

Limpie los recursos innecesarios

Como práctica recomendada, recomendamos limpiar los recursos de Storage Gateway para evitar cargos inesperados o innecesarios. Por ejemplo, si creó una puerta de enlace como ejercicio de demostración o prueba, considere eliminarla y su dispositivo virtual de la implementación. Utilice el siguiente procedimiento para limpiar los recursos.

Para eliminar los recursos innecesarios

1. Si ya no piensa 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 has creado tu gateway en una EC2 instancia de Amazon, finaliza la instancia.

Recursos adicionales de Storage Gateway

Esta sección contiene los siguientes temas, que proporcionan información y recursos adicionales relacionados con la configuración y el uso 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.
- Obtener la clave de activación: obtenga información sobre dónde encontrar la clave de activación que debe proporcionar al implementar una nueva puerta de enlace.
- Compatibilidad con los atributos de los archivos- Aprenda cómo gestiona su puerta de enlace los atributos de los archivos de DOS y Windows.
- Usando AWS 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- Aprenda qué permisos debe tener su cuenta de servicio para poder unir su puerta de enlace a su 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 File Gateway, incluidas las limitaciones mínimas y máximas para los recursos compartidos de archivos y los discos de caché locales.
- Uso de clases de almacenamiento- Obtenga información sobre las clases de almacenamiento de Amazon S3 que admite File Gateway y qué hay que tener en cuenta a la hora de elegir una clase de almacenamiento.

- Uso de los controladores CSI de Kubernetes- Aprenda a instalar y configurar los controladores de la interfaz de almacenamiento de contenedores (CSI) para permitir que las instancias de Kubernetes utilicen File Gateway para el almacenamiento.
- Módulo Terraform- Aprenda a usar Terraform para implementar File Gateway como una máquina virtual.

Implementación y configuración del host de la máquina virtual de la puerta de enlace

En los temas siguientes se proporciona información sobre la configuración de la plataforma de alojamiento de la máquina virtual para su puerta de enlace.

Temas

- Implemente un EC2 host de Amazon predeterminado para S3 File Gateway
- Implemente un EC2 host Amazon personalizado para S3 File Gateway
- Modificar las opciones de metadatos de las EC2 instancias de Amazon
- 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 EC2 host de Amazon predeterminado para S3 File Gateway

En este tema se enumeran los pasos para implementar un EC2 host de Amazon con las especificaciones predeterminadas.

Puede implementar y activar un Amazon S3 File Gateway 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 EC2 instancia de Amazon, elige Amazon EC2 como plataforma de alojamiento en la sección Opciones de plataforma del flujo de trabajo. Para obtener instrucciones sobre la configuración de la EC2 instancia de Amazon, consulte Implementación de una EC2 instancia de Amazon para alojar su Amazon S3 File Gateway .
2. Seleccione Launch instance para abrir la plantilla de AWS Storage Gateway AMI en la EC2 consola de Amazon 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 EC2 instancia de Amazon con la configuración predeterminada.

   La EC2 instancia de Amazon que crea Use default settings tiene las siguientes especificaciones predeterminadas:

   - Tipo de instancia: m5.xlarge
   - Configuración de red
     - En el caso de la VPC, selecciona la VPC en la que quieres que se ejecute la EC2 instancia.
     - En Subnet, especifica la subred en la que se debe lanzar la EC2 instancia.

       > **Note**
       >
       > Las subredes de VPC aparecerán en el menú desplegable solo si tienen activada la configuración de asignación automática de IPv4 direcciones públicas desde la consola de administración de VPC.

     - Asignar una IP pública de forma automática: Activada
     - Se crea un grupo EC2 de seguridad y se asocia a la instancia. 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 podrá acceder a la EC2 instancia a través de los demás puertos de la VPC seleccionada.
       > Solo se puede acceder a los archivos compartidos de su puerta de enlace desde los hosts de la misma VPC que la puerta de enlace. Si es necesario acceder a los

archivos compartidos 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 EC2 instancia de Amazon, 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
111	TCP, UDP	NFSv3
139	TCP, UDP	SMB
445	TCP	SMB
2049	TCP, UDP	NFS
20048	TCP, UDP	NFSv3

- Configurar almacenamiento

Configuración predeterminada	Volumen raíz de AMI	Caché de volumen 2				
Nombre de dispositivo		'/dev/sdb'				
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 EC2 host Amazon personalizado para S3 File Gateway

Puede implementar y activar un Amazon S3 File Gateway 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.
> S3 File Gateway FSx 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_S3-1.25.0
```

Para implementar una EC2 instancia de Amazon para alojar su Amazon S3 File Gateway

1. Empiece configurando una nueva puerta de enlace mediante la consola de Storage Gateway. Para obtener instrucciones, consulte Configuración de una puerta de enlace de archivos de Amazon S3 Configuración de una puerta . Cuando llegues a la sección de opciones de plataforma, elige Amazon EC2 como plataforma de alojamiento y, a continuación, sigue estos pasos para lanzar la EC2 instancia de Amazon que alojará tu File Gateway.
2. Elija Launch instance para abrir la plantilla de AWS Storage Gateway AMI en la EC2 consola de Amazon, donde podrá configurar ajustes adicionales.

   Usa Quicklaunch para lanzar la EC2 instancia de Amazon con la configuración predeterminada. Para obtener más información sobre las especificaciones predeterminadas de Amazon EC2 Quicklaunch, consulte Especificaciones de configuración de Quicklaunch para Amazon Quicklaunch Especificaciones de configuración de Amazon EC2 Amazon. EC2
3. En Nombre, introduce un nombre para la EC2 instancia de Amazon. Una vez implementada la instancia, puedes buscar este nombre para encontrarla en las páginas de listas de la EC2 consola de Amazon.
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 EC2 instancias de Amazon.

   Puede cambiar el tamaño de la instancia después de lanzarla, si es necesario. Para obtener más información, consulta Cómo cambiar el tamaño de una instancia en la Guía del EC2 usuario de Amazon.

   > **Note**
   >
   > Algunos tipos de instancias, especialmente la i3 EC2, utilizan discos NVMe SSD. Estos pueden causar problemas al iniciar o detener File Gateway; por ejemplo, puede perder datos de la memoria 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 el caso de la VPC (obligatorio), elige la VPC en la que quieres lanzar tu 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 Subnet, elige la subred en la que quieres lanzar tu 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 deseas, puedes cambiar el nombre y la descripción predeterminados del nuevo grupo de seguridad que se va a crear para tu EC2 instancia de Amazon, o bien optar por aplicar reglas de firewall desde 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 S3 File Gateway , consulte Requisitos de . 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 S3 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.
> Si planea crear recursos compartidos de archivos NFS, debe abrir el TCP/UDP puerto 2049 para el acceso a NFS, el TCP/UDP puerto 111 para el acceso y TCP/UDP el puerto 20048 para el NFSv3 acceso. NFSv3
> Si planea crear recursos compartidos de archivos SMB, debe abrir el puerto TCP 445 para acceder a SMB.

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 añadir 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 Launch instance para lanzar su nueva instancia de Amazon EC2 Gateway con los ajustes configurados.
13. Para comprobar que la nueva instancia se lanzó correctamente, vaya a la página de instancias de la EC2 consola de Amazon 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 IPv4dirección pública de la sección de resumen de la instancia y, a continuación, vuelva a la página Configurar puerta de enlace de la consola de Storage Gateway para reanudar la configuración de Amazon S3 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 Configuración de una puerta de enlace de archivos de Amazon S3 Configuración de una puerta . Cuando llegue a la sección de 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 EC2 consola de Amazon.

  Se le redirigirá a la página de AMI de la EC2 comunidad, donde podrá ver el ID de la 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_S3/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_S3/latest
```

El comando de la CLI devuelve un resultado similar al siguiente.

```
{
    "Parameter": {
        "Type": "String",
        "LastModifiedDate": 1561054105.083,
        "Version": 4,
        "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/
FILE_S3/latest",
        "Name": "/aws/service/storagegateway/ami/FILE_S3/latest",
        "Value": "ami-123c45dd67d891000"
    }
}
```

Modificar las opciones de metadatos de las EC2 instancias de Amazon

El servicio de metadatos de instancias (IMDS) es un componente de la instancia que proporciona acceso seguro a los metadatos de las EC2 instancias de Amazon. 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 () del IMDS. IMDSv2 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.

Le recomendamos que lo requiera IMDSv2 para todas las EC2 instancias de Amazon que alojen 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.

Para 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 tiempo. A continuación, en el cuadro de diálogo Opciones de NTP Daemon (ntpd), elija Configuración de NTP en el panel de la izquierda.

   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:

- Maximizar el rendimiento: es posible que desee maximizar el rendimiento de una puerta de enlace cuando los adaptadores de red son un obstáculo.

- 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). A excepción de este adaptador, los iniciadores deben estar en la misma subred que el adaptador que contiene los recursos compartidos de archivos a los que se conectan. 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 de ese destino y el AWS tráfico fluyen a través del mismo adaptador.

En algunos casos, puede configurar un adaptador para que se conecte a la consola Storage Gateway y, a continuación, añadir un segundo adaptador. En tal caso, Storage Gateway configura automáticamente la tabla de enrutamiento para usar el segundo adaptador como ruta preferida. Para obtener instrucciones sobre cómo configurar varios adaptadores, consulte los siguientes temas:

Temas

- Configuración de su puerta de enlace para varios NICs en un VMware ESXi host
- Configuración de su puerta de enlace para varios NICs servidores en Microsoft Hyper-V

Configuración de su puerta de enlace para varios NICs en un VMware ESXi host

En el siguiente procedimiento se supone que la máquina virtual de puerta de enlace ya tiene definido un adaptador de red y se 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.

   > **Note**
   >
   > Los ejemplos de comandos de montaje que se proporcionan en la página de información de un recurso compartido de archivos en la consola de Storage Gateway siempre

incluirán la dirección IP del adaptador de red que se agregó más recientemente a la puerta de enlace asociada al recurso compartido de archivos.

Para obtener información sobre las tareas de la consola local comunes a los VMware hosts de Hyper-V y KVM, consulte Realizar 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.

Para configurar la gateway 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 de 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.

> **Note**
>
> Los ejemplos de comandos de montaje que se proporcionan en la página de información de un recurso compartido de archivos en la consola de Storage Gateway siempre incluirán la dirección IP del adaptador de red que se agregó más recientemente a la puerta de enlace asociada al recurso compartido de archivos.

Para obtener información sobre las tareas de la consola local comunes a los VMware hosts de Hyper-V y KVM, consulte Realizar 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 .ova de VMware ESX que contiene la máquina virtual Storage Gateway en un solo host de un clúster.
> - Al implementar 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 la agrupación en clústeres, si implementa el paquete .ova en el clúster, seleccione un host cuando se le pida 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
- Configure su tipo de puerta de enlace
- Implementar la gateway
- (Opcional) Agregue opciones de anulación para otras opciones de VMs su 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, es posible 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 de VMs su clúster.

Configure su tipo de puerta de enlace

Utilice el siguiente procedimiento para configurar la puerta de enlace

Para descargar la imagen .ova según el tipo de gateway

- Descargue la imagen .ova según el tipo de gateway desde:
  - Puerta de enlace de archivos: Creación y activación de una puerta de enlace de archivo de Amazon S3

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.

Para implementar la imagen .ova de la gateway

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 de VMs su 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 Revisar la configuración y activar la configuración de revisión de Amazon S3 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 de S3 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 AWS Storage Gateway Hardware Appliance, las plantillas de imágenes de máquinas virtuales y EC2 Amazon Machine Images (AMI) 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.

Para obtener una clave de activación para la puerta de enlace desde la consola local

1. Inicie sesión en la consola local. Si te conectas a tu EC2 instancia de Amazon desde un ordenador Windows, inicia sesión 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 la AWS región en la 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.

Support para atributos de archivos en Amazon S3 File Gateway

Amazon S3 File Gateway admite los atributos de archivos de DOS o Windows de forma predeterminada. Con S3 File Gateway, puede conservar los datos y metadatos de los archivos y actualizar la configuración, como marcar los elementos como archivados cuando se colocan en Amazon S3. Para obtener más información sobre los atributos de los archivos de DOS y Windows, consulte el artículo sobre las constantes de los atributos de los archivos en el sitio web de documentación de desarrollo de aplicaciones de Windows.

S3 File Gateway admite los siguientes atributos:

- ReadOnly— El S3 File Gateway impide los cambios en los archivos que tienen el ReadOnly atributo establecido.
- Archivo: la puerta de enlace de archivos de S3 establece este atributo cuando los archivos se agregan por primera vez a la puerta de enlace.

> **Note**
>
> Las aplicaciones de backup suelen hacer copias de seguridad de los archivos que tienen el bit Archive establecido y, después, borran el bit después de realizar correctamente la copia de seguridad.

- Oculto: los clientes del bloque de mensajes del servidor (SMB) ocultan los archivos que utilizan este conjunto de bits.
- Sistema: este atributo persiste una vez que lo haya configurado.

Al copiar un archivo a la puerta de enlace de archivos de S3 con los atributos establecidos, los atributos de DOS o Windows del archivo se conservan en la puerta de enlace de archivos de S3 y en Amazon S3. Puede actualizar estos atributos para los archivos de la puerta de enlace y esas actualizaciones también se aplican al objeto en Amazon S3. Si se desaloja un archivo de la puerta de enlace, la puerta de enlace extrae el archivo, sus metadatos y sus atributos persistentes de Amazon S3 cuando usted lo solicita.

> **Note**
>
> Los atributos de DOS solo se admiten en los recursos compartidos SMB y si el acceso está controlado por las listas de control de acceso de Windows.

Uso AWS Direct Connect con Storage Gateway

AWS Direct Connect vincula su red interna a la nube de Amazon Web Services. Al usarlo AWS 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 AWS 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 AWS Direct Connect ubicación o en una AWS región diferente.

En la siguiente ilustración se muestra un ejemplo de cómo AWS 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 AWS 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 AWS Direct Connect en la Guía del usuario de AWS Direct Connect .
2. Connect el dispositivo Storage Gateway local al AWS 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 AWS Direct Connect .

Para obtener más información AWS Direct Connect, consulte ¿Qué es? AWS Direct Connect en la Guía AWS Direct Connect del usuario.

requisitos de permiso para la cuenta de servicio de Active Directory

Si planea usar Microsoft Active Directory para proporcionar acceso autenticado por el usuario a los compartidos 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 le ha delegado permiso para realizar determinadas tareas. Debe proporcionar las credenciales de nombre de usuario y contraseña de esta cuenta al unir un Storage Gateway a su dominio de Active Directory.

A la cuenta de servicio de Active Directory se le deben delegar los siguientes permisos en la OU 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. En el caso de EC2 las pasarelas de Amazon, también puede obtener la dirección IP de su EC2 instancia de Amazon en Amazon EC2 Management Console. 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
- EC2 anfitrión: Obtener una dirección IP de un EC2 host de Amazon

Cuando encuentre la dirección IP, anótela. A continuación, vuelva a la consola de Storage Gateway y escriba la dirección IP en la consola.

Obtener una dirección IP de un EC2 host de Amazon

Para obtener la dirección IP de la EC2 instancia de Amazon en la que está desplegada tu puerta de enlace, inicia sesión en la consola local de la EC2 instancia. 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 de Amazon EC2 Management Console. 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. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instances y, a continuación, seleccione la EC2 instancia en la que está desplegada la puerta de enlace.
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. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instances y, a continuación, seleccione la EC2 instancia en la que está desplegada la puerta de enlace.
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.
4. Una vez activada la gateway, elija la gateway que acaba de activar y, a continuación, elija la pestaña VTL devices en el panel inferior.
5. Obtenga los nombres de todos los dispositivos VTL.
6. Ejecute el siguiente comando para configurar cada uno de los destinos.

   ```
   iscsiadm -m node -o new -T [$TARGET_NAME] -p [$Elastic_IP]:3260
   ```

7. Ejecute el siguiente comando para iniciar sesión en cada uno de los destinos.

   ```
   iscsiadm -m node -p [$ELASTIC_IP]:3260 --login
   ```

   La puerta de enlace ahora está conectada mediante la dirección IP elástica de la EC2 instancia.

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 los archivos compartidos. Los archivos compartidos se denominan 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.

IDs Los recursos de Storage Gateway están en mayúsculas. Sin embargo, cuando utilizas estos recursos IDs con la EC2 API de Amazon, Amazon EC2 espera que el recurso esté IDs en minúsculas. Debes cambiar tu ID de recurso a minúsculas para usarlo con la API. EC2 Por ejemplo, en Storage Gateway el ID para un volumen podría ser `vol-1122AABB`. Cuando utilices este ID con la EC2 API, debes cambiarlo a. `vol-1122aabb` De lo contrario, es posible que la EC2 API no se comporte como se esperaba.

> **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 los 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.

En el caso de File Gateway, 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.

Para 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).

Para 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. Elige el icono del lápiz situado junto a la etiqueta que deseas editar y, a continuación, edita la etiqueta.
5. Cuando haya acabado de editar la etiqueta, elija Save (Guardar).

Para 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 AWS Storage Gateway funcionalidad.

Temas

- Componentes de código abierto para Storage Gateway
- Componentes de código abierto para Amazon S3 File Gateway

Componentes de código abierto para Storage Gateway

Se utilizan varias herramientas y licencias de terceros para ofrecer funciones para Volume Gateway, Tape Gateway y Amazon S3 File Gateway.

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 Storage Gateway implementados en Microsoft Hyper-V: sources_hyperv.tar
- Para los dispositivos Storage Gateway implementados en una máquina virtual basada en el núcleo de Linux (KVM): 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 S3 File Gateway

Se utilizan varias herramientas y licencias de terceros para ofrecer la funcionalidad de Amazon S3 File Gateway (S3 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 S3 File Gateway:

- Para Amazon S3 File Gateway: sgw-file-s3-open-source.tgz

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.

Límites y cuotas de Amazon S3 File Gateway

Cuotas para compartir archivos

En la siguiente tabla se muestran las cuotas para los recursos compartidos de archivos.

Descripción	Límite
Número máximo de recursos compartidos de archivos por gateway **Note** Cada recurso compartido de archivos solo se puede conectar a un depósito de S3, pero varios recursos compartidos de archivos se pueden conectar al mismo depósito. Si conecta más de un recurso compartido de archivos al mismo depósito, debe configurar cada recurso compartido de archivos para que utilice un nombre de prefijo único y que no se superponga para evitar read/write conflictos. La cantidad 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 la Guía de rendimiento para puertas de enlace con varios recursos compartidos de archivos.	50
El número máximo de archivos para los que una puerta de enlace puede almacenar metadatos en caché de forma simultánea **Note** Como S3 File Gateway está respaldado por Amazon S3, no hay un tamaño máximo de carpeta ni un límite en cuanto al número de archivos que	Capacidad de la puerta de enlace: Pequeño: 5 millones de archivos Mediano: 10 millones de archivos Archivos grandes: 20 millones de archivos

Descripción	Límite
puede almacenar o a los que puede acceder mediante una puerta de enlace. Cada puerta de enlace tiene un límite configurable que determina la cantidad de archivos para los que puede almacenar metadatos en caché de forma simultánea. Puede usar la acción de la UpdateGatewayInformationAPI GatewayCapacitypara establecer en `SmallMedium`, o`Large`. Esta configuración afecta al rendimiento de la puerta de enlace y a las recomendaciones de hardware. Para obtener más información, consulte la Guía de rendimiento para puertas de enlace con varios recursos compartidos de archivos.	
Tamaño máximo de un archivo individual, que es el tamaño máximo de un objeto individual en Amazon S3 **Note** Si escribe un archivo de más de 5 TB, obtendrá el mensaje de error "file too large" y solamente se cargarán los primeros 5 TB del archivo.	5 TB

Descripción	Límite
Longitud máxima de la ruta **Note** Los clientes no pueden crear una ruta que supere esta longitud; si lo hacen, se producirá un error. Este límite se aplica a los dos protocolos compatibles con File Gateways, NFS y SMB. La longitud de la ruta en bytes se calcula a partir de los valores de bits de caracteres en la codificación UTF-8.	1024 bytes
Longitud máxima del nombre de archivo **Note** File Gateway no admite nombres de archivo que superen esta longitud. La longitud del nombre de archivo en bytes se calcula a partir de los valores de bits de caracteres en la codificación UTF-8.	255 bytes

Tamaños de disco local recomendados para la puerta de enlace

En la siguiente tabla se recomiendan los tamaños para el almacenamiento en disco local de gateway implementada.

Tipo de gateway	Caché (mínimo)	Caché (máximo)	Otros discos locales necesarios
Puerta de enlace de archivo de S3	150 GiB	64 TiB	—

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

Uso de clases de almacenamiento

Amazon S3 File Gateway es compatible con las clases de almacenamiento Amazon S3 Standard, Amazon S3 Standard-Infrequent Access, Amazon S3 One Zone-Infrequent Access, Amazon S3 Intelligent-Tiering y S3 Glacier. Para obtener más información sobre las clases de almacenamiento, consulte las clases de almacenamiento de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

> **Note**
>
> S3 File Gateway no admite actualmente la clase de almacenamiento Amazon S3 Glacier Instant Retrieval.

Temas

- Uso de clases de almacenamiento con un File Gateway
- Uso de la clase de almacenamiento GLACIER con File Gateway

Uso de clases de almacenamiento con un File Gateway

Al crear o actualizar un recurso compartido de archivos, tiene la opción de seleccionar una clase de almacenamiento para los objetos. Puede elegir la clase de almacenamiento Amazon S3 Standard o cualquiera de las clases de almacenamiento S3 Standard-IA, S3 One Zone-IA o S3 Intelligent-Tiering. Los objetos almacenados en cualquiera de estas clases de almacenamiento se pueden transferir a GLACIER mediante una política de ciclo de vida.

Clase de almacenamiento de Amazon S3	Consideraciones
Estándar	Elija Estándar para almacenar los archivos de acceso frecuente de forma redundant e en varias zonas de disponibilidad que se encuentran distanciadas geográficamente. Esta es la clase de almacenamiento predeterm inada. Consulte los precios de Amazon S3 para obtener más información.
S3 Intelligent-Tiering	Elija Intelligent-Tiering para optimizar los costos de almacenamiento moviendo automátic amente los datos a la capa de acceso de almacenamiento más rentable. Los objetos de menos de 128 KB no son aptos para la estratificación automática en la clase de almacenamiento por niveles inteligentes. Estos objetos se cobran según las tarifas de los niveles de acceso frecuente y no incurren en la tarifa de supervisión que se cobra por los objetos que se organizan automáticamente en niveles. S3 Intelligent-Tiering ahora admite un nivel de acceso a archivos y un nivel de acceso profundo a archivos. S3 Intelligent-Tiering mueve automáticamente los objetos a los que no se ha accedido durante 90 días al nivel de acceso al archivo y, después de 180 días sin

Clase de almacenamiento de Amazon S3	Consideraciones
	acceso, al nivel de acceso al archivo profundo. Cada vez que se restaura un objeto de uno de los niveles de acceso al archivo, el objeto pasa al nivel de acceso frecuente en unas horas y está listo para su recuperación. Esto crea errores de tiempo de espera para los usuarios o las aplicaciones que intentan acceder a los archivos a través de un recurso compartido de archivos si el objeto solo existe en uno de los dos niveles de archivo. No utilice los niveles de archivado con S3 Intelligent-Tiering si sus aplicaciones acceden a los archivos a través de los recursos compartidos de archivos que ofrece File Gateway. Cuando las operaciones de archivo que actualizan los metadatos (como el propietar io, la marca de tiempo, los permisos y ACLs) se realizan en archivos administrados por File Gateway, el objeto existente se elimina y se crea una nueva versión del objeto en esta clase de almacenamiento de Amazon S3. Valide el impacto que tienen las operaciones de archivos en la creación de objetos antes de utilizar esta clase de almacenamiento en producció n. Consulte los precios de Amazon S3 para obtener más información.

Clase de almacenamiento de Amazon S3	Consideraciones
S3 Standard-IA	Elija Estándar - Acceso poco frecuente de S3 para almacenar los archivos de acceso poco frecuente de forma redundante en varias zonas de disponibilidad que se encuentran distancia das geográficamente. Los objetos almacenados en la clase de almacenamiento Standard-IA pueden incurrir en cargos adicionales si se sobrescriben, eliminan, solicitan, recuperan o transfieren objetos entre clases de almacenamiento en un plazo de 30 días. La duración mínima de almacenamiento es de 30 días. Los objetos que se eliminen antes de 30 días incurren en un cargo prorrateado igual al cargo de almacenamiento de los días restantes. Considere la frecuencia con la que estos objetos cambian, el tiempo que tiene previsto conservar estos objetos y la frecuencia con la que necesita obtener acceso a ellos. A los objetos de menos de 128 KB se les cobrará 128 KB y se aplicará una tarifa por eliminación anticipada. Cuando las operaciones de archivo que actualizan los metadatos (como el propietar io, la marca de tiempo, los permisos y ACLs) se realizan en archivos administrados por File Gateway, el objeto existente se elimina y se crea una nueva versión del objeto en esta clase de almacenamiento de Amazon S3. Debe validar cómo afectan las operacion es de archivos a la creación de objetos antes de utilizar esta clase de almacenamiento en producción, ya que se aplican tarifas por

Clase de almacenamiento de Amazon S3	Consideraciones
	eliminación anticipada. Consulte los precios de Amazon S3 para obtener más información.

Clase de almacenamiento de Amazon S3	Consideraciones
S3 One Zone-IA	Elija One Zone-IA para almacenar los archivos a los que accede con poca frecuencia en una única zona de disponibilidad. Los objetos almacenados en la clase de almacenamiento One Zone-IA pueden incurrir en cargos adicionales si se sobrescriben, eliminan, solicitan, recuperan o transfieren objetos de una clase de almacenamiento a otra en un plazo de 30 días. La duración mínima de almacenamiento es de 30 días, y los objetos que se eliminen antes de los 30 días conllevan un cargo prorrateado igual al cargo por almacenamiento de los días restantes . Considere la frecuencia con la que estos objetos cambian, el tiempo que tiene previsto conservar estos objetos y la frecuencia con la que necesita obtener acceso a ellos. A los objetos de menos de 128 KB se les cobrarán 128 KB y se aplicarán tarifas por eliminación anticipada. Cuando las operaciones de archivo que actualizan los metadatos (como el propietar io, la marca de tiempo, los permisos y ACLs) se realizan en archivos administrados por File Gateway, el objeto existente se elimina y se crea una nueva versión del objeto en esta clase de almacenamiento de Amazon S3. Debe validar cómo afectan las operacion es de archivos a la creación de objetos antes de utilizar esta clase de almacenamiento en producción, ya que se aplican tarifas por eliminación anticipada. Consulte los precios de Amazon S3 para obtener más información.

Si bien puede escribir objetos directamente desde un recurso compartido de archivos a la clase de almacenamiento S3-Standard-IA, S3-One Zone-IA o S3 Intelligent-Tiering, le recomendamos que utilice una política de ciclo de vida para realizar la transición de los objetos en lugar de escribirlos directamente desde el recurso compartido de archivos, especialmente si prevé actualizar o eliminar el objeto en un plazo de 30 días a partir de su archivado. Para obtener información sobre la política del ciclo de vida, consulte Administración del ciclo de vida de los objetos.

Uso de la clase de almacenamiento GLACIER con File Gateway

Si realiza la transición de un archivo a S3 Glacier a través de las políticas de ciclo de vida de Amazon S3 y sus clientes de compartición de archivos pueden ver el archivo a través de la memoria caché, se producirán I/O errores al actualizar el archivo. Le recomendamos que configure CloudWatch Events para recibir notificaciones cuando se produzcan estos I/O errores y que utilice la notificación para tomar medidas. Por ejemplo, puede tomar medidas para restaurar el objeto archivado en Amazon S3. Una vez que el objeto se restaure en S3, los clientes del recurso compartido de archivos pueden tener acceso y actualizarlo correctamente mediante un recurso compartido de archivos.

Para obtener información sobre cómo restaurar objetos archivados, consulte Restauración de objetos archivados en la Guía del usuario de Amazon Simple Storage Service.

> **Important**
>
> S3 File Gateway no admite oficialmente la clase de almacenamiento S3 Glacier Instant Retrieval. Si bien puede designar objetos en un depósito compartido de archivos para S3 Glacier Instant Retrieval mediante políticas de ciclo de vida o PUT solicitudes directas, S3 File Gateway no puede reconocer qué archivos se encuentran en esa clase de almacenamiento y realizará operaciones con ellos como cualquier otro objeto. Dado que S3 Glacier Instant Retrieval tiene costes de acceso más altos que otras clases de almacenamiento de Amazon S3, las operaciones masivas de archivos, `rsync` como los análisis de virus y los cambios de nombre, pueden generar grandes facturas de Amazon S3 si no se gestionan con cuidado. Por este motivo, no recomendamos utilizar S3 Glacier Instant Retrieval con S3 File Gateway.

Uso de los controladores de la interfaz de almacenamiento de contenedores de Kubernetes

Kubernetes es un sistema de código abierto para automatizar la implementación, escalado y administración de las aplicaciones en contenedores. En un entorno de Kubernetes, un contenedor

es similar a una máquina virtual, pero un contenedor tiene propiedades de aislamiento relajadas para compartir el sistema operativo (SO) entre sus aplicaciones. Por lo tanto, se considera que los contenedores son más livianos que. VMs Al igual que una máquina virtual, un contenedor tiene su propio sistema de archivos, una parte de la CPU asignada, la memoria, el espacio de proceso y más. Al estar desacoplados de la infraestructura subyacente, se pueden transportar entre nubes y distribuciones de sistemas operativos. Si tiene un clúster de Kubernetes, puede instalar y configurar los controladores de la interfaz de almacenamiento de contenedores (CSI) de Kubernetes en todas las instancias del clúster para que puedan utilizar una puerta de enlace de archivos Amazon S3 existente para el almacenamiento.

Después de instalar los controladores CSI para el tipo de recurso compartido de archivos que desea usar, debe crear uno o más objetos de almacenamiento. Según el tipo de aprovisionamiento que desee que utilice Kubernetes cuando sus pods soliciten almacenamiento, debe crear un único objeto de Kubernetes o bien un objeto y un `StorageClass` `PersistentVolumeClaim` objeto para conectar los pods de `PersistentVolume` cómputo de Kubernetes al recurso compartido de archivos. Para obtener más información, consulta la documentación en línea de Kubernetes en. https://kubernetes.io/docs/concepts/storage/

Temas

- Trabajar con controladores CSI para pequeñas y medianas empresas
- Trabajando con controladores CSI de NFS

Trabajar con controladores CSI para pequeñas y medianas empresas

Siga los procedimientos de esta sección para instalar, configurar o eliminar los controladores CSI necesarios para usar un recurso compartido de archivos SMB en una puerta de enlace de archivos de Amazon S3 para su almacenamiento en su clúster de Kubernetes. Para obtener más información, consulte la documentación de código abierto sobre el controlador SMB CSI en. GitHub https://github.com/kubernetes-csi/csi-driver-smb/blob/master/docs/install-csi-driver-master.md

> **Note**
>
> Al crear un `PersistentVolume` objeto o un `StorageClass` objeto, puede especificar un `ReclaimPolicy` parámetro para determinar qué ocurre con el almacenamiento externo cuando se eliminan los objetos. El controlador CSI SMB admite las `Recycle` opciones `Retain` y, pero actualmente no admite ninguna opción. `Delete`

Instale los controladores

Para instalar los controladores CSI SMB de Kubernetes:

1. Desde un terminal de línea de comandos con acceso a tu clúster de Kubernetes, `kubectl` ejecuta el siguiente comando:

   curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-smb/master/deploy/install-driver.sh | bash -s master --

2. Espere a que finalice el comando anterior y, a continuación, utilice los siguientes comandos para asegurarse de que los módulos de controladores CSI se estén ejecutando:

   kubectl -n kube-system get pod -o wide --watch -l app=csi-smb-controller

   kubectl -n kube-system get pod -o wide --watch -l app=csi-smb-node

   El resultado debería tener un aspecto similar al siguiente:

```
NAME                                 READY   STATUS    RESTARTS   AGE     IP
            NODE
csi-smb-controller-56bfddd689-dh5tk  4/4     Running   0          35s
 10.240.0.19    k8s-agentpool-22533604-0
csi-smb-controller-56bfddd689-8pgr4  4/4     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-smb-node-cvgbs                   3/3     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-smb-node-dr4s4                   3/3     Running   0          35s
 10.240.0.4     k8s-agentpool-22533604-0
```

Cree un objeto SMB StorageClass

Para crear un nuevo StorageClass objeto SMB para tu clúster de Kubernetes:

1. Crea un archivo de configuración con un nombre `storageclass.yaml` con un contenido similar al del siguiente ejemplo. Sustituya la que se muestra por su propia información específica de la implementación. *`ExampleValues`*

```
---
```

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
    name: ExampleStorageClassName
provisioner: smb.csi.k8s.io
parameters:
    source: "//gateway-dns-name-or-ip-address/example-share-name"
    # if csi.storage.k8s.io/provisioner-secret is provided, will create a sub
 directory
    # with PV name under source
    csi.storage.k8s.io/provisioner-secret-name: "examplesmbcreds"
    csi.storage.k8s.io/provisioner-secret-namespace: "examplenamespace"
    csi.storage.k8s.io/node-stage-secret-name: "examplesmbcreds"
    csi.storage.k8s.io/node-stage-secret-namespace: "examplenamespace"
volumeBindingMode: Immediate
reclaimPolicy: Retain
mountOptions:
    - dir_mode=0777
    - file_mode=0777
    - uid=1001
    - gid=1001
```

2. Desde un terminal de línea de comandos con acceso a `kubectl` `ystorageclass.yaml`, ejecute el siguiente comando:

   kubectl apply -f storageclass.yaml

   > **Note**
   >
   > También puedes crearlo StorageClass proporcionando el texto de `.yaml` configuración del paso anterior a la mayoría de las plataformas de administración y contenedorización de Kubernetes de terceros.

3. Configura los pods de tu clúster de Kubernetes para que usen los nuevos que has creado. StorageClass Para obtener más información, consulta la documentación en línea de Kubernetes en. https://kubernetes.io/docs/concepts/storage/

Cree SMB y objetos PersistentVolume PersistentVolumeClaim

Para crear nuevos PersistentVolumeClaim objetos PersistentVolume y SMB:

1. Cree dos archivos de configuración. Uno con nombre `persistentvolume.yaml` y otro con nombre`persistentvolumeclaim.yaml`.
2. Para`persistentvolume.yaml`, añada contenido similar al siguiente ejemplo. Sustituya la que se muestra por su propia información específica de la implementación. *`ExampleValues`*

```
---
apiVersion: v1
kind: PersistentVolume
metadata:
    name: pv-smb-example-name
    namespace: smb-example-namespace # PersistentVolume and PersistentVolumeClaim
 must use the same namespace parameter
spec:
    capacity:
        storage: 100Gi
    accessModes:
        - ReadWriteMany
    persistentVolumeReclaimPolicy: Retain
    mountOptions:
        - dir_mode=0777
        - file_mode=0777
        - vers=3.0
    csi:
        driver: smb.csi.k8s.io
        readOnly: false
        volumeHandle: examplehandle  # make sure it's a unique id in the cluster
        volumeAttributes:
            source: "//gateway-dns-name-or-ip-address/example-share-name"
        nodeStageSecretRef:
            name: example-smbcreds
            namespace: smb-example-namespace
```

3. O bien`persistentvolumeclaim.yaml`, añada contenido similar al del siguiente ejemplo. Sustituya la que se muestra por su propia información específica de la implementación. *`ExampleValues`*

```
---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
    name: examplename-pvc-smb-static
    namespace: smb-example-namespace # PersistentVolume and PersistentVolumeClaim
 must use the same namespace parameter
spec:
    accessModes:
        - ReadWriteMany
    resources:
        requests:
            storage: 10Gi
        volumeName: pv-smb-example-name # make sure specfied volumeName matches the
 name of the PersistentVolume you created
        storageClassName: ""
```

4. Desde un terminal de línea de comandos con acceso a `kubectl` los dos `.yaml` archivos que creó, ejecute los siguientes comandos:

   kubectl apply -f persistentvolume.yaml

   kubectl apply -f persistentvolumeclaim.yaml

   > **Note**
   >
   > También puedes crear los PersistentVolumeClaim objetos PersistentVolume y proporcionando el texto de `.yaml` configuración del paso anterior a la mayoría de las plataformas de administración y contenedorización de Kubernetes de terceros.

5. Configura los pods de tu clúster de Kubernetes para que usen los nuevos que has creado. PersistentVolumeClaim Para obtener más información, consulta la documentación en línea de Kubernetes en. https://kubernetes.io/docs/concepts/storage/

Desinstale los controladores

Para desinstalar los controladores SMB CSI de Kubernetes:

- Desde un terminal de línea de comandos con acceso a tu clúster de Kubernetes, `kubectl` ejecuta el siguiente comando:

curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-smb/master/deploy/uninstall-driver.sh | bash -s --

Trabajando con controladores CSI de NFS

Siga los procedimientos de esta sección para instalar, configurar o eliminar los controladores CSI necesarios para usar un recurso compartido de archivos NFS en una puerta de enlace de archivos de Amazon S3 para su almacenamiento en su clúster de Kubernetes. Para obtener más información, consulte la documentación de código abierto sobre el controlador CSI de NFS en. GitHub https://github.com/kubernetes-csi/csi-driver-nfs/blob/master/docs/install-csi-driver-master.md

Instale los controladores

Para instalar los controladores CSI NFS de Kubernetes:

1. Desde un terminal de línea de comandos con acceso a tu clúster de Kubernetes, `kubectl` ejecuta el siguiente comando:

   curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-nfs/master/deploy/install-driver.sh | bash -s master --

2. Espere a que finalice el comando anterior y, a continuación, utilice los siguientes comandos para asegurarse de que los módulos de controladores CSI se estén ejecutando:

   kubectl -n kube-system get pod -o wide -l app=csi-nfs-controller

   kubectl -n kube-system get pod -o wide -l app=csi-nfs-node

   El resultado debería tener un aspecto similar al siguiente:

```
NAME                                  READY   STATUS    RESTARTS   AGE     IP
            NODE
csi-nfs-controller-56bfddd689-dh5tk       4/4     Running   0          35s
 10.240.0.19    k8s-agentpool-22533604-0
csi-nfs-controller-56bfddd689-8pgr4       4/4     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-nfs-node-cvgbs                        3/3     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
```

```
csi-nfs-node-dr4s4                          3/3     Running   0          35s
 10.240.0.4     k8s-agentpool-22533604-0
```

Cree un objeto NFS StorageClass

Para crear un StorageClass objeto NFS para tu clúster de Kubernetes:

1. Cree un archivo de configuración con un nombre `storageclass.yaml` con un contenido similar al del siguiente ejemplo. Sustituya la que se muestra por su propia información específica de la implementación. *`ExampleValues`*

```
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
    name: example-nfs-classname
    namespace: example-namespace
provisioner: nfs.csi.k8s.io
parameters:
    server: gateway-dns-name-or-ip-address
    share: /example-share-name
reclaimPolicy: Retain
volumeBindingMode: Immediate
mountOptions:
    - hard
    - nfsvers=4.1
```

2. Desde un terminal de línea de comandos con acceso a `kubectl` `ystorageclass.yaml`, ejecute el siguiente comando:

   kubectl apply -f storageclass.yaml

> **Note**
>
> También puedes crearlo StorageClass proporcionando el texto de `.yaml` configuración del paso anterior a la mayoría de las plataformas de administración y contenedorización de Kubernetes de terceros.

3. Configura los pods de tu clúster de Kubernetes para que usen el nuevo objeto que has creado. StorageClass Para obtener más información, consulta la documentación en línea de Kubernetes en. https://kubernetes.io/docs/concepts/storage/

Cree NFS y objetos PersistentVolume PersistentVolumeClaim

Para crear nuevos PersistentVolumeClaim objetos PersistentVolume y NFS:

1. Cree dos archivos de configuración denominados `persistentvolume.yaml` y. `persistentvolumeclaim.yaml`
2. Para`persistentvolume.yaml`, añada contenido similar al siguiente ejemplo. Sustituya la que se muestra por su propia información específica de la implementación. *`ExampleValues`*

```
---
apiVersion: v1
kind: PersistentVolume
metadata:
    name: pv-nfs-examplename
spec:
    capacity:
        storage: 10Gi
    accessModes:
        - ReadWriteMany
    persistentVolumeReclaimPolicy: Retain
    mountOptions:
        - hard
        - nolock
        - nfsvers=4.1
    csi:
        driver: nfs.csi.k8s.io
        readOnly: false
        volumeHandle: unique-volumeid-example # make sure it's a unique id in the
 cluster
        volumeAttributes:
            server: gateway-dns-name-or-ip-address
            share: /example-share-name
```

3. O bien`persistentvolumeclaim.yaml`, añada contenido similar al del siguiente ejemplo. Sustituya la que se muestra por su propia información específica de la implementación. *`ExampleValues`*

```
---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
    name: examplename-pvc-nfs-static
spec:
    accessModes:
        - ReadWriteMany
    resources:
        requests:
            storage: 10Gi
    volumeName: pv-nfs-examplename # make sure specfied volumeName matches the name
 of the PersistentVolume you created
    storageClassName: ""
```

4. Desde un terminal de línea de comandos con acceso a ambos `.yaml` archivos `kubectl` y a ambos, ejecute los siguientes comandos:

   kubectl apply -f persistentvolume.yaml

   kubectl apply -f persistentvolumeclaim.yaml

   > **Note**
   >
   > También puedes crear los PersistentVolumeClaim objetos PersistentVolume y proporcionando el texto de `.yaml` configuración del paso anterior a la mayoría de las plataformas de administración y contenedorización de Kubernetes de terceros.

5. Configura los pods de tu clúster de Kubernetes para que usen el nuevo objeto que has creado. PersistentVolumeClaim Para obtener más información, consulta la documentación en línea de Kubernetes en. https://kubernetes.io/docs/concepts/storage/

Desinstale los controladores

Para desinstalar los controladores CSI de Kubernetes NFS:

- Desde un terminal de línea de comandos con acceso a tu clúster de Kubernetes, `kubectl` ejecuta el siguiente comando:

```
curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-nfs/master/deploy/
uninstall-driver.sh | bash -s master --
```

AWS Storage Gateway Módulo Terraform

HashiCorpTerraform es un motor de infraestructura como código (IaC) de código abierto desarrollado con el lenguaje de HashiCorp configuración (HCL). Terraform proporciona un flujo de trabajo de interfaz de línea de comandos (CLI) coherente que, junto con Amazon S3 File Gateway para la infraestructura de back-end, puede gestionar cientos de servicios en la nube y codificar la nube en archivos de configuración declarativos. APIs

Puede usar Terraform para implementar de forma segura un Amazon S3 File Gateway como una máquina virtual (VM) en su infraestructura virtual local. Terraform proporciona automatización para la infraestructura virtual local. Consulte Automatizar las implementaciones de Amazon S3 File Gateway VMware con Terraform by HashiCorp para obtener información sobre cómo implementar rápidamente una puerta de enlace de archivos Amazon S3 mediante Terraform en un entorno virtual local VMware .

> **Note**
>
> Es posible que necesite configurar Terraform para obtener la versión más reciente de la imagen de la AWS Storage Gateway máquina para su plataforma de hipervisor preferida. Las imágenes de máquinas Storage Gateway utilizan la siguiente convención de nomenclatura. El número de versión adjunto al nombre de la imagen cambia con cada versión publicada.
> `aws-storage-gateway-FILE_S3-1.25.0`

Esta automatización le proporciona un módulo Terraform personalizable que puede utilizar para aprovisionar una puerta de enlace de archivos de Amazon S3 con todos los recursos y dependencias necesarios para implementar completamente la puerta de enlace y los recursos compartidos de archivos en su entorno de máquinas virtuales. El módulo Terraform aprovisiona la máquina virtual de la puerta de enlace, activa la puerta de enlace, configura el disco caché, une la puerta de enlace a un dominio, crea los buckets de Amazon S3, crea los archivos compartidos y los asigna a los buckets. Para ver un ejemplo completo de un repositorio que contiene código de Terraform para crear los recursos necesarios para ejecutar Amazon S3 File Gateway de forma local, consulte el código fuente del módulo Terraform Storage Gateway en. GitHub

> **Note**
>
> El módulo Amazon S3 File Gateway para Terraform es una iniciativa apoyada por la comunidad. No forma parte de un AWS servicio. La comunidad de AWS almacenamiento proporciona el mejor soporte.

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 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	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	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 ISO86 01 Basic en el formato YYYYMMDD' T'HHMMSS'Z'. Si se utilizan tanto el encabezado como el encabezado, el `Date` formato `x-amz-date` del encabezado de fecha no tiene que ser 01. ISO86 `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 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 del punto final de la Asociación de Sistemas de Archivos existente entra en conflicto con la configuración especificada.	AssociateFileSystem
FileSystemAssociationEndpointIpAddressAlreadyInUse	La dirección IP del punto final especificada ya está en uso.	AssociateFileSystem
FileSystemAssociationEndpointIpAddressMissing	Falta la dirección IP del punto final de File System Association.	AssociateFileSystem
FileSystemAssociationNotFound	No se encontró la asociación de sistemas de archivos especificada.	UpdateFileSystemAssociation DisassociateFileSystem DescribeFileSystemAssociations

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
FileSystemNotFound	No se encontró 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 especific ada contiene parámetros no válidos.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRec overyPoint 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 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 S3 File Gateway

- Versión de la API: 30-06-2013
- Última actualización de la documentación: 6 de junio de 2024

En la siguiente tabla se describen los cambios importantes en cada versión de esta guía del usuario después de abril de 2018. Para recibir notificaciones sobre los cambios en esta documentación, puede suscribirse a una fuente RSS.

Cambio	Descripción	Fecha
Se agregó una guía de rendimiento y optimización	El capítulo sobre rendimiento y optimización ahora incluye recomendaciones y prácticas recomendadas para maximizar el rendimiento de su S3 File Gateway y optimizar la implementación para los casos de uso de copias de seguridad de bases de datos de SQL Server. Para obtener más información, consulte Maximizar el rendimiento de S3 File Gateway y Optimizar S3 File Gateway para las copias de seguridad de bases de datos de SQL Server.	13 de junio de 2025
Se agregó la funcionalidad de informes en caché	S3 File Gateway ahora puede generar un informe de los metadatos de los archivos que se encuentran actualmente en la memoria caché de carga local de un recurso compartid	31 de marzo de 2025

	o de archivos específico. Para obtener más información, consulte Crear un informe de caché para su S3 File Gateway, Ver y administrar los informes de caché de su S3 File Gateway y Comprender la información proporcionada en los informes de caché de S3 File Gateway.	
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 agregó compatibilidad con el cifrado de doble capa del lado del servidor con AWS KMS claves (DSSE-KMS)	Ahora puede utilizar el cifrado de doble capa del lado del servidor con AWS KMS claves para cifrar los archivos que S3 File Gateway carga en Amazon S3. Para obtener más información sobre DSSE-KMS, consulte Cifrar objetos almacenados por File Gateway en Amazon S3.	13 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 Administrar las actualizaciones de la puerta de enlace mediante la AWS Storage Gateway consola Administrar las actualizaciones la consola. AWS Storage Gateway	6 de junio de 2024

Se agregó un nuevo nivel de seguridad para pequeñas y medianas empresas	S3 File Gateway ahora admite un nivel de seguridad adicional que puede utilizar para aplicar el cifrado AES de 256 bits en las conexiones de clientes SMB. Para obtener más información, consulte Establecer un nivel de seguridad para su puerta de enlace.	23 de mayo de 2024
Informes sobre la versión del software del dispositivo Gateway y notas de lanzamiento para S3 File Gateway	Se agregaron notas de la versión para describir las funciones, mejoras y correcciones nuevas y actualizadas que se incluyen con cada versión del dispositivo Amazon S3 File Gateway. Puede determinar el número de versión del software de una puerta de enlace desde la consola de Storage Gateway o mediante el AWS CLI. Para obtener más información, consulte las notas de la versión: Gateway Appliance Software.	5 de octubre de 2023

CloudWatch Alarmas recomendadas actualizadas	La CloudWatch `HealthNotifications` alarma ahora se aplica y se recomienda para todos los tipos de puertas de enlace y plataformas host. Los ajustes de configuración recomendados también se han actualizado para `HealthNotifications` y `AvailabilityNotifications` . Para obtener más información, consulte Descripción de CloudWatch las alarmas .	2 de octubre de 2023
Aumento del número máximo de archivos compartidos por puerta de enlace	S3 File Gateway ahora admite hasta 50 archivos compartidos por puerta de enlace, lo que supone un aumento respecto al límite anterior de 10. Esto le permite crear más recursos compartidos de archivos en una sola puerta de enlace, lo que reduce la cantidad de puertas de enlace que debe administrar. Para obtener más información, consulte Cuotas de los recursos compartidos de archivos.	18 de enero de 2023

Se agregó soporte para los atributos de DOS	S3 File Gateway ahora admite los atributos de DOS para los archivos almacenados en Amazon S3. Esto le permite conservar los atributos de los archivos de Windows, como los de solo lectura, ocultos, de sistema y de archivado, cuando los archivos se cargan en Amazon S3. Para obtener más información, consulte Support for file attributes in Amazon S3 File Gateway.	18 de enero 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 agregó una limitación del ancho de banda de red basada en la programación	S3 File Gateway ahora admite la limitación del ancho de banda de red basada en horarios para la carga de datos a Amazon S3. Esta función le permite limitar la cantidad de ancho de banda de red que utiliza su puerta de enlace durante períodos de tiempo específicos, lo que le ayuda a administrar el uso de la red durante las horas pico de trabajo. Para obtener más información, consulte Administrar el ancho de banda de su S3 File Gateway.	18 de enero de 2022
Actualización de procedimientos de creación de puerta de enlace	El procedimiento para crear una nueva puerta de enlace se ha actualizado para reflejar los cambios en la consola de Storage Gateway. Para obtener más información, consulte Crear y activar una pasarela de archivos de Amazon S3.	12 de octubre de 2021

Support para forzar el cierre de archivos en archivos compartidos SMB	Ahora puede usar la configuración del grupo local para asignar permisos de administrador de Gateway. Los administradores de Gateway pueden usar el complemento Carpetas compartidas de Microsoft Management Console para forzar el cierre de los archivos que están abiertos y bloqueados en los recursos compartidos de archivos SMB. Para obtener más información, consulte Configurar grupos locales para su puerta de enlace.	12 de octubre de 2021
Soporte de registro de auditoría para recursos compartidos de archivos NFS	Ahora puede configurar los recursos compartidos de archivos NFS para generar registros de auditoría que proporcionen detalles sobre el acceso de los usuarios a los archivos y carpetas de un recurso compartido de archivos. Puede utilizar estos registros para supervisar las actividades de los usuarios y tomar medidas si se identifican patrones de actividad inadecuados. Para obtener más información, consulte Descripción de los registros de auditoría de File Gateway.	12 de octubre de 2021

Compatibilidad con alias de puntos de acceso	Los archivos compartidos de File Gateway ahora se pueden conectar al almacenamiento de Amazon S3 mediante alias de puntos de acceso tipo bucket. Para obtener más información, consulte Creación de un recurso compartido de archivos.	12 de octubre de 2021
Compatibilidad con puntos de acceso y puntos de acceso de VPC	Los archivos compartidos de File Gateway ahora se pueden conectar a depósitos S3 a través de puntos de acceso o puntos finales de interfaz en su VPC con tecnología. AWS PrivateLink Para obtener más información, consulte Creación de un recurso compartido de archivos.	7 de julio de 2021
Soporte de bloqueo oportunista	Los archivos compartidos de File Gateway ahora pueden utilizar el bloqueo oportunista para optimizar su estrategia de almacenamiento en búfer de archivos, lo que mejora el rendimiento en la mayoría de los casos, especialmente en lo que respecta a los menús contextuales de Windows. Para obtener más información, consulte Crear un recurso compartido de archivos SMB.	7 de julio de 2021

Conformidad con FedRAMP	Storage Gateway ahora es compatible con FedRAMP. Para obtener más información, consulte Validación de conformidad para Storage Gateway.	24 de noviembre de 2020
Notificación de carga de archivos para File Gateway	File Gateway ahora proporciona una notificación de carga de archivos, que le notifica cuando File Gateway ha cargado completamente un archivo en Amazon S3. Para obtener más información, consulte Recibir una notificación de carga de archivos.	9 de noviembre de 2020
Enumeración basada en el acceso para File Gateway	File Gateway ahora proporciona una enumeración basada en el acceso, que filtra la enumeración de archivos y carpetas de un recurso compartido de archivos SMB en función del recurso compartido. ACLs Para obtener más información, consulte Crear un recurso compartido de archivos SMB.	9 de noviembre de 2020

Migración de File Gateway	File Gateway ahora proporciona un proceso documentado para reemplazar un File Gateway existente por uno nuevo. Para obtener más información, consulte Sustitución de una puerta de enlace de archivos por una nueva puerta de enlace de archivos.	30 de octubre de 2020
El rendimiento de lectura en caché fría de File Gateway se ha cuadruplicado	Storage Gateway ha multiplicado por 4 el rendimiento de lectura de la caché en frío. Para obtener más información, consulte la guía de rendimiento de las puertas de enlace de archivos.	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 AWS Storage Gateway consola. Para obtener más información, consulte Uso del dispositivo de hardware AWS Storage Gateway.	12 de agosto de 2020

Compatibilidad con los puntos de enlace del estándar federal de procesamiento de información (FIPS) en las regiones de AWS nuevas	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

Support para múltiples recursos compartidos de archivos adjuntos a un único bucket de Amazon S3	File Gateway ahora permite crear varios recursos compartidos de archivos para un único bucket de S3 y sincronizar la caché local de File Gateway con un bucket en función de la frecuenci a de acceso al directorio. Puede limitar el número de depósitos necesarios para administrar los recursos compartidos de archivos que cree en su File Gateway. Puede definir varios prefijos de S3 para un bucket de S3 y asignar un único prefijo de S3 a un único recurso compartido de archivos de puerta de enlace. También puede definir los nombres de los recursos compartidos de archivos de puerta de enlace para que sean independi entes del nombre del bucket y se ajusten a la convenció n de nomenclatura de los recursos compartidos de archivos locales. Para obtener más información, consulte Crear un recurso compartid o de archivos NFS o Crear un recurso compartido de archivos SMB.	7 de julio de 2020

El almacenamiento en caché local de File Gateway se ha multiplicado por 4	Storage Gateway ahora admite una caché local de hasta 64 TB para File Gateway, lo que mejora el rendimiento de las aplicaciones locales 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 su 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 final FIPS para una puerta de enlace de archivos, consulte Elegir un punto final de servicio.	22 de mayo de 2020

Nuevas regiones AWS	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

Soporte para compartir archivos SMB para Microsoft Windows ACLs	En el caso de las puertas de enlace de archivos, ahora puede utilizar las listas de control de acceso de Microsoft Windows (ACLs) para controlar el acceso a los recursos compartid os de archivos del bloque de mensajes del servidor (SMB). Para obtener más información, consulte Uso de Microsoft Windows ACLs para controlar el acceso a un recurso compartido de archivos SMB.	8 de mayo de 2019
Compatibilidad con File Gateway para la autorización basada en etiquetas	File Gateway ahora admite la autorización basada en etiquetas. Puede controlar el acceso a los recursos de File Gateway en función de 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 información, 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 informaci ón, 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 reemplaza r 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 administr ar el dispositivo desde la AWS Management Console. El dispositivo puede alojar puertas de enlace de archivos, cintas y volúmenes. Para obtener más información, consulte Uso del dispositi vo de hardware de Storage Gateway.	18 de septiembre de 2018

Compatibilidad con el protocolo Server Message Block (SMB)	Se ha añadido compatibilidad con el protocolo Server Message Block (SMB) para los recursos compartidos de archivos en las puertas de enlace de archivo. Para obtener más información, consulte Creación de un recurso compartido de archivos.	20 de junio 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
Support para la clase de almacenamiento S3 One Zone-IA	En el caso de las pasarelas de archivos, ahora puede elegir S3 One Zone-IA como la clase de almacenamiento predeterminada para sus recursos compartidos de archivos. El uso de esta clase de almacenamiento le permite almacenar los datos de objetos en una única zona de disponibilidad en Amazon S3. Para obtener más información, consulte Creación de un recurso compartido de archivos.	4 de abril de 2018
¿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
Support para notificaciones de actualiza	Las puertas de enlace de archivo ahora le permiten recibir una notificación cuando la puerta de enlace termine de actualizar la caché para el bucket de	1 de marzo de 2018

Cambio	Descripción	Fecha de modificación
ción de caché, Requester Pays y almacenamiento predeterminado ACLs para buckets de Amazon S3	Amazon S3. Para obtener más información, consulte RefreshCache.html en la referencia de la API de Storage Gateway. En el caso de File Gateways, ahora puede especific ar que el solicitante o el lector paguen los cargos de acceso y no el propietario del bucket. File Gateway ahora puede ceder el control total de los archivos escritos al propietario del depósito de S3 que se asigna al recurso compartido de archivos de NFS. Para obtener más información, consulte Creación de un recurso compartido de archivos.	
¿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 para la notificación de carga de archivos y la adivinación del tipo Multipurp ose Internet Mail Extension (MIME)	File Gateway ahora puede enviar notificaciones cuando todos los archivos escritos en su recurso compartido de archivos NFS se hayan cargado en Amazon S3. Para obtener más información, consulte la referencia NotifyWhenUploadedde la API de Storage Gateway. File Gateway ahora puede adivinar el tipo de MIME de los objetos cargados en función de las extension es de archivo. Para obtener más información, consulte Creación de un recurso compartido de archivos.	21 de noviembre de 2017

Cambio	Descripción	Fecha de modificación
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
Actualizaciones en los ajustes de los recursos compartidos de archivos Compatibilidad con la actualización de la caché para recursos compartidos de archivos	Las puertas de enlace de archivo ahora incorporan opciones de montaje a la configuración de recursos compartidos de archivos. A partir de ahora, puede establecer opciones de agrupación y de solo lectura para el recurso compartido de archivos. Para obtener más información, consulte Creación de un recurso compartido de archivos. Las puertas de enlace de archivo ahora son capaces de encontrar objetos en el bucket de Amazon S3 que se han agregado o quitado después de que la puerta de enlace elaborase la última lista del contenido del bucket y almacenase en caché el resultado. Para obtener más información, consulte RefreshCachela referencia de la API.	28 de marzo de 2017

Cambio	Descripción	Fecha de modificación
Support para File Gateways en Amazon EC2	AWS Storage Gateway ahora ofrece la posibilidad de implementar un File Gateway en Amazon EC2. Puede lanzar una puerta de enlace de archivos en Amazon EC2 mediante la Amazon Machine Image (AMI) de Storage Gateway, que ahora está disponible como AMI comunitaria. Para obtener información sobre cómo crear una puerta de enlace de archivos e implementarla en una EC2 instancia , consulteCreación y activación de una puerta de enlace de archivo de Amazon S3. Para obtener información acerca de cómo lanzar una AMI de File Gateway, consulteImplemente un EC2 host de Amazon predeterminado para S3 File Gateway. Además, File Gateway ahora admite la configura ción de proxy HTTP. Para obtener más informaci ón, consulte Enrutamiento de su puerta de enlace implementada en Amazon EC2 a través de un proxy HTTP.	08 de febrero de 2017
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

Notas de versión del software del dispositivo de puerta de enlace

Estas notas de la versión describen las funciones, mejoras y correcciones nuevas y actualizadas que se incluyen con cada versión del dispositivo Amazon S3 File Gateway . Cada versión de software se identifica por su fecha de lanzamiento y un número de versión único.

Para determinar el número de versión del software de una puerta de enlace, consulte su página de detalles en la consola de Storage Gateway o llame a la acción de la DescribeGatewayInformationAPI mediante un AWS CLI comando similar al siguiente:

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

El número de versión se devuelve en el campo de `SoftwareVersion` de la respuesta de la API.

> **Note**
>
> Una puerta de enlace no proporcionará información sobre la versión de software en las siguientes circunstancias:
>
> - La puerta de enlace está fuera de línea.
> - La puerta de enlace ejecuta software antiguo que no admite la generación de informes de versiones.
> - El tipo de puerta de enlace no es S3 File Gateway.

Para obtener más información sobre las actualizaciones de File Gateway de S3 FSx , incluida la forma de modificar la programación automática predeterminada de mantenimiento y actualización de una puerta de enlace, consulte Administración de las actualizaciones de la puerta de enlace mediante la consola de AWS Storage Gateway .

Fecha de lanzamiento	Versión del software	Notas de la versión
15 de julio de 2021	1.27,10	Actualizaciones de mantenimiento:

Fecha de lanzamiento	Versión del software	Notas de la versión
		• Se actualizaron los elementos del sistema operativo y el software para mejorar la seguridad y el rendimiento. • Se resolvieron los problemas relacionados con el registro Upload Rename Order para pasarelas.
23-06-2020	1,279	Actualizaciones de mantenimiento: • Se resolvieron los problemas relacionados con el registro de carga y cambio de nombre de las pasarelas. • Se ha activado el registro de carga y cambio de nombre para las nuevas pasarelas.
16-06-2020	1,278	Actualizaciones de mantenimiento: • Se actualizaron los elementos del sistema operativo y el software para mejorar la seguridad y el rendimiento.

Fecha de lanzamiento	Versión del software	Notas de la versión
26 de mayo de 2020	1,27.7	Actualizaciones de mantenimiento: • Se resolvieron los problemas relacionados con el pedido de cambio de nombre. **Note** Este problema solo afecta a algunas pasarelas. Se le notificará si es necesario actualizar su puerta de enlace. • Se actualizaron los elementos del sistema operativo y del software para mejorar la seguridad y el rendimiento.
15-05-2020	1,276	Actualizaciones de mantenimiento: • Se actualizaron los elementos del sistema operativo y el software para mejorar la seguridad y el rendimiento.

Fecha de lanzamiento	Versión del software	Notas de la versión
28-04-2020	1,275	Actualizaciones de mantenimiento: • Se han corregido los problemas relacionados con la subida y el cambio de nombre del registro de pedidos. • Se han añadido herramientas de depuración para ayudar a determinar las causas de los problemas de carga. • Se agregaron estadísticas y métricas del sistema para obtener una visión más profunda del rendimiento de la puerta de enlace. • Se actualizaron los elementos del sistema operativo y el software para mejorar la seguridad y el rendimiento.
14 de abril de 2020	1.27.4	Actualizaciones de mantenimiento: • Se actualizaron los elementos del sistema operativo y el software para mejorar la seguridad y el rendimiento.

Fecha de lanzamiento	Versión del software	Notas de la versión
2025-04-01	1,27.3	Actualizaciones de mantenimiento: • Actualización de la configuración de registro de la puerta de enlace. El cliente no requiere ninguna acción.

Fecha de lanzamiento	Versión del software	Notas de la versión
17-03-2025	1.27,2	Actualizaciones de mantenimiento: • Se agregó una acción de API que elimina los datos y metadatos de los archivos compartidos en caché de los archivos que no se pudieron cargar desde su puerta de enlace a Amazon S3. Cuenta de AWS Debe estar en la lista de permitidos para usar esta función. Si tu pasarela tiene problemas con los archivos que no se cargan correctamente, AWS Support puedes desbloquear la función y proporcionarte instrucciones sobre su uso. • Se ha añadido la posibilidad de que las nuevas pasarelas registren el orden de las operaciones de carga y cambio de nombre de los objetos. Esto ayuda a evitar que los archivos no se carguen en Amazon S3 tras operaciones de cambio de nombre repetidas o superpuestas. • Se ha corregido un problema relacionado con

Fecha de lanzamiento	Versión del software	Notas de la versión
		la apertura involuntaria de puertos por parte de SMB. • Se actualizaron los elementos del sistema operativo y del software para mejorar la seguridad y el rendimiento.
2025-02-17	1.27,1	Actualizaciones de mantenimiento: • Se eliminó Java 11. • Se agregó la función de caché para Soporte su uso. • Se actualizaron el sistema operativo y los elementos de software para mejorar la seguridad y el rendimiento.

Fecha de lanzamiento	Versión del software	Notas de la versión
2025-01-17	1.27.0	Características: • Informes de caché (próximamente): se ha actualizado el software de puerta de enlace para permitir el lanzamiento de una próxima función diseñada para generar informes sobre los metadatos de los archivos actualmente almacenados en caché por una puerta de enlace de archivos de S3. Podrá utilizar estos informes para solucionar problemas si sus archivos no se cargan correctamente desde su puerta de enlace a Amazon S3. Actualizaciones de mantenimiento: • Se actualizaron los elementos del sistema operativo y el software para mejorar la seguridad y el rendimiento.

Fecha de lanzamiento	Versión del software	Notas de la versión
2025-01-09	1,269	Actualizaciones de mantenimiento: • Se actualizaron los elementos del sistema operativo y el software para mejorar la seguridad y el rendimiento.
18 de diciembre de 2022	1.26,8	Actualizaciones de mantenimiento: • Se actualizaron los elementos del sistema operativo y el software para mejorar la seguridad y el rendimiento.
18-11-2022	1.26,7	Actualizaciones de mantenimiento: • Se actualizaron los elementos del sistema operativo y el software para mejorar la seguridad y el rendimiento.
17 de octubre de 2022	1.26.6	Actualizaciones de mantenimiento: • Se actualizaron los elementos del sistema operativo y el software para mejorar la seguridad y el rendimiento.

Fecha de lanzamiento	Versión del software	Notas de la versión
30-09-2020	1,26.5	Actualizaciones de mantenimiento: • Se ha corregido un problema por el que las pasarelas locales no permitían los canales de soporte • Se actualizaron los elementos del sistema operativo y del software para mejorar la seguridad y el rendimiento.
16-09-20	1.26.3	Actualizaciones de mantenimiento: • Se actualizaron los elementos del sistema operativo y el software para mejorar la seguridad y el rendimiento.
2024-08-21	1.26,1	Actualizaciones de mantenimiento: • Se ha corregido un problema relacionado con el registro.

Fecha de lanzamiento	Versión del software	Notas de la versión
19 de agosto de 2024	1,26.0	Actualizaciones de mantenimiento: • Se actualizaron los elementos del sistema operativo y el software para mejorar la seguridad y el rendimiento.
2024-07-16	1.25.2	Actualizaciones de mantenimiento: • Se actualizaron los elementos del sistema operativo y el software para mejorar la seguridad y el rendimiento.
-17 de junio de 2024	1.25.1	Actualizaciones de mantenimiento: • Se ha corregido un problema con las actualizaciones cuando se utilizaba un proxy y el DNS estaba desactivado. • Se actualizaron los elementos del sistema operativo y del software para mejorar la seguridad y el rendimiento.

Fecha de lanzamiento	Versión del software	Notas de la versión
15-05-2022	1,25,0	Características: • Se agregó la capacidad de establecer el cifrado AES-128 o AES-256 como mínimo. Se trata únicament e de un cambio de puerta de enlace y estará disponibl e en la consola de Storage Gateway en una próxima versión. • Aumento de la rotación de los registros del sistema cuando hay poco espacio en disco. Anteriormente, la escritura de registros que llenaba el disco raíz hacía que la puerta de enlace se detuviera. Ahora, a medida que disminuya el espacio, la puerta de enlace dejará más espacio para los registros más nuevos al eliminar los registros más antiguos. • Se agregó la ruta S3 en las notificaciones de estado para los errores de carga de archivos. Anteriormente, las notificaciones de estado solo mostraban la ruta al archivo en la puerta de enlace. Las notificaciones ahora muestran la ruta para

Fecha de lanzamiento	Versión del software	Notas de la versión
		ayudar a los usuarios a localizar el archivo en S3. • El servicio ahora ignora los bloqueadores de back-end durante las eliminaciones forzadas de archivos compartidos. Anteriormente, las eliminaciones forzadas se detenían sin explicación alguna cuando se detectaban bloqueadores. Las eliminaciones forzadas ahora continúan sin interrupciones en estos escenarios. Actualizaciones de mantenimiento: • Se actualizó la pila de NFS. • Java 17 JRE actualizado. • Se actualizaron el sistema operativo y los elementos de software para mejorar la seguridad y el rendimiento.
15-04-2020	1,24,5	Actualizaciones de mantenimiento: • Se actualizaron los elementos del sistema operativo y el software para mejorar la seguridad y el rendimiento.

Fecha de lanzamiento	Versión del software	Notas de la versión
2024-04-01	1,24,4	Actualizaciones de mantenimiento: • Se solucionó la falta del componente Network Time Protocol (NTP).
18-03-2022	1,24,3	Actualizaciones de mantenimiento: • Se ha corregido un problema relacionado con el rendimiento de las búsquedas que distinguen mayúsculas de minúsculas. • Se ha corregido un problema que provocaba el bloqueo de los procesos. • Se actualizaron los elementos del sistema operativo y del software para mejorar la seguridad y el rendimiento.
2024-01-12	1.24.2	Actualizaciones de mantenimiento: • Se solucionó el problema de registro de SMB.
27 de diciembre de 2023	1.24.1	Actualizaciones de mantenimiento: • Se solucionó el problema de estabilidad de las pymes.

Fecha de lanzamiento	Versión del software	Notas de la versión

01/12/2020	1,24,0	Características:
		• Pila SMB actualizada.
		  • Se agregó compatibilidad con el cifrado AES-256, además de variantes más seguras del cifrado y la firma AES-128 cuando se utiliza un cliente SMB 3.1.1 que lo solicite.
		  • SMBv1 (LANMAN/C IFS) se han eliminado las funciones de copia del lado del servidor y de expansión con caracteres comodín del lado del servidor. SMBv2 SMBv3 (y no se ven afectados). Esto puede afectar negativamente al rendimiento de determina das cargas de SMBv1 trabajo. Si lo usa SMBv1, le recomendamos que migre a SMBv2 o SMBv3.
		
		Actualizaciones de mantenimi ento:
		• Se actualizaron los elementos del sistema operativo y el software para mejorar la seguridad y el rendimiento.

Fecha de lanzamiento	Versión del software	Notas de la versión
24 de octubre de 2023	1.23.2	Actualizaciones de mantenimiento: • Se ha corregido un problema relacionado con que Support Channel no se conectaba correctamente para algunos usuarios.
14 de agosto de 2023	1,23.1	Actualizaciones de mantenimiento: • Se actualizó el servidor NTP para usar el servidor de sincronización en las nuevas puertas de enlace.

Fecha de lanzamiento	Versión del software	Notas de la versión
12/06/2020	1,2330	Características: • Se han incrementado los hilos de subida en algunas cuentas AWS . Actualizaciones de mantenimiento: • Se ha corregido un problema de infracción de acceso en copias grandes. • Se ha corregido un problema de NFS. • Se ha eliminado Java 8. • Se actualizaron los elementos del sistema operativo y del software para mejorar la seguridad y el rendimiento.
2023-04-19	1.22.1	Actualizaciones de mantenimiento: • Se ha corregido un problema relacionado con el cambio de nombre de carpetas y archivos.

Fecha de lanzamiento	Versión del software	Notas de la versión
18-01-2020	1,22.0	Características: • Se agregó soporte para los atributos de DOS. • Se aumentó el número de archivos compartidos admitidos por puerta de enlace de 10 a 50. • Se implementó un mecanismo de detección del sesgo del reloj para determinar cuándo una puerta de enlace y un servicio no están sincroniz ados. Actualizaciones de mantenimi ento: • Pila SMB actualizada.
6 de julio de 2022	1.21.2	Actualizaciones de mantenimi ento: • Se actualizaron los elementos del sistema operativo y el software para mejorar la seguridad y el rendimiento.

Fecha de lanzamiento	Versión del software	Notas de la versión
2022-02-16	1.21.1	Características: • Se han añadido nuevas métricas para el cambio de nombre y la eliminación de la memoria caché. Actualizaciones de mantenimiento: • Se corrigieron varios problemas.
18/01/2022	1.21.0	Características: • Se agregaron nuevas métricas CloudWatch . • Se ha añadido una limitación del ancho de banda para la carga de datos.
12/12/2021	1.20.0	***URGENT UPDATE***: • Se solucionó la vulnerabilidad de Log4j.

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.