Guía del usuario

AWSStorage Gateway

Versión de API 2013-06-30

AWSStorage Gateway: Guía del usuario

Table of Contents

Qué es Amazon S3 File Gateway

AWSStorage Gateway conecta un dispositivo de software local con almacenamiento basado en la nube para ofrecer una integración fluida con características de seguridad entre el entorno de TI local y laAWSinfraestructura de almacenamiento. Puede utilizar el servicio para almacenar datos en elAWSCloud para obtener un almacenamiento escalable y rentable que contribuye a mantener la seguridad de los datos.AWS Storage Gateway ofrece soluciones de almacenamiento basadas en archivos, en volúmenes y en cintas.

Temas

Amazon S3 File Gateway

Amazon S3 File Gateway—Amazon S3 File Gateway admite una interfaz de archivos enAmazon Simple Storage Service (Amazon S3)y combina un servicio y un dispositivo de software virtual. Mediante esta combinación, puede almacenar y recuperar objetos en Amazon S3 a través de protocolos de archivo estándar del sector como Network File System (NFS) y Server Message Block (SMB). El dispositivo de software, o gateway, se implementa en las instalaciones como una máquina virtual (VM) que se ejecuta en el hipervisor VMware ESXi, Microsoft Hyper-V o máquina virtual de Linux basada en el kernel (KVM). 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 obtener acceso a los datos directamente en Amazon S3 desde cualquierAWSAplicación o servicio en la nube.
- Puede administrar los datos de S3 mediante políticas del ciclo de vida, replicación entre regiones y control de versiones. Puede considerar una puerta de enlace de archivos S3 como un montaje de un sistema de archivos en Amazon S3.

Una puerta de enlace de archivos S3 simplifica el almacenamiento de archivos en Amazon S3, se integra con aplicaciones existentes a través de protocolos de sistemas de archivos estándar del

sector y proporciona una alternativa económica 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 administra la transferencia de datos hacia y desdeAWS, sirve de búfer para las aplicaciones frente a la congestión de la red, optimiza y transmite los datos en paralelo y administra el consumo de ancho de banda. S3 File Gateway se integra conAWSservicios, como los siguientes:

- Administración de acceso común mediante AWS Identity and Access Management (IAM)
- Cifrado mediante AWS Key Management Service (AWS KMS)
- Supervisión mediante Amazon CloudWatch (CloudWatch)
- Auditoría medianteAWS CloudTrail(CloudTrail)
- Operaciones mediante la 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. Muestra cómo crear un archivo compartido, asignar la unidad a un bucket de Amazon S3 y cargar archivos y carpetas en Amazon S3.

- describe cómo realizar tareas de administración para todos los tipos de gateways 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 laAWSReferencia de la API de Storage.

Cómo funciona Storage Gateway (arquitectura)

A continuación, encontrará una visión general de la arquitectura de las soluciones de Storage Gateway disponibles.

Temas

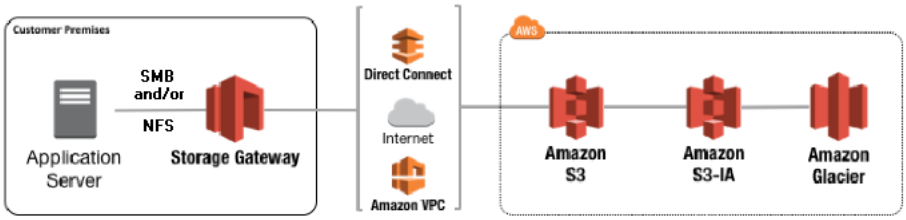
Gateways de archivos Amazon S3

Para utilizar una puerta de enlace de archivos de S3, comience por descargar una imagen de máquina virtual de la puerta de enlace. A continuación, activa la puerta de enlace desde elAWS Management Consoleo mediante la API de Storage Gateway. También puede crear una puerta de enlace de archivos de S3 mediante una imagen de Amazon EC2.

Una vez que la puerta de enlace de archivos de S3 esté activa, debe crear y configurar el recurso compartido de archivos y asociarlo al bucket de Amazon Simple Storage Service (Amazon S3). De este modo, los clientes pueden tener acceso al recurso compartido mediante el protocolo Network File System (NFS) o el protocolo Server Message Block (SMB). Los archivos que se escriben en un recurso compartido de archivos se convierten en objetos en Amazon S3, con la ruta como clave. Existe una correlación de uno a uno entre archivos y objetos y la puerta de enlace actualiza de forma asíncrona los objetos de Amazon S3 cuando se realizan cambios en los archivos. Los objetos existentes en el bucket de Amazon S3 aparecen como archivos en el sistema de archivos y la clave se convierte en la ruta. Los objetos se cifran con claves de cifrado del lado del servidor de Amazon S3 (SSE-S3). Todas las transferencias de datos se realizan a través de HTTPS.

El servicio optimiza la transferencia de datos entre la puerta de enlace yAWSmediante cargas paralelas de varias partes o descargas de rango de bytes, para utilizar mejor el ancho de banda disponible. Se mantiene una caché local para proporcionar acceso de baja latencia a los datos a los que se ha tenido acceso recientemente y reducir los cargos por salida de datos. Las métricas de CloudWatch proporcionan información sobre el uso de los recursos de la máquina virtual y la transferencia de datos a y desdeAWS. CloudTrail rastrea todas las llamadas a la API.

Con el almacenamiento de S3 File Gateway, puede realizar tareas como llevar cargas de trabajo de nube a Amazon S3, realizar copias de seguridad y archivado y estratificar y migrar datos de almacenamiento alAWSCloud. En el diagrama siguiente se proporciona información general de la implementación del almacenamiento de archivos en Storage Gateway.



S3 File Gateway convierte los archivos en objetos S3 al cargar archivos en Amazon S3. La interacción entre las operaciones de archivos realizadas con recursos compartidos de archivos en S3 File Gateway y objetos S3 requiere que ciertas operaciones se tengan en cuenta cuidadosamente al convertir entre archivos y objetos.

Las operaciones comunes de archivos cambian los metadatos de los archivos, lo que da como resultado la eliminación del objeto S3 actual y la creación de un nuevo objeto S3. En la tabla siguiente se muestran ejemplos de operaciones de archivos y el impacto en los objetos S3.

Operación de archivos	Impacto del objeto de S	Implicación de clase de almacenamiento
Cambie el nombre de archivo	Reemplaza el objeto S3 existente y crea un nuevo objeto S3 para cada archivo	Es posible que se apliquen tarifas de eliminación anticipad a y de recuperación
Cambiar de nombre las carpetas	Sustituye todos los objetos S3 existentes y crea nuevos objetos S3 para cada carpeta y archivos de la estructura de carpetas	Es posible que se apliquen tarifas de eliminación anticipad a y de recuperación
Cambiar los permisos de archivos/carpetas	Reemplaza el objeto S3 existente y crea un nuevo objeto S3 para cada archivo o carpeta	Es posible que se apliquen tarifas de eliminación anticipad a y de recuperación
Cambiar la propiedad de archivos/carpetas	Reemplaza el objeto S3 existente y crea un nuevo objeto S3 para cada archivo o carpeta	Es posible que se apliquen tarifas de eliminación anticipad a y de recuperación

Operación de archivos	Impacto del objeto de S	Implicación de clase de almacenamiento
Anexar a un archivo	Reemplaza el objeto S3 existente y crea un nuevo objeto S3 para cada archivo	Es posible que se apliquen tarifas de eliminación anticipada y de recuperación

Cuando un cliente NFS o SMB escribe un archivo en la puerta de enlace de archivos S3, la puerta de enlace de archivos carga los datos del archivo en Amazon S3 seguidos de sus metadatos (propiedad, marcas de tiempo, etc.). Al cargar los datos de 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 la puerta de enlace de archivos S3 después de cargarlo en Amazon S3, S3 File Gateway carga los datos nuevos o modificados en lugar de cargar el archivo completo. La modificación del archivo da como resultado la creación de una nueva versión del objeto S3.

Cuando S3 File Gateway carga archivos más grandes, es posible que tenga que cargar fragmentos más pequeños del archivo antes de que el cliente termine de escribir en S3 File Gateway. Algunas de las razones para ello incluyen liberar espacio en la caché o una alta tasa de escritura en un recurso compartido de archivos. Esto puede dar como resultado varias versiones de un objeto en el bucket de S3.

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

Configuración para Amazon S3 File Gateway

Esta sección ofrece instrucciones para la introducción a Amazon S3 File Gateway. Lo primero que debe hacer es inscribirse enAWS. Si es la primera vez que lo utiliza, le recomendamos que lea lasRegiones deyRequisitossecciones.

Temas

- Inscribirse en Amazon Web Services
- Creación de un usuario de IAM
- Requisitos de configuración de gateway
- Acceso a AWS Storage Gateway
- Regiones de AWS compatibles

Inscribirse en Amazon Web Services

Si no dispone de una Cuenta de AWS, siga los pasos que figuran a continuación para crear una.

Para registrarse en Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones en línea.

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

Creación de un usuario de IAM

Después de crear suAWS, siga los siguientes pasos para crear unaAWS Identity and Access Management(IAM) usuario para ti mismo. A continuación, agrega ese usuario a un grupo que tenga permisos administrativos.

Para crearse usted mismo un usuario administrador y agregarlo a un grupo de administradores (consola)

1. Inicie sesión en la consola de IAM como el propietario de la cuenta; para ello, elija Root user (Usuario raíz) e ingrese el email de su Cuenta de AWS. En la siguiente página, escriba su contraseña.

   > **Note**
   >
   > Le recomendamos que siga la práctica recomendada de utilizar el usuario de IAM **`Administrator`** como se indica a continuación y guardar de forma segura las credenciales del usuario raíz. Inicie sesión como usuario raíz únicamente para realizar algunas tareas de administración de servicios y de cuentas.

2. En el panel de navegación, elija Users (Usuarios) y, a continuación, elija Add user (Añadir usuario).
3. En User name (Nombre de usuario), escriba **`Administrator`**.
4. Seleccione la casilla de verificación situada junto a AWS Management Console access (Acceso a la consola). A continuación, seleccione Custom password (Contraseña personalizada) y luego escriba la nueva contraseña en el cuadro de texto.
5. (Opcional) De forma predeterminada, AWS requiere al nuevo usuario que cree una nueva contraseña la primera vez que inicia sesión. Puede quitar la marca de selección de la casilla de verificación situada junto a User must create a new password at next sign-in (El usuario debe crear una nueva contraseña en el siguiente inicio de sesión) para permitir al nuevo usuario restablecer su contraseña después de iniciar sesión.
6. Seleccione Next (Siguiente): Permisos.
7. En Set permissions (Establecer permisos), elija Add user to group (Añadir usuario a grupo).
8. Elija Create group (Crear grupo).
9. En el cuadro de diálogo Create group (Crear grupo), en Group name (Nombre del grupo) escriba **`Administrators`**.
10. Elija Filter policies (Filtrar políticas) y, a continuación, seleccione AWS managed - job function (función de trabajo administrada) para filtrar el contenido de la tabla.
11. En la lista de políticas, active la casilla de verificación AdministratorAccess. A continuación, elija Create group (Crear grupo).

> **Note**
>
> Debe activar el acceso de usuarios y roles de IAM a Facturación para poder utilizar los permisos `AdministratorAccess` para acceder a la consola de AWS Billing and Cost Management. Para ello, siga las instrucciones que se indican en el paso 1 del tutorial sobre cómo delegar el acceso a la consola de facturación.

12. Retroceda a la lista de grupos y active la casilla de verificación del nuevo grupo. Elija Refresh si es necesario para ver el grupo en la lista.
13. Seleccione Next (Siguiente): Tags (Etiquetas).
14. (Opcional) Añadir metadatos al rol asociando las etiquetas como pares de clave-valor. Para obtener más información sobre el uso de etiquetas en IAM, consulte Etiquetado de entidades de IAM en la guía del usuario de IAM.
15. Seleccione Next (Siguiente): Review (Revisar)Para ver la lista de suscripciones a grupos que se van a añadir al nuevo usuario. Cuando esté listo para continuar, elija Create user (Crear usuario).

Puede usar este mismo proceso para crear más grupos y usuarios, y para otorgar a los usuarios acceso a los recursos de la Cuenta de AWS. Para obtener información acerca de cómo usar las políticas que restringen los permisos de los usuarios a recursos de AWS específicos, consulte Administración de accesos y Ejemplos de políticas.

Requisitos de configuración de gateway

A menos que se especifique lo contrario, los siguientes requisitos son comunes a todos los tipos de gateway de archivos enAWS 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 implementar la puerta de enlace.

Temas

- Requisitos previos requeridos
- Requisitos de hardware y almacenamiento
- Requisitos de red y firewall
- Hipervisores compatibles y requisitos de host

- Clientes de NFS compatibles con una gateway de archivos
- Clientes de SMB compatibles con una gateway de archivos
- Operaciones del sistema de archivos compatibles con una gateway de archivos

Requisitos previos requeridos

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

- Cree y configure un sistema de archivos FSx for Windows File Server. Para obtener instrucciones, consulte Paso 1: Crear su sistema de archivos en la Guía del usuario de Amazon FSx for Windows File Server.
- Configurar Microsoft Active Directory (AD).
- 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.
- Configura tu red privada, VPN o AWS Direct Connect entre Amazon Virtual Private Cloud (Amazon VPC) y el entorno local en el que está implementando la gateway de archivos FSx.
- Asegúrese de que la puerta de enlace pueda resolver el nombre del controlador de dominio de Active Directory. Puede utilizar DHCP en su dominio de Active Directory para gestionar la resolución o especificar un servidor DNS manualmente desde el menú Configuración de red de la consola local de la puerta de enlace.

Requisitos de hardware y almacenamiento

Las siguientes secciones proporcionan información acerca de los requisitos mínimos de hardware y la configuración necesarios para la gateway y la cantidad mínima de espacio en disco que se debe asignar para el almacenamiento necesario.

Para obtener información sobre las prácticas recomendadas de rendimiento de la gateway de archivos, consulte Guía de desempeño de las gateways de archivos.

Requisitos de hardware para las máquinas virtuales locales

Cuando implemente la gateway localmente, asegúrese de que el hardware subyacente en el que implemente la máquina virtual de gateway (MV) pueda dedicar los siguientes recursos mínimos:

- Cuatro procesadores virtuales asignados a la máquina virtual
- 16 GiB de RAM reservada para gateways de archivos
- 80 GiB de espacio de disco para la instalación de los datos del sistema y la imagen de la MV

Para obtener más información, consulte Optimización del rendimiento de la gateway. Para obtener información acerca de cómo afecta el hardware al rendimiento de la MV de la gateway, consulte Cuotas para los recursos compartidos de archivos.

Requisitos para los tipos de instancias Amazon EC2

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

Recomendadas para los tipos de gateway de archivos

- Familia de instancias de uso general: tipo de instancia m4 o m5.
- Familia de instancias optimizadas para computación: tipos de instancia c4 o c5. Seleccione el tamaño de instancia 2xlarge o superior para cumplir los requisitos de RAM necesarios.
- Familia de instancias optimizadas para memoria: tipos de instancia r3.
- Familia de instancias optimizadas para almacenamiento: tipos de instancia i3.

> **Note**
>
> Cuando se lanza la gateway en Amazon EC2 y el tipo de instancia que se ha elegido es compatible con almacenamiento efímero, los discos se muestran de forma automática. Para obtener más información sobre el almacenamiento de instancias de Amazon EC2, consulteStorage Instanceen laGuía del usuario de Amazon EC2.
> Las operaciones de escritura de las aplicaciones se almacenan en la memoria caché de forma síncrona y, a continuación, se cargan de forma asíncrona en el almacenamiento duradero en Amazon S3. Si el almacenamiento efímero se pierde debido a que una instancia se detiene antes de que haya finalizado la carga, los datos que todavía se encuentran en la caché y todavía no se ha escrito en Amazon Simple Storage Service (Amazon S3) se pueden perder. Antes de detener la instancia que aloja la gateway, asegúrese de que el`CachePercentDirty`Metric CloudWatch es`0`. Para obtener información sobre el almacenamiento efímero, consulte Uso del almacenamiento efímero

con puertas de enlace EC2. Para obtener información sobre la monitorización de métricas para la gateway de almacenamiento, consulteSupervisión de la gateway de archivos. Si tiene más de cinco millones de objetos en el bucket de S3 y utiliza un volumen SSD de uso general, se necesita un volumen EBS raíz mínimo de 350 GiB para tener un rendimiento aceptable durante el inicio de la gateway. Para obtener información sobre cómo aumentar el tamaño del volumen, consulteModificación de un volumen de EBS utilizando volúmenes elásticos (consola).

Requisitos de almacenamiento

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

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

Note

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

Para obtener información acerca de las cuotas de gateway, consulte Cuotas para los recursos compartidos de 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 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, es posible implementar FSx File Gateway en Amazon EC2 o utilizar otros tipos de implementación (incluida la local) con políticas de seguridad de red que restringenAWSRangos de direcciones IP. En estos casos, la gateway podría experimentar problemas de conectividad con elAWSCambios en los valores del rango de IP. LaAWSLos valores del rango de direcciones IP que necesita utilizar se encuentran en el subconjunto de servicio de Amazon para elAWSRegión en la que activa la gateway. Para conocer los valores actuales de rango de IP, consulteAWSRangos de direcciones IPen laAWSReferencia general de.

Temas

Requisitos de los puertos

Storage Gateway requiere que determinados puertos estén permitidos para funcionar. Las siguientes ilustraciones muestran los puertos necesarios que deben permitirse para cada tipo de gateway. Algunos puertos son requeridos por todos los tipos de gateway y otros son requeridos solo por algunos tipos específicos. Para obtener más información sobre los requisitos de puertos, consulte Requisitos de los puertos.

Puertos comunes para todos los tipos de gateway

Los siguientes puertos son comunes y obligatorios para todos los tipos de gateways.

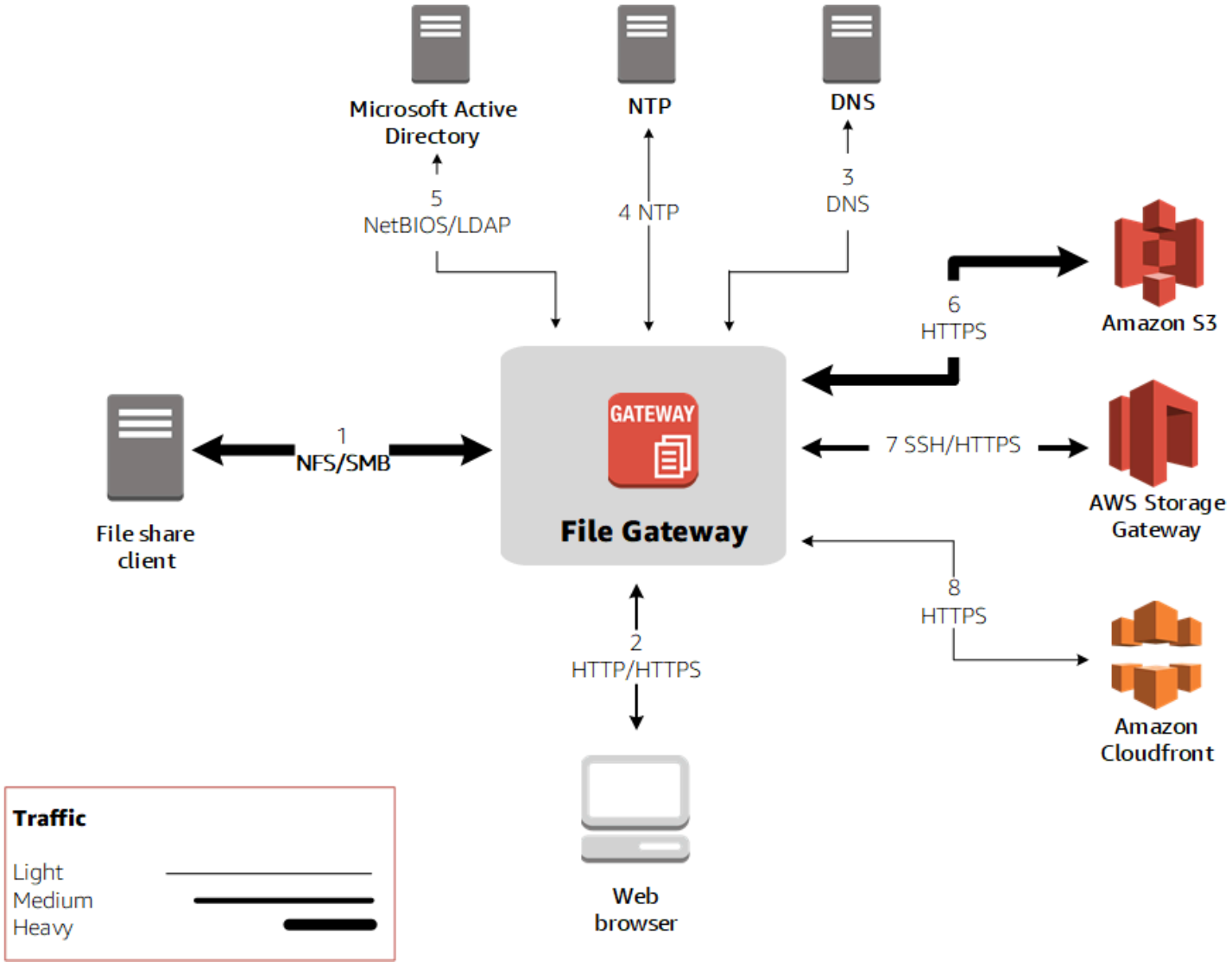
Protocolo	Puerto	Dirección	Fuente	Destino	Cómo se utiliza
TCP	443 (HTTPS)	Salida	Storage Gatewa	AWS	Para la comunicación desde Storage Gateway alAWSpunto de enlace de servicio. Para obtener más información acerca de los puntos de enlace de servicio, consulte Permisos de acceso de AWS Storage Gateway a través de firewalls y routers.
TCP	80 (HTTP)	Entrada	El host desde el que te conectas alAWS Management Console.	Storage Gatewa	Los sistemas locales lo utilizan para obtener la clave de activación de Storage Gateway. El puerto 80

Protocolo	Puerto	Dirección	Fuente	Destino	Cómo se utiliza
					solo se usa durante la activación del dispositivo Storage Gateway. 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 red. Si activa la gateway desde la consola de Storage Gateway, el host desde el que se conecta a la consola debe tener acceso al puerto 80 de la gateway.

Protocolo	Puerto	Dirección	Fuente	Destino	Cómo se utiliza
UDP/UDP	53 (DNS)	Salida	Storage Gatewa	Servidor DNS	Para la comunicación entre Storage Gateway y el servidor DNS.
TCP	22 (canal de soporte)	Salida	Storage Gatewa	AWS Support	PermiteAWS SupportPara acceder a la gateway para ayudarle con la solución de problemas de gateway. No necesita este puerto abierto para el funcionamiento normal de la gateway, pero se exige para la solución de problemas.
UDP	123 (NTP)	Salida	Cliente NTP	Servidor NTP	Lo utilizan los sistemas locales para sincronizar la hora de la VM con la hora del host.

Puertos para las gateways de archivos

En la siguiente ilustración se muestran los puertos que se deben abrir para una gateway de archivos de S3.



> **Note**
>
> Para conocer los requisitos específicos de puertos, consulte Requisitos de los puertos.

Para S3 File Gateway, solo necesita utilizar Microsoft Active Directory cuando desee permitir que los usuarios del dominio tengan acceso a un recurso compartido de archivos de Server Message Block (SMB). Puede unir la gateway de archivos a cualquier dominio válido de Microsoft Windows (que se pueda resolver por DNS).

También puede utilizar laAWS Directory Servicepara crear unAWS Managed Microsoft ADen Amazon Web Services Cloud. Para la mayoríaAWS Managed Microsoft ADimplementaciones, necesita configurar el servicio de protocolo de configuración dinámica de host (DHCP) para la VPC. Para obtener información sobre la creación de un conjunto de opciones de DHCP, consulteCrear un conjunto de opciones de DHCPen laAWS Directory ServiceGuía de administración.

Además de los comunes, Amazon S3 File Gateway necesita los siguientes puertos.

Protocolo	Puerto	Dirección	Fuente	Destino	Cómo se utiliza
TCP/UDP	2049 (NFS)	Entrada	Clientes NFS	Storage Gatewa	Para que los sistemas locales se conecten con las rutas compartidas NFS que expone la gateway.
TCP/UDP	111 (NFsV3)	Entrada	cliente NFSv3	Storage Gatewa	Para que los sistemas locales se conecten con el mapeador de puertos que expone la gateway. **Note** Este puerto solo es necesario

Protocolo	Puerto	Dirección	Fuente	Destino	Cómo se utiliza
					para NFSv3.
TCP/UDP	20048 (NFsV3)	Entrada	cliente NFSv3	Storage Gatewa	Para que los sistemas locales se conecten con montajes que expone la gateway. **Note** Este puerto solo es necesario para NFSv3.

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

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

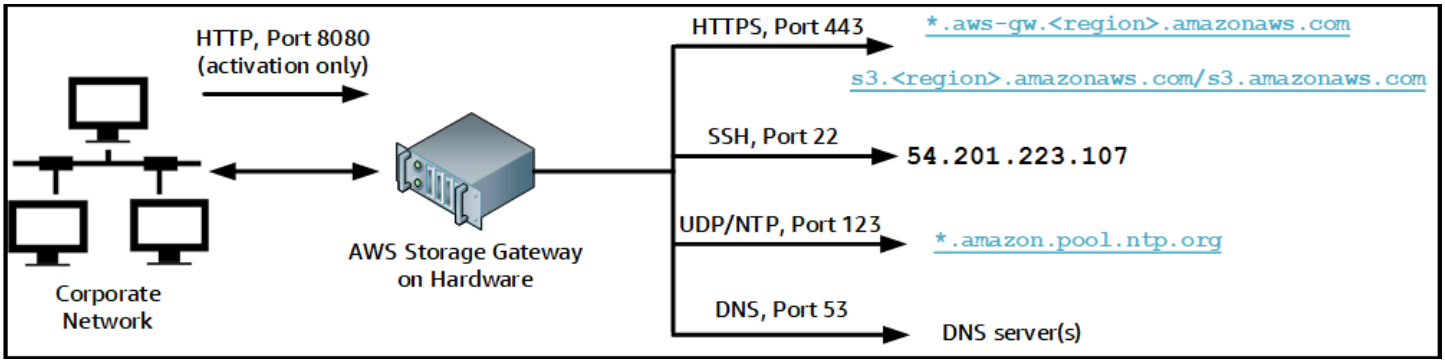
- acceso a Internet— una conexión de red siempre activa a Internet a través de cualquier interfaz de red del servidor.
- Servicios DNS— Servicios DNS para la comunicación entre el dispositivo de hardware y el servidor DNS.
- Sincronización horaria: se debe tener acceso a un servicio de hora Amazon NTP configurado automáticamente.

- dirección IP— Una dirección DHCP o IPv4 estática asignada. No puede asignar una dirección IPv6.

Existen 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	Fuente	Destino	Cómo se utiliza
SSH	22	Salida	Dispositivo de hardware	`54.201.223.107`	canal de soporte
DNS	53	Salida	Dispositivo de hardware	Servidores DNS	Resolución de nombres

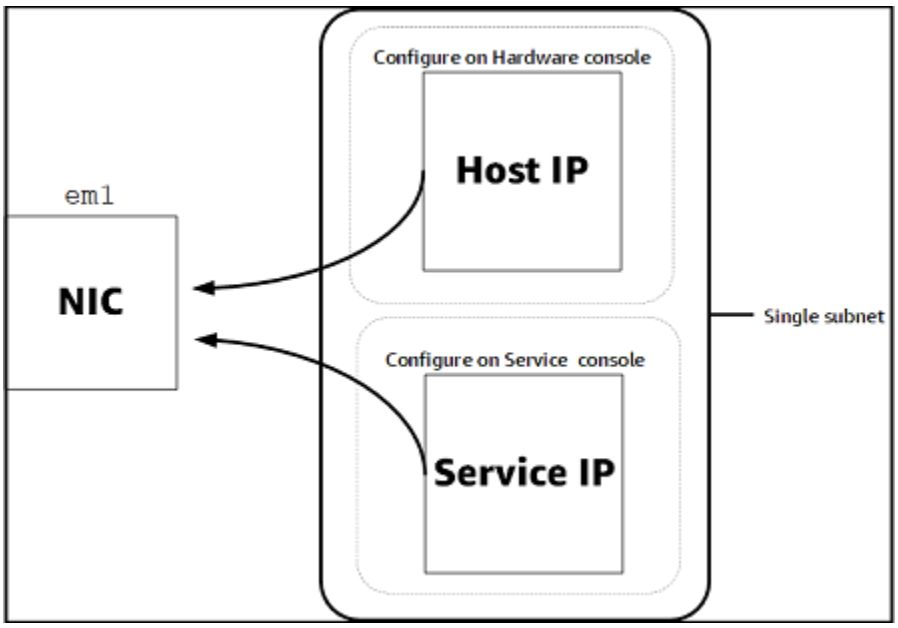
Protocolo	Puerto	Dirección	Fuente	Destino	Cómo se utiliza
UDP/NTP	123	Salida	Dispositivo de hardware	`*.amazon.pool.ntp.org`	Sincronización horaria
HTTPS	443	Salida	Dispositivo de hardware	`*.amazonaws.com`	Transferencia de datos
HTTP	8080	Entrada	AWS	Dispositivo de hardware	Activación (solo brevemente)

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 parámetros de red.

> **Note**
>
> Para ver una ilustración que muestra la parte posterior del servidor con sus puertos, consulteMontaje en bastidor de su dispositivo de hardware y conectarlo a la alimentación.

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 la configuración de un dispositivo de hardware, consulteUso del dispositivo de hardware Storage Gateway.

Permisos de acceso de AWS Storage Gateway a través de firewalls y routers

La gateway necesita obtener acceso a los siguientes puntos de enlace de servicio para comunicarse conAWS. Si utiliza un firewall o un router para filtrar o limitar el tráfico de red, debe configurarlos para dar permiso a los puntos de enlace de servicio paraAWS.

> **Important**
>
> En función de la puerta de enlaceAWSRegión, sustituir*región*en el extremo de servicio con la cadena Region correcta.

Todas las gateways requieren el punto de enlace de servicio siguiente para las operaciones de head-bucket.

```
s3.amazonaws.com:443
```

Todas las puertas de enlace requieren los siguientes extremos de servicio para la ruta de control (`anon-cp`,`client-cp`,`proxy-app`) y 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 enlace de servicio de la gateway en la región EE.UU. Oeste (Oregón) (`us-west-2`).

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

El punto de enlace de servicio Amazon S3, que se muestra a continuación, únicamente lo utilizan las gateways de archivos. Una gateway de archivos necesita este punto de enlace para obtener acceso al bucket de Amazon S3 al que se asigna un recurso compartido de archivos.

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

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

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

> **Note**
>
> Si la puerta de enlace no puede determinar laAWSRegión en la que se encuentra el bucket de S3, este punto de enlace de servicio utiliza de forma predeterminada`s3.us-east-1.amazonaws.com`. Le recomendamos que permita el acceso a la región US East (N. Virginia) (`us-east-1`), además de las regiones en las que se active la gateway y en las que se encuentre su bucket de S3.

Los siguientes son los puntos de enlace de servicio de Amazon S3 paraAWS 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))
```

El siguiente ejemplo es un punto de enlace de servicio de FIPS para un bucket de S3 en elAWSRegión GovCloud (US-West).

```
bucket-name.s3-fips-us-gov-west-1.amazonaws.com
```

El punto de enlace de Amazon CloudFront que sigue es necesario para que Storage Gateway obtenga la lista de disponiblesAWSRegiones.

```
https://d4kdq0yaxexbo.cloudfront.net/
```

Una máquina virtual de Storage Gateway está configurada para utilizar los siguientes servidores NTP.

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

- Storage Gateway: para soporteAWSRegiones y lista deAWSpuntos finales de servicio que puede utilizar con Storage Gateway, consulteAWS Storage GatewayCuotas y puntos de enlace deen laAWSReferencia general de.
- Dispositivo de hardware de Storage Gateway: Para compatibleAWSRegiones que puede utilizar con el dispositivo de hardware, consulteRegiones de dispositivos de hardware de Storageen laAWSReferencia general de.

Configuración de grupos de seguridad para la instancia de gateway de Amazon EC2

EnAWS Storage Gateway, un grupo de seguridad controla el tráfico a la instancia de la gateway de Amazon EC2. A la hora de configurar un grupo de seguridad, recomendamos las siguientes acciones:

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

Si necesita permitir que se conecten instancias con la gateway desde el exterior de su grupo de seguridad, le recomendamos que solo permita conexiones en los puertos 3260 (para conexiones iSCSI) y 80 (para la activación).

- Si desea activar la gateway desde un host Amazon EC2 fuera del grupo de seguridad de la gateway, permita las conexiones entrantes en el puerto 80 desde la dirección IP de ese host. Si no puede determinar la dirección IP del host de activación, puede abrir el puerto 80, activar la gateway y, a continuación, cerrar el acceso en el puerto 80 tras completar la activación.
- Permita el acceso al puerto 22 únicamente si utiliza AWS Support para propósitos de solución de problemas. Para obtener más información, consulte ¿Quieres?AWS Supportpara ayudar a solucionar problemas de la puerta de enlace EC2.

En algunos casos, es posible utilizar una instancia de Amazon EC2 como iniciador (es decir, para conectarse a destinos iSCSI en una gateway implementada en Amazon EC2). En tal caso, se recomienda un enfoque de dos pasos:

1. Debe lanzar la instancia del iniciador en el mismo grupo de seguridad que la gateway.
2. Debe configurar el acceso de modo que el iniciador pueda comunicarse con la gateway.

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 o como un dispositivo de hardware físico, o enAWScomo instancia Amazon EC2.

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

- VMware ESXi Hypervisor (versión 6.0, 6.5 o 6.7): hay una versión gratuita de VMware disponible en elSitio web de VMware. Para esta configuración, también necesitará un cliente VMware vSphere para conectarse al host.
- Microsoft Hyper-V Hypervisor (versión 2012 R2 o 2016): hay una versión gratuita independiente de Hyper-V disponible en elCentro de descargas de Microsoft. Para esta configuración, necesitará Microsoft Hyper-V Manager en un equipo cliente Microsoft Windows para conectarse al host.
- Máquina virtual basada en Linux Kernel (KVM): una tecnología de virtualización gratuita de código abierto. KVM se incluye en todas las versiones de Linux versión 2.6.20 y posteriores. Storage

Gateway se ha probado y es compatible con las distribuciones Centos/RHEL 7.7, 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.

- Instancia de Amazon EC2: Storage Gateway proporciona una imagen de máquina de Amazon (AMI) que contiene la imagen de MV de la gateway. Para obtener información sobre cómo implementar una gateway en Amazon EC2, consulteImplementación de una gateway de archivos en un host Amazon EC2.
- Dispositivo de hardware de Storage Gateway: Storage Gateway proporciona un dispositivo de hardware físico como opción de implementación local para ubicaciones con infraestructura de máquina virtual limitada.

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

Clientes de NFS compatibles con una gateway de archivos

Las gateways de archivos admiten los siguientes clientes de Network File System (NFS):

- Amazon Linux
- Mac OS X

> **Note**
>
> Recomendamos configurar la`rsize`y`wsize`opciones de montaje a 64 KB para mejorar el rendimiento al montar recursos compartidos de archivos NFS en Mac OS X.

- RHEL 7
- SUSE Linux Enterprise Server 11 y SUSE Linux Enterprise Server 12

- Ubuntu 14.04
- Microsoft Windows 10 Enterprise, Windows Server 2012 y Windows Server 2016. Los clientes nativos solo son compatibles con NFS versión 3.
- Windows 7 Enterprise y Windows Server 2008.

  Los clientes nativos solo son compatibles con NFS v3. El tamaño máximo admitido de E/S NFS es de 32 KB, por lo que podría experimentar una reducción del rendimiento en estas versiones de Windows.

> **Note**
>
> Ahora puede utilizar recursos compartidos de archivos SMB cuando necesite tener acceso a través de clientes SMB de Windows en lugar de utilizar clientes NFS de Windows.

Clientes de SMB compatibles con una gateway de archivos

Las gateways de archivos admiten los siguientes clientes Service Message Block (SMB):

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

> **Note**
>
> El cifrado de Server Message Block requiere clientes compatibles con SMB v2.1.

Operaciones del sistema de archivos compatibles con una gateway de archivos

El cliente de NFS o SMB puede escribir, leer, eliminar y truncar archivos. Cuando los clientes envían escrituras aAWS Storage Gateway, escribe en la caché local de forma síncrona. 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. Las eliminaciones quitan los objetos de Amazon S3. Los directorios se administran como objetos de carpeta en S3, utilizando la misma sintaxis de 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).

Acceso a AWS Storage Gateway

Puede utilizar elAWS Storage Gatewayconsolapara realizar diversas tareas de configuración y administración de la puerta de enlace. En la sección Introducción y otras secciones de esta guía se utiliza la consola para ilustrar la funcionalidad de la gateway.

Además, puede utilizar el API de AWS Storage Gateway para configurar y administrar las gateways mediante programación. Para obtener más información sobre la API, consulte Referencia de API para Storage Gateway.

También puede utilizar laAWSSDK para desarrollar aplicaciones que interactúen con Storage Gateway. LaAWSLos SDK para Java, .NET y PHP integran el API de Storage Gateway subyacente para simplificar las tareas de programación. Para obtener información sobre la descarga de las bibliotecas de SDK, consulte laAWSCentro de desarrolladores.

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

Regiones de AWS compatibles

- Storage Gateway: para soporteAWSRegiones y lista deAWSpuntos finales de servicio que puede utilizar con Storage Gateway, consulteAWS Storage GatewayCuotas y puntos de enlace deen laAWSReferencia general de.
- Dispositivo de hardware de Storage Gateway: para conocer las regiones compatibles que puede utilizar con el dispositivo de hardware, consulteAWS Storage GatewayRegiones de dispositivos de hardwareen laAWSReferencia general de.

Uso del dispositivo de hardware Storage Gateway

Storage Gateway es un dispositivo de hardware físico con el software Storage Gateway preinstalado en una configuración de servidor validada. Puede administrar su dispositivo de hardware desde laHardware(Se ha creado elAWS Storage Gatewayconsola de .

El dispositivo de hardware es un servidor 1U de alto rendimiento que puede implementar en su centro de datos o en su firewall corporativo. Cuando compre y active su dispositivo de hardware, el proceso de activación asocia su dispositivo de hardware a suAWSaccount. Después de la activación, el dispositivo de hardware aparece en la consola como una gateway en elHardware(Se ha creado el certificado). Puede configurar su dispositivo de hardware como una gateway de archivos, una gateway de cintas o una gateway de volumen. El procedimiento que se utiliza para implementar y activar estos tipos de gateways en un dispositivo de hardware es el mismo que en una plataforma virtual.

El dispositivo de hardware de Storage Gateway se puede solicitar directamente desde elAWS Storage Gatewayconsola de .

Para solicitar un dispositivo de hardware

1. Abra la consola Storage Gateway enhttps://console.aws.amazon.com/storagegateway/homey elige elAWSRegión en la que desea que instale su dispositivo.
2. ElegirHardwareen el panel de navegación.
3. ElegirDispositivo de pedidoy luegoProceder. Se le redirigirá alAWSElemental Appliances and Software Management Console para solicitar un presupuesto de ventas.
4. Rellene la información necesaria y elijaEnviar.

Una vez revisada la información, se genera un presupuesto de venta y podrá continuar con el proceso de pedido y enviar una orden de compra u organizar el pago por adelantado.

Para ver una cotización de ventas o un historial de pedidos del dispositivo de hardware

1. Abra la consola Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
2. ElegirHardwareen el panel de navegación.
3. ElegirCotizaciones y pedidosy luegoProceder. Se le redirigirá alAWSElemental Appliances and Software Management Console para revisar las cotizaciones de ventas y el historial de pedidos.

En las secciones siguientes, encontrará instrucciones para configurar, configurar, activar, lanzar y utilizar un dispositivo de hardware de Storage Gateway.

Temas

Regiones de AWS compatibles

Storage Gateway Hardware Appliance está disponible para su envío a todo el mundo donde el gobierno de EE. UU. lo permite legalmente y permite exportar. Para obtener información sobre los admitidosAWSRegiones, consulteRegiones del dispositivo de hardware de Storageen laAWSReferencia general de.

Configuración del dispositivo de hardware

Después de recibir su dispositivo de hardware de Storage Gateway, utilice la consola del dispositivo de hardware para configurar las redes con el fin de ofrecer una conexión permanente aAWSy active el aparato. La activación asocia el dispositivo con elAWScuenta que se utiliza durante el proceso de activación. Después de la activación del dispositivo, puede lanzar una gateway de archivos, volumen o cintas desde la consola de 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 Montaje en bastidor de su dispositivo de hardware y conectarlo a la alimentación.

2. Establezca las direcciones de Protocolo de Internet versión 4 (IPv4) para el dispositivo de hardware (host) y Storage Gateway (servicio). Para obtener más información, consulte Configuración de parámetros de red.
3. Activar el dispositivo de hardware en la consolaHardware(Se ha creado elAWSRegión de su elección. Para obtener más información, consulte Activación del dispositivo de hardware.
4. Instale Storage Gateway en su dispositivo de hardware. Para obtener más información, consulte Configuración de la gateway.

   Las gateways se configuran de de la misma manera que las gateways en VMware ESXi, Microsoft Hyper-V, la máquina virtual de Linux basada en el kernel (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. Esto proporciona una caché más grande para un acceso de baja latencia a los datos almacenados enAWS. Si ha solicitado el modelo de 5 TB, puede aumentar el almacenamiento utilizable hasta 12 TB comprando cinco SSD (unidades de estado sólido) de 1,92 TB, que están disponibles para su pedido en la consola de.Hardware(Se ha creado el certificado). Puede solicitar las SSD adicionales siguiendo el mismo proceso de pedido que pedir un dispositivo de hardware y solicitar un presupuesto de ventas desde la consola de Storage Gateway.

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. ContactoAWSSupport instrucciones sobre cómo hacerlo.
2. Añada cinco SSD de 1,92 TB al dispositivo.

Opciones de tarjeta de interfaz de red

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

- Configuración NIC 10G-Base-T:
  - Utilice cables CAT6 para 10G o CAT5 (e) para 1G
- Configuración NIC 10G DA/SFP+:

- 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 1G-Base-T o 10G-Base-T

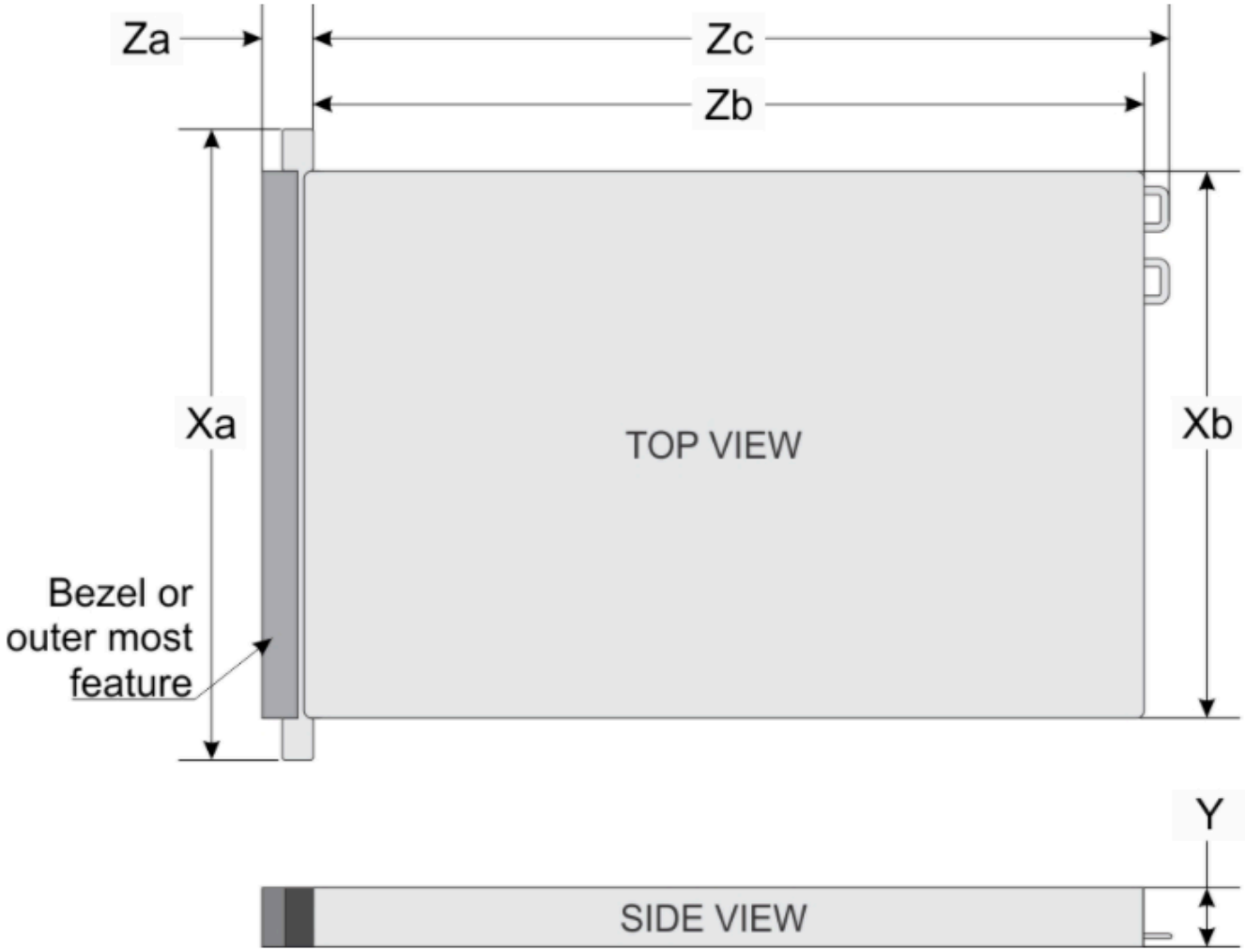
Montaje en bastidor de su dispositivo de hardware y conectarlo a la alimentación

Cuando abra su dispositivo de hardware de Storage Gateway, siga las instrucciones que se encuentran en la caja para montar el servidor en un bastidor. Su dispositivo tiene un factor de forma de 1U y encaja en un bastidor de 19 pulgadas que cumple la Comisión Electrotécnica Internacional (CEI) estándar.

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) incluida en el dispositivo de hardware). Twinax Copper DAC, 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).

Dimensiones del dispositivo de hardware



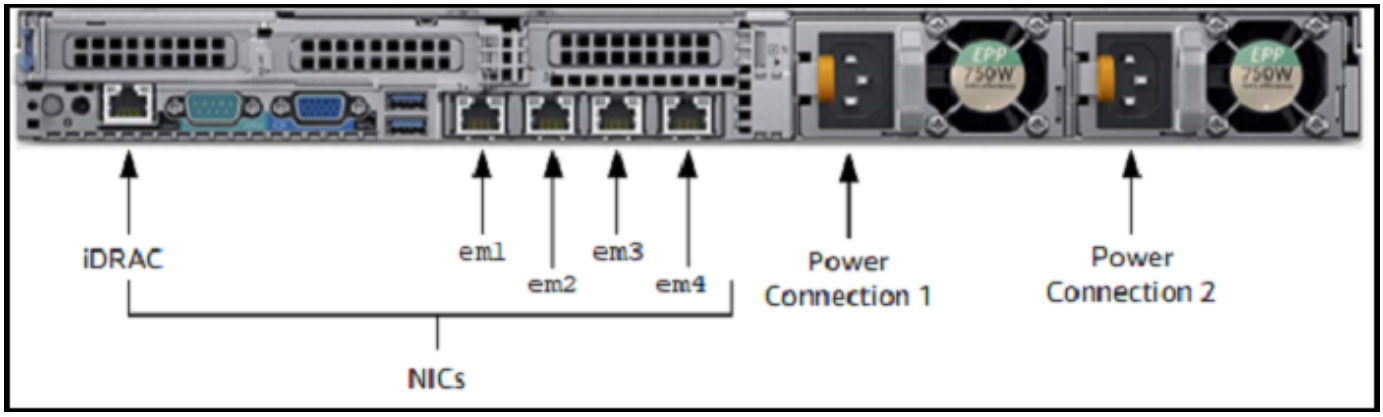
System	Xa	Xb	Y	Za (with bezel)	Za (without bezel)	Zb*	Zc
10 x 2.5-inches	482.0 mm (18.97-inches)	434.0 mm (17.08-inches)	42.8 mm (1.68-inches)	35.84 mm (1.41-inches)	22.0 mm (0.87-inches)	733.82 mm (29.61-inches)	772.67 mm (30.42-inches)

Para conectar el dispositivo de hardware a la alimentación

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

1. 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.

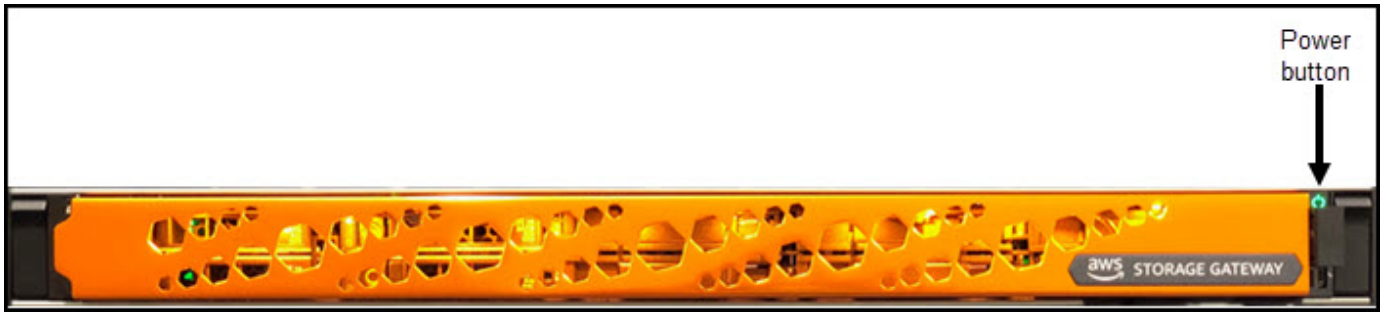
   En la siguiente imagen, puede ver el dispositivo de hardware con las diferentes conexiones.

2. 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 es compatible con las redes troncales VLAN. Configure el puerto del conmutador al que va a conectar el dispositivo de hardware como puerto de red VLAN no troncal.

3. Conecte el teclado y el monitor.
4. Encienda el servidor presionando el botón Power del panel delantero, como se muestra en la siguiente imagen.



Después de que el servidor se inicie, la consola de hardware aparecerá en el monitor. La consola de hardware presenta una interfaz de usuario específica deAWSque puede utilizar para configurar los parámetros de red iniciales. Estos parámetros se configuran para conectar el dispositivo aAWSy abra un canal de soporte para la solución de problemas medianteAWSSupport.

Para trabajar con la consola de hardware, introduzca 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.

Para establecer una contraseña por primera vez

1. En Set Password, introduzca una contraseña y, a continuación, presione `Down arrow`.
2. En Confirm, vuelva a introducir la contraseña y, a continuación, seleccione Save Password.

En este momento está en la consola de hardware, que aparece a continuación.

Paso siguiente

Configuración de parámetros de red

Configuración de parámetros de red

Después de que el servidor se inicie, puede introducir su primera contraseña en la consola de hardware como se describe en Montaje en bastidor de su dispositivo de hardware y conectarlo a la alimentación.

A continuación, en la consola de hardware siga los siguientes pasos para configurar los parámetros de red para que su dispositivo de hardware se pueda conectar aAWS.

Para establecer una dirección de red

1. Seleccione Configure Network y pulse la tecla `Enter`. La pantalla Configure Network aparece a continuación.

2. En IP Address, introduzca una dirección IPv4 válida desde una de las siguientes fuentes:

   - Utilice la dirección IPv4 asignada por su servidor de protocolo de configuración dinámica de host (DHCP) a su puerto de red físico.

     Si realiza este paso, anote esta dirección IPv4 para utilizarla más adelante en el paso de activación.

   - Asignar una dirección IPv4 estática Para hacer esto, seleccione Static en la sección `em1` y pulse `Enter` para ver la pantalla Configurar IP estática a continuación.

     La sección `em1` está en la sección superior izquierda del grupo de configuración de puertos.

   Después de introducir una dirección IPv4 válida, pulse `Down arrow` o `Tab`.

   > **Note**
   >
   > Si configura otra interfaz, debe proporcionar la misma conexión permanente alAWSpuntos finales enumerados en los requisitos.

3. En Subnet, introduzca una máscara de subred válida y, a continuación, pulse `Down arrow`.
4. En Gateway, introduzca la dirección IPv4 de su gateway de red y, a continuación, pulse `Down arrow`.
5. En DNS1, introduzca la dirección IPv4 de su servidor del servicio de nombres de dominio (DNS) y, a continuación, pulse `Down arrow`.
6. (Opcional) En DNS2, introduzca una segunda dirección IPv4 y, a continuación, pulse `Down arrow`. Una segunda asignación del servidor DNS proporcionará redundancia adicional si el primer servidor DNS no está disponible.
7. Seleccione Save y, a continuación, pulse `Enter` para guardar la configuración de la dirección IPv4 estática para el dispositivo.

Para cerrar sesión en la consola de hardware

1. Seleccione Back para volver a la Pantalla principal.
2. Seleccione Logout para volver a la Pantalla de inicio de sesión.

Paso siguiente

Activación del dispositivo de hardware

Activación del dispositivo de hardware

Después de configurar la dirección IP, introdúzcala en la página Hardware de la consola, como se describe a continuación. El proceso de activación valida que su dispositivo de hardware tenga las credenciales de seguridad apropiadas y registra el dispositivo en suAWSaccount.

Puede activar el dispositivo de hardware en cualquiera de lasAWSRegiones. Para obtener una lista de los admitidosAWSRegiones, consulteRegiones del dispositivo de hardware de Storageen laAWSReferencia general de.

Para activar el dispositivo por primera vez o en unaAWSRegión en la que no tiene implementadas puertas de enlace

1. Inicie sesión en laAWS Management Consoley abra la consola de Storage Gateway enAWS Storage GatewayConsola de administración decon las credenciales de cuenta que utilizar para activar el hardware.

   Si esta es su primera puerta de enlace en unAWSRegiones, verá una pantalla de bienvenida. Después de crear una gateway en esteAWSRegión, la pantalla ya no se muestra.

   > **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. Seleccione Get started para ver el asistente de creación de gateways y, a continuación, seleccione Hardware Appliance en la página Select host platform, como se muestra a continuación.
3. Seleccione Next para ver la pantalla Connect to hardware que se muestra a continuación.
4. ParaDirección IPen laConnect al dispositivo de hardware, introduzca la dirección IPv4 de su dispositivo y, a continuación, seleccioneConectarPara ir a la pantalla Activar hardware que se muestra a continuación.

5. En Hardware name, escriba un nombre para su dispositivo. Los nombres pueden tener una longitud máxima de 225 caracteres y no pueden incluir barras inclinadas.
6. ParaZona horaria de hardware, introduzca su configuración local.

   La zona horaria controla cuándo se realizan las actualizaciones de hardware, utilizando la hora local 2:00 para las actualizaciones.

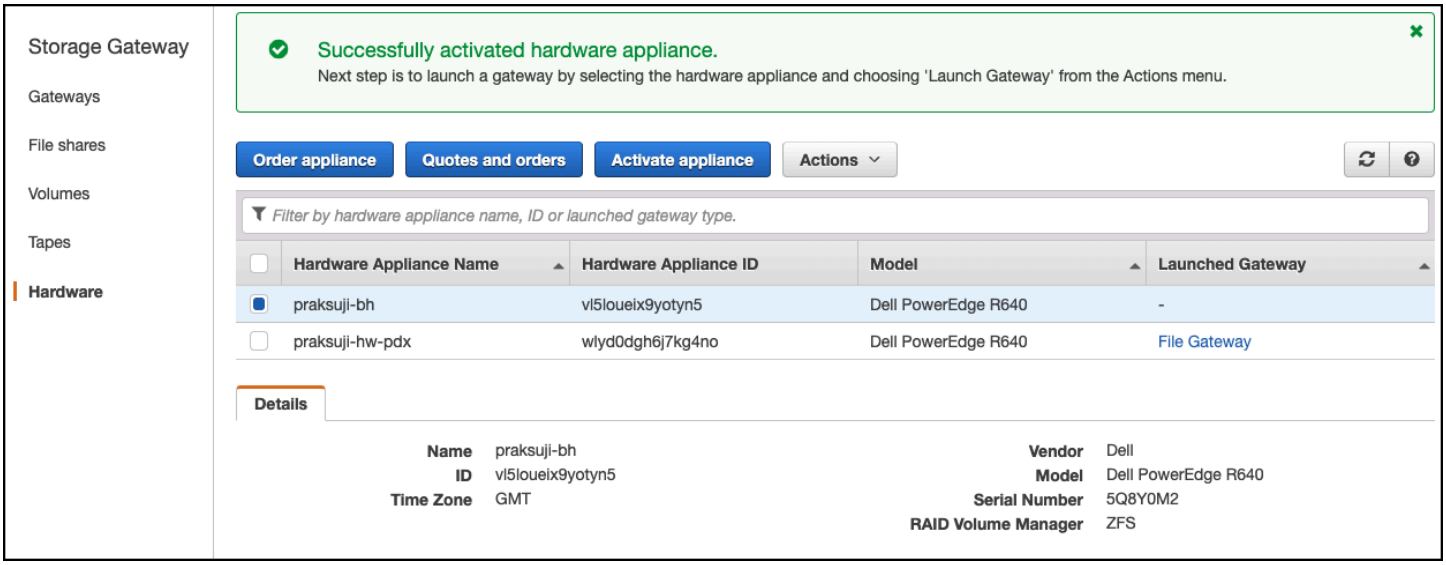
   > **Note**
   >
   > Recomendamos configurar la zona horaria de su dispositivo, ya que determina que la hora de actualización estándar esté fuera del periodo de la jornada laboral.

7. (Opcional) Mantenga el RAID Volume Manager establecido en ZFS.

   ZFS se utiliza como administrador de volúmenes RAID en el dispositivo de hardware para proporcionar un mejor rendimiento y protección de datos. ZFS es un sistema de archivos de código abierto basado en software y un administrador lógico de volumen. Este dispositivo de hardware ha sido adaptado específicamente para ZFS RAID. Para obtener más información acerca de ZFS RAID, consulte la página de Wikipedia de ZFS.
8. Seleccione Next para finalizar la activación.

En la página Hardware, aparece un banner de consola que indica que el dispositivo de hardware ha sido activado correctamente, como se muestra a continuación.

En este momento, el dispositivo está asociado a su cuenta. El siguiente paso es lanzar una gateway de archivos, cinta o volumen almacenada en caché en su dispositivo.



Paso siguiente

Lanzamiento de gateway

Lanzamiento de gateway

Puede lanzar cualquiera de las tres puertas de enlace de almacenamiento del dispositivo: puerta de enlace de archivos, puerta de enlace de volúmenes (en caché) o gateway de cinta.

Para lanzar una gateway en su dispositivo de hardware

1. Inicie sesión en laAWS Management Consoley abra la consola de Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
2. Seleccione Hardware.
3. En Actions, elija Launch gateway.
4. En Gateway Type, seleccione File Gateway, Tape Gateway o Volume Gateway (Cached).
5. En Gateway name, introduzca un nombre para la gateway. Los nombres pueden tener una longitud de 225 caracteres y no pueden incluir barras inclinadas.
6. Seleccione Launch gateway.

El software Storage Gateway del tipo de gateway elegida se instala en el dispositivo. Una gateway puede tardar hasta 5 a 10 minutos en aparecer comoonlineEn la consola de.

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 para la gateway

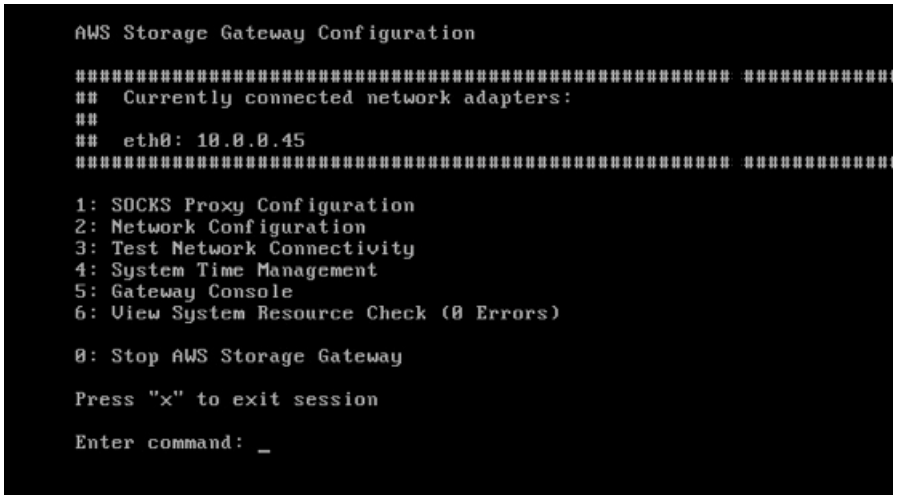
Configuración de una dirección IP para la gateway

Antes de activar el dispositivo de hardware, asignó una dirección IP a su interfaz de red física. Ahora que ha activado el dispositivo y ha iniciado Storage Gateway en él, debe asignar otra dirección IP a la máquina virtual Storage Gateway que se ejecuta en el dispositivo de hardware. Para asignar una dirección IP estática a una gateway instalada en su dispositivo de hardware, configura la dirección IP desde la consola local de la gateway. Sus aplicaciones (como sus clientes de NFS o SMB, su iniciador iSCSI, etc.) se conectan a esta dirección IP. Puede acceder a la consola local de la gateway desde la consola del dispositivo de hardware.

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

1. En la consola de hardware, seleccione Open Service Console para abrir una pantalla de inicio de sesión para la consola local de la gateway.
2. Introduzca la contraseña de login del host local y, a continuación, pulse `Enter`.

   La cuenta predeterminada es `admin` y la contraseña predeterminada es `password`.
3. Cambiar la contraseña predeterminada. Elija Actions (Acciones) y, a continuación, Set Local Password (Establecer la contraseña local) e introduzca sus credenciales nuevas en el cuadro de diálogo Set Local Password (Establecer la contraseña local).
4. (Opcional) Definir la configuración del proxy. Para obtener instrucciones, consulte Montaje en bastidor de su dispositivo de hardware y conectarlo a la alimentación.
5. Vaya a la página Configuración de red de la consola local de la gateway como se muestra a continuación.



6. Escriba 2 para ir a la página Network Configuration que se muestra a continuación.

7. Configure una dirección IP estática o DHCP para que el puerto de red de su dispositivo de hardware presente una gateway de archivos, volumen o cinta para las aplicaciones. Esta dirección IP 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.

Paso siguiente

Configuración de la gateway

Configuración de la gateway

Después de activar y configurar su dispositivo de hardware, este aparece en la consola. Ahora puede crear el tipo de gateway que desee. Continúe la instalación del tipo de gateway que desee. Para obtener instrucciones, consulte Configuración de Amazon S3 File Gateway.

Eliminación de una puerta de enlace del dispositivo de hardware

Para eliminar el software de la gateway de su dispositivo de hardware, realice el siguiente procedimiento. Después de realizarlo, el software de la gateway se desinstala de su dispositivo de hardware.

Eliminar una gateway de un dispositivo de hardware

1. Seleccione la casilla de verificación de la gateway.
2. En Actions, elija Remove gateway.
3. En el cuadro de diálogo Remove gateway from hardware appliance, elija Confirm.

> **Note**
>
> Al eliminar una gateway, no se puede 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 gateway mediante el uso de la consola de AWS Storage Gateway y eliminación de los recursos asociados.

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

Eliminación del dispositivo de hardware

Después de activar el dispositivo de hardware en suAWSCuenta, es posible que tenga que mover y activar la en otraAWSaccount. En este caso, primero debe eliminar el dispositivo de laAWScuenta y actívala en otraAWSaccount. También es posible que desee eliminar por completo el dispositivo

de suAWScuenta porque ya no la necesita. Siga estas instrucciones para eliminar el dispositivo de hardware.

Para eliminar el dispositivo de hardware

1. Si ha instalado una gateway en el dispositivo de hardware, primero debe eliminar la gateway antes de eliminar el dispositivo. Para obtener instrucciones sobre cómo eliminar una gateway de su dispositivo de hardware, consulteEliminación de una puerta de enlace del dispositivo de hardware.
2. En la página Hardware, elija el dispositivo de hardware que desee eliminar.
3. En Actions (Acciones), elija Delete appliance (Eliminar dispositivo).
4. En el cuadro de diálogo Confirm deletion of resource(s) (Confirmar eliminación de recursos), elija la casilla de confirmación y, a continuación, Delete (Eliminar). Se muestra un mensaje que indica que se ha completado la eliminación.

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

Introducción a AWS Storage Gateway

En esta sección, encontrará instrucciones sobre cómo crear y activar una gateway de archivos enAWS Storage Gateway. Antes de empezar, asegúrese de que la configuración cumple los requisitos previos requeridos y otros requisitos descritos enConfiguración para Amazon S3 File Gateway.

Temas

- Crear y activar una puerta de enlace de archivos de Amazon S3

Crear y activar una puerta de enlace de archivos de Amazon S3

En esta sección, encontrará instrucciones sobre cómo crear, implementar y activar una gateway de archivos enAWS Storage Gateway.

Temas

- Configurar una gateway de archivos de Amazon S3
- Connect su puerta de enlace de archivos de Amazon S3 aAWS
- Revisar la configuración y activar Amazon S3 File Gateway
- Configuración de Amazon S3 File Gateway

Configurar una gateway de archivos de Amazon S3

Para configurar una gateway de archivos nueva de S3

1. Abra el iconoAWS Management Consoleahttps://console.aws.amazon.com/storagegateway/home/, y elija laRegión de AWSdonde va a crear la gateway.
2. ElegirCrear gatewaypara abrirConfigurar gateway(Se ha creado el certificado).
3. En el navegadorConfiguración de pasarela, haga lo siguiente:

    a. En Gateway name, introduzca un nombre para la gateway. Después de crear la puerta de enlace, puede buscar este nombre para encontrar la puerta de enlace en las páginas de lista delAWS Storage Gatewayconsola de .

    b. ParaZona horaria Gateway, elija la zona horaria local de la parte del mundo en la que desea desplegar la puerta de enlace.

4. En el navegadorOpciones de gatewaysección, paraTipo de gateway, eligeGateway de archivos de Amazon S3.
5. En el navegadorOpciones de la plataforma, haga lo siguiente:

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

      - VMware ESXi: descargue, implemente y configure la máquina virtual gateway mediante VMware ESXi.
      - Microsoft Hyper-V: descargue, implemente y configure la máquina virtual gateway mediante Microsoft Hyper-V.
      - Linux KVM— Descargue, implemente y configure la máquina virtual gateway mediante la máquina virtual de Linux basada en el kernel (KVM).
      - Amazon EC2Configure e inicie una instancia Amazon EC2 para alojar su gateway.
      - Dispositivo de hardware— Solicite un dispositivo de hardware físico dedicado desdeAWSPara alojar la gateway.

   b. ParaConfirmar configuración puerta de enlace, active la casilla de verificación para confirmar que ha realizado los pasos de implementación de la plataforma host que ha elegido. Este paso no es aplicable a laDispositivo de hardwareplataforma de host.
6. Ahora que está configurada, debe elegir cómo desea que se conecte y se comunique conAWS. ElegirPróximopara continuar.

Connect su puerta de enlace de archivos de Amazon S3 aAWS

Para conectar una nueva puerta de enlace de archivos S3 aAWS

1. Si todavía no lo ha hecho, complete el procedimiento descrito enConfigurar una gateway de archivos de Amazon S3. Cuando haya terminado, seleccionePróximopara abrirConnect toAWSde laAWS Storage Gatewayconsola de .
2. En el navegadorOpciones de endpointsección, paraPunto de enlace de servicio, elija el tipo de punto de enlace con el que utilizará la gateway para comunicarseAWS. Puede elegir entre las siguientes opciones:

- Publicly accessible (Accesible públicamente)— Su puerta de enlace se comunica conAWSa través de la red de Internet pública. Si selecciona esta opción, utilice laPunto de enlace habilitado para FIPSpara especificar si la conexión debe cumplir los Estándares Federales de Procesamiento de la Información (FIPS).

  > **Note**
  >
  > Si necesita módulos criptográficos validados FIPS 140-2 al acceder aAWSa través de una interfaz de línea de comandos o una API, utilice un punto de enlace compatible con FIPS. Para obtener más información, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.
  > El punto de enlace de servicio de FIPS solo está disponible en algunosAWSRegiones. Para obtener más información, consulteAWS Storage GatewayCuotas y puntos de enlace deen laAWSReferencia general de.

- VPC alojada— Su puerta de enlace se comunica conAWSmediante una conexión privada con la nube virtual privada (VPC), que le permite controlar la configuración de red. Si selecciona esta opción, debe especificar un endpoint de VPC existente eligiendo su ID de endpoint de la VPC en la lista desplegable. También puede proporcionar su nombre o la dirección IP de su sistema de nombres de dominio (DNS) de la VPC.

3. En el navegadorOpciones de conexión de gatewaysección, paraOpciones de conexión, elija cómo identificar su puerta de enlace aAWS. Puede elegir entre las siguientes opciones:

   - dirección IP— Proporcione la dirección IP de la gateway en el campo correspondiente. Esta dirección IP debe ser pública o accesible desde la red actual y debe poder conectarse a ella desde su navegador web.

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

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

4. Ahora que ha elegido cómo desea que se conecte la puerta de enlaceAWS, debe activar la puerta de enlace. ElegirPróximopara continuar.

Revisar la configuración y activar Amazon S3 File Gateway

Para activar una nueva puerta de enlace de archivos S3

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

   - Configurar una gateway de archivos de Amazon S3
   - Connect su puerta de enlace de archivos de Amazon S3 aAWS

   Cuando haya terminado, seleccionePróximopara abrirRealice la revisión y activede laAWS Storage Gatewayconsola de .
2. Revise los detalles iniciales de la puerta de enlace de cada sección de la página.
3. Si una sección contiene errores, elijaEditarpara volver a la página de configuración correspondiente y realizar cambios.

   > **Important**
   >
   > No puede modificar las opciones de puerta de enlace ni la configuración de conexión después de activar la puerta de enlace.
4. Ahora que ha activado la puerta de enlace, debe realizar la primera configuración para asignar discos de almacenamiento locales y configurar el registro. ElegirPróximopara continuar.

Configuración de Amazon S3 File Gateway

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

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

   - Configurar una gateway de archivos de Amazon S3
   - Connect su puerta de enlace de archivos de Amazon S3 aAWS
   - Revisar la configuración y activar Amazon S3 File Gateway

   Cuando haya terminado, seleccionePróximopara abrirConfigurar gatewayde laAWS Storage Gatewayconsola de .

2. En el navegadorConfigurar el almacenamiento en caché, utilice las listas desplegables para asignar al menos un disco local con al menos 150 gibibytes (GiB) de capacidad aCaché. Los discos locales enumerados en esta sección corresponden al almacenamiento físico que aprovisionó en la plataforma host.
3. En el navegadorGrupo de registros CloudWatch, elija cómo configurar Amazon CloudWatch Logs para supervisar el estado de la puerta de enlace. Puede elegir entre las siguientes opciones:

   - Crear un nuevo grupo de registros— Configure un nuevo grupo de registros para supervisar la gateway.
   - Uso de un grupo de registros existente: elija un grupo de registros existente de la lista desplegable correspondiente.
   - Desactivar registro: no utilice Amazon CloudWatch Logs para supervisar la puerta de enlace.
4. En el navegadorAlarmas de CloudWatch, elija cómo configurar las alarmas de Amazon CloudWatch para notificarle cuando las métricas de la puerta de enlace se desvían de los límites definidos. Puede elegir entre las siguientes opciones:

   - Desactivar alarmas: no utilice alarmas de CloudWatch para recibir notificaciones sobre las métricas de su puerta de enlace.
   - Crear una alarma de CloudWatch personalizada: configure una nueva alarma de CloudWatch para que se le notifique sobre las métricas de su puerta de enlace. ElegirCrear alarmapara definir métricas y especificar acciones de alarma en la consola de Amazon CloudWatch Para obtener instrucciones, consulteUso de alarmas de Amazon CloudWatchen laGuía del usuario de Amazon CloudWatch.
5. (Opcional) En elEtiquetassección, elijaAñadir nueva etiquetay, a continuación, introduzca un par clave-valor que distingue entre mayúsculas y minúsculas y que le ayude a buscar y filtrar la gateway en las páginas de lista delAWS Storage Gatewayconsola de . Repita este pasos para añadir cuantas etiquetas necesite.
6. (Opcional) En elComprobar la configuración de alta disponibilidad de VMware, si la gateway se implementa en un host VMware como parte de un clúster que está habilitado para la alta disponibilidad (HA) de VMware, elijaVerificación de VMware HApara comprobar si la configuración de alta disponibilidad funciona correctamente.

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

7. ElegirConfigurarPara terminar de crear la gateway.

   Para comprobar el estado de la nueva gateway, búscala en laGateways dePágina de laAWS Storage Gatewayconsola de .

Ahora que ha creado la gateway, debe crear un recurso compartido de archivos para usarlo. Para obtener instrucciones, consulteCreación de un recurso compartido de archivos.

Creación de un recurso compartido de archivos

En esta sección, encontrará instrucciones sobre cómo crear un recurso compartido de archivos. Puede crear un recurso compartido de archivos al que se puede obtener acceso mediante el protocolo Network File System (NFS) o el protocolo Server Message Block (SMB).

> **Note**
>
> Cuando un cliente NFS o SMB escribe un archivo en la puerta de enlace de archivos, la puerta de enlace de archivos carga los datos del archivo en Amazon S3 seguido de sus metadatos (propiedad, marcas de tiempo, etc.). Al cargar los datos de 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 almacenan ambas versiones.
> Si cambia los metadatos de un archivo almacenado en la puerta de enlace de archivos, se crea un nuevo objeto S3 que reemplaza al objeto S3 existente. Este comportamiento es distinto del de editar un archivo en un sistema de archivos, en el que la edición de un archivo no da lugar a la creación de un nuevo archivo. Probar todas las operaciones de archivos que planea utilizar conAWSStorage Gateway para que comprenda cómo interactúa cada operación de archivos 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 carga datos desde la puerta de enlace de archivos. La carga de archivos desde la puerta de enlace de archivos a Amazon S3 cuando se habilita el control de versiones de S3 da como resultado al menos dos versiones de un objeto S3. Ciertos flujos de trabajo que incluyen archivos grandes y patrones de escritura de archivos, como las subidas de archivos que se realizan en varios pasos, pueden aumentar el número de versiones de objetos S3 almacenadas. Si la caché de puerta de enlace de archivos necesita liberar espacio debido a las altas velocidades de escritura de archivos, se pueden crear varias versiones de objetos de S3. Estos escenarios aumentan el almacenamiento de S3 si el control de versiones de S3 está habilitado y aumentan los costos de transferencia asociados con CRR. Pruebe todas las operaciones de archivos que planea utilizar con Storage Gateway para comprender cómo interactúa cada operación de archivos con el almacenamiento de Amazon S3.
> El uso de la utilidad Rsync con la puerta de enlace de archivos da lugar a la creación de archivos temporales en la caché y a la creación de objetos S3 temporales en Amazon S3. Esta situación produce cargos de eliminación temprana en las clases de almacenamiento

S3 Estándar - Acceso poco frecuente de S3 (S3 Standard-IA) y S3 Intelligent-Tiering (Capas inteligentes de S3).

De forma predeterminada, al crear un recurso compartido de archivos NFS, cualquier persona que tenga acceso al servidor NFS pueden obtener acceso a dicho recurso. Puede limitar el acceso a los clientes por dirección IP.

Para SMB, puede utilizar uno de estos tres tipos 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 les permitirá el acceso a los usuarios y grupos del dominio especificados (a través de una lista de permitidos). También es posible denegar el acceso a los usuarios y grupos (a través de una lista de denegación).
- Un recurso compartido de archivos SMB con acceso de invitado. Los usuarios que facilitan la contraseña de invitado obtienen acceso a este recurso compartido de archivos.

> **Note**
>
> Los recursos compartidos de archivos exportados a través de la gateway para recursos compartidos de archivos de NFS son compatibles con los permisos de POSIX. Para los recursos compartidos de archivos de SMB puede utilizar la lista de control de acceso (ACL) para gestionar los permisos de los archivos y carpetas en su recurso compartido de archivo. Para obtener más información, consulte Uso de las ACL de Microsoft Windows para controlar el acceso a un recurso compartido de archivos SMB.

Una gateway de archivos puede alojar uno o varios recursos compartidos de archivos de diferentes tipos. Es posible tener varios recursos compartidos de archivos NFS y SMB en una gateway de archivos.

> **Important**
>
> Para poder crear un recurso compartido de archivos, la puerta de enlace de archivos requiere que se active AWS Security Token Service (AWS STS). Asegúrese de queAWS STSse activa en elRegión de AWSen la que esté creando la puerta de enlace de archivos. SiAWS STSno se activa en esoRegión de AWS, actívalo. Para obtener información sobre cómo

activarAWS STS, consulteActivación y desactivación deAWS STSen unRegión de AWSen laAWS Identity and Access ManagementGuía del usuario de.

> **Note**
>
> Puede usarAWS Key Management Service(AWS KMS) para cifrar los objetos que la puerta de enlace de archivos almacena en Amazon S3. Para ello, a través de la consola de Storage Gateway, consulte.Creación de un recurso compartido de archivos NFSoCreación de un recurso compartido de archivos SMB. También puede hacerlo a través de la API de Storage Gateway. Para obtener instrucciones, consulteCreateNFSFileShareoCreateSMBFileShareen laAWSReferencia de la API de Storage.
>
> De forma predeterminada, la gateway de archivos utiliza el cifrado del lado del servidor administrado con Amazon S3 (SSE-S3) cuando escribe datos en un bucket de S3. Si realiza SSE-KMS (cifrado del lado del servidor conAWS KMS—managed keys) el cifrado predeterminado para el bucket de S3, los objetos que almacene en él una puerta de enlace de archivos se cifran con SSE-KMS.
>
> Para realizar el cifrado con SSE-KMS con su propia clave de AWS KMS, debe habilitar el cifrado SSE-KMS. Cuando lo haga, 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 mediante la operación de la API UpdateFsFileShare o UpdateSmbFileShare. Esta actualización se aplica a los objetos almacenados en los buckets de Amazon S3 después de la actualización.
>
> Si configura la puerta de enlace de archivos para utilizar SSE-KMS para el cifrado, debe agregar manualmente`kms:Encrypt`,`kms:Decrypt`,`kms:ReEncrypt`,`kms:GenerateDataKey`, y`kms:DescribeKey`permisos para el rol de IAM asociado al recurso compartido de archivos. Para obtener más información, consulteUso de políticas basadas en identidad (políticas de IAM) para Storage Gateway.

Temas

- Creación de un recurso compartido de archivos NFS
- Creación de un recurso compartido de archivos SMB

Creación de un recurso compartido de archivos NFS

Utilice el procedimiento siguiente para crear un recurso compartido de archivos de red (NFS).

> **Note**
>
> Cuando un cliente NFS escribe un archivo en la puerta de enlace de archivos, la puerta de enlace de archivos carga los datos del archivo en Amazon S3 seguidos de sus metadatos (propiedad, marcas de tiempo, etc.). Al cargar los datos de 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 almacenan ambas versiones.
> Si cambia los metadatos de un archivo almacenado en la puerta de enlace de archivos, se crea un nuevo objeto S3 que reemplaza al objeto S3 existente. Este comportamiento es distinto del de editar un archivo en un sistema de archivos, en el que la edición de un archivo no da lugar a la creación de un nuevo archivo. Probar todas las operaciones de archivos que planea utilizar conAWSStorage Gateway para que comprenda cómo interactúa cada operación de archivos 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 carga datos desde la puerta de enlace de archivos. La carga de archivos desde la puerta de enlace de archivos a Amazon S3 cuando se habilita el control de versiones de S3 da como resultado al menos dos versiones de un objeto S3. Ciertos flujos de trabajo que incluyen archivos grandes y patrones de escritura de archivos, como las subidas de archivos que se realizan en varios pasos, pueden aumentar el número de versiones de objetos S3 almacenadas. Si la caché de puerta de enlace de archivos necesita liberar espacio debido a las altas velocidades de escritura de archivos, se pueden crear varias versiones de objetos de S3. Estos escenarios aumentan el almacenamiento de S3 si el control de versiones de S3 está habilitado y aumentan los costes de transferencia asociados con CRR. Pruebe todas las operaciones de archivos que planea utilizar con Storage Gateway para comprender cómo interactúa cada operación de archivos con el almacenamiento de Amazon S3.
> El uso de la utilidad Rsync con la puerta de enlace de archivos da lugar a la creación de archivos temporales en la caché y a la creación de objetos S3 temporales en Amazon S3. Esta situación produce cargos de eliminación temprana en las clases de almacenamiento S3 Estándar - Acceso poco frecuente de S3 (S3 Standard-IA) y S3 Intelligent-Tiering (Capas inteligentes de S3).

Para crear un recurso compartido de archivos NFS

1. Abra el iconoAWSStorage Gateway enhttps://console.aws.amazon.com/storagegateway/home/.
2. ElegirCreación de recurso compartido de archivospara abrirConfiguración de recurso compartido de archivos(Se ha creado el certificado).
3. ParaPortal, elija su Amazon S3 File Gateway de la lista.
4. ParaUbicación de Amazon S3, realice una de las siguientes operaciones:

   - Para conectar el recurso compartido de archivos directamente a un bucket de S3, elijaNombre del bucket de S3y, a continuación, introduzca el nombre del bucket de S3 y, opcionalmente, un nombre de prefijo para los objetos creados por el recurso compartido de archivos. La puerta de enlace utiliza este depósito para almacenar y recuperar archivos. Para obtener información acerca de cómo crear un nuevo bucket, consulte.¿Cómo se puede crear un bucket de S3?en laGuía del usuario de Amazon S3.
   - Para conectar el recurso compartido de archivos a un bucket de S3 a través de un punto de acceso, elijaPunto de acceso S3y, a continuación, introduzca el nombre del punto de acceso de S3 y, opcionalmente, un nombre de prefijo para los objetos creados por el recurso compartido de archivos. La política de bucket debe configurarse para delegar el control de acceso en el punto de acceso. Para obtener información acerca de los puntos de acceso, consulte.Administración del acceso a datos con puntos de acceso de Amazon S3yDelegar el control de acceso a los puntos de accesoen laGuía del usuario de Amazon S3.
   - Para conectar el recurso compartido de archivos a un bucket de S3 a través de un alias de punto de acceso, elijaAlias de punto de acceso de S3y, a continuación, introduzca el nombre del alias del punto de acceso de S3 y, opcionalmente, un nombre de prefijo para los objetos creados por el recurso compartido de archivos. Si elige esta opción, la puerta de enlace de archivos no puede crear una nuevaAWS Identity and Access Management(IAM) y política de acceso en su nombre. Debe seleccionar un rol de IAM existente y configurar una política de acceso en elAcceder a su bucket de S3sección que sigue. Para obtener más información acerca de los alias de puntos de acceso, consulte.Uso de un alias estilo cubo para el punto de accesoen laGuía del usuario de Amazon S3.

> **Note**
>
> - Si introduce un nombre de prefijo o elige conectarse a través de un punto de acceso o alias de punto de acceso, debe introducir un nombre de recurso compartido de archivos.
> - El nombre del prefijo debe terminar con una barra diagonal: (/).
> - Una vez creado el recurso compartido de archivos, el nombre del prefijo no se puede modificar ni eliminar.
> - Para obtener información acerca del uso de nombres de prefijo, consulte.Organizar objetos con prefijosen laGuía del usuario de Amazon S3.

5. ParaRegión de AWS, elige elRegión de AWSdel bucket de S3.
6. ParaNombre del recurso compartido de archivos, escriba un nombre para el recurso compartido de archivos. El nombre predeterminado es el nombre del bucket de S3 o el nombre del punto de acceso.

> **Note**
>
> - Si ha introducido un nombre de prefijo o ha optado por conectarse a través de un punto de acceso o alias de punto de acceso, debe introducir un nombre de recurso compartido de archivos.
> - Una vez creado el recurso compartido de archivos, no se puede eliminar el nombre del recurso compartido de archivos.

7. (Opcional) ParaAWS PrivateLinkpara S3, realice una de las siguientes opciones:

    1. Para configurar el recurso compartido de archivos para conectarse a S3 a través de un punto de enlace de interfaz de su nube virtual privada (VPC) con tecnología deAWS PrivateLink, eligeUsar punto de enlace de la VPC.
    2. Para identificar el extremo de la interfaz de la VPC por el que desea que se conecte el recurso compartido de archivos, elija uno de los dosID de punto de enlace de la VPCoNombre DNS del punto de enlace de VPCy, a continuación, proporcione la información requerida en el campo correspondiente.

> **Note**
>
> - Este paso es necesario si el recurso compartido de archivos se conecta a S3 a través de un punto de acceso de VPC o a través de un alias asociado a un punto de acceso de VPC.
> - Conexión de recurso compartido de archivos medianteAWS PrivateLinkno se admiten en las puertas de enlace FIPS.
> - Para obtener información sobreAWS PrivateLink, consulteAWS PrivateLinkpara Amazon S3en laGuía del usuario de Amazon S3.

8. En Access objects using (Obtener acceso a los objetos mediante), elija Network File System (NFS).
9. En Audit logs (Registros de auditoría), elija una de las siguientes opciones:

   - Para desactivar el registro de, elijaDisable logging (Deshabilitar el registro).
   - Para crear un nuevo registro de auditoría, elijaCreación de un nuevo grupo de registros.
   - Para utilizar un registro de auditoría existente, elijaUse un grupo de registros existentey, a continuación, elija un registro de auditoría de la lista.

   Para obtener más información acerca de auditorías, consulte Descripción de los registros de auditoría de file gateway.
10. ParaActualización automatizada de la caché desde S3, eligeEstablecer intervalo de actualizacióny establezca la hora 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. Una vez transcurrido el intervalo TTL, el acceso al directorio hace que la puerta de enlace de archivos actualice primero el contenido del directorio desde el bucket de Amazon S3.
11. ParaNotificación de carga de archivo, eligeTiempo de ajuste (segundos)que se le notificará cuando la puerta de enlace de archivos haya cargado completamente un archivo en S3. Establecimiento de la propiedad deTiempo de asentamientoen segundos para controlar el número de segundos que se espera después del último punto en el tiempo que un cliente escribió en un archivo antes de generar un`ObjectUploaded`Notificación de. Dado que los clientes pueden realizar muchas escrituras pequeñas en archivos, es mejor configurar este

parámetro durante el mayor tiempo posible para evitar generar varias notificaciones para el mismo archivo en un período de tiempo reducido. Para obtener más información, consulte Obtener notificación de subida de archivos.

> **Note**
>
> Esta configuración no afecta a la sincronización de la carga del objeto a S3, solo en el momento de la notificación.

12. (Opcional) En la sección Add tags (Añadir etiquetas), escriba una clave y un valor para añadir etiquetas al recurso compartido de archivos. Una etiqueta es un par clave-valor que distingue entre mayúsculas y minúsculas y que le ayuda a administrar, filtrar y buscar un recurso compartido de archivos.
13. Elija Next (Siguiente). LaConfigurar cómo se almacenan los archivos en Amazon S3Se mostrará la página.
14. ParaClase de almacenamiento para objetos nuevos, elija una clase de almacenamiento para utilizarlo con los nuevos objetos creados en el bucket de Amazon S3:

    - Para almacenar los datos de objetos de acceso frecuente de forma redundante en varias zonas de disponibilidad que se encuentran distanciadas geográficamente, elijaS3 Standard. Para obtener más información acerca de la clase de almacenamiento estándar de S3, consulte.Clases de almacenamiento para objetos a los que se obtiene acceso con frecuenciaen laAmazon Simple Storage Service.
    - Para optimizar los costos de almacenamiento moviendo automáticamente los datos a la capa de acceso de almacenamiento más rentable, elijaS3 Intelligent-Tiering. Para obtener más información acerca de la clase de almacenamiento S3 Intelligent-Tiering, consulteClase de almacenamiento para optimizar automáticamente los objetos a los que se obtiene acceso con mucha y poca frecuenciaen laAmazon Simple Storage Service.
    - Para almacenar los datos de objetos a los que se accede con poca frecuencia de forma redundante en varias zonas de disponibilidad que se encuentran distanciadas geográficamente, elijaEstándar - Acceso poco frecuente de S3. Para obtener más información acerca de la clase de almacenamiento Estándar - Acceso poco común de S3, consulte.Clases de almacenamiento para objetos a los que se obtiene acceso con poca frecuenciaen laAmazon Simple Storage Service.
    - Para almacenar los datos de objetos a los que se accede con poca frecuencia en una única zona de disponibilidad, elijaÚnica zona - Acceso poco frecuente de S3. Para obtener más

información acerca de la clase de almacenamiento Único zona - Acceso poco común de S3, consulte.Clases de almacenamiento para objetos a los que se obtiene acceso con poca frecuenciaen laAmazon Simple Storage Service.

Para ayudar a supervisar la facturación de S3, utiliceAWS Trusted Advisor. Para obtener más información, consulteHerramientas de monitoreoen laAmazon Simple Storage Service.

15. En Object metadata (Metadatos de objetos), elija los metadatos que desea utilizar:

    - Para poder adivinar el tipo MIME de los objetos cargados en función de las extensiones de archivo, elijaAdivinar el tipo MIME.
    - Para dar control total al propietario del bucket de S3 que se mapea al recurso compartido de archivos NFS, elijaDar control total al propietario del bucket. Para obtener más información acerca del uso del recurso compartido de archivos para obtener acceso a objetos de un bucket perteneciente a otra cuenta, consulteUso de un recurso compartido de archivos para el acceso entre cuentas.
    - Si utiliza este recurso compartido de archivos en un bucket que requiere que el pago por los cargos de acceso lo realice el solicitante o el lector en lugar del propietario del bucket, elijaHabilitar pagos del solicitante. Para obtener más información, consulte Buckets de pago por solicitante.

16. ParaAcceder a su bucket de S3, elige elAWS Identity and Access Management(IAM) que desea que utilice la puerta de enlace de archivos para obtener acceso al bucket de Amazon S3:

    - Para habilitar la puerta de enlace de archivos para crear un nuevo rol de IAM y una política de acceso en su nombre, elijaCrear un nuevo rol de IAM. Esta opción no está disponible si el recurso compartido de archivos se conecta a Amazon S3 mediante un alias de punto de acceso.
    - Para seleccionar un rol de IAM existente y configurar la política de acceso manualmente, elijaUtilizar un rol de IAM existente. Debe utilizar esta opción si el recurso compartido de archivos se conecta a Amazon S3 mediante un alias de punto de acceso. En el navegadorRol de IAM, escriba el nombre de recurso de Amazon (ARN) para el rol utilizado para obtener acceso al bucket de. Para obtener información sobre los roles de IAM, consulteIAM rolesen laAWS Identity and Access ManagementGuía del usuario de.

Para obtener más información sobre el acceso al bucket de S3, consulte Concesión de acceso a un bucket de Amazon S3.

17. ParaCriptografía, elija el tipo de claves de cifrado que desea utilizar para cifrar los objetos que almacene la puerta de enlace de archivos en Amazon S3:

    - Para utilizar el cifrado del lado del servidor administrado con Amazon S3 (SSE-S3), elijaClaves administradas por S3 (SSE-S3).
    - Para utilizar el cifrado del lado del servidor administrado conAWS Key Management Service(SSE-KMS), elijaClaves administradas por KMS (SSE-KMS). En el navegadorClave principal, elija una existenteAWS KMS keyo eligeCreación de una nueva clave KMSpara crear una nueva clave KMS en laAWS Key Management Service(AWS KMS). Para obtener más información acerca deAWS KMS, consulte¿Qué es ?AWS Key Management Service?en laAWS Key Management ServiceGuía para desarrolladores.

    > **Note**
    >
    > Para especificar unAWS KMSclave con un alias que no aparece en la lista o para utilizar unAWS KMSclave de otroCuenta de AWS, debe utilizar elAWS Command Line Interface(AWS CLI). Para obtener más información, consulteCreateNFSFileShareen laAWSReferencia de la API de Storage.
    > No se admiten claves KMS asimétricas.

18. ElegirPróximopara configurar los ajustes de acceso a archivos.

Para configurar los valores de acceso a archivos

1. ParaClientes permitidos, especifique si desea permitir o restringir el acceso de cada cliente al recurso compartido de archivos. Proporcione la dirección IP o la notación CIDR de los clientes que desea permitir el acceso. Para obtener información acerca de los clientes de NFS compatibles, consulte Clientes de NFS compatibles con una gateway de archivos.
2. ParaOpciones de montaje, especifique las opciones que desee paraNivel de squashyExportar como.

   En Squash level (Nivel de agrupación), elija una de las siguientes opciones:

   - Todos los squash: El acceso de todos los usuarios se asigna al ID de usuario (UID) (65534) y al ID de grupo (GID) (65534).
   - Sin calabaza de raíz: El superusuario remoto (raíz) recibe acceso como usuario raíz.

- Squash raíz (predeterminado): El acceso del superusuario remoto (raíz) se asigna al UID (65534) y al GID (65534).

En Export as (Exportar como), elija una de las siguientes opciones:

- Lectura y escritura
- Solo lectura

> **Note**
>
> Para los recursos compartidos de archivos montados en un cliente Microsoft Windows, si lo deseaSolo lectura, es posible que aparezca un mensaje de error que indica que no se puede crear la carpeta. Puede hacer caso omiso del mensaje.

3. En File metadata defaults (Valores predeterminados de metadatos de archivos), puede editar los Directory permissions (Permisos de directorio), los File permissions (Permisos de archivo), el User ID (ID de usuario) y el Group ID (ID de grupo). Para obtener más información, consulte Edición de los valores predeterminados de los metadatos del recurso compartido del archivo NFS.
4. Elija Next (Siguiente).
5. Revise la configuración del recurso compartido de archivos y, a continuación, elijaAcabado.

   Una vez creado el recurso compartido de archivos NFS, puede consultar su configuración en la pestaña Details (Detalles).

Paso siguiente

Monte el recurso compartido de archivos NFS en el cliente

Creación de un recurso compartido de archivos SMB

Antes de crear un recurso compartido de archivos de bloque de mensajes del servidor (SMB), asegúrese de que configura los ajustes de seguridad de SMB para la gateway de archivos. También debe configurar el Microsoft Active Directory (AD) o el acceso de invitado para la autenticación. Un recurso compartido de archivos proporciona solo un tipo de acceso de SMB. Para obtener instrucciones, consulteEdición de la configuración de SMB para una puerta de enlace.

> **Note**
>
> Un recurso compartido de archivos SMB no funciona correctamente a menos que los puertos necesarios estén abiertos en el grupo de seguridad. Para obtener más información, consulte Requisitos de los puertos.

> **Note**
>
> Cuando un cliente SMB escribe un archivo en la puerta de enlace de archivos, la puerta de enlace de archivos carga los datos del archivo en Amazon S3 seguidos de sus metadatos (propiedad, marcas de tiempo, etc.). Al cargar los datos de 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 almacenan ambas versiones.
> Si cambia los metadatos de un archivo almacenado en la puerta de enlace de archivos, se crea un nuevo objeto S3 que reemplaza al objeto S3 existente. Este comportamiento es distinto del de editar un archivo en un sistema de archivos, en el que la edición de un archivo no da lugar a la creación de un nuevo archivo. Probar todas las operaciones de archivos que planea utilizar conAWSStorage Gateway para que comprenda cómo interactúa cada operación de archivos 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 carga datos desde la puerta de enlace de archivos. La carga de archivos desde la puerta de enlace de archivos a Amazon S3 cuando se habilita el control de versiones de S3 da como resultado al menos dos versiones de un objeto S3. Ciertos flujos de trabajo que incluyen archivos grandes y patrones de escritura de archivos, como las subidas de archivos que se realizan en varios pasos, pueden aumentar el número de versiones de objetos S3 almacenadas. Si la caché de puerta de enlace de archivos necesita liberar espacio debido a las altas velocidades de escritura de archivos, se pueden crear varias versiones de objetos de S3. Estos escenarios aumentan el almacenamiento de S3 si el control de versiones de S3 está habilitado y aumentan los costos de transferencia asociados con CRR. Pruebe todas las operaciones de archivos que planea utilizar con Storage Gateway para comprender cómo interactúa cada operación de archivos con el almacenamiento de Amazon S3.
> El uso de la utilidad Rsync con la puerta de enlace de archivos da lugar a la creación de archivos temporales en la caché y a la creación de objetos S3 temporales en Amazon S3. Esta situación produce cargos de eliminación temprana en las clases de almacenamiento

S3 Estándar - Acceso poco frecuente de S3 (S3 Standard-IA) y S3 Intelligent-Tiering (Capas inteligentes de S3).

Creación de un recurso compartido de archivos SMB

Para crear un recurso compartido de archivos SMB

1. Abra el iconoAWSStorage Gateway enhttps://console.aws.amazon.com/storagegateway/home/.
2. ElegirCreación de recurso compartido de archivospara abrirConfiguración de recurso compartido de archivos(Se ha creado el certificado).
3. ParaPortal, elija su Amazon S3 File Gateway de la lista.
4. ParaUbicación de Amazon S3, realice una de las siguientes operaciones:

   - Para conectar el recurso compartido de archivos directamente a un bucket de S3, elijaNombre del bucket de S3y, a continuación, introduzca el nombre del depósito y, opcionalmente, un nombre de prefijo para los objetos creados por el recurso compartido de archivos. La puerta de enlace utiliza este depósito para almacenar y recuperar archivos. Para obtener información acerca de cómo crear un nuevo bucket, consulte.¿Cómo se puede crear un bucket de S3?en laGuía del usuario de Amazon S3.
   - Para conectar el recurso compartido de archivos a un bucket de S3 a través de un punto de acceso, elijaPunto de acceso S3y, a continuación, introduzca el nombre del punto de acceso de S3 y, opcionalmente, un nombre de prefijo para los objetos creados por el recurso compartido de archivos. La política de bucket debe configurarse para delegar el control de acceso en el punto de acceso. Para obtener información acerca de los puntos de acceso, consulte.Administración del acceso a datos con puntos de acceso de Amazon S3yDelegar el control de acceso a los puntos de accesoen laGuía del usuario de Amazon S3.
   - Para conectar el recurso compartido de archivos a un bucket de S3 a través de un alias de punto de acceso, elijaAlias de punto de acceso S3y, a continuación, introduzca el nombre del alias del punto de acceso de S3 y, opcionalmente, un nombre de prefijo para los objetos creados por el recurso compartido de archivos. Si elige esta opción, la puerta de enlace de archivos no puede crear una nuevaAWS Identity and Access Management(IAM) y política de acceso en su nombre. Debe seleccionar un rol de IAM existente y configurar una política de acceso en elAcceder a su bucket de S3sección que sigue. Para obtener más información acerca de los alias de puntos de acceso, consulte.Uso de un alias estilo cubo para el punto de accesoen laGuía del usuario de Amazon S3.

> **Note**
>
> - Si introduce un nombre de prefijo o elige conectarse a través de un punto de acceso o alias de punto de acceso, debe introducir un nombre de recurso compartido de archivos.
> - El nombre del prefijo debe terminar con una barra diagonal: (/).
> - Una vez creado el recurso compartido de archivos, el nombre del prefijo no se puede modificar ni eliminar.
> - Para obtener información acerca del uso de nombres de prefijo, consulte.Organizar objetos con prefijosen laGuía del usuario de Amazon S3.

5. ParaRegión de AWS, elige elRegión de AWSdel bucket de S3.
6. ParaNombre del recurso compartido de archivos, escriba un nombre para el recurso compartido de archivos. El nombre predeterminado es el nombre del bucket de S3 o el nombre del punto de acceso.

> **Note**
>
> - Si ha introducido un nombre de prefijo o ha optado por conectarse a través de un punto de acceso o alias de punto de acceso, debe introducir un nombre de recurso compartido de archivos.
> - Una vez creado el recurso compartido de archivos, no se puede eliminar el nombre del recurso compartido de archivos.

7. (Opcional) ParaAWS PrivateLinkpara S3, realice una de las siguientes opciones:

    1. Para configurar el recurso compartido de archivos para conectarse a S3 a través de un punto de enlace de interfaz de su nube virtual privada (VPC) con tecnología deAWS PrivateLink, eligeUsar punto de enlace de la VPC.
    2. Para identificar el extremo de la interfaz de la VPC por el que desea que se conecte el recurso compartido de archivos, elija uno de los dosID de punto de enlace de la VPCoNombre DNS del punto de enlace de VPCy, a continuación, proporcione la información requerida en el campo correspondiente.

> **Note**
>
> - Este paso es necesario si el recurso compartido de archivos se conecta a S3 a través de un punto de acceso de VPC o a través de un alias asociado a un punto de acceso de VPC.
> - Conexión de recurso compartido de archivos medianteAWS PrivateLinkno se admiten en las puertas de enlace FIPS.
> - Para obtener información sobreAWS PrivateLink, consulteAWS PrivateLinkpara Amazon S3en laAmazon Simple Storage Service.

8. En Access Objects using (Obtener acceso a los objetos mediante), elija Server Message Block (SMB).
9. En Audit logs (Registros de auditoría), elija una de las siguientes opciones:

   - Para desactivar el registro de, elijaDisable logging (Deshabilitar el registro).
   - Para crear un nuevo registro de auditoría, elijaCreación de un nuevo grupo de registros.
   - Para utilizar un grupo de registros existente, elijaUse un grupo de registros existentey, a continuación, elija un registro de auditoría de la lista.

   Para obtener más información acerca de auditorías, consulte Descripción de los registros de auditoría de file gateway.
10. ParaActualización automatizada de la caché desde S3, eligeEstablecer intervalo de actualizacióny, a continuación, establezca la hora 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. Una vez transcurrido el intervalo TTL, el acceso al directorio hace que la puerta de enlace de archivos actualice primero el contenido del directorio desde el bucket de Amazon S3.
11. ParaNotificación de carga de archivo, eligeTiempo de ajuste (segundos)que se le notificará cuando la puerta de enlace de archivos haya cargado completamente un archivo en S3. Establecimiento de la propiedad deTiempo de asentamientoen segundos para controlar el número de segundos que se espera después del último punto en el tiempo que un cliente escribió en un archivo antes de generar un`ObjectUploaded`Notificación de. Dado que los clientes pueden realizar muchas escrituras pequeñas en archivos, es mejor configurar este

parámetro durante el mayor tiempo posible para evitar generar varias notificaciones para el mismo archivo en un período de tiempo reducido. Para obtener más información, consulte Obtener notificación de subida de archivos.

> **Note**
>
> Esta configuración no afecta a la sincronización de la carga del objeto a S3, solo en el momento de la notificación.

12. (Opcional) En elEtiquetassección, elijaAñadir nueva etiquetay, a continuación, introduzca una clave y un valor para añadir etiquetas al recurso compartido de archivos. Una etiqueta es un par clave-valor que distingue entre mayúsculas y minúsculas y que le ayuda a administrar, filtrar y buscar un recurso compartido de archivos.
13. Elija Next (Siguiente). LaConfiguración de almacenamiento de Amazon S3Se mostrará la página.
14. ParaClase de almacenamiento para objetos nuevos, elija una clase de almacenamiento para utilizarlo con los nuevos objetos creados en el bucket de Amazon S3:

    - Para almacenar los datos de objetos de acceso frecuente de forma redundante en varias zonas de disponibilidad que se encuentran distanciadas geográficamente, elijaS3 Standard. Para obtener más información acerca de la clase de almacenamiento estándar de S3, consulte.Clases de almacenamiento para objetos a los que se obtiene acceso con frecuenciaen laAmazon Simple Storage Service Service.
    - Para optimizar los costos de almacenamiento moviendo automáticamente los datos a la capa de acceso de almacenamiento más rentable, elijaS3 Intelligent-Tiering. Para obtener más información acerca de la clase de almacenamiento S3 Intelligent-Tiering, consulteClase de almacenamiento para optimizar automáticamente los objetos a los que se obtiene acceso con mucha y poca frecuenciaen laAmazon Simple Storage Service Service.
    - Para almacenar los datos de objetos a los que se accede con poca frecuencia de forma redundante en varias zonas de disponibilidad que se encuentran distanciadas geográficamente, elijaEstándar - Acceso poco frecuente de S3. Para obtener más información acerca de la clase de almacenamiento Estándar - Acceso poco común de S3, consulte.Clases de almacenamiento para objetos a los que se obtiene acceso con poca frecuenciaen laAmazon Simple Storage Service.
    - Para almacenar los datos de objetos a los que se accede con poca frecuencia en una única zona de disponibilidad, elijaÚnica zona - Acceso poco frecuente de S3. Para obtener más

información acerca de la clase de almacenamiento Único zona - Acceso poco común de S3, consulte.Clases de almacenamiento para objetos a los que se obtiene acceso con poca frecuenciaen laAmazon Simple Storage Service.

Para ayudar a supervisar la facturación de S3, utiliceAWS Trusted Advisor. Para obtener más información, consulteHerramientas de monitoreoen laAmazon Simple Storage Service.

15. En Object metadata (Metadatos de objetos), elija los metadatos que desea utilizar:

    - Para poder adivinar el tipo MIME de los objetos cargados en función de las extensiones de archivo, elijaAdivinar el tipo MIME.
    - Para dar control total al propietario del bucket de S3 que se mapea al recurso compartido de archivos SMB, elijaDar control total al propietario del bucket. Para obtener más información acerca del uso del recurso compartido de archivos para obtener acceso a objetos de un bucket perteneciente a otra cuenta, consulteUso de un recurso compartido de archivos para el acceso entre cuentas.
    - Para dar control total al propietario del bucket de S3 que se mapea al recurso compartido de archivos SMB, elijaHabilitar pagos del solicitante. Para obtener más información, consulte Buckets de pago por solicitante.

16. ParaAcceder a su bucket de S3, elige elAWS Identity and Access Management(IAM) que desea que utilice la puerta de enlace de archivos para obtener acceso al bucket de Amazon S3:

    - Para habilitar la puerta de enlace de archivos para crear un nuevo rol de IAM y una política de acceso en su nombre, elijaCrear un nuevo rol de IAM. Esta opción no está disponible si el recurso compartido de archivos se conecta a Amazon S3 mediante un alias de punto de acceso.
    - Para seleccionar un rol de IAM existente y configurar la política de acceso manualmente, elijaUtilizar un rol de IAM existente. Debe utilizar esta opción si el recurso compartido de archivos se conecta a Amazon S3 mediante un alias de punto de acceso. En el navegadorRol de IAM, escriba el nombre de recurso de Amazon (ARN) para el rol utilizado para obtener acceso al bucket de. Para obtener información sobre los roles de IAM, consulteIAM rolesen laAWS Identity and Access ManagementGuía del usuario de.

    Para obtener más información sobre el acceso al bucket de S3, consulte Concesión de acceso a un bucket de Amazon S3.

17. ParaCriptografía, elija el tipo de claves de cifrado que desea utilizar para cifrar los objetos que almacene la puerta de enlace de archivos en Amazon S3:

    - Para utilizar el cifrado del lado del servidor administrado con Amazon S3 (SSE-S3), elijaClaves administradas por S3 (SSE-S3).
    - Para utilizar el cifrado del lado del servidor administrado conAWS Key Management Service(SSE-KMS), elijaClaves administradas por KMS (SSE-KMS). En el navegadorClave principal, elija una existenteAWS KMS keyo eligeCreación de una nueva clave KMSpara crear una nueva clave KMS en laAWS Key Management Service(AWS KMS). Para obtener más información acerca deAWS KMS, consulte¿Qué es ?AWS Key Management Service?en laAWS Key Management ServiceGuía para desarrolladores.

    > **Note**
    >
    > Para especificar unAWS KMSclave con un alias que no aparece en la lista o para utilizar unAWS KMSclave de otroCuenta de AWS, debe utilizar elAWS Command Line Interface(AWS CLI). Para obtener más información, consulteCreateNFSFileShareen laAWSReferencia de la API de Storage.
    > No se admiten claves KMS asimétricas.

18. Elija Next (Siguiente). LaConfiguración del acceso a archivosSe mostrará la página.
19. ParaMétodo de autenticación, elija el método de autenticación que desee utilizar.

    - Para utilizar su Microsoft AD corporativo para autenticar el acceso de los usuarios al recurso compartido de archivos SMB, elijaActive Directory. La puerta de enlace de archivos debe estar unida a un dominio.
    - Para proporcionar acceso solo a los huéspedes, elijaAcceso de invitados. Si selecciona este método de autenticación, la puerta de enlace de archivos no tiene que formar parte de un dominio de Microsoft AD. También puede utilizar una gateway de archivos que sea miembro del dominio de AD para crear recursos compartidos de archivos con acceso de invitado. Debe establecer una contraseña de invitado para su servidor SMB en el campo correspondiente.

    > **Note**
    >
    > Ambos tipos de acceso están disponibles al mismo tiempo.

20. En el navegadorConfiguración del recurso compartido de SMB, elija la configuración.

En Export as (Exportar como), elija una de las siguientes opciones:

- Lectura y escritura (el valor predeterminado)
- Solo lectura

> **Note**
>
> Para los recursos compartidos de archivos montados en un cliente Microsoft Windows, si lo deseaSolo lectura, es posible que aparezca un mensaje de error que indica que no se puede crear la carpeta. Puede hacer caso omiso del mensaje.

Para File/directory access controlled by (Acceso al archivo/directorio controlado por) seleccione una de las siguientes opciones:

- Para establecer permisos específicos en los archivos y carpetas de un recurso compartido de archivos SMB, elijaLista de control de acceso de Windows. Para obtener más información, consulte Uso de las ACL de Microsoft Windows para controlar el acceso a un recurso compartido de archivos SMB.
- Para utilizar los permisos POSIX para controlar el acceso a los archivos y directorios almacenados en un recurso compartido de archivos NFS o SMB, elijaPermisos POSIX.

Si el método de autenticación esActive Directory, paraUsuarios/grupos administradores, introduzca una lista separada por comas de usuarios y grupos de AD. Haga esto si desea que el usuario administrador tenga privilegios para actualizar las listas de control de acceso (ACL) en todos los archivos y carpetas del recurso compartido de archivos. Estos usuarios y grupos cuentan con derechos de administrador para el recurso compartido de archivos. Un grupo debe tener un prefijo con la@carácter, por ejemplo,`@group1`.

ParaSensibilidad de mayúsculas y minúsculas, elija una de las siguientes opciones:

- Para permitir que la puerta de enlace controle la sensibilidad entre mayúsculas y minúsCliente especificado.
- Para permitir al cliente controlar la sensibilidad entre mayúsculas y minúsculas, elijaFuerza la sensibilidad entre mayús.

> **Note**
>
> - Si se selecciona, esta configuración se aplica inmediatamente a las nuevas conexiones de cliente SMB. Las conexiones de cliente SMB existentes deben desconectarse del recurso compartido de archivos y volver a conectarse para que la configuración surta efecto.

ParaEnumeración basada en acceso, elija una de las siguientes opciones:

- Para que los archivos y carpetas del recurso compartido sean visibles solo para los usuarios que tienen acceso de lectura, elijaDeshabilitado para archivos y directorios.
- Para que los archivos y carpetas del recurso compartido sean visibles para todos los usuarios durante la enumeración de directorios, elijaHabilitado para archivos y directorios.

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

ParaBloqueo oportunista (oplock), elija una de las siguientes opciones:

- Para permitir que el recurso compartido de archivos utilice el bloqueo oportunista para optimizar la estrategia de almacenamiento en búfer de archivos, elijaEnabled (Habilitado). En la mayoría de los casos, habilitar el bloqueo oportunista mejora el rendimiento, especialmente en lo que respecta a los menús contextuales de Windows.
- Para evitar el uso del bloqueo oportunista, elijaDiscapacitado. Si varios clientes Windows de su entorno editan con frecuencia los mismos archivos simultáneamente, deshabilitar el bloqueo oportunista a veces puede mejorar el rendimiento.

> **Note**
>
> No se recomienda habilitar el bloqueo oportunista de recursos compartidos que distinguen mayúsculas de minúsculas para cargas de trabajo que implican acceso a archivos con el mismo nombre en distintos casos.

21. (Opcional) En elAcceso compartido de archivos de usuarios y grupos, elija la configuración.

    ParaUsuarios y grupos permitidos, eligeAñada el usuario permitidooAñada un grupo permitidoe introduzca un usuario o grupo de AD que desee permitir el acceso compartido de archivos. Repita este proceso para permitir tantos usuarios y grupos como sea necesario.

    ParaUsuarios y grupos denegados, eligeAñadir usuario denegadooAñadir grupo denegadoe introduzca un usuario o grupo de AD que desee denegar el acceso compartido de archivos. Repita este proceso para denegar tantos usuarios y grupos como sea necesario.

    > **Note**
    >
    > LaAcceso compartido de archivos de usuarios y gruposla sección aparece solo siActive Directoryestá seleccionado.
    > 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 especifica ningún usuario o grupo permitidos o denegados, cualquier usuario autenticado de AD puede exportar el recurso compartido de archivos.

22. Elija Next (Siguiente).
23. Revise la configuración del recurso compartido de archivos y, a continuación, elijaAcabado.

    Una vez creado el recurso compartido de archivos SMB, puede consultar su configuración en la pestaña Details (Detalles).

Paso siguiente

Monte el recurso compartido de archivos SMB en el cliente

Monte y use el recurso compartido de archivos

A continuación, encontrará instrucciones sobre cómo montar el recurso compartido de archivos en el cliente, utilizarlo, probar la gateway de archivos y limpiar los recursos según sea necesario. Para obtener más información sobre los clientes de Network File System (NFS) compatibles, consulte Clientes de NFS compatibles con una gateway de archivos. Para obtener más información sobre los clientes de Service Message Block (SMB) compatibles, consulte Clientes de SMB compatibles con una gateway de archivos.

Puede encontrar ejemplos de comandos para montar el recurso compartido de archivos en la AWS Management Console. En las secciones siguientes, puede encontrar información sobre cómo montar el recurso compartido de archivos en el cliente, utilizarlo, probar la gateway de archivos y limpiar los recursos según sea necesario.

Temas

Monte el recurso compartido de archivos NFS en el cliente

Ahora, monte el recurso compartido de archivos NFS en una unidad del cliente y asígnelo al 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 [Your gateway VM IP address]:/[S3
bucket name] [mount path on your client]
```

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

```
sudo mount_nfs -o vers=3,nolock,rwsize=65536,hard -v [Your gateway VM
IP address]:/[S3 bucket name] [mount path on your client]
```

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

```
mount –o nolock -o mtype=hard [Your gateway VM IP address]:/[S3 bucket
name] [Drive letter on your windows client]
```

Por ejemplo, suponga que en un cliente Windows la dirección IP de la máquina virtual es 123.123.1.2 y su bucket de Amazon S3 es`test-bucket`. 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-bucket T:
```

> **Note**
>
> Cuando monte recursos compartidos de archivos, tenga en cuenta lo siguiente:
>
> - Puede ocurrir que una carpeta y un objeto estén en un bucket de Amazon S3 y tengan el mismo nombre. En ese caso, si el nombre del objeto no contiene una barra final, solo la carpeta está visible en una gateway de archivos. Por ejemplo, si un bucket contiene un objeto denominado`testotest/`y una carpeta con el nombre`test/test1`, solo`test/ytest/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.
> - De forma predeterminada, Windows utiliza un montaje flexible para el recurso compartido NFS. Los montajes flexibles agotan el tiempo de espera con más facilidad si existen problemas de conexión. Recomendamos utilizar un montaje forzado, ya que es más seguro y conserva mejor los datos. El comando de montaje flexible omite el conmutador **`-o mtype=hard`**. El comando de montaje forzado de Windows utiliza el conmutador `-o mtype=hard`.
> - 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

Probar la puerta de enlace de archivos S3

Monte el recurso compartido de archivos SMB en el cliente

Ahora, monte el recurso compartido de archivos SMB y asígnelo a una unidad a la que el cliente pueda obtener acceso. La sección File Gateway de la consola muestra los comandos de montaje compatibles que se pueden utilizar para los clientes de 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 (`cmdkeyynet use`) — Utilice el símbolo del sistema para montar el recurso compartido de archivos. Almacena tus credenciales con`cmdkeyy`, a continuación, monte la unidad con`net use`Inclusión del`/persistent:yesy/savecred`Si desea que la conexión se mantenga tras los reinicios del sistema. Los comandos específicos que utilice serán diferentes según si desea montar la unidad para el acceso de Microsoft Active Directory (AD) o para el acceso de usuario invitado. A continuación se ofrecen ejemplos.
- Explorador de archivos (Map Network Drive): utilice el Explorador de archivos de Windows para montar el recurso compartido de archivos. Configure los ajustes para especificar si desea que la conexión se mantenga en los reinicios del sistema y solicite credenciales de red.
- Script de PowerShell: cree un script de PowerShell personalizado para montar el recurso compartido de archivos. Según los parámetros especificados en el script, la conexión puede ser persistente en los reinicios del sistema y el recurso compartido puede ser 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 que dispone de la contraseña de la cuenta de 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 el símbolo del sistema:

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. Escriba lo siguiente en el símbolo de sistema 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 nombre de usuario y contraseña específica mediante el símbolo del sistema:

1. Asegúrese de que la cuenta de usuario tiene acceso al recurso compartido de archivos SMB antes de montarlo en el sistema.
2. Escriba lo siguiente en el símbolo del sistema para guardar las credenciales de usuario en el Administrador de credenciales de Windows:

   ```
   cmdkey /add:GatewayIPAddress /user:DomainName\UserName /pass:Password
   ```
3. Escriba lo siguiente en el símbolo de sistema 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 el símbolo del sistema:

1. Asegúrese de que dispone de la contraseña de la cuenta de usuario invitado antes de montar el recurso compartido de archivos.
2. Escriba lo siguiente en el símbolo del sistema para guardar las credenciales de invitado en el Administrador de credenciales de Windows:

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

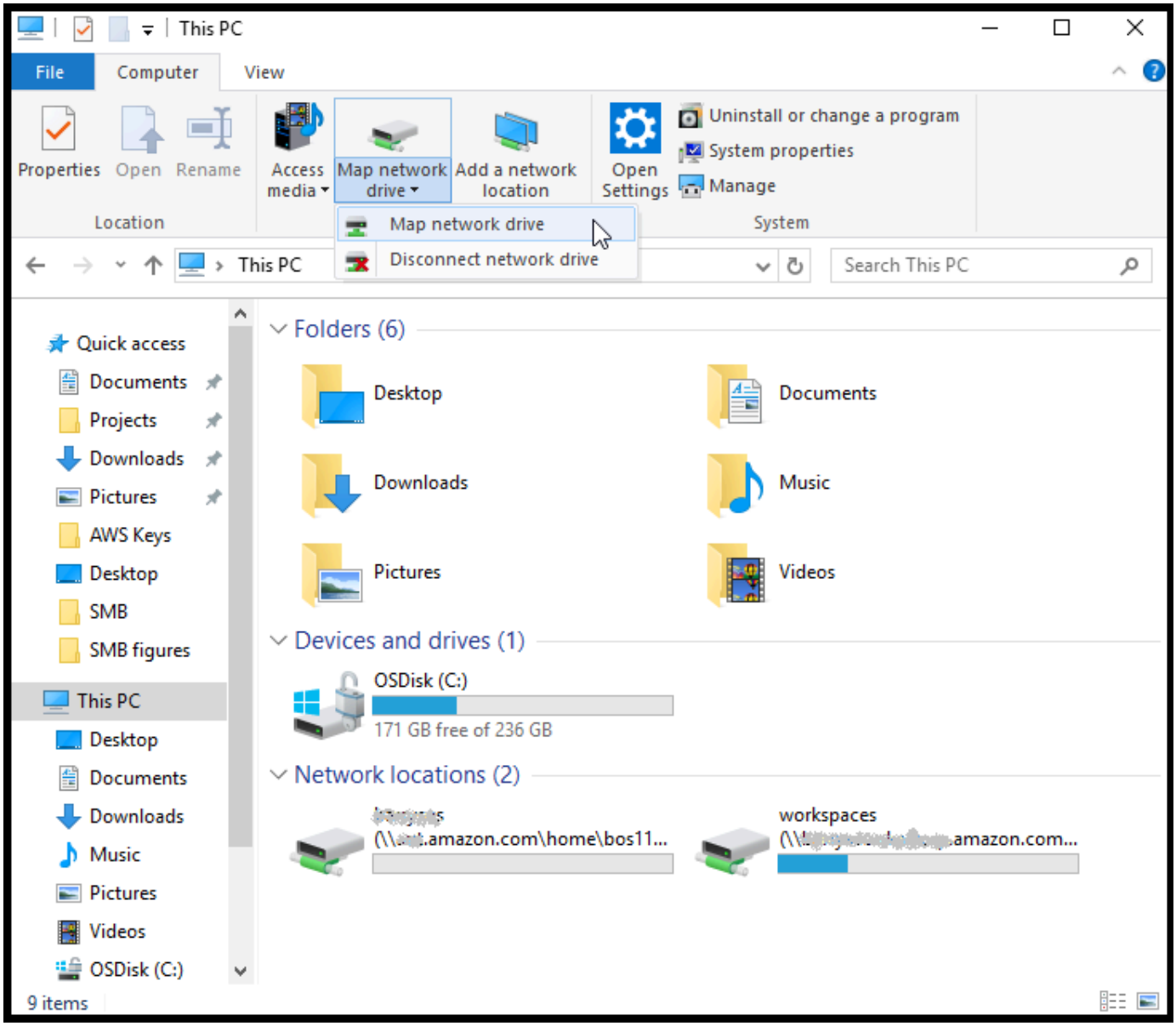
3. Escriba lo siguiente en el símbolo del sistema.

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

> **Note**
>
> Cuando monte recursos compartidos de archivos, tenga en cuenta lo siguiente:
>
> - Puede ocurrir que una carpeta y un objeto estén en un bucket de Amazon S3 y tengan el mismo nombre. En ese caso, si el nombre del objeto no contiene una barra final, solo la carpeta está visible en una gateway de archivos. Por ejemplo, si un bucket contiene un objeto denominado`testotest/`y una carpeta con el nombre`test/test1`, solo`test/ytest/test1`están visibles en una puerta de enlace de archivos.
> - A menos que configure la conexión de recursos compartidos de archivos para guardar las credenciales de usuario y persistir en 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, seleccione This PC y elija Map Network Drive en Map Network Drive en la pestaña Computer, tal y como se muestra en la siguiente captura de pantalla.



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.

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 enhttps://console.aws.amazon.com/storagegateway/home.
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.
   - Elija Edit allowed/denied users para agregar o eliminar usuarios o grupos y, a continuación, escriba los usuarios y grupos permitidos y denegados en los cuadros Allowed Users, Denied Users, Allowed Groups y Denied Groups. Utilice los botones Add Entry para crear nuevos derechos de acceso y el botón (X) para eliminar el acceso.
5. Cuando haya terminado, elija Save.

   Al introducir usuarios y grupos permitidos está creando una lista de permitidos. Sin una lista de permisos, todos los usuarios de Microsoft AD autenticados pueden obtener acceso al recurso compartido de archivos SMB. Los usuarios y grupos que están marcados como denegados se agregan a una lista de denegación y no pueden obtener acceso al recurso compartido de archivos SMB. En los casos en los que un usuario o grupo está tanto en la lista de denegación como en la lista de permitidos, la lista de denegación tiene prioridad.

   Puede habilitar listas de control de acceso (ACL) en un recurso compartido de archivos SMB. Para obtener información sobre cómo habilitar las ACL, consulte Uso de las ACL de Microsoft Windows para controlar el acceso a un recurso compartido de archivos SMB.

Paso siguiente

Probar la puerta de enlace de archivos S3

Trabajo con recursos compartidos de archivos en un bucket con objetos preexistentes

Puede utilizar tanto NFS como SMB para exportar un recurso compartido de archivos en un bucket de Amazon S3 con objetos creados fuera de la gateway de archivos. 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 los archivos se vuelven a escribir en un bucket de Amazon S3, asumen las propiedades y los derechos de acceso que se les conceden.

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 “Refrescar objetos en el bucket de Amazon S3”.

> **Note**
>
> No recomendamos que haya varios escritores para un bucket de Amazon S3. Si los tiene, asegúrese de leer la sección «¿Puedo permitir que haya varios escritores en mi bucket de Amazon S3?» en laPreguntas frecuentes 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 Gestionar el Amazon S3 File Gateway.

Para SMB, se puede exportar un recurso compartido con acceso de invitado o mediante Microsoft AD para 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)

Probar la puerta de enlace de archivos S3

Puede copiar archivos y carpetas en la unidad asignada. Los archivos se cargarán de forma automática en el bucket de Amazon S3.

Para cargar archivos desde el 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, vaya al bucket asignado. Deberían aparecer los archivos y las carpetas que copió en el bucket de Amazon S3 especificado.

   El recurso compartido de archivos creado en elUso compartido de archivosen la pestañaAWSConsola de administración Storage Gateway

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

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

Tenga en cuenta estas consideraciones sobre el funcionamiento de las puertas de enlace de archivos en 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, utilizando la misma sintaxis de 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.

Paso siguiente

[¿Qué tengo que hacer ahora?]

¿Qué tengo que hacer ahora?

En las secciones anteriores, creó y empezó a usar una gateway de archivos, incluido el montaje de un recurso compartido de archivos y la comprobación de la configuración.

Otras secciones de esta guía incluyen información sobre cómo hacer lo siguiente:

- Para administrar la gateway de archivos, consulte Gestionar el Amazon S3 File Gateway.
- Para optimizar la gateway de archivos, consulte Optimización del rendimiento de la gateway.
- Para resolver problemas con la gateway, consulte Solución de problemas de la gateway.
- Para obtener información sobre las métricas de Storage Gateway y cómo monitorizar el rendimiento de la gateway, consulte.

Limpieza de los recursos innecesarios

Si creó la gateway como un ejemplo de un ejercicio o una prueba, puede ser conveniente eliminarla para evitar incurrir en gastos innecesarios o inesperados.

Para eliminar los recursos innecesarios

1. A menos que planee seguir utilizando la gateway, elimínela. Para obtener más información, consulte Eliminación de la gateway mediante el uso de la consola de AWS Storage Gateway y eliminación de los recursos asociados.
2. Elimine la máquina virtual de Storage Gateway desde el host on-premise. Si creó su gateway en una instancia Amazon EC2, termine la instancia.

Activar una gateway en una virtual private cloud

Puede crear una conexión privada entre su dispositivo de software local y una infraestructura de almacenamiento basada en la nube. Puede utilizar entonces el dispositivo de software para transferir datos aAWSAlmacenamiento sin que su puerta de enlace se comunique conAWSservicios de almacenamiento a través de la red de Internet pública. Con el servicio Amazon VPC, puede iniciarAWSrecursos de una red virtual personalizada. Puede utilizar una Virtual Private Cloud (VPC) para controlar la configuración de red, como el rango de direcciones IP, las subredes, las tablas de ruteo y las gateways de red. Para obtener más información acerca de las VPC, consulte¿Qué es Amazon VPC?en laAmazon VPC User Guide.

Para utilizar una gateway con punto de enlace de la VPC de Storage Gateway en su VPC, haga lo siguiente:

- Utilice la consola de la VPC para crear un punto de enlace de la VPC para Storage Gateway y obtener el ID de punto de enlace de la VPC. Especifique este ID de endpoint de VPC al crear y activar la puerta de enlace.
- Si está activando una gateway de archivos, cree un punto de enlace de la VPC para Amazon S3. Especifique este extremo de VPC cuando cree recursos compartidos de archivos para la puerta de enlace.
- Si va a activar una gateway de archivos, configure un proxy HTTP y configúrelo en la consola local de la máquina virtual de la gateway de archivos. Necesita este proxy para gateways de archivos en las instalaciones basadas en hipervisor, como las basadas en VMware, Microsoft HyperV y máquina virtual de Linux basada en el kernel (KVM). En estos casos, necesita el proxy para habilitar los puntos de enlace privados de Amazon S3 de de desde fuera de su VPC. Para obtener información acerca de cómo configurar un proxy HTTP, consulte Configuración de un proxy HTTP

> **Note**
>
> La gateway se tiene que activar en la misma región en la que se creó el punto de enlace de la VPC.
>
> En el caso de la gateway de archivos, el almacenamiento de Amazon S3 configurado para el archivo compartido debe estar en la misma región en la que creó el punto de enlace de la VPC para Amazon S3.

Temas

Crear un punto de enlace de la VPC para Storage Gateway

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

Para crear un punto de enlace de la VPC para Storage Gateway

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon VPC 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 páginaCreación de un punto de enlacepágina, elijaAWSServiciosparaCategoría 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 Create endpoint. 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 sección DNS Names (Nombres de DNS), utilice el primer nombre de DNS que no especifique una zona de disponibilidad. El nombre de la DNS tiene un aspecto similar a este: `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

Ahora que ha creado un punto de enlace de la VPC, puede crear su gateway.

> **Important**
>
> Si está creando una gateway de archivos, tiene que crear también un punto de enlace para Amazon S3. Siga los mismo pasos que se indican en la sección anterior Para crear un punto de enlace de la VPC para Storage Gateway, pero elija`com.amazonaws.us-east-2.s3`en Nombre de servicio en su lugar. A continuación, seleccione la tabla de enrutamiento a la que desea asociar el punto de enlace de S3 en vez del grupo de seguridad/subret. Para obtener instrucciones, consulteCreación de un punto de enlace de gateway.

Configuración y configuración de un proxy HTTP (solo puertas de enlace de archivos locales)

Si va a activar una gateway de archivos, tiene que configurar un proxy HTTP y ajustarlo en la consola local de la máquina virtual de la gateway de archivos. Este proxy es necesario para una gateway de archivos local para acceder a los puntos de enlace privados de Amazon S3 desde fuera de su VPC. Si ya tiene un proxy HTTP en Amazon EC2, puede utilizarlo. Sin embargo, tiene que verificar que todos los siguientes puertos TCP estén permitidos en su grupo de seguridad:

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031

- TCP 2222

Si no tiene un proxy Amazon EC2, utilice el siguiente procedimiento para configurar y configurar un proxy HTTP de.

Para configurar un servidor proxy

1. Lance una AMI de Amazon EC2 Linux. Se recomienda utilizar una familia de instancias, que es una red optimizada como c5n.large.
2. Utilice el siguiente comando para instalar squid: **`sudo yum install squid`**. Esto crea un archivo de configuración predeterminado en`/etc/squid/squid.conf`.
3. Reemplace el contenido del archivo de configuración con lo siguiente:

```
#
# Recommended minimum configuration:
#

# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
acl localnet src 10.0.0.0/8              # RFC1918 possible internal network
acl localnet src 172.16.0.0/12       # RFC1918 possible internal network
acl localnet src 192.168.0.0/16    # RFC1918 possible internal network
acl localnet src fc00::/7       # RFC 4193 local private network range
acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged) machines

acl SSL_ports port 443
acl SSL_ports port 1026
acl SSL_ports port 1027
acl SSL_ports port 1028
acl SSL_ports port 1031
acl SSL_ports port 2222
acl CONNECT method CONNECT

#
# Recommended minimum Access Permission configuration:
#
# Deny requests to certain unsafe ports
http_access deny !SSL_ports

# Deny CONNECT to other than secure SSL ports
```

```
http_access deny CONNECT !SSL_ports

# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localnet
http_access allow localhost

# And finally deny all other access to this proxy
http_access deny all

# Squid normally listens to port 3128
http_port 3128

# Leave coredumps in the first cache dir
coredump_dir /var/spool/squid

#
# Add any of your own refresh_pattern entries above these.
#
refresh_pattern ^ftp:                    1440       20%        10080
refresh_pattern ^gopher:            1440       0%          1440
refresh_pattern -i (/cgi-bin/|\?) 0             0%          0
refresh_pattern .                              0              20%        4320
```

4. Si no tiene que bloquear el servidor proxy ni hacer ningún cambio, habilítelo e inícielo utilizando los siguientes comandos. Estos comandos iniciarán el servidor cuando arranque.

```
sudo chkconfig squid on
sudo service squid start
```

Configure ahora el proxy HTTP de Storage Gateway para utilizarlo. Al configurar la gateway para utilizar un proxy, use el puerto 3128 de Squid predeterminado. El archivo squid.conf que se genera abarca los siguientes puertos TCP necesarios de forma predeterminada:

- TCP 443
- TCP 1026

- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

Para usar la consola local de la máquina virtual para configurar el proxy HTTP

1. Inicie sesión en la consola local de VM de la gateway. Para obtener información sobre cómo iniciar sesión, consulte Inicio de sesión en la consola local de la gateway de archivos.
2. En el menú principal, elija Configure HTTP proxy (Configurar proxy HTTP).
3. En el menú Configuration (Configuración), elija Configure HTTP proxy (Configurar proxy HTTP).
4. Facilite el nombre del host y el puerto del servidor proxy.

Para obtener información detallada acerca de cómo configurar un proxy HTTP, consulte Configuración de un proxy HTTP.

Permitir tráfico a los puertos requeridos en el proxy HTTP

Si utiliza un proxy HTTP, asegúrese de permitir el tráfico desde Storage Gateway a los destinos y puertos enumerados a continuación.

Cuando Storage Gateway se está comunicando a través de los puntos de enlace públicos, se comunica con los siguientes servicios de Storage Gateway.

```
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
storagegateway.region.amazonaws.com:443 (Required for making API calls)
s3.region.amazonaws.com (Required only for File Gateway)
```

> **Important**
>
> En función de la puerta de enlaceAWSRegión, sustituir*región*en el punto de enlace con la cadena de región correspondiente. Por ejemplo, si crea una gateway de la región de

EE. UU. Oeste (Oregón), el punto de enlace tendrá este aspecto:`storagegateway.us-west-2.amazonaws.com:443`.

Cuando Storage Gateway se está comunicando a través del punto de enlace de la VPC, se comunica con elAWSservicios a través de varios puertos en el punto de enlace de la VPC de Storage Gateway y en el puerto 443 en el punto de enlace privado de Amazon S3.

- Puertos TCP en el punto de enlace de la VPC de la gateway de almacenamiento.
  - 443, 1026, 1027, 1028, 1031 y 2222
- Puerto TPC en el punto de enlace privado de S3
  - 443

Gestionar el Amazon S3 File Gateway

A continuación, encontrará información acerca de cómo administrar los recursos de Amazon S3 File Gateway.

Temas

Añada un recurso compartido de archivos

Una vez que la gateway de archivos de S3 esté activada y en funcionamiento, puede agregar recursos compartidos de archivos adicionales y conceder acceso a buckets de Amazon S3. Cubos a los que puede conceder acceso para incluir los buckets en otroCuenta de AWSque el recurso compartido de archivos. Para obtener información sobre cómo agregar un recurso compartido de archivos, consulte Creación de un recurso compartido de archivos.

Temas

Concesión de acceso a un bucket de Amazon S3

Al crear un recurso compartido de archivos, la puerta de enlace de archivos requiere acceso para cargar archivos en el depósito de Amazon S3 y realizar acciones en cualquier punto de acceso o endpoints de nube privada virtual (VPC) que utilice para conectarse al bucket. Para conceder este acceso, la puerta de enlace de archivos asume unAWS 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, el bucket de S3 y cualquier punto de acceso asociado o endpoints de VPC deben tener una política de acceso que permita el rol de IAM para obtener acceso a ellos.

Puede crear el rol y la política de acceso manualmente o dejar que su gateway de archivos lo haga. Si su gateway de archivos crea la política, contendrá una lista de acciones de S3. Para obtener más información acerca de los roles de y permisos de, consulteCreación de un rol para delegar permisos a unServicio de AWSen laIAM User Guide.

El ejemplo siguiente es una política de confianza que permite que su gateway de archivos adopte un rol de IAM.

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

Si no desea que su gateway de archivos cree una política en su nombre, puede crear la suya propia y adjúntela al recurso compartido de archivos. Para obtener más información acerca de cómo hacerlo, consulte Creación de un recurso compartido de archivos.

La siguiente política de ejemplo permite que su gateway de archivos realice todas las acciones de Amazon S3 que aparecen 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 `TestBucket`. La segunda parte permite las acciones que se muestran en todos los objetos de `TestBucket`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:GetAccelerateConfiguration",
                "s3:GetBucketLocation",
                "s3:GetBucketVersioning",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:ListBucketMultipartUploads"
            ],
            "Resource": "arn:aws:s3:::TestBucket",
            "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:::TestBucket/*",
            "Effect": "Allow"
        }
    ]
}
```

La siguiente política de ejemplo es similar a la anterior, pero permite que la puerta de enlace de archivos realice las acciones necesarias para acceder a un bucket a través de un punto de acceso.

```
{
    "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-1:123456789:accesspoint/
TestAccessPointName/*",
            "Effect": "Allow"
        }
    ]
}
```

> **Note**
>
> Si necesita conectar el recurso compartido de archivos a un bucket de S3 a través de un endpoint de VPC, consulte Políticas de punto de enlace para Amazon S3 en la AWS PrivateLink Guía del usuario de.

Prevención del suplente confuso entre servicios

El problema del suplente confuso 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 entre servicios puede dar lugar al problema del suplente confuso. La suplantación entre servicios puede 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 puede 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.

Le recomendamos que utilice las claves de contexto de condición global `aws:SourceArn` y `aws:SourceAccount` en las políticas de recursos a fin de limitar los permisos que AWS Storage Gateway le concede a otro servicio para el recurso. Si se utilizan ambas claves de contexto 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 de Storage Gateway al que está asociado el recurso compartido de archivos.

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

El siguiente ejemplo muestra cómo puede utilizar la`aws:SourceArn`y`aws:SourceAccount`claves de contexto de condición global en Storage Gateway para evitar el confuso problema de adjunto.

```
{
  "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

Cuenta entre cuentasEl acceso se realiza cuando a una cuenta de Amazon Web Services y a los usuarios de dicha cuenta se les concede acceso a recursos que pertenecen a otra cuenta de Amazon Web Services. Con las gateways de archivos, puede utilizar un recurso compartido de

archivos de una cuenta de Amazon Web Services para obtener acceso a los objetos de un bucket de Amazon S3 que pertenezca a otra cuenta de Amazon Web Services.

Para utilizar un recurso compartido de archivos propiedad de una cuenta de Amazon Web Services para obtener acceso a un bucket de S3 de otra cuenta de Amazon Web Services

1. Asegúrese de que el propietario del bucket de S3 le haya concedido a su cuenta de Amazon Web Services el acceso que necesita al bucket de S3 y a los objetos contenidos en dicho bucket. Para obtener más información acerca de cómo conceder este acceso, consulteEjemplo 2: Propietario del bucket que concede permisos de bucket entre cuentasen laAmazon Simple Storage Service usuario Guide. 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. Abrir la consola de Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
4. Elija Give bucket owner full control (Conceder control total al propietario del bucket) en los ajustes de Object metadata (Metadatos de objetos) del cuadro de diálogo Configure file share setting (Configuración del recurso compartido de archivos).

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. De lo contrario, las actualizaciones

de archivos realizadas a través de su aplicaciones locales no se propagarán al bucket de Amazon S3 con el que está 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 disponiblesen laAmazon Simple Storage Service usuario Guide

Información general de la lista de control de acceso (ACL)en laAmazon Simple Storage Service usuario Guide

Eliminación de un recurso compartido de archivos

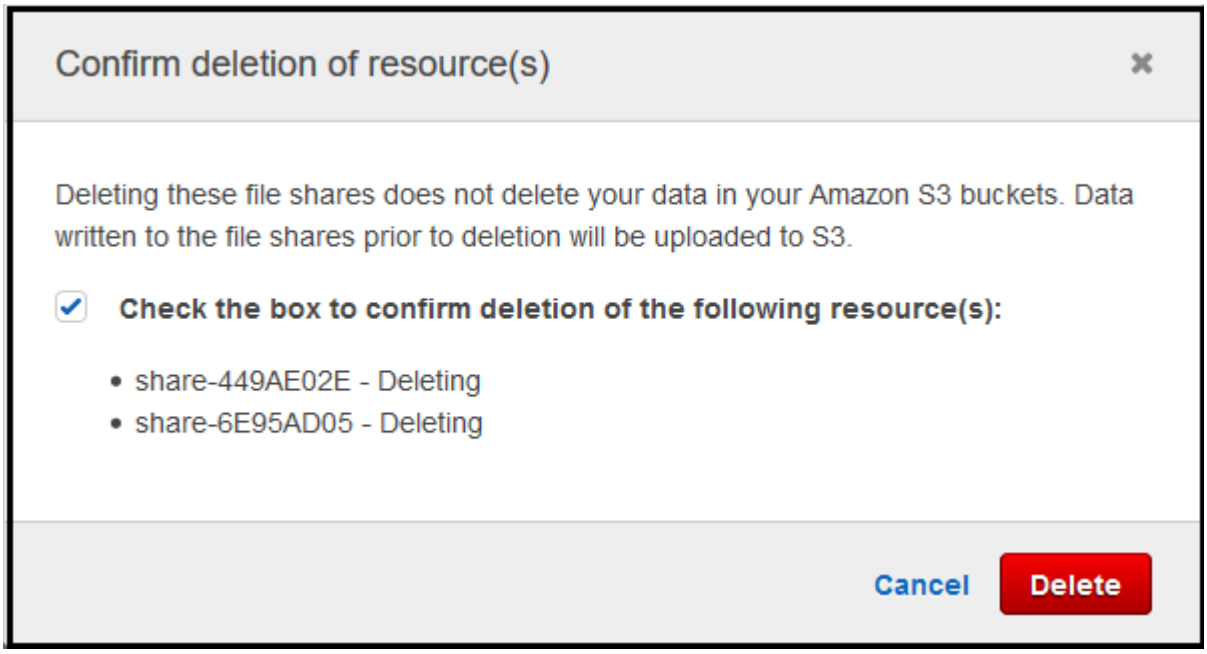
Si ya no necesita un recurso compartido de archivos, puede eliminarlo desde la consola de Storage Gateway. Al eliminar un recurso compartido de archivos, la gateway se separa del bucket de Amazon S3 al que estaba asignado dicho recurso compartido. Sin embargo, el bucket de S3 y su contenido no se eliminan.

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 desea que sus datos se carguen completamente, utilice el procedimiento para eliminar un recurso compartido de archivos a continuación. 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. Abrir la consola de Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
2. Elija File shares (Recursos compartidos de archivos) y seleccione el recurso compartido de archivos que desee eliminar.
3. En ActionsAPI (Acciones), elija Delete file share (Eliminar recurso compartido de archivos). Aparecerá el siguiente cuadro de diálogo de confirmación.



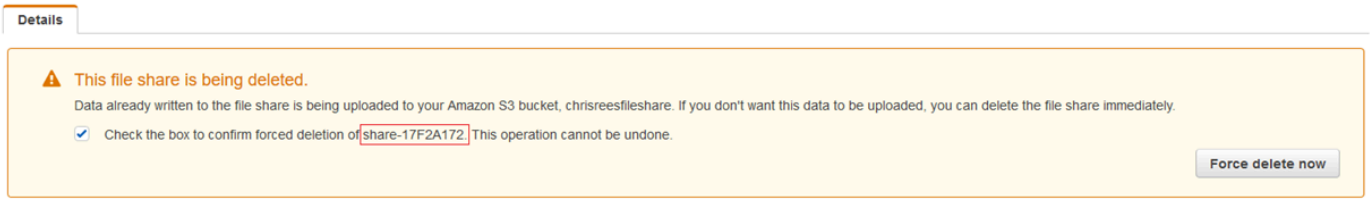
4. En el cuadro de diálogo de confirmación, marque las casillas de los recursos compartidos de archivos que desea eliminar y elija Delete (Eliminar).

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 eliminar de forma intencionada datos que se han escrito, pero que no se han cargado. En otro ejemplo, el bucket de Amazon S3 o los objetos que respaldan el recurso compartido de archivos pueden haberse eliminado, lo que significa que ya no es posible cargar los datos especificados.

En estos casos, puede eliminar el recurso compartido de archivos de manera forzada compartir a través de laAWS Management Consoleo el`DeleteFileShare`Operación API. Esta operación anula el proceso de carga de datos. Cuando concluya este procedimiento, el recurso compartido de archivos pasa al estado FORCE_DELETING. Para eliminar un recurso compartido de archivos de manera forzada desde la consola, consulte el procedimiento explicado a continuación.

Para eliminar un recurso compartido de archivos de manera forzada

1. Abrir la consola de Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
2. Elija File shares (Recursos compartidos de archivos), seleccione el recurso compartido de archivos que desea eliminar de manera forzada y espere unos segundos. En la pestaña Details (Detalles) aparecerá un mensaje de eliminación.



> **Note**
>
> La eliminación forzada no se puede deshacer.

3. En el mensaje que aparece en la pestaña Details (Detalles), verifique el ID del recurso compartido de archivos que desea eliminar de manera forzada, marque la casilla de confirmación y elija Force delete now (Eliminar de manera forzada ahora).

También puede usar la operación de la API DeleteFileShare para eliminar el recurso compartido de archivos de manera forzada.

Edición de la configuración para el recurso compartido de archivos NFS

Puede editar la clase de almacenamiento de su depósito de Amazon S3, nombre del recurso compartido de archivos, metadatos de objeto, nivel de squash, exportación como y configuración de actualización automática de la caché.

> **Note**
>
> No se puede editar un recurso compartido de archivos existente para apuntar a un nuevo bucket o punto de acceso, ni para modificar la configuración del endpoint de la VPC. Puede establecer esta configuración únicamente al crear un nuevo recurso compartido de archivos.

Para editar la configuración del recurso compartido de archivos

1. Abrir la consola de Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
2. Elija File shares (Recursos compartidos de archivos) y, a continuación, seleccione el recurso compartido de archivos que desee actualizar.
3. ParaActions, eligeEditar la configuración de recursos.

4. Realice una o más de las siguientes acciones:

   - (Opcional) ParaNombre del recurso compartido de archivos, escriba un nuevo nombre para el recurso compartido de archivos.
   - En Audit logs (Registros de auditoría), elija una de las siguientes opciones:
     - ElegirDisable logging (Deshabilitar el registro)para desactivar el registro.
     - ElegirCree un nuevo grupo de registrospara crear un nuevo registro de auditoría.
     - ElegirUso de un grupo de registros existentey, a continuación, elija un registro de auditoría existente de la lista.

     Para obtener más información acerca de auditorías, consulte Descripción de los registros de auditoría de file gateway.
   - (Opcional) ParaActualización automatizada de la caché desde S3, active la casilla de verificación y establezca la hora 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. Una vez transcurrido el intervalo TTL, el acceso al directorio hace que la puerta de enlace de archivos actualice primero el contenido del directorio desde el bucket de Amazon S3.
   - (Opcional) ParaNotificación de carga de archivo, active la casilla de verificación que desea notificar cuando S3 File Gateway haya cargado completamente un archivo en S3. Establecimiento de la propiedad deTiempo de asentamientoen segundos para controlar el número de segundos que se espera después del último punto en el tiempo que un cliente escribió en un archivo antes de generar un`ObjectUploaded`notificación de. Dado que los clientes pueden realizar muchas escrituras pequeñas en archivos, es mejor configurar este parámetro durante el mayor tiempo posible para evitar generar varias notificaciones para el mismo archivo en un período de tiempo reducido. Para obtener más información, consulte Obtener notificación de subida de archivos.

     > **Note**
     >
     > Esta configuración no afecta a la sincronización de la carga del objeto a S3, solo en el momento de la notificación.

   - ParaClase de almacenamiento para objetos nuevos, elija una clase de almacenamiento para utilizarlo con los nuevos objetos creados en el bucket de Amazon S3:

- Elija S3 Standard para almacenar los datos de objetos de acceso frecuente de forma redundante en varias zonas de disponibilidad que se encuentran distanciadas geográficamente. Para obtener más información acerca de la clase de almacenamiento estándar de S3, consulteClases de almacenamiento para objetos a los que se obtiene acceso con frecuenciaen laAmazon Simple Storage Service usuario Guide.
- Elija S3 Intelligent-Tiering para optimizar los costos de almacenamiento moviendo automáticamente los datos a la capa de acceso de almacenamiento más rentable. Para obtener más información acerca de la clase de almacenamiento en capas avanzadas de S3, consulteClase de almacenamiento para optimizar automáticamente los objetos a los que se obtiene acceso con mucha y poca frecuenciaen laAmazon Simple Storage Service usuario Guide.
- Elija S3 Standard-IA para almacenar los datos de objetos a los que se accede con poca frecuencia de forma redundante en varias zonas de disponibilidad que se encuentran distanciadas geográficamente. Para obtener más información acerca de la clase de almacenamiento estándar - Acceso poco común de S3, consulteClases de almacenamiento para objetos a los que se obtiene acceso con poca frecuenciaen laAmazon Simple Storage Service usuario Guide.
- Elija S3 One Zone-IA para almacenar los datos de objetos a los que se accede con poca frecuencia en una única zona de disponibilidad. Para obtener más información acerca de la clase de almacenamiento Única zona - Acceso poco común de S3, consulteClases de almacenamiento para objetos a los que se obtiene acceso con poca frecuenciaen laAmazon Simple Storage Service usuario Guide.

- En Object metadata (Metadatos de objetos), elija los metadatos que desea utilizar:
  - Elija Guess MIME type para poder adivinar el tipo MIME de los objetos cargados en función de las extensiones de archivo.
  - Elija Give bucket owner full control (Conceder control total al propietario del bucket) para dar control total al propietario del buket de S3 que se mapea al Sistema de archivos de red (NFS) del archivo o al recurso compartido de archivos del bloque del mensaje del servidor (SMB). Para obtener más información sobre el uso del recurso compartido de archivos para obtener acceso a objetos de un bucket perteneciente a otra cuenta, consulte Uso de un recurso compartido de archivos para el acceso entre cuentas.
  - Elija Enable requester pays (Habilitar el pago por el solicitante) si utiliza este recurso compartido de archivos en un bucket que requiere que el pago por los cargos de acceso lo realice el solicitante o el lector en lugar del propietario del bucket. Para obtener más información, consulte Buckets de pago por solicitante.

- En Squash level (Nivel de agrupación), elija el ajuste de nivel de agrupación que desee aplicar al recurso compartido de archivos NFS y, a continuación, elija Save (Guardar).

  > **Note**
  >
  > Solo es posible elegir un ajuste de nivel de agrupación para los recursos compartidos de archivos NFS. Los recursos compartidos de archivos SMB no utilizan los ajustes de agrupación.

  Los valores posibles son los siguientes:

  - Root squash (default) – El acceso para el super usuario (raíz) remoto se asigna al UID (65534) y al GID (65534).
  - No root squash (Sin agrupación en raíz): el superusuario remoto (raíz) recibe acceso como usuario raíz.
  - All squash – El acceso de todos los usuarios se asigna al UID (65534) y al GID (65534).

  El valor predeterminado del nivel de agrupación es Root squash (Agrupación en raíz).
- ParaExportar como, elija una opción para el recurso compartido de archivos. El valor predeterminado es Read-write (Lectura/escritura).

  > **Note**
  >
  > En el caso de recursos compartidos de archivos montados en un cliente de Microsoft Windows, si selecciona la opción Read-only (Solo lectura) en Export as (Exportar como), es posible que aparezca un mensaje de error indicando que no se puede crear la carpeta. Este mensaje de error es un problema conocido con la versión 3 de NFS. Puede hacer caso omiso de él.

5. Elija Save (Guardar).

Edición de los valores predeterminados de los metadatos del recurso compartido del archivo NFS

Si no configura valores de metadatos para los archivos o directorios del bucket, la puerta de enlace de archivos de S3 establece unos 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 de Storage Gateway.

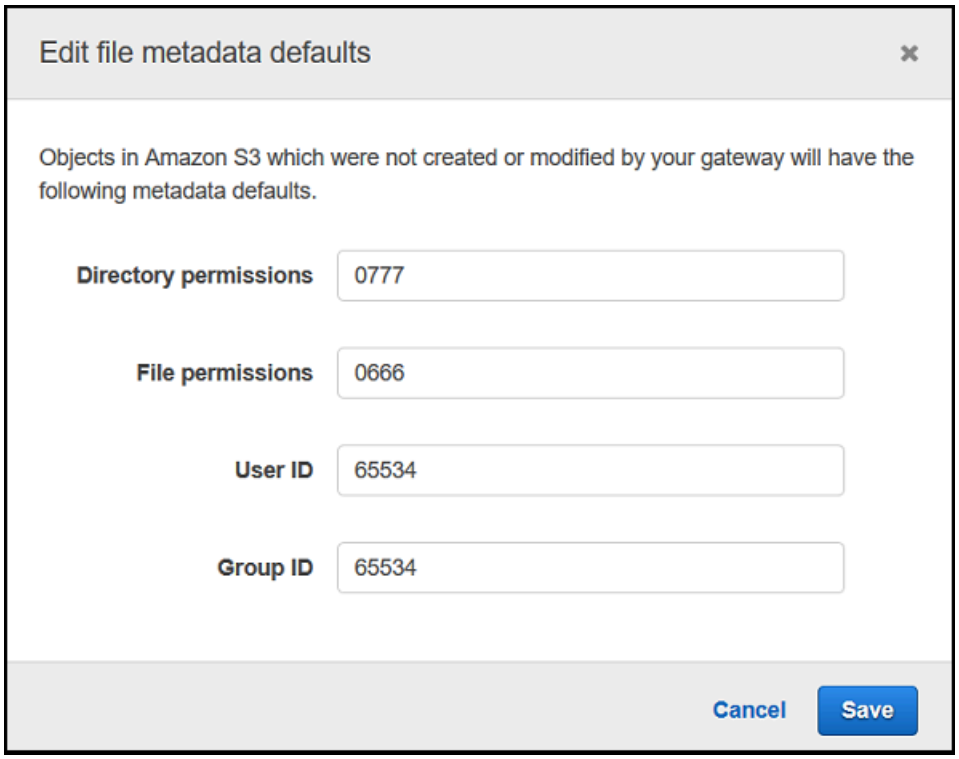
Cuando su S3 File Gateway almacena archivos y carpetas en Amazon S3, los permisos de archivos de Unix se almacenan en los metadatos de los objetos. Cuando su gateway de archivos de S3 detecta objetos que la gateway de archivos de S3 no ha almacenado, se les asignan permisos de archivos de Unix predeterminados. Los permisos de Unix predeterminados se muestran en la tabla siguiente.

Metadatos	Description (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.
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. Abrir la consola de Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
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).



Edición de la configuración de acceso a su recurso compartido de archivos NFS

Recomendamos cambiar la configuración de permisos del cliente de NFS relativa al recurso compartido de archivos NFS. Si no lo hace, cualquier cliente de la red podrá realizar una operación de montaje en el recurso compartido de archivos.

Para editar la configuración de acceso de NFS

1. Abrir la consola de Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
2. Elija File shares (Recursos compartidos de archivos) y, a continuación, elija el recurso compartido de archivos NFS que desee editar.
3. En Actions (Acciones), elija Edit share access settings (Editar configuración de acceso compartido).
4. En el navegadorEditar los clientes permitidos, seleccioneAñadir entrada, indique la dirección IP o la notación CIDR para los clientes que desea permitir y, a continuación, elijaGuardar.

Edición de la configuración de SMB para una puerta de enlace

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

Para editar la configuración SMB de nivel de puerta de enlace

1. Abrir la consola de Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
2. ElegirGateways dey, a continuación, elija la gateway para la que desea editar la configuración de SMB.
3. desde lasActions, seleccione el menú desplegableEditar la configuración de SMBy, a continuación, elija la configuración que desea editar.

Consulte los temas siguientes para obtener más información.

Temas

- Establecimiento de un nivel de seguridad para la puerta de enlace
- Uso de Active Directory para autenticar usuarios
- Proporcionar acceso de invitado a su recurso compartido de archivos
- Configure los grupos locales para su gateway
- Configuración de la visibilidad del recurso compartido

Establecimiento de un nivel de seguridad para la puerta de enlace

Al utilizar una gateway de archivos de S3, puede especificar un nivel de seguridad para la gateway. Al especificar el nivel de seguridad, puede establecer si su gateway precisa del inicio de sesión en un bloque de mensajes del servidor (SMB) o un cifrado de SMB o si desea activar el SMB versión 1.

Para configurar el nivel de seguridad

1. Abrir la consola de Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
2. ElegirGateways dey, a continuación, elija la gateway para la que desea editar la configuración de SMB.
3. desde lasActions, seleccione el menú desplegableEditar la configuración de SMBy, después,Configuración de seguridad de SMB.

4. En Security level (Nivel de seguridad) elija una de las siguientes opciones:

> **Note**
>
> Esta configuración se llama `SMBSecurityStrategy` en la Referencia de API.
> Un nivel de seguridad más alto puede afectar al rendimiento.

- Aplicación de la codificación— Si elige esta opción, S3 File Gateway solo permite conexiones desde clientes SMBv3 que tienen el cifrado habilitado. Esta opción es muy recomendable para entornos que manejen información confidencial. Esta opción funciona con clientes SMB en Microsoft Windows 8, Windows Server 2012 o posterior.
- Aplicación de la firma— Si elige esta opción, S3 File Gateway solo permite conexiones desde clientes SMBv2 o SMBv3 que tienen habilitada la firma. Esta opción funciona con clientes SMB en Microsoft Windows Vista, Windows Server 2008 o posterior.
- Negociación del cliente— Si elige esta opción, las solicitudes se establecen en función de lo que negocia 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. Elija Save (Guardar).

Uso de Active Directory para autenticar usuarios

Para utilizar su Active Directory corporativo para autenticar el acceso de los usuarios a un recurso compartido de archivos SMB, edite la configuración de SMB de la gateway con las credenciales del 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**
>
> Uso deAWS Directory Service, puede crear un servicio de dominio de Active Directory alojado en laNube de AWS.

Cualquier usuario que facilite la contraseña correcta puede obtener acceso de invitado al recurso compartido de archivos SMB.

También puede habilitar las listas de control de acceso (ACL) en el recurso compartido de archivos SMB. Para obtener información sobre cómo habilitar las ACL, consulte Uso de las ACL de Microsoft Windows para controlar el acceso a un recurso compartido de archivos SMB.

Para habilitar la autenticación con Active Directory

1. Abrir la consola de Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
2. ElegirGateways dey, a continuación, elija la gateway para la que desea editar la configuración de SMB.
3. desde lasActions, seleccione el menú desplegableEditar la configuración de SMBy, después,Configuración de Active Directory.
4. En Domain name (Nombre del dominio), especifique el dominio al que desea que se una la gateway. Puede unir un dominio utilizando su dirección IP o su unidad organizativa. Una unidad organizativa es una subdivisión de Active Directory que puede contener usuarios, grupos, equipos y otras unidades organizativas.

   > **Note**
   >
   > Si la gateway no puede unirse a un directorio de Active Directory, intente unirse con la dirección IP del directorio mediante la operación de la API JoinDomain.

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

5. Proporcione el usuario y la contraseña del dominio y, a continuación, elija Save (Guardar).

Un mensaje que aparece en la parte superior de la sección Gateways de la consola le indica que la gateway se ha unido correctamente al dominio de AD.

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

1. En la consola de Storage Gateway, elija el recurso compartido de archivos al que desea limitar el acceso.
2. desde lasActionsmenú desplegable, elijaEditar configuración de acceso a recursos compartidos.
3. En el navegadorAcceso compartido de archivos de usuarios y grupos, elija la configuración.

   ParaUsuarios y grupos permitidos, eligeAñada un usuario permitidooAñada un grupo permitidoe introduzca un usuario o grupo de AD que desee permitir el acceso compartido de archivos. Repita este proceso para permitir tantos usuarios y grupos como sea necesario.

   ParaUsuarios y grupos denegados, eligeAñadir usuario denegadooAñadir grupo denegadoe introduzca un usuario o grupo de AD que desee denegar el acceso a los recursos compartidos de archivos. Repita este proceso para denegar tantos usuarios y grupos como sea necesario.

   > **Note**
   >
   > LaAcceso compartido de archivos de usuarios y gruposaparece solo siActive Directoryestá seleccionado.
   > 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 especifica ningún usuario o grupo permitidos o denegados, cualquier usuario autenticado de AD puede exportar el recurso compartido de archivos.

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

Proporcionar acceso de invitado a su recurso compartido de archivos

Si solo desea proporcionar acceso de invitado, la gateway de archivos de S3 no tiene que formar parte de un dominio de Microsoft AD. También puede utilizar una gateway de archivos de S3 que sea miembro de un dominio de AD para crear recursos compartidos de archivos con acceso de

invitado. Antes de crear un recurso compartido de archivos con acceso de invitado, debe cambiar la contraseña predeterminada.

Para cambiar la contraseña de acceso de invitado

1. Abrir la consola de Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
2. ElegirGateways dey, a continuación, elija la gateway para la que desea editar la configuración de SMB.
3. desde lasActionsmenú desplegable, elijaEditar la configuración de SMBy, después,Configuración de acceso de invitados.
4. ParaLa contraseña de invitado, proporcione una contraseña y, a continuación, elijaGuardar.

Configure los grupos locales para su gateway

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

Puede utilizar la configuración de grupo local para asignar permisos de administrador de puerta de enlace. Los administradores de puerta de enlace pueden utilizar el complemento Carpetas compartidas Microsoft Management Console para cerrar forzosamente los archivos abiertos y bloqueados.

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

Para asignar administradores de puerta de enlace

1. Abrir la consola de Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
2. ElegirGateways dey, a continuación, elija la gateway para la que desea editar la configuración de SMB.
3. desde lasActions, seleccione el menú desplegableEditar la configuración de SMBy, después,Configuración del grupo local.
4. En el navegadorConfiguración del grupo local, elija la configuración. Esta sección aparece solo para los recursos compartidos de archivos que utilizan Active Directory.

ParaAdministradores de puerta de enlace, agregue usuarios y grupos de Active Directory a los que desea conceder permisos de administrador local de Gateway. Agregue un usuario o grupo por línea, incluido el nombre de dominio. Por ejemplo, **`corp\Domain Admins`**. Para crear líneas adicionales, elijaAgregar nuevo administrador de puerta de enlace.

> **Note**
>
> Editar administradores de puerta de enlace desconecta y vuelve a conectar todos los recursos compartidos de archivos SMB.

5. ElegirGuarde los cambiosy, después,Procederpara confirmar el mensaje de advertencia que aparece.

Configuración de la visibilidad del recurso compartido

La visibilidad del recurso compartido de archivos controla si los recursos compartidos de una gateway son visibles al publicar recursos compartidos a los usuarios.

Para configurar la visibilidad del recurso compartido de archivos

1. Abrir la consola de Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
2. ElegirGateways dey, a continuación, elija la gateway para la que desea editar la configuración de SMB.
3. desde lasActionsmenú desplegable, elijaEditar la configuración de SMBy, después,Configuración de visibilidad de recursos compartidos.
4. ParaEstado de visibilidad, active la casilla de verificación para que aparezcan las acciones de esta puerta de enlace al publicar acciones a los usuarios. Mantén la casilla de verificación desactivada para que las acciones de esta puerta de enlace no aparezcan al publicar acciones a los usuarios.

Edición de la configuración para el recurso compartido de archivos SMB

Después de crear un recurso compartido de archivos SMB, puede editar la clase de almacenamiento de su bucket de Amazon S3, metadatos de objetos, distinción de mayúsculas y minúsculas,

enumeración basada en el acceso, registros de auditoría, actualización automática de la caché y exportación como configuración para el recurso compartido de archivos.

> **Note**
>
> No se puede editar un recurso compartido de archivos existente para apuntar a un nuevo bucket o punto de acceso, ni para modificar la configuración del endpoint de la VPC. Puede establecer esta configuración únicamente al crear un nuevo recurso compartido de archivos.

Para editar la configuración del recurso compartido de archivos SMB

1. Abrir la consola de Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
2. Elija File shares (Recursos compartidos de archivos) y, a continuación, seleccione el recurso compartido de archivos que desee actualizar.
3. ParaActions, eligeEditar la configuración de recursos.
4. Realice una o más de las siguientes acciones:

   - (Opcional) ParaNombre del recurso compartido de archivos, escriba un nuevo nombre para el recurso compartido de archivos.
   - En Audit logs (Registros de auditoría), elija una de las siguientes opciones:
     - ElegirDisable logging (Deshabilitar el registro)para desactivar el registro.
     - ElegirCree un nuevo grupo de registrospara crear un nuevo registro de auditoría.
     - ElegirUso de un grupo de registros existentey, a continuación, elija un registro de auditoría existente de la lista.

     Para obtener más información acerca de auditorías, consulte Descripción de los registros de auditoría de file gateway.
   - (Opcional) ParaActualización automatizada de la caché desde S3 tras, active la casilla de verificación y establezca la hora 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. Una vez transcurrido el intervalo TTL, el acceso al directorio hace que la puerta de enlace de archivos actualice primero el contenido del directorio desde el bucket de Amazon S3.
   - (Opcional) ParaNotificación de carga de archivo, active la casilla de verificación que desea notificar cuando S3 File Gateway haya cargado completamente un archivo en S3.

Establecimiento de la propiedad deTiempo de asentamientoen segundos para controlar el número de segundos que se espera después del último punto en el tiempo que un cliente escribió en un archivo antes de generar un`ObjectUploaded`notificación de. Dado que los clientes pueden realizar muchas escrituras pequeñas en archivos, es mejor configurar este parámetro durante el mayor tiempo posible para evitar generar varias notificaciones para el mismo archivo en un período de tiempo reducido. Para obtener más información, consulte Obtener notificación de subida de archivos.

> **Note**
>
> Esta configuración no afecta a la sincronización de la carga del objeto a S3, solo en el momento de la notificación.

- ParaClase de almacenamiento para objetos nuevos, elija una clase de almacenamiento para utilizarlo con los nuevos objetos creados en el bucket de Amazon S3:
  - Elija S3 Standard para almacenar los datos de objetos de acceso frecuente de forma redundante en varias zonas de disponibilidad que se encuentran distanciadas geográficamente. Para obtener más información acerca de la clase de almacenamiento estándar de S3, consulteClases de almacenamiento para objetos a los que se obtiene acceso con frecuenciaen laAmazon Simple Storage Service usuario Guide.
  - Elija S3 Intelligent-Tiering para optimizar los costos de almacenamiento moviendo automáticamente los datos a la capa de acceso de almacenamiento más rentable. Para obtener más información acerca de la clase de almacenamiento en capas avanzadas de S3, consulteClase de almacenamiento para optimizar automáticamente los objetos a los que se obtiene acceso con mucha y poca frecuenciaen laAmazon Simple Storage Service usuario Guide.
  - Elija S3 Standard-IA para almacenar los datos de objetos a los que se accede con poca frecuencia de forma redundante en varias zonas de disponibilidad que se encuentran distanciadas geográficamente. Para obtener más información acerca de la clase de almacenamiento estándar - Acceso poco común de S3, consulteClases de almacenamiento para objetos a los que se obtiene acceso con poca frecuenciaen laAmazon Simple Storage Service usuario Guide.
  - Elija S3 One Zone-IA para almacenar los datos de objetos a los que se accede con poca frecuencia en una única zona de disponibilidad. Para obtener más información acerca de la clase de almacenamiento Única zona - Acceso poco común de S3, consulteClases de

almacenamiento para objetos a los que se obtiene acceso con poca frecuenciaen laAmazon Simple Storage Service usuario Guide.

- En Object metadata (Metadatos de objetos), elija los metadatos que desea utilizar:
  - Elija Guess MIME type para poder adivinar el tipo MIME de los objetos cargados en función de las extensiones de archivo.
  - Elija Give bucket owner full control (Conceder control total al propietario del bucket) para dar control total al propietario del buket de S3 que se mapea al Sistema de archivos de red (NFS) del archivo o al recurso compartido de archivos del bloque del mensaje del servidor (SMB). Para obtener más información acerca del uso del recurso compartido de archivos para obtener acceso a objetos de un bucket perteneciente a otra cuenta, consulteUso de un recurso compartido de archivos para el acceso entre cuentas.
  - Elija Enable requester pays (Habilitar el pago por el solicitante) si utiliza este recurso compartido de archivos en un bucket que requiere que el pago por los cargos de acceso lo realice el solicitante o el lector en lugar del propietario del bucket. Para obtener más información, consulte Buckets de pago por solicitante.
- ParaExportar como, elija una opción para el recurso compartido de archivos. El valor predeterminado es Read-write (Lectura/escritura).

  > **Note**
  >
  > Para los recursos compartidos de archivos montados en un cliente Microsoft Windows, si seleccionaSolo lecturaparaExportar como, es posible que aparezca un mensaje de error indicando que no se puede crear la carpeta. Este mensaje de error es un problema conocido con la versión 3 de NFS. Puede hacer caso omiso de él.

- Para File/directory access controlled by (Acceso al archivo/directorio controlado por) seleccione una de las siguientes opciones:
  - Seleccione Windows Access Control List (Lista de control de acceso de Windows) para establecer permisos específicos en los archivos y carpetas de un recurso compartido de archivos SMB. Para obtener más información, consulte Uso de las ACL de Microsoft Windows para controlar el acceso a un recurso compartido de archivos SMB.
  - Seleccione POSIX permissions (permisos de POSIX) para controlar el acceso a los archivos y directorios almacenados en un recurso compartido de archivos NFS o SMB.

  Si el método de autenticación esActive Directory, paraUsuarios/grupos administradores, introduzca una lista separada por comas de usuarios y grupos de AD. Si desea que dicho

usuario tenga privilegios para actualizar las ACL de todos los archivos y carpetas del recurso compartido de archivos debe realizar esto. Estos usuarios y grupos cuentan con derechos de administrador para el recurso compartido de archivos. Un grupo debe tener un prefijo con la@carácter, por ejemplo,`@group1`.

- ParaSensibilidad de mayúsculas y minúsculas, active la casilla de verificación para permitir que la puerta de enlace controle la distinción de mayúsculas y minúsculas o desactive la casilla de verificación para permitir al cliente controlar la distinción de mayúsculas y minús

  > **Note**
  >
  > - Si está activando esta casilla de verificación, esta configuración se aplica inmediatamente a las nuevas conexiones de cliente SMB. Las conexiones de cliente SMB existentes deben desconectarse del recurso compartido de archivos y volver a conectarse para que la configuración surta efecto.
  > - Si desactiva esta casilla de verificación, esta configuración podría provocar que pierda el acceso a los archivos con nombres que solo difieren en su caso.

- ParaEnumeración basada en acceso, active la casilla de verificación para que los archivos y carpetas del recurso compartido sean visibles solo para los usuarios que tienen acceso de lectura. Mantenga la casilla de verificación desactivada para que los archivos y carpetas del recurso compartido sean visibles para todos los usuarios durante la enumeración de directorios.

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

- ParaBloqueo oportunista (oplock), elija una de las siguientes opciones:
  - ElegirEnabled (Habilitado)para permitir que el recurso compartido de archivos utilice el bloqueo oportunista para optimizar la 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.
  - ElegirDiscapacitadopara evitar el uso del bloqueo oportunista. Si varios clientes Windows de su entorno editan con frecuencia los mismos archivos simultáneamente, deshabilitar el bloqueo oportunista a veces puede mejorar el rendimiento.

> **Note**
>
> No se recomienda habilitar el bloqueo oportunista de recursos compartidos que distinguen mayúsculas de minúsculas para cargas de trabajo que implican acceso a archivos con el mismo nombre en distintos casos.

5. Elija Save changes (Guardar cambios).

Refrescar objetos en el bucket de Amazon S3

Mientras el cliente de NFS o SMB realiza operaciones en el sistema de archivos, la gateway mantiene un inventario de los objetos contenidos en el bucket de S3 asociados al recurso compartido de archivos. La gateway utiliza este inventario en caché para reducir la latencia y frecuencia de las solicitudes de S3. Esta operación no importa archivos al almacenamiento de caché de S3 File Gateway. Solo actualiza el inventario almacenado en caché para reflejar los cambios en el inventario de los objetos del bucket de S3.

Para actualizar el bucket de S3 del recurso compartido de archivos, puede utilizar la consola de Storage Gateway, laRefreshCacheen la API de Storage Gateway o unAWS Lambdafunción.

Para actualizar objetos en un bucket de S3 desde la consola

1. Abrir la consola de Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
2. Elija File shares (Recursos compartidos de archivos) y, a continuación, elija el recurso compartido de archivos asociado al bucket de S3 que desea actualizar.
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.

Para actualizar objetos en un bucket de S3 mediante unAWS Lambdafunción

1. Identifique el bucket de S3 utilizado por S3 File Gateway.
2. Compruebe que lasEventoestá en blanco. Se rellena automáticamente más tarde.
3. Crear un rol de IAM y permitir la relación de confianza para Lambda`lambda.amazonaws.com`.

4. Utilice la siguiente política de.

```
{
    "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 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-2:672406774878:share/
share-E51FBD9C'
    )
    print(response)
    return 'Your FileShare cache has been refreshed'
```

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

8. Opcional: agregue un activador para Amazon S3 y seleccione el eventoObjectCreatedoObjectRemoved.

> **Note**
>
> `RefreshCache`necesita completar un proceso antes de iniciar otro. Al crear o eliminar muchos objetos de un depósito, el rendimiento podría degradarse. Por lo tanto, recomendamos no utilizar activadores de S3. En su lugar, utilice la regla de Amazon CloudWatch descrita a continuación.

9. Cree una regla de CloudWatch en la consola de CloudWatch y agregue una programación. En general, recomendamos unTipo fijode 30 minutos. Sin embargo, puede usar de 1 a 2 horas en un cubo S3 grande.
10. Agregue un nuevo activador para eventos de CloudWatch y elija la regla que acaba de crear.
11. Guarde la configuración de Lambda. Seleccione Test (Probar).
12. ElegirS3 PUTy personaliza la prueba según tus necesidades.
13. La prueba debería realizarse correctamente. Si no, modifique el JSON según sus requisitos y vuelva a realizar la prueba.
14. Abra la consola de Amazon S3 y compruebe que el evento que creó y el ARN de la función Lambda están presentes.
15. Cargue un objeto en el bucket de S3 utilizando la consola de Amazon S3 o laAWS CLI.

    La consola de CloudWatch genera un resultado de CloudWatch 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:::MY-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 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 su cliente reflejará esta actualización.

> **Note**
>
> En el caso de las memorias caché 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 de Amazon S3 oAWS 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. Compruebe los registros de CloudWatch para ver el registro de su eliminación 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**
>
> Para trabajos cron o tareas programadas, el evento de registro de CloudWatch esu'detail-type': u'Scheduled Event'.

Al actualizar la memoria caché solo se inicia la operación de actualización. 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, puede suscribirse para que se le envíen notificaciones a través de un evento de Amazon CloudWatch cuando suRefreshCachese completa la operación. Para obtener más información, consulte Cómo recibir notificaciones de las operaciones de archivos.

Uso de S3 Object Lock con una gateway de archivos de Amazon S3

Amazon S3 File Gateway permite el acceso a los buckets de S3 que tienen habilitado Amazon S3 Object Lock. El bloqueo de objetos de Amazon S3 le permite almacenar objetos con un modelo de escritura única y lectura múltiple (WORM). Cuando se utiliza el bloqueo de objetos de Amazon S3, se puede evitar que se elimine o se sobrescriba un objeto del bucket de S3. Amazon S3 Object Lock funciona junto con el control de versiones de objetos para proteger los datos.

Si habilita el bloqueo de objetos de Amazon S3, puede modificar el objeto. Por ejemplo, se puede escribir, eliminar o cambiar el nombre a través de un recurso compartido de archivos de S3 File Gateway. Cuando se modifica un objeto de esta forma, S3 File Gateway coloca una versión nueva del objeto sin que ello afecte a la versión anterior (es decir, el objeto bloqueado).

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

Para obtener más información acerca de Amazon S3 Object Lock, consulteBloqueo de objetos mediante Bloqueo de objetos de S3en laAmazon Simple Storage Service usuario Guide.

Descripción del estado del recurso compartido de

Cada recurso compartido de archivos tiene una indicación de estado asociada que permite ver de inmediato en qué estado se encuentra. En la mayoría de los casos, el estado indica que el recurso compartido de archivos funciona normalmente y que no se requiere ninguna intervención por parte del usuario. En ocasiones, el estado indica algún problema; en este caso, podría o no ser preciso que intervenga.

Puede ver el estado del recurso compartido de archivos en la consola de Storage Gateway. El estado del recurso compartido de archivos aparece en la columna Status (Estado) de cada recurso compartido de archivos en la gateway. El estado de un recurso compartido de archivos que funciona normalmente es AVAILABLE.

En la tabla siguiente, encontrará una descripción de cada estado de recurso compartido de archivos, y si debe hacer algo según cada estado y cuándo. El estado de un recurso compartido de archivos debe ser AVAILABLE la totalidad o la mayor parte del tiempo que se esté usando.

Estado	Significado
AVAILABLE	El recurso compartido de archivos está configurado correctamente y se encuentra disponible para su uso. El estado AVAILABLE es el estado normal de funcionamiento de un recurso compartido de archivos.
CREATING	El recurso compartido de archivos se está creando y no está listo para utilizarlo. El estado CREATING es transitorio. No hay que hacer nada más. Si el recurso compartido de archivos se queda bloqueado en este estado, probablemente se deba a que la máquina virtual de gateway ha perdido la conexión conAWS.
UPDATING	Se está actualizando la configuración del recurso compartido de archivos. Si un recurso compartido de archivos se queda bloqueado en este estado, probablemente se deba a que la máquina virtual de gateway ha perdido la conexión conAWS.
DELETING	Se está eliminando el recurso compartido de archivos. El archivo compartido no se elimina hasta que todos los datos se han cargado aAWS. El estado DELETING es transitorio y no se requiere ninguna acción.

Estado	Significado
FORCE_DELETING	Se está eliminando de forma forzada el recurso compartido de archivos. El archivo compartido se elimina inmediatamente y se carga aAWSse ha anulado. El estado FORCE_DELETING es transitorio y no se requiere ninguna acción.
UNAVAILABLE	El recurso compartido de archivos se encuentra en mal estado. Algunos problemas pueden provocar que un recurso compartido de archivos deje de funcionar correctamente. Esto puede ser ocacionado, por ejemplo, por errores en las políticas de roles pueden o porque el recurso compartido de archivos se mapee a un bucket de Amazon S3 que no existe. Cuando se resuelve el problema que ha provocado el mal estado, el archivo recupera el estado AVAILABLE.

Prácticas recomendadas para compartir archivos

En esta sección, encontrará información sobre las prácticas recomendadas para crear recursos compartidos de archivos.

Temas

- Impedir que varios archivos compartidos se escriban en el bucket de Amazon S3
- Permitir que clientes NFS específicos monten el recurso compartido de archivos

Impedir que varios archivos compartidos se escriban en el bucket de Amazon S3

Al crear un recurso compartido de archivos, recomendamos configurar un bucket de Amazon S3 de modo que solamente pueda escribir en él un recurso compartido de archivos. Si configura el bucket de S3 para que varios recursos compartidos de archivos puedan escribir en él, podría obtener resultados impredecibles. Para evitarlo, cree una política de bucket de S3 que deniegue la posibilidad de incluir o eliminar objetos en el bucket a todos los roles excepto al del recurso compartido de archivos. A continuación, asocie dicha política al bucket de S3.

En el siguiente ejemplo de una política se deniega a todos los roles, excepto aquel que creó el bucket, la posibilidad de escribir en el bucket de S3. 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:::TestBucket/*"`.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyMultiWrite",
         "Effect":"Deny",
         "Principal":"*",
         "Action":[
            "s3:DeleteObject",
            "s3:PutObject"
         ],
         "Resource":"arn:aws:s3:::TestBucket/*",
         "Condition":{
            "StringNotLike":{
               "aws:userid":"TestUser:*"
            }
         }
      }
   ]
}
```

Permitir que clientes NFS específicos monten el recurso compartido de archivos

Recomendamos que cambie la configuración del cliente de NFS permitido relativa al recurso compartido de archivos. Si no lo hace, cualquier cliente de la red podrá montar el recurso compartido de archivos. Para obtener información sobre cómo editar la configuración de los clientes de NFS, consulte Edición de la configuración de acceso a su recurso compartido de archivos NFS.

Supervisión de la gateway de archivos

Puede monitorizar la gateway de archivos y los recursos asociados enAWS Storage Gatewaymediante métricas de Amazon CloudWatch y registros de auditoría de recursos compartidos de archivos. También puede utilizar CloudWatch Events para recibir notificaciones cuando hayan terminado las operaciones con los archivos. Para obtener información acerca de las métricas de tipo de puerta de enlace de archivos, consulte Supervisión de la gateway de archivos.

Temas

Obtener registros de estado de puerta de enlace de archivos con grupos de registros de CloudWatch

Puede utilizar Amazon CloudWatch Logs para obtener información acerca del estado de la gateway de archivos y los recursos relacionados. Puede utilizar los registros para monitorizar los errores que detecte la gateway. Además, puede utilizar los filtros de suscripción de Amazon CloudWatch para automatizar el procesamiento de la información de los registros en tiempo real. Para obtener más información, consulteProcesamiento en tiempo real de datos de registros con suscripcionesen laGuía del usuario de Amazon CloudWatch.

Por ejemplo, puede configurar un grupo de registros de CloudWatch para monitorizar la gateway y recibir notificaciones cuando la gateway de archivos falle al cargar los archivos en un bucket de Amazon S3. Puede configurar el grupo cuando active la gateway o cuando ya esté activada y en funcionamiento. Para obtener información acerca de cómo configurar un grupo de registros de CloudWatch al activar una gateway, consulteConfiguración de Amazon S3 File Gateway. Para obtener información general acerca de los grupos de registros de CloudWatch, consulteTrabajo con grupos y flujos de logsen laGuía del usuario de Amazon CloudWatch.

A continuación se muestra un ejemplo de un error notificado por una gateway de archivos.

```
{
    "severity": "ERROR",
    "bucket": "bucket-smb-share2",
    "roleArn": "arn:aws:iam::123456789012:role/my-bucket",
    "source": "share-E1A2B34C",
    "type": "InaccessibleStorageClass",
    "operation": "S3Upload",
    "key": "myFolder/myFile.text",
    "gateway": "sgw-B1D123D4",
    "timestamp": "1565740862516"
}
```

Este error significa que la puerta de enlace de archivos no puede cargar el objeto`myFolder/myFile.text`a Amazon S3 porque ha cambiado de la clase de almacenamiento estándar de Amazon S3 a la clase 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, se ha detectado el error cuando la gateway intentaba cargar el objeto especificado en Amazon S3 o realizar una lectura desde Amazon S3. Sin embargo, en este caso, el objeto ha cambiado a Amazon S3 Glacier. El valor de `"type"` puede ser cualquier error que la gateway de archivos detecte. Para obtener una lista de posibles errores, consulte Resolución de problemas de gateways de archivos
- `"operation": "S3Upload"`indica que este error se ha producido cuando la gateway intentaba cargar este objeto a S3.
- `"key": "myFolder/myFile.text"` indica el objeto que ha provocado el fallo.
- `gateway": "sgw-B1D123D4` indica la gateway de archivos que ha detectado este error.
- `"timestamp": "1565740862516"`indica el momento en el que se ha producido el error.

Para obtener información acerca de cómo solucionar este tipo de errores, consulte Resolución de problemas de gateways de archivos.

Configuración de un grupo de registros de CloudWatch después de activar la gateway

En el siguiente procedimiento, se muestra cómo configurar un grupo de registros de CloudWatch después de activar la gateway.

Para configurar un grupo de registros de CloudWatch para que funcione con la gateway de archivos

1. Inicie sesión enAWS Management Consoley abra la consola de Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
2. En el panel de navegación, seleccioneGateways dey, a continuación, seleccione la gateway en la que desea configurar el grupo de registros de CloudWatch.
3. ParaActions, eligeEdición de la información de gateway. O, en elDetalles depestaña, debajoRegistros de HealthyNo está habilitado, eligeConfigurar grupo de registrospara abrirEditarNombre de puerta de enlace del clientecuadro de diálogo.
4. ParaGrupo de registros de estado de gateway, elija una de las siguientes opciones:

   - Disable logging (Deshabilitar el registro)si no desea supervisar la puerta de enlace mediante grupos de registros de CloudWatch.
   - Creación de un nuevo grupo de registrosPara crear un nuevo grupo de registros de CloudWatch.
   - Uso de un grupo de registros existentepara utilizar un grupo de registros de CloudWatch que ya existe.

     Elija un grupo de registros enLista de grupos de registros existentes.
5. Elija Save changes (Guardar cambios).
6. Para ver los registros de estado de la gateway, haga lo siguiente:

   1. En el panel de navegación, seleccioneGateways dey, a continuación, seleccione la gateway en la que configuró el grupo de registros de CloudWatch.
   2. Elija el iconoDetalles depestaña, y debajoRegistros de Health, eligeRegistros de CloudWatch. LaDetalles del grupo de registrosse abre en la consola de CloudWatch.

Para configurar un grupo de registros de CloudWatch para que funcione con la gateway de archivos

1. Inicie sesión enAWS Management Consoley abra la consola de Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
2. ElegirGateways dey, a continuación, seleccione la gateway en la que desea configurar el grupo de registros de CloudWatch.
3. ParaActions, eligeEdición de la información de gateway. O, en elDetalles depestaña, junto aRegistro de, enNo está habilitado, eligeConfigurar grupo de registrospara abrirEdición de la información de gatewaycuadro de diálogo.
4. ParaGrupo de registros de gateway de, eligeUso de un grupo de registros existentey, a continuación, elija el grupo de registros que desea utilizar.

   Si no tiene un grupo de registros, elija Crear un nuevo grupo de registros para crear uno. Se le dirigirá a la consola de CloudWatch Logs, donde puede crear el grupo de registros de. Si crea un nuevo grupo de registros, seleccione el botón de actualizar en la lista desplegable para ver el grupo de registros nuevo.
5. Cuando haya terminado, elija Save.
6. Para ver los registros de la gateway, seleccione la gateway y, a continuación, seleccione laDetalles dePestaña.

Para obtener información acerca de cómo solucionar errores, consulte Resolución de problemas de gateways de archivos.

Uso de métricas de Amazon CloudWatch

Puede obtener datos de monitorización de la gateway de archivos mediante laAWS Management Consoleo API de CloudWatch. La consola muestra una serie de gráficos basados en los datos sin procesar de la API de CloudWatch. La API de CloudWatch también se puede utilizar a través de uno de losAWSSDK deoAPI de Amazon CloudWatchherramientas. 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 consola de CloudWatch, puede utilizar el`Gateway`

`Metrics`vista para seleccionar cotas específicas de la puerta de enlace. Para obtener más información acerca de las dimensiones, consulte.Dimensionesen laGuía del usuario de Amazon CloudWatch.

- 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 nombres de Amazon CloudWatch	Dimensión	Description (Descripción)
`AWS/StorageGateway`	`GatewayId` , `GatewayName`	Estas dimensiones filtran datos de métricas que describen aspectos de la gateway. Puede identificar una gateway de archivos con la que trabajar especificando las dimensiones `GatewayId` y `GatewayName` . 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 métricas disponibles
- Obtener estadísticas de una métrica
- Creación de alarmas de CloudWatch

Cómo recibir notificaciones de las operaciones de archivos

Storage Gateway puede iniciar CloudWatch Events cuando hayan terminado las operaciones con los archivos:

- Puede recibir una notificación cuando la gateway termine de cargar archivos de forma asíncrona desde el recurso compartido de archivos a Amazon S3. Usar`NotificationPolicy`Para solicitar una notificación de carga de archivos. Se envía una notificación por cada carga de archivos completada a Amazon S3. Para obtener más información, consulte Obtener notificación de subida de archivos.
- Puede recibir una notificación cuando la gateway termine de cargar de forma asíncrona el conjunto de archivos de trabajo desde el recurso compartido de archivos a Amazon S3. UsarNotifyWhenUploadedOperación de API para solicitar una notificación de carga de conjuntos de archivos que funcione. 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 Obtener notificación de carga de conjuntos de archivos de trabajo.
- Puede recibir una notificación cuando la gateway termine de actualizar la caché para el bucket de S3. Cuando invocas elRefreshCachea través de la consola de Storage Gateway o la API, suscríbase a la notificación cuando finalice la operación. Para obtener más información, consulte Obtener notificación de memoria caché de actualización.

Cuando finalice la operación de archivos que ha solicitado, Storage Gateway le envía una notificación a través de CloudWatch Events. Puede configurar CloudWatch Events para que envíe la notificación a través de destinos de eventos como, por ejemplo, Amazon SNS, Amazon SQS o unAWS Lambdafunción. Por ejemplo, puede configurar un destino de Amazon SNS para que envíe la notificación a los consumidores de Amazon SNS, por ejemplo, un correo electrónico o un mensaje de texto. Para obtener información sobre CloudWatch Events, consulte¿Qué es CloudWatch Events?

Para configurar la notificación de eventos de CloudWatch

1. Cree un destino, como un tema de Amazon SNS o una función Lambda, para invocar cuando se active el evento que ha solicitado en Storage Gateway.
2. Cree una regla en la consola de CloudWatch Events para invocar 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 se activa cuando el evento coincide con este patrón de reglas.
4. Seleccione el destino y configure los ajustes.

En el siguiente ejemplo, se muestra una regla que inicia el tipo de evento especificado en la gateway y la especificada.AWSRegión . 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 acerca de cómo utilizar CloudWatch Events para activar reglas, consulteCreación de una regla de CloudWatch Events que se active en función de un eventoen laGuía del usuario de Amazon CloudWatch Events.

Obtener notificación de subida de archivos

Existen dos casos de uso en los que puede utilizar la notificación de carga de archivos:

- Para la automatización del procesamiento en la nube de los archivos que se cargan, puede llamar al`NotificationPolicy`y recupera un ID de notificación. La notificación que se activa cuando se cargan archivos tiene el mismo ID de notificación que el que devuelve la API. Si utiliza este ID de notificación para realizar un seguimiento de la lista de archivos que está cargando, puede activar el procesamiento del archivo que se ha cargado enAWScuando se genera el evento con el mismo ID.
- En el caso de uso de distribución de contenido, puede tener dos gateways de archivos asignadas al mismo bucket de Amazon S3. El cliente del recurso compartido de archivos de Gateway1 podría cargar los archivos nuevos en Amazon S3 y los clientes del recurso compartido de archivos de Gateway2 podrían leerlos. Los archivos se cargan en Amazon S3, pero Gateway2 no puede verlos porque utiliza una versión almacenada locamente en caché de los archivos de Amazon S3. Para que los archivos sean visibles en Gateway2, puede utilizar el`NotificationPolicy`para solicitar la notificación de carga de archivos a Gateway1 para que le envíe una notificación cuando haya terminado el archivo de carga. A continuación, puede utilizar CloudWatch Events

para emitir automáticamente unRefreshCacheSolicitud de recurso compartido en Gateway2. CuandoRefreshCachela solicitud se ha completado, el nuevo archivo está visible en Gateway2.

Example Ejemplo: Notificación de carga de archivos

En el siguiente ejemplo, se muestra una notificación de carga de archivos que se envía a través de 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 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": "my-bucket",
    }
}
```

Nombres de los campos	Description (Descripción)
version	Versión actual de la política de IAM.
id	ID que identifica la política de IAM.

Nombres de los campos	Description (Descripción)
detail-type	Descripción del evento que activó la notificación que se envió.
origen	LaAWSServicio que es el origen de la solicitud y la notificación.
cuenta	El ID de laAWScuenta desde la que se generaron la solicitud y la notificación.
tiempo	Fecha y hora en el que se realizó la solicitud de carga de archivos en Amazon S3.
region	LaAWSRegión desde la que se enviaron la solicitud y la notificación.
recursos	Recursos de la gateway de almacenamiento a los que se aplica la política.
tamaño de objeto	El tamaño del objeto en bytes.
Hora de modificación	Hora en que el cliente modificó el archivo.
clave de objeto	La ruta al archivo.
event-type	CloudWatch Events que activaron la notificación.
prefix	Nombre del prefijo del bucket de S3.
nombre-bucket	Nombre del bucket de S3.

Obtener notificación de carga de conjuntos de archivos de trabajo

Hay dos casos de uso en los que puede utilizar la notificación de subida del conjunto de archivos de trabajo:

- Para la automatización del procesamiento en la nube de los archivos que se cargan, puede llamar al`NotifyWhenUploaded`API y recupera un ID de notificación. La notificación que se activa

cuando se ha cargado el conjunto de archivos de trabajo tiene el mismo ID de notificación que el que devuelve la API. Si utiliza este ID de notificación para realizar un seguimiento de la lista de archivos que está cargando, puede activar el procesamiento del conjunto de archivos que se han cargado enAWScuando se genera el evento con el mismo ID.

- En el caso de uso de distribución de contenido, puede tener dos gateways de archivos asignadas al mismo bucket de Amazon S3. El cliente del recurso compartido de archivos de Gateway1 puede cargar los archivos nuevos en Amazon S3 y los clientes del recurso compartido de archivos de Gateway2 pueden leerlos. Los archivos se cargan en Amazon S3, pero Gateway2 no puede verlos porque utiliza una versión almacenada locamente en caché de los archivos de S3. Para que los archivos sean visibles en Gateway2, utilice elNotifyWhenUploadedOperación API para solicitar la notificación de carga de archivos a Gateway1 para que le envíe una notificación cuando haya terminado la carga del conjunto de archivos de trabajo. A continuación, puede utilizar CloudWatch Events para emitir automáticamente unRefreshCacheSolicitud de recurso compartido en Gateway2. CuandoRefreshCacheSe ha completado la solicitud, los nuevos archivos están visibles en Gateway2. Esta operación no importa archivos al almacenamiento de la caché de la puerta de enlace de archivos. Solo actualiza el inventario almacenado en caché para reflejar los cambios en el inventario de los objetos del bucket de S3.

Example Ejemplo: notificación de carga de conjuntos de archivos de trabajo

En el siguiente ejemplo, se muestra una notificación de carga de conjuntos de archivos en funcionamiento que se envía a través de 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 Upload Notification 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	Description (Descripción)
version	Versión actual de la política de IAM.
id	ID que identifica la política de IAM.
detail-type	Descripción del evento que activó la notificac ión que se envió.
origen	LaAWSServicio que es el origen de la solicitud y la notificación.
cuenta	El ID de laAWScuenta desde la que se generaron la solicitud y la notificación.
tiempo	Fecha y hora en el que se realizó la solicitud de carga de archivos en Amazon S3.
region	LaAWSRegión desde la que se enviaron la solicitud y la notificación.
recursos	Recursos de Storage Gateway a los que se aplica la política.
event-type	CloudWatch Events que activaron la notificac ión.
notification-id	ID generado de forma aleatoria de la notificac ión que se envió. Este ID tiene el formato UUID. Este es el ID de notificación que se devuelve cuando se llama a `NotifyWhe nUploaded` .

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

Obtener notificación de memoria caché de actualización

En el caso de uso de una notificación de actualización de la caché, puede tener dos gateways de archivos asignadas al mismo bucket de Amazon S3 y el cliente NFS de Gateway1 podría cargar archivos nuevos en el bucket de S3. Los archivos se cargan en Amazon S3, pero no aparecen en Gateway2 hasta que se actualiza la caché. Esto se debe a que Gateway2 utiliza una versión almacenada localmente de los archivos 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 de gran tamaño pueden tardar algún tiempo en aparecer en Gateway2, por lo que puede interesarle recibir una notificación cuando haya finalizado la actualización de la 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 envía a través de 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	Description (Descripción)
version	Versión actual de la política de IAM.
id	ID que identifica la política de IAM.
detail-type	Descripción del tipo de evento que activó la notificación que se envió.
origen	LaAWSServicio que es el origen de la solicitud y la notificación.
cuenta	El ID de laAWScuenta desde la que se generaron la solicitud y la notificación.
tiempo	Fecha y hora en que se realizó la solicitud de actualización de los archivos del conjunto de trabajo.
region	LaAWSRegión desde la que se enviaron la solicitud y la notificación.
recursos	Recursos de Storage Gateway a los que se aplica la política.
event-type	CloudWatch Events que activaron la notificac ión.

Nombres de los campos	Description (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` .
started	cuando la gateway recibió el`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 tabla siguiente se describen las métricas de que abarcan las gateways de archivos de S3. Cada gateway tiene un conjunto de métricas asociado. Algunas de las métricas específicas de gateway tienen el mismo nombre que determinadas métricas específicas de recursos compartidos de archivos. 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 puerta de enlace o de recurso compartido. En concreto, cuando se trabaja con métricas de gateway, debe especificar la`Gateway Name`Para la gateway cuyos datos de métrica desea ver. Para obtener más información, consulte Uso de métricas de Amazon CloudWatch.

En la tabla siguiente se describen las métricas de que puede utilizar para obtener información sobre lasGateway de archivos S3.

Métrica	Description (Descripción)
`AvailabilityNotifications`	Esta métrica registra el número de notificaciones de estado relacionadas con la disponibi

Métrica	Description (Descripción)
	lidad que ha generado la gateway en el período de notificación. Unidades: Recuento
`CacheFileSize`	Esta métrica controla el tamaño de los archivos en la caché de la gateway. Utilice esta métrica con el`Average`estadística para medir el tamaño medio de un archivo en la caché de la puerta de enlace. Utilice esta métrica con el`Max`estadística para medir el tamaño máximo de un archivo en la caché de la puerta de enlace. Unidades: Bytes
`CacheFree`	Esta métrica indica el número de bytes disponibles en la caché de gateway. Unidades: Bytes
`CacheHitPercent`	Porcentaje de operaciones de lectura de la aplicación desde la gateway que se sirven desde la caché. La muestra se obtiene al final del período de notificación. Cuando no hay operaciones de lectura de la aplicación desde la gateway, esta métrica registra un valor del 100%. Unidades: Porcentaje

Métrica	Description (Descripción)
`CachePercentDirty`	Porcentaje total de memoria caché de gateway que no se ha almacenado de forma persisten te enAWS. La muestra se obtiene al final del período de notificación. Unidades: Porcentaje
`CachePercentUsed`	Porcentaje general del almacenamiento de caché de puerta de enlace que se utiliza. La muestra se obtiene al final del período de notificación. Unidades: Porcentaje
`CacheUsed`	Esta métrica indica el número de bytes usados en la caché de gateway. Unidades: Bytes
`CloudBytesDownloaded`	El número total de bytes que la gateway ha cargado aAWSdurante el período de que se informa. 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	Description (Descripción)
`CloudBytesUploaded`	El número total de bytes que la gateway ha descargado deAWSdurante el período de que se informa. 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
`FilesFailingUpload`	Esta métrica hace el seguimiento del número de archivos que no se cargan enAWS. Estos archivos generarán notificaciones de estado que contienen más información sobre el problema. Utilice esta métrica con el`Sum`estadística para mostrar el número de archivos que no se cargan actualmente enAWS. Unidades: Recuento
`FileSharesUnavailable`	Esta métrica proporciona el número de recursos compartidos de archivos de estas puertas de enlace que se encuentran en elNo disponibleestado. Si esta métrica informa que los recursos compartidos de archivos no están disponibl es, es probable que haya un problema con la puerta de enlace que pueda causar interrupc iones en el flujo de trabajo. Se recomienda crear una alarma para cuando esta métrica indica un valor distinto de cero. Unidades: Recuento

Métrica	Description (Descripción)
FilesRenamed	Esta métrica hace el seguimiento del número de archivos que se cambiaron de nombre en el período del informe. Unidades: Recuento
HealthNotifications	Esta métrica informa del número de notificac iones de estado generadas por esta puerta de enlace durante el período del informe. Unidades: Recuento
IoWaitPercent	Esta métrica registra el porcentaje de tiempo que la CPU está a la espera de una respuesta del disco local. Unidades: Porcentaje
MemTotalBytes	Esta métrica informa de la cantidad total de memoria de la puerta de enlace. Unidades: Bytes
MemUsedBytes	Esta métrica informa de la cantidad de memoria utilizada en la puerta de enlace. Unidades: Bytes
NfsSessions	Esta métrica indica el número de sesiones de NFS que están activas en la gateway. Unidades: Recuento

Métrica	Description (Descripción)
RootDiskFreeBytes	Esta métrica indica el número de bytes disponibles en el disco raíz de la gateway. Si esta métrica informa que menos de 20 GB son libres, debería aumentar el tamaño del disco raíz. Unidades: Bytes
S3GetObjectRequestTime	Esta métrica informa del tiempo para que la puerta de enlace complete las solicitudes de obtención de objetos de S3. Unidades: Milisegundos
S3PutObjectRequestTime	Esta métrica informa del tiempo para que la puerta de enlace complete las solicitudes de objetos de venta de S3. Unidades: Milisegundos
S3UploadPartRequestTime	Esta métrica informa del tiempo para que la puerta de enlace complete las solicitudes de artículos de carga de S3. Unidades: Milisegundos
SmbV1Sessions	Esta métrica indica el número de sesiones de SMBv1 que están activas en la gateway. Unidades: Recuento
SmbV2Sessions	Esta métrica indica el número de sesiones de SMBv2 que están activas en la gateway. Unidades: Recuento

Métrica	Description (Descripción)
`SmbV3Sessions`	Esta métrica indica el número de sesiones de SMBv3 que están activas en la gateway. Unidades: Recuento
`TotalCacheSize`	Esta métrica informa del tamaño total de la caché. Unidades: Bytes
`UserCpuPercent`	Esta métrica informa del porcentaje de tiempo dedicado al procesamiento de la puerta de enlace. Unidades: Porcentaje

Descripción de las métricas para compartir archivos

A continuación puede encontrar información acerca de las métricas de Storage Gateway que cubren 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 métricas de Amazon CloudWatch.

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

Métrica	Description (Descripción)
`CacheHitPercent`	Porcentaje de operaciones de lectura de la aplicación desde los recursos compartidos

Métrica	Description (Descripción)
	de archivos que se sirven desde la caché. La muestra se obtiene al final del período de notificación. Cuando no hay operaciones de lectura de la aplicación desde el recurso compartido de archivos, esta métrica registra un valor del 100%. Unidades: Porcentaje
`CachePercentDirty`	La contribución del recurso compartido de archivos al porcentaje total de memoria caché de la gateway que no se ha almacenado de forma persistente enAWS. La muestra se obtiene al final del período de notificación. Usar`CachePercentDirty` métrica de la gateway para ver el porcentaje total de memoria caché de la gateway que no se ha almacenado de forma persistente enAWS. Unidades: Porcentaje
`CachePercentUsed`	La contribución del recurso compartido de archivos al porcentaje de uso total de almacenamiento en memoria caché de la gateway. La muestra se obtiene al final del período de notificación. Use la métrica `CachePercentUsed` de la gateway para ver el porcentaje de uso total de almacenamiento en memoria caché de la gateway. Unidades: Porcentaje

Métrica	Description (Descripción)
`CloudBytesUploaded`	El número total de bytes que la gateway ha cargado aAWSdurante el período de que se informa. 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 que la gateway ha descargado deAWSdurante el período de que se informa. 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
`ReadBytes`	El número total de bytes leídos desde las aplicaciones on-premises en el período de notificación de 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

Métrica	Description (Descripción)
`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 file gateway

Los registros de auditoría de Amazon S3 File Gateway (S3 File Gateway) proporcionan detalles sobre el acceso de los usuarios a archivos y carpetas dentro 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 tabla siguiente se describen las operaciones de acceso al archivo de registro de auditoría de gateway de archivos.

Nombre de operación	Definición
Leer datos	Leer el contenido de un archivo.
Escribir datos	Cambiar el contenido de un archivo.
Create	Crear un nuevo archivo o carpeta.
Cambio de nombre	Cambiar el nombre de un archivo o carpeta existente.
Eliminar	Eliminar un archivo o carpeta.

Nombre de operación	Definición
Atributos de escritura	Actualizar metadatos de archivo o carpeta (ACL, propietario, grupo, permisos).

Atributos

En la tabla siguiente 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 PYME)	El dominio de Directorio Activo (AD) al que pertenece la cuenta del cliente.
`accountName` (solo PYME)	El nombre de usuario de Active Directory del cliente.
`bucket`	El nombre de bucket de S3.
`clientGid` (solo NFS)	Identificador del grupo de usuarios que tiene acceso al objeto.
`clientUid` (solo NFS)	El identificador del usuario que accede al objeto.
`ctime`	Hora en la que se modificó el contenido o los metadatos del objeto, establecida por el cliente.
`groupId`	Identificador del propietario del grupo 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.

Atributo	Definición
`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 PYME)	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.
`status`	El estado de la operación. Solo se registra el éxito (los errores se registran con la excepción de los errores que surgen de permisos denegados).
`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 tabla siguiente se describen los atributos de registro de auditoría de Gateway de archivos de S3 registrados en cada operación de acceso a archivos.

	Leer datos	Escribir datos	Create Folder	Crear archivo	Cambiar nombre de archivo/carpeta	Eliminar archivo/carpeta	Atributos de escritura (cambiar ACL -Solo para pymes)	Atributos de escritura (chown)	Atributos de escritura (chmod)	Atributos de escritura (chgrp)
`access`			X	X					X	
`accoun` `main` (solo PYME)	X	X	X	X	X	X	X	X	X	X
`accoun` `me` (solo PYME)	X	X	X	X	X	X	X	X	X	X
`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

	Leer datos	Escribir datos	Create Folder	Crear archivo	Cambiar nombre de archivo/carpeta	Eliminar archivo/carpeta	Atributos de escritura (cambiar ACL -Solo para pymes)	Atributos de escritura (chown)	Atributos de escritura (chmod)	Atributos de escritura (chgrp)
ctime			X	X						
groupI			X	X						
fileSinBytes				X						
gatewa	X	X	X	X	X	X	X	X	X	X
mtime			X	X						
newObjName					X					
objecte	X	X	X	X	X	X	X	X	X	X
objecte	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		
securiescrip (solo PYME)							X	X		

	Leer datos	Escribir datos	Create Folder	Crear archivo	Cambiar nombre de archivo/c arpeta	Eliminar archivo/c arpeta	Atributos de escritura (cambiar ACL -Solo para pymes)	Atributos de escritura (chown)	Atributos de escritura (chmod)	Atributos de escritura (chgrp)
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
versio	X	X	X	X	X	X	X	X	X	X

Mantenimiento de la gateway

El mantenimiento de la gateway incluye tareas tales como configurar el almacenamiento en caché y el espacio del búfer de carga y realizar el mantenimiento general del rendimiento de la gateway. Estas tareas son comunes para todos los tipos de gateways.

Temas

Apague la MV de la gateway

Puede que tenga que apagar la máquina virtual o reiniciarla para realizar tareas de mantenimiento, como aplicar un parche al hipervisor. Antes de apagar la MV, primero debe detener la gateway. En el caso de la gateway de archivos, apague la MV. Aunque esta sección se centra en iniciar y detener su gateway desde Storage Gateway Management Console, tenga en cuenta que también hacerlo desde la consola local de la MV o con la API de Storage Gateway. Cuando encienda la MV, recuerde reiniciar su gateway.

Puede que tenga que apagar la máquina virtual o reiniciarla para realizar tareas de mantenimiento, como aplicar un parche al hipervisor. En el caso de la gateway de archivos, apague la MV. No detenga la gateway. Aunque esta sección se centra en iniciar y detener su gateway desde Storage Gateway Management Console, tenga en cuenta que también hacerlo desde la consola local de la MV o con la API de Storage Gateway. Cuando encienda la MV, recuerde reiniciar su gateway.

- Consola local de la MV de la gateway: consulteRealización de tareas de mantenimiento en la consola local.
- API de Storage Gateway: consulteShutdownGateway

Administración de discos locales para Storage Gateway

La máquina virtual (VM) de la gateway utiliza los discos locales que se le asignan on-premise para almacenamiento en búfer y permanente. Las gateways creadas en instancias de Amazon EC2 utilizan volúmenes de Amazon EBS como discos locales.

Temas

Decidir la cantidad de almacenamiento en disco local

Puede elegir el número y el tamaño de los discos que va a asignar a la gateway. La gateway requiere el siguiente almacenamiento adicional:

Las gateways de archivos requieren al menos un disco para utilizar como caché. En la siguiente tabla se recomiendan los tamaños para el almacenamiento en disco local de gateway implementada. Puede agregar almacenamiento local más adelante, después de haber configurado la gateway, para responder al aumento de las cargas de trabajo.

Almacenamiento local	Description (Descripción)	Tipo de gateway
Almacenamiento en caché	El almacenamiento en caché funciona como un almacén on-premise permanente para los datos que están pendientes de carga en Amazon S3 o en file system.	• Gateways de archivos

> **Note**
>
> Los recursos de almacenamiento físico subyacente 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. Cuando aprovisione un disco local (por ejemplo, para utilizarlo como almacenamiento en caché), tiene la opción de almacenar el disco virtual en el mismo almacén de datos que la MV 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 respaldado por un único disco físico subyacente puede provocar un rendimiento deficiente en algunas situaciones cuando se utiliza para respaldar el almacenamiento en caché. Lo mismo sucede si el disco tiene una configuración RAID de menor rendimiento, como RAID1.

Tras la configuración e implementación iniciales de la gateway, puede ajustar el almacenamiento local agregando discos para el almacenamiento en caché.

Determinación del tamaño del almacenamiento de caché que se va a asignar

La gateway utiliza el almacenamiento en caché para proporcionar acceso de baja latencia a los datos a los que se ha tenido acceso recientemente. El almacenamiento en caché funciona como un almacén on-premise permanente para los datos que están pendientes de carga en Amazon S3 o en file system. Para obtener más información sobre cómo calcular el tamaño del almacenamiento en caché, consulte Administración de discos locales para Storage Gateway.

Inicialmente se puede utilizar esta aproximación para aprovisionar los discos para el almacenamiento en caché. A continuación, puede utilizar las métricas operativas de Amazon CloudWatch para monitorizar el uso del almacenamiento en caché y aprovisionar más almacenamiento según sea necesario desde la consola. Para obtener información sobre cómo usar las métricas y configurar las alarmas, consulte Desempeño.

Agregar almacenamiento en caché

A medida que cambian las necesidades de la aplicación, puede aumentar la capacidad de almacenamiento en caché de la gateway. Puede agregar más capacidad de caché a la gateway sin interrumpir las funciones de esta. Cuando aumente la capacidad de almacenamiento, hágalo con la máquina virtual de gateway encendida.

> **Important**
>
> Cuando se agrega caché a una gateway existente, es importante crear nuevos discos en el host (hipervisor o instancia de Amazon EC2). No cambie el tamaño de los discos si se han asignado previamente como caché. No elimine discos de almacenamiento en caché que se hayan asignado para esa función.

En el siguiente procedimiento se muestra cómo configurar o almacenar en caché el almacenamiento en caché para la gateway.

Para agregar y configurar o almacenar en caché

1. Aprovisione un disco nuevo en el host (el hipervisor o la instancia de Amazon EC2). Para obtener información sobre cómo aprovisionar un disco en un hipervisor, consulte el manual de usuario del hipervisor. Debe configurar este disco como almacenamiento en caché.
2. Abrir la consola de Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
3. En el panel de navegación, elija Gateways.
4. En el menú Actions (Acciones), elija Edit local disks (Editar discos locales).
5. En el cuadro de diálogo Edit local disks, identifique los discos que ha aprovisionado y decida cuáles de ellos desea utilizar para el almacenamiento en caché.

   Si los discos no aparecen, seleccione el botón Refresh (Actualizar).
6. Elija Save (Guardar) para guardar la configuración.

Uso del 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 ofrecen un almacenamiento de nivel de bloques temporal para la instancia de Amazon EC2. Los discos efímeros son perfectos para el almacenamiento temporal de datos que se modifican con frecuencia, como los datos de un almacenamiento en caché de una gateway. Cuando se lanza la gateway con una Amazon EC2 Amazon Machine Image de y el tipo de instancia seleccionado es compatible con el almacenamiento efímero, los discos se muestran automáticamente y puede seleccionar uno de ellos para almacenar datos en la memoria caché de la

gateway. Para obtener más información, consulteAlmacén de instancias Amazon EC2en laGuía del usuario de Amazon EC2 para instancias de Linux.

Las operaciones de escritura de las aplicaciones en los discos se almacenan en la memoria caché de forma síncrona y se cargan de forma asíncrona en el almacenamiento duradero en Amazon S3. Si los datos almacenados en el almacenamiento efímero se pierden debido a que una instancia de Amazon EC2 se detiene antes de que haya finalizado la carga de datos, los datos que todavía se encuentran en la memoria caché y no se han cargado en Amazon S3 se pueden perder. Puede evitar dicha pérdida de datos realizando los pasos siguientes antes de reiniciar o detener la instancia EC2 que aloja la gateway.

> **Note**
>
> Si utiliza el almacenamiento efímero y detiene e inicia la gateway, esta se desconectará permanentemente. Esto sucede porque se ha reemplazado el disco de almacenamiento físico. No hay solución para este problema, por lo que tendrá que eliminar la gateway y activar una nueva en una nueva instancia EC2.

Los pasos del procedimiento siguiente son específicos para las gateways de archivos.

Para evitar la pérdida de datos de las gateways de archivos que utilizan discos efímeros

1. Detenga todos los procesos de escritura en el recurso compartido de archivos.
2. Suscríbase para recibir notificaciones de CloudWatch Events. Para obtener información, consulte Cómo recibir notificaciones de las operaciones de archivos.
3. Llame a lasNotifyWhenUploaded la APIpara recibir notificaciones cuando los datos que se han escrito, hasta que se perdió 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.

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

Administración del ancho de banda para la gateway de archivos de Amazon S3

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

Puede configurar una programación límite de tasa de ancho de banda mediante laAWS Management Console, unAWSEl kit de desarrollo de software (SDK) o laAWS Storage GatewayAPI (consulteActualización del calendario límite de velocidad de ancho de bandaen laAWSReferencia de la API de Storage.). Mediante un programa de límites de velocidad de ancho de banda, puede configurar los límites para que cambien automáticamente durante el día o la semana. Para obtener más información, consulte Ver y editar la programación límite de velocidad de ancho de banda de la puerta de enlace mediante la consola de Storage Gateway.

> **Note**
>
> Actualmente, el tipo Amazon FSx File Gateway no admite la configuración de límites de velocidad de ancho de banda y programas.

Temas

- Ver y editar la programación límite de velocidad de ancho de banda de la puerta de enlace mediante la consola de Storage Gateway
- Actualización de los límites de ancho de banda de la gateway medianteAWS SDK for Java
- Actualización de los límites de ancho de banda de la gateway medianteAWS SDK for .NET
- Actualización de los límites de ancho de banda de la gateway medianteAWS Tools for Windows PowerShell

Ver y editar la programación límite de velocidad de ancho de banda de la puerta de enlace mediante la consola de Storage Gateway

En esta sección se describe cómo ver y editar la programación de límites de ancho de banda de la gateway.

Para ver y editar la programación de los límites de ancho de banda

1. Abra la consola Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
2. En el panel de navegación izquierdo, elijaGateways dey, a continuación, elija la gateway que desee administrar.
3. ParaActions, eligeEdición de la programación límite de velocidad de ancho.

   La programación límite de velocidad de ancho de banda actual de la puerta de enlace se muestra en elEdición de la programación límite de velocidad de ancho(Se ha creado el certificado). De forma predeterminada, una nueva puerta de enlace no tiene límites de velocidad de ancho de banda definidos.
4. (Opcional) ElijaAñadir nuevo límite de velocidad de ancho de bandapara añadir un nuevo intervalo configurable a la programación. Para cada intervalo que agregue, especifique la siguiente información:

   - Velocidad de subida— Introduzca el límite de velocidad de carga, en megabits por segundo (Mbps). El valor mínimo es 100 Mbps.
   - Días de la semana— Seleccione el día o los días de cada semana en que desea que se aplique el intervalo. Puede aplicar el intervalo entre semana (de lunes a viernes), fines de semana (sábado y domingo), todos los días de la semana o un día específico cada semana. Para aplicar el límite de ancho de banda de forma uniforme y constante en todos los días y en todo momento, elijaSin horario.
   - Hora de inicio— Introduzca la hora de inicio del intervalo de ancho de banda, utilizando el formato HH:MM y el desplazamiento de zona horaria con respecto a UTC para su puerta de enlace.

     > **Note**
     >
     > El intervalo límite de velocidad de ancho de banda 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 desplazamiento de zona horaria con respecto a GMT para la puerta de enlace.

> **Important**
>
> El intervalo límite de velocidad de ancho de banda finaliza al final del minuto especificado aquí. Para programar un intervalo que finaliza al final de una hora, introduzca**59**.
> Para programar intervalos continuos consecutivos, la transición al comienzo de la hora, sin interrupción entre los intervalos, introduzca**59**para el minuto final del primer intervalo. Entrar**00**para el minuto de inicio del intervalo siguiente.

5. (Opcional) Repita el paso anterior según sea necesario hasta que finalice el calendario de límite de ancho de banda. Si necesitas eliminar un intervalo de tu programación, eligeRemove.

> **Important**
>
> Los intervalos límite de velocidad de ancho de banda no se pueden solapar. La hora de inicio de un intervalo debe producirse después de la hora final de un intervalo anterior y antes de la hora de inicio de un intervalo siguiente.

6. Cuando haya terminado, seleccioneGuarde los cambios.

Actualización de los límites de ancho de banda de la gateway medianteAWS SDK for Java

Si actualiza los límites de ancho de banda mediante programación, puede ajustar estos límites automáticamente durante un periodo de tiempo, por ejemplo, mediante la utilización de tareas programadas. En el siguiente ejemplo se ilustra cómo actualizar los límites de ancho de banda de una gateway medianteAWS SDK for 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 for Java.

Example : Actualización de los límites de ancho de banda de la gateway medianteAWS SDK for Java

El siguiente ejemplo de código Java actualiza los límites de ancho de banda de una gateway. Para utilizar este código de ejemplo, debe proporcionar el punto de enlace de servicio, el Nombre de recurso de Amazon (ARN) y el límite de carga. Para obtener una lista deAWSpuntos finales de servicio que puede utilizar con Storage Gateway, consulteAWS Storage GatewayCuotas y puntos de enlace deen laAWSReferencia general de.

```
   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 la gateway medianteAWS SDK for .NET

Si actualiza los límites de ancho de banda mediante programación, puede ajustar estos límites automáticamente durante un periodo de tiempo, por ejemplo, mediante la utilización de tareas programadas. En el siguiente ejemplo se ilustra cómo actualizar los límites de ancho de banda de una gateway medianteAWSKit de desarrollo de software (SDK) para .NET. 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 for .NET.

Example : Actualización de los límites de ancho de banda de la gateway medianteAWS SDK for .NET

El siguiente ejemplo de código C# actualiza los límites de ancho de banda de una gateway. Para utilizar este código de ejemplo, debe proporcionar el punto de enlace de servicio, el Nombre de recurso de Amazon (ARN) y el límite de carga. Para obtener una lista deAWSpuntos finales de servicio que puede utilizar con Storage Gateway, consulteAWS Storage GatewayCuotas y puntos de enlace deen laAWSReferencia general de.

```
    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 =
updateBandwidthRateLimitScheduleResponse.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 la gateway medianteAWS Tools for Windows PowerShell

Si actualiza los límites de ancho de banda mediante programación, puede ajustar estos límites automáticamente durante un periodo de tiempo, por ejemplo, mediante la utilización de tareas programadas. En el siguiente ejemplo se ilustra cómo actualizar los límites de ancho de banda de una gateway medianteAWS Tools for Windows PowerShell. Para utilizar el código del ejemplo, debe haberse familiarizado con la ejecución de scripts de PowerShell. Para obtener más información, consulte la introducción de la Guía del usuario de AWS Tools for Windows PowerShell.

Example : Actualización de los límites de ancho de banda de la gateway medianteAWS Tools for Windows PowerShell

El siguiente ejemplo de script de PowerShell actualiza los límites de ancho de banda de una gateway. Para utilizar este script de ejemplo, debe proporcionar el Nombre de recurso de Amazon (ARN) de la gateway 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)
```

Administración de actualizaciones de gateways mediante la consola de AWS Storage Gateway

Storage Gateway publica periódicamente versiones de software importantes para su gateway. Puede aplicar actualizaciones manualmente en Storage Gateway de administración de o automáticamente durante el periodo de mantenimiento que haya configurado. Aunque Storage Gateway comprueba si hay actualizaciones cada minuto, solo realiza el proceso de mantenimiento y reinicio si hay actualizaciones.

Las versiones de software Gateway incluyen periódicamente actualizaciones del sistema operativo y parches de seguridad que han sido validados porAWS. Estas actualizaciones se publican normalmente cada seis meses y se aplican como parte del proceso de actualización normal de la puerta de enlace durante los períodos de mantenimiento programados.

> **Note**
>
> Debe tratar el dispositivo Storage Gateway como un dispositivo integrado administrado y no debe intentar acceder ni modificar su instalación de ninguna manera. Si se intenta instalar o actualizar cualquier paquete de software mediante métodos distintos del mecanismo de actualización de la puerta de enlace normal (por ejemplo, herramientas de SSM o hipervisor) puede provocar un mal funcionamiento de la puerta de enlace.

Antes de aplicar cualquier actualización a la puerta de enlace,AWSle avisa con un mensaje en la consola de Storage Gateway y enAWS Health Dashboard. Para obtener más información, consulte AWS Health Dashboard. La máquina virtual no se reinicia, pero la puerta de enlace no está disponible durante un breve periodo mientras se actualiza y se reinicia.

Cuando implemente y active la gateway, se establecerá un calendario de mantenimiento semanal predeterminado. Puede modificar el calendario de mantenimiento en cualquier momento. Cuando haya actualizaciones disponibles, la pestaña Details (Detalles) mostrará un mensaje de mantenimiento. Podrá ver la fecha y la hora en que se aplicó la última actualización correcta de la gateway en la pestaña Details (Detalles).

Para modificar el calendario de mantenimiento

1. Abra la consola Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
2. En el panel de navegación, elija Gateways y, a continuación, elija la gateway cuyo calendario de actualizaciones desea modificar.
3. En Actions (Acciones), elija Edit maintenance window (Editar periodo de mantenimiento) para abrir el cuadro de diálogo Edit maintenance start time (Editar hora de inicio del periodo de mantenimiento).
4. En Schedule, (Programación), elija Weekly (Semanal) o Monthly (Mensual) para programar las actualizaciones.
5. Si elige Weekly (Semanal), modifique los valores de Day of the week (Día de la semana) y Time (Hora).

Si elige Monthly (Mensual), modifique los valores de Day of the month (Día del mes) y Time (Hora). Si selecciona esta opción y se produce un error, significa que la gateway tiene una versión antigua y que aún no se ha actualizado a la versión más reciente.

> **Note**
>
> El valor máximo que se puede establecer para el día del mes es 28. Si se selecciona 28, la hora de inicio del mantenimiento será el día 28 de cada mes.

La hora de inicio del mantenimiento aparece en elDetalles depara la puerta de enlace la próxima vez que abra elDetalles dePestaña.

Realización de tareas de mantenimiento en la consola local

Puede realizar las siguientes tareas de mantenimiento utilizando la consola local del host. Las tareas de la consola local pueden realizarse en el host de la MV o en la instancia de Amazon EC2. Muchas de las tareas son comunes entre los distintos hosts, pero también hay algunas diferencias.

Temas

Realización de tareas en la consola local de la máquina virtual (gateway de archivos)

En una gateway de archivos implementada de forma local, puede realizar las siguientes tareas de mantenimiento utilizando la consola local del host de la máquina virtual. Estas tareas son comunes a hipervisores de VMware, Microsoft Hyper-V y de la máquina virtual de Linux basada en el kernel (KVM).

Temas

- Configuración de un proxy HTTP
- Configuración de la red de la puerta de enlace
- Probar la conectividad de red de su gateway
- Ver el estado de los recursos del sistema de gateway
- Configuración de un servidor NTP (Network Time Protocol) para la gateway
- Ejecución de comandos de gateway de almacenamiento en la consola local
- Configuración de adaptadores de red para la gateway

Inicio de sesión en la consola local de la gateway de archivos

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 de local, utilice el nombre de usuario y la contraseña predeterminados para iniciar sesión. Estas credenciales de inicio de sesión predeterminadas proporcionan acceso a menús donde puede configurar los ajustes de red y cambiar la contraseña de la consola local.AWS Storage Gatewayle permite definir su propia contraseña desde la consola de Storage Gateway en lugar de cambiar la contraseña desde la consola local. No es necesario que conozca la contraseña predeterminada para establecer una nueva contraseña. Para obtener más información, consulte Inicio de sesión en la consola local de la gateway de archivos.

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**
>
> Le recomendamos que cambie la contraseña predeterminada. Para ello, ejecute el comando `passwd` desde el menú de la consola local (elemento 6 del menú principal).

Para obtener información acerca de cómo ejecutar el comando, consulte Ejecución de comandos de gateway de almacenamiento en la consola local. También puede establecer la contraseña desde la consola de Storage Gateway. Para obtener más información, consulte Inicio de sesión en la consola local de la gateway de archivos.

Configuración de la contraseña de la consola local desde la consola de 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. Puede establecer esta contraseña desde la consola de AWS Storage Gateway en lugar de hacerlo desde la consola local, si lo desea. 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. Abrir la consola de Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
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 MV.

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

Configuración de un proxy HTTP

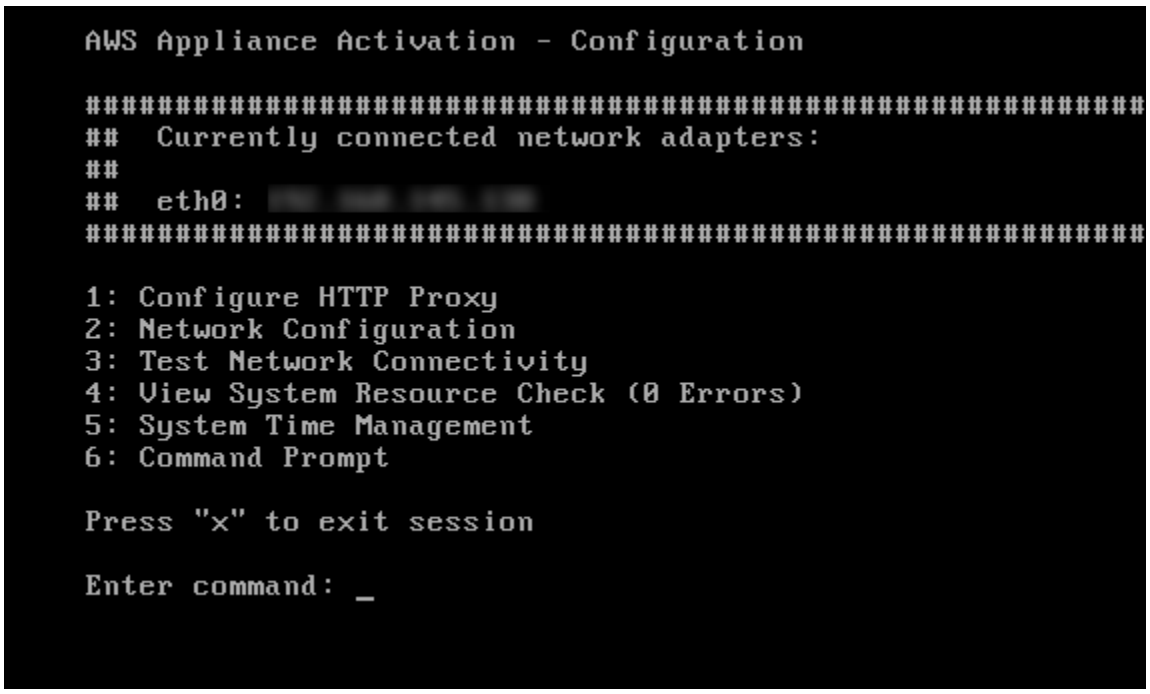
Las gateways de archivos admiten la configuración de un proxy HTTP.

> **Note**
>
> La única configuración de proxy que admiten las gateways de archivos es HTTP.

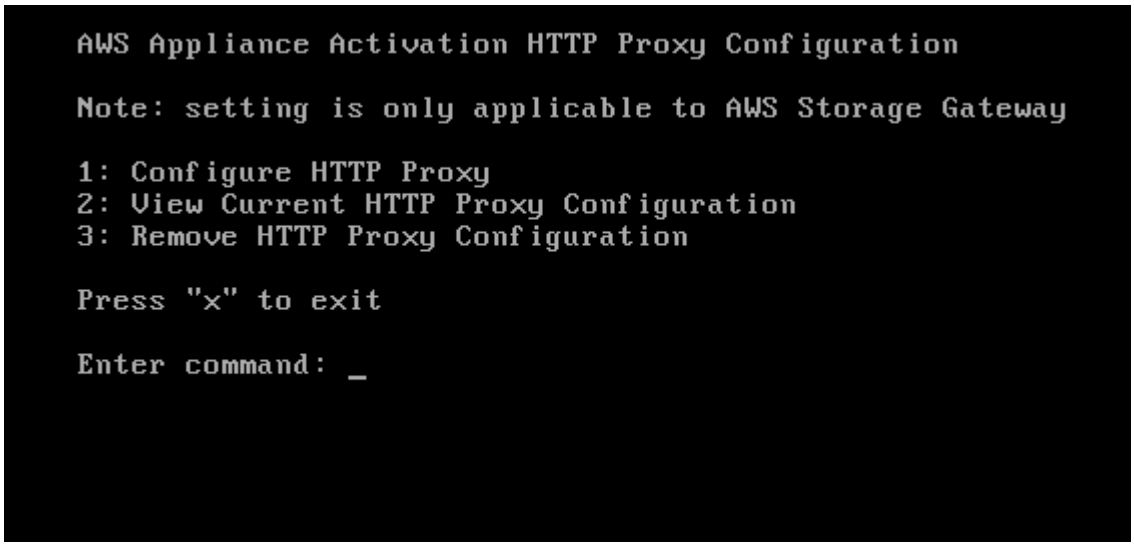
Si la gateway debe utilizar un servidor proxy para comunicarse con Internet, debe configurar los ajustes del proxy HTTP para la gateway. Para ello, especifique una dirección IP y un número de puerto para el host en el que se ejecuta el proxy. Después de hacerlo, Storage Gateway rutea todosAWSTráfico de endpoint a través del servidor proxy. Las comunicaciones entre la puerta de enlace y los endpoints se cifran, 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 gateway de archivos

1. Inicie sesión en la consola local de la gateway:
   - Para obtener más información sobre el inicio de sesión en la consola local de VMware ESXi, consulte Acceso a la consola local de la 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 la páginaAWSActivación del dispositivo: configuraciónMenú principal, introduzca**1**para empezar a configurar el proxy HTTP.



3. En el menú HTTP Proxy Configuration (Configuración de proxy HTTP), introduzca **1** y proporcione el nombre de host del servidor proxy HTTP.



Puede configurar otras opciones de HTTP en este menú, como se muestra a continuación.

Para	Haga lo siguiente
Configurar un proxy HTTP	Escriba **1**.

Para	Haga lo siguiente
	Debe proporcionar un nombre de host y un puerto para completar la configuración.
Ver la configuración del proxy HTTP actual	Escriba **2**. Si no se ha 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	Escriba **3**. Se muestra el mensaje `HTTP Proxy Configuration Removed` .

4. Reinicie la máquina virtual para aplicar la configuración de HTTP.

Configuración de la red de la puerta de enlace

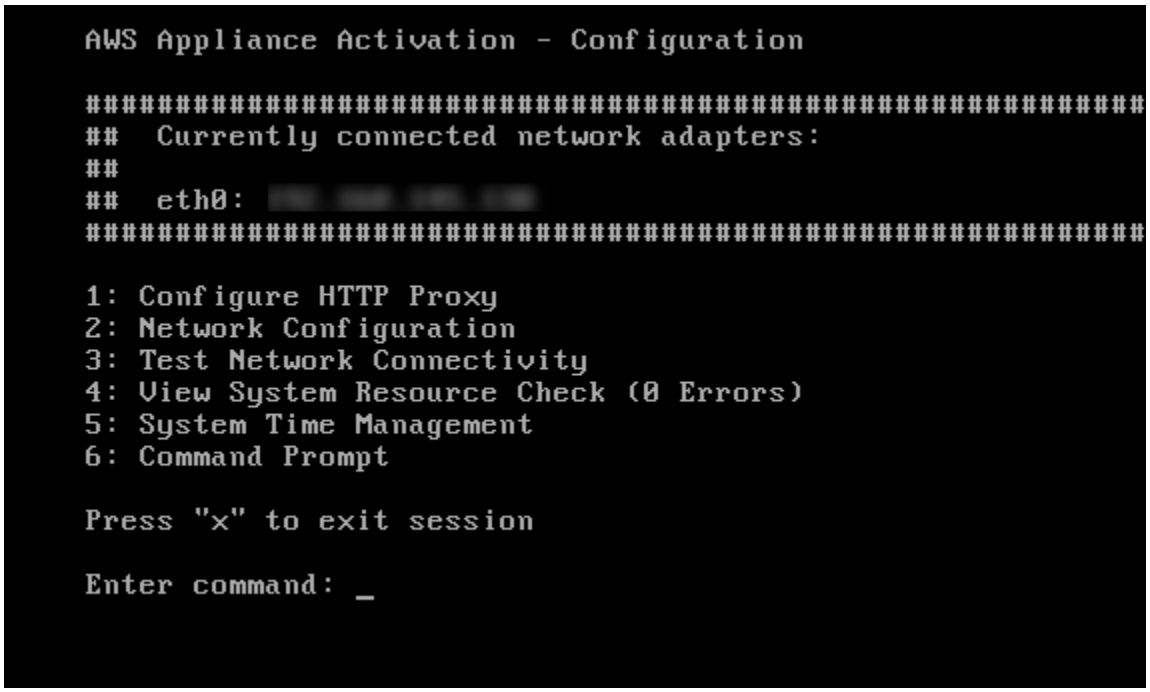
La configuración de red predeterminada de la gateway es DHCP (Dynamic Host Configuration Protocol). Con DHCP, a la gateway se le asigna automáticamente una dirección IP. En algunos casos, es posible que tenga que asignar manualmente la IP de la gateway como una dirección IP estática, como se describe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

Para configurar la gateway para que utilice direcciones IP estáticas

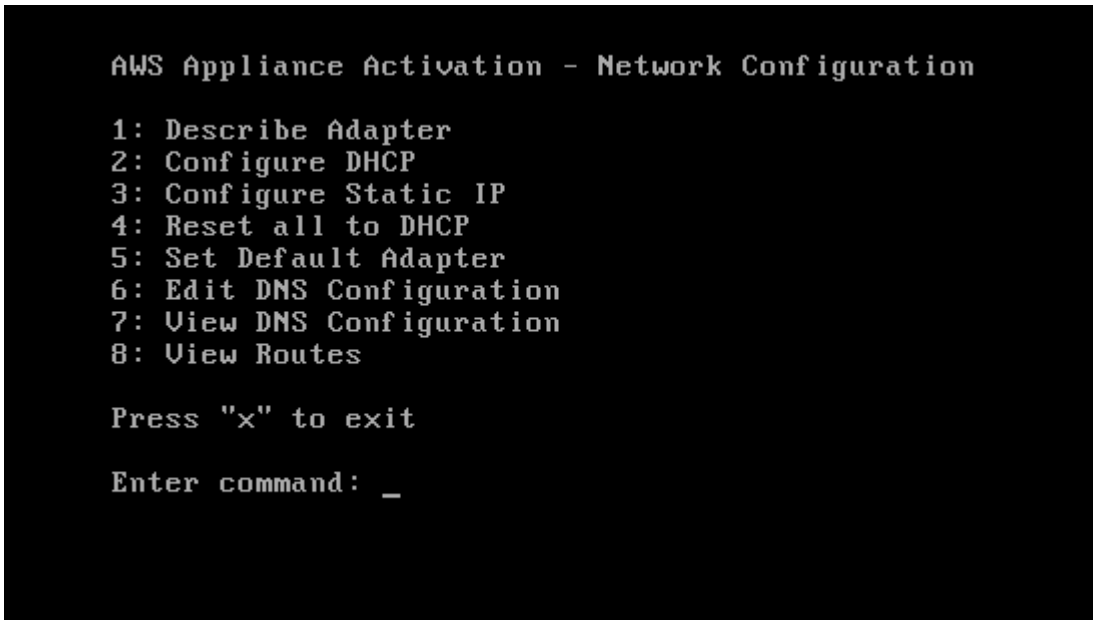
1. Inicie sesión en la consola local de la gateway:

   - Para obtener más información sobre el inicio de sesión en la consola local de VMware ESXi, consulte Acceso a la consola local de la 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 la páginaAWSActivación del dispositivo: configuraciónMenú principal, introduzca**2**para empezar a configurar la red.

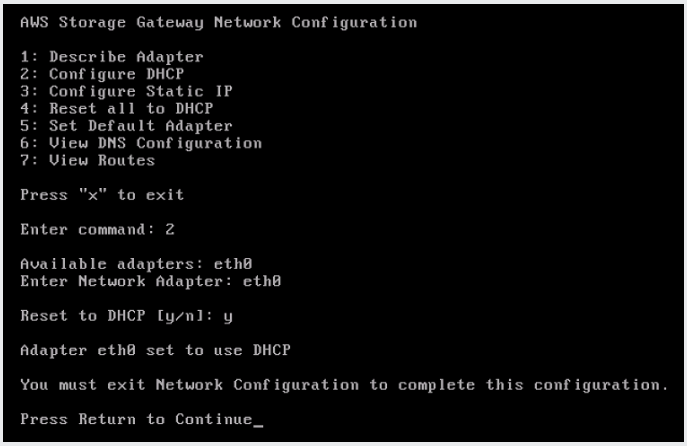


3. Elija una de las siguientes opciones en el menú Network Configuration (Configuración de red).



Para	Haga lo siguiente
Obtener información sobre el adaptador de red	Escriba **1**.

Para	Haga lo siguiente
	Aparecerá una lista de nombres de adaptador y se le pedirá que introduzca el nombre de un adaptador; por ejemplo,**`eth0`**. Si el adaptador que especifique está en uso, se mostrará la siguiente información acerca del adaptador: • Dirección MAC (Media Access Control) • Dirección IP • Máscara de red • Dirección IP de la gateway • Estado de habilitación de DHCP Puede utilizar el mismo nombre de adaptador cuando configure una dirección IP estática (opción 3) que cuando configure el adaptador de ruta predeterminada de la gateway (opción 5).

Para	Haga lo siguiente
Configuración de DHCP	Escriba **2**. Se le pedirá que configure la interfaz de red para utilizar DHCP. 

Para	Haga lo siguiente
Configurar una dirección IP estática para la gateway	Escriba **3**. 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 gateway 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 Apague la MV de la gateway. Si la gateway utiliza más de una interfaz de red, debe configurar todas las interfaces habilitadas para que utilicen DHCP o direcciones IP estáticas.

Para	Haga lo siguiente
	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 deshabilitará. Para habilitar 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.
Restablecer toda la configuración de red de la gateway a DHCP	Escriba **4**. Todas las interfaces de red se configuran para utilizar DHCP. **Important** Si la gateway 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 Apague la MV de la gateway.
Establecer el adaptador de ruta predeterm inada del gateway	Escriba **5**. Se mostrarán los adaptadores disponibles para la gateway y se le pedirá que elija uno de los adaptadores; por ejemplo,**eth0**.

Para	Haga lo siguiente
Editar la configuración de DNS de la gateway	Escriba **6**. Se muestran los adaptadores disponibles de los servidores DNS primario y secundario. Se le pedirá que proporcione la dirección IP nueva.
Ver la configuración de DNS de la ruta de enlace	Escriba **7**. Se muestran los adaptadores disponibles de los servidores DNS primario y secundario. **Note** En algunas versiones del hipervisor de VMware es posible editar la configura ción del adaptador en este menú.
Ver tablas de ruteo	Escriba **8**. Se muestra la ruta predeterminada de la gateway.

Probar la conectividad de red de su gateway

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

Para probar la conectividad de red de la gateway

1. Inicie sesión en la consola local de la gateway:
   - Para obtener más información sobre el inicio de sesión en la consola local de VMware ESXi, consulte Acceso a la consola local de la 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. Desde lasAWSActivación del dispositivo: configuraciónmenú principal, introduzca el número correspondiente para seleccionarPrueba de conectividad de red.

   Si la puerta de enlace ya se ha activado, la prueba de conectividad comienza inmediatamente. Para las puertas de enlace que aún no se han activado, debe especificar el tipo de punto final yRegión de AWStal y 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 final de la puerta de enlace.
4. Si ha seleccionado el tipo de punto final público, introduzca el número correspondiente para seleccionar laRegión de AWSque quieres probar. Para admitidoRegiones de AWSy una lista deAWSendpoints de servicio que puede utilizar con Storage Gateway, consulteAWS Storage GatewayCuotas y puntos de enlace deen laAWSReferencia general de.

A medida que avanza la prueba, cada punto final se muestra[PASSED]o[FAILED], indicando el estado de la conexión de la siguiente manera:

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

Ver el estado de los recursos del sistema de gateway

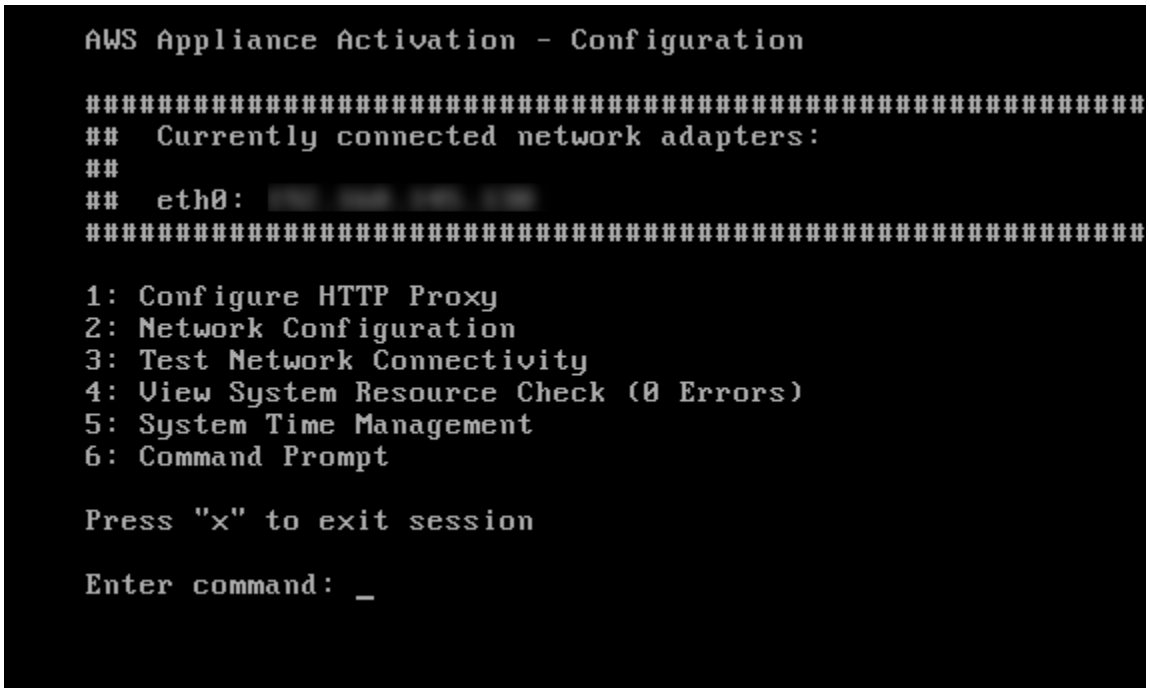
Cuando la gateway se inicia, comprueba sus núcleos de CPU virtuales, el tamaño del volumen raíz y la RAM. Acto seguido, determina si estos recursos del sistema son suficientes para que la gateway funcione correctamente. Puede ver los resultados de esta comprobación en la consola local de la gateway.

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 el inicio de sesión en la consola de VMware ESXi, consulte Acceso a la consola local de la 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 navegadorAWSActivación del dispositivo: configuraciónMenú principal, introduzca**4**Para ver los resultados de una comprobación de recursos del sistema.



La consola muestra un mensaje [OK], [WARNING] o [FAIL] para cada recurso, como se describe en la tabla siguiente.

Mensaje	Description (Descripción)
[OK]	El recurso ha superado la comprobación de recursos del sistema.
[WARNING]	El recurso no satisface los requisitos recomendados, pero la gateway puede continuar funcionando. Storage Gateway

Mensaje	Description (Descripción)
	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 gateway no funcione correctamente. Storage Gateway muestra un mensaje en el que se describen los resultados de la comprobación de recursos.

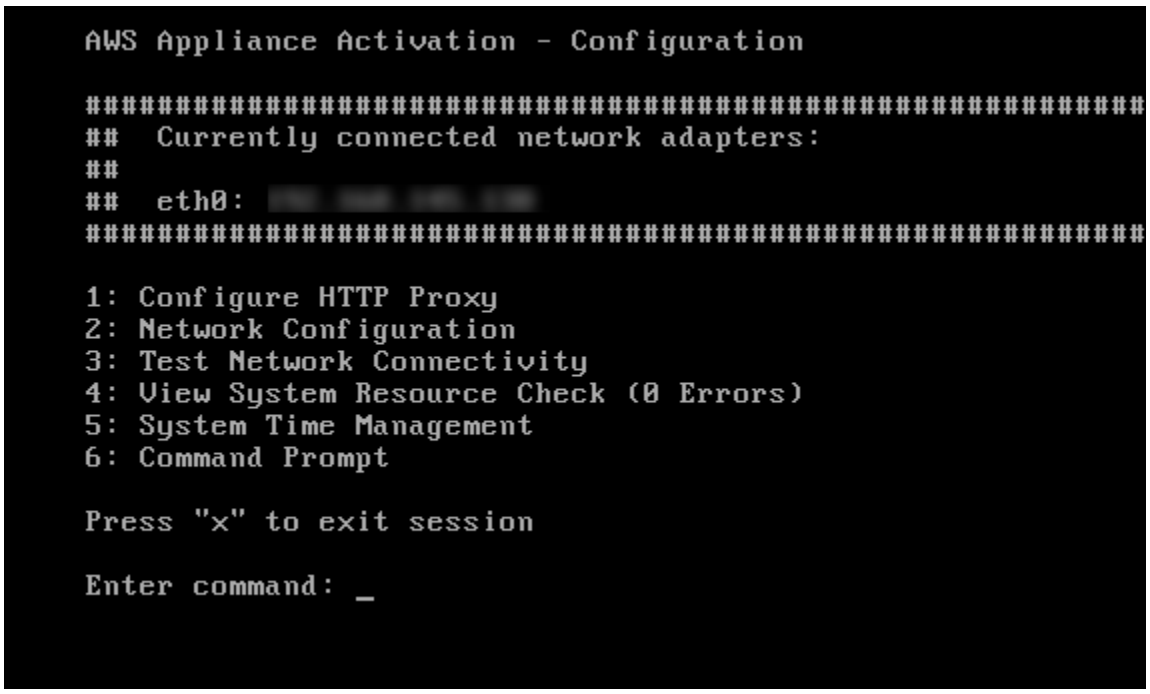
La consola también muestra el número de errores y advertencias junto a la opción de menú de comprobación de recursos.

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

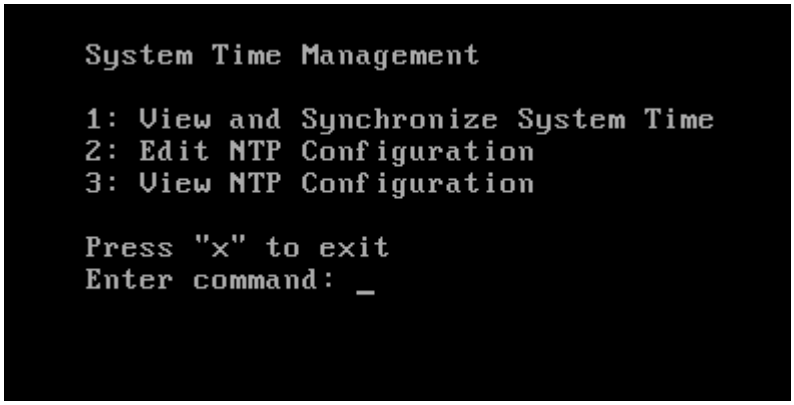
Puede ver y editar las configuraciones del servidor NTP (Network Time Protocol) y sincronizar la hora de la máquina virtual de la gateway con el host del hipervisor.

Para administrar la hora del sistema

1. Inicie sesión en la consola local de la gateway:
   - Para obtener más información sobre el inicio de sesión en la consola local de VMware ESXi, consulte Acceso a la consola local de la 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 navegadorAWSActivación del dispositivo: configuraciónMenú principal, introduzca**5**para administrar el tiempo de su sistema.



3. En el menú System Time Management (Administración de la hora del sistema), elija una de las siguientes opciones.



Para	Haga lo siguiente
Ver y sincronizar la hora de la máquina virtual con la hora del servidor NTP.	Escriba **1**. Se muestra la hora actual de la máquina virtual. La gateway de archivos determina la diferencia horaria entre la máquina virtual de la gateway y la hora del servidor NTP, y le pide

Para	Haga lo siguiente
	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 tales como las instantáneas y las horas reales a las que se producen las operaciones. Para una gateway implementada en VMware ESXi, el ajuste de la hora del host del hiperviso r y la sincronización de la hora de la MV con el host es suficiente para evitar desviacio nes de tiempo. Para obtener más informaci ón, consulte Sincronización de la hora de la máquina virtual y el host. 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 MV de la gateway. 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.

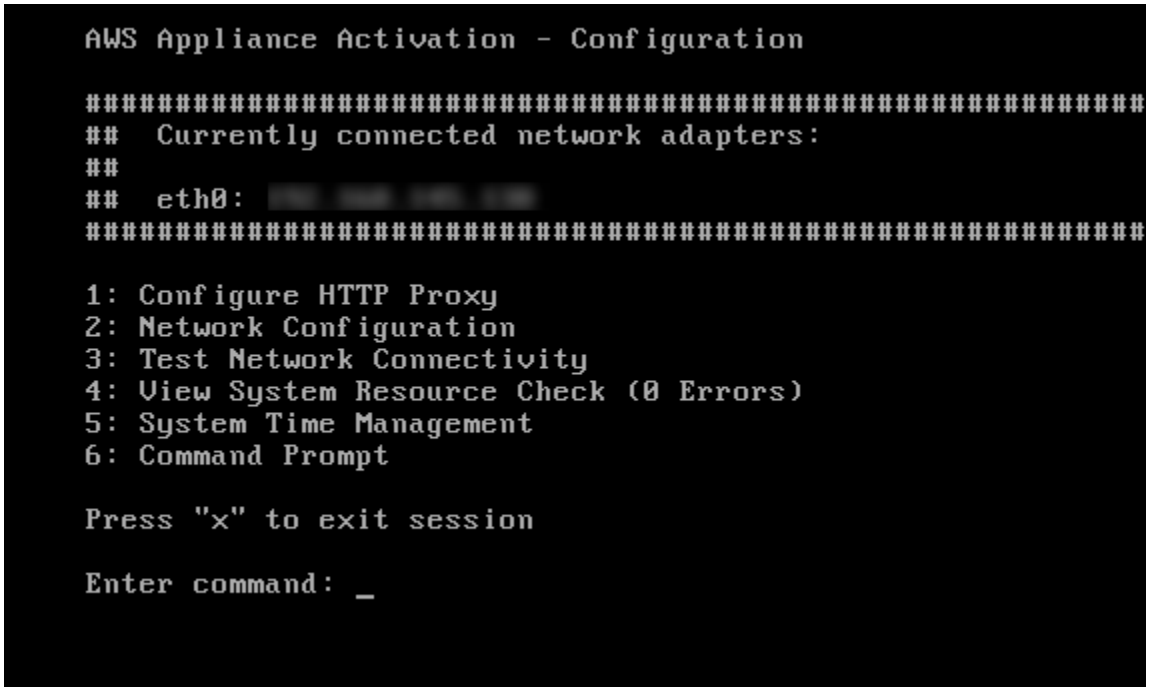
Para	Haga lo siguiente
Editar la configuración del servidor NTP	Escriba **2**. El sistema le pedirá que proporcione un servidor NTP preferido y uno secundario.
Ver la configuración del servidor NTP	Escriba **3**. Se mostrará la configuración del servidor NTP.

Ejecución de comandos de gateway de almacenamiento 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 gateway. Puede utilizar los comandos de la consola local para realizar tareas de mantenimiento, tales como guardar tablas de enrutamiento, conectarse a Amazon Web Services Support, etc.

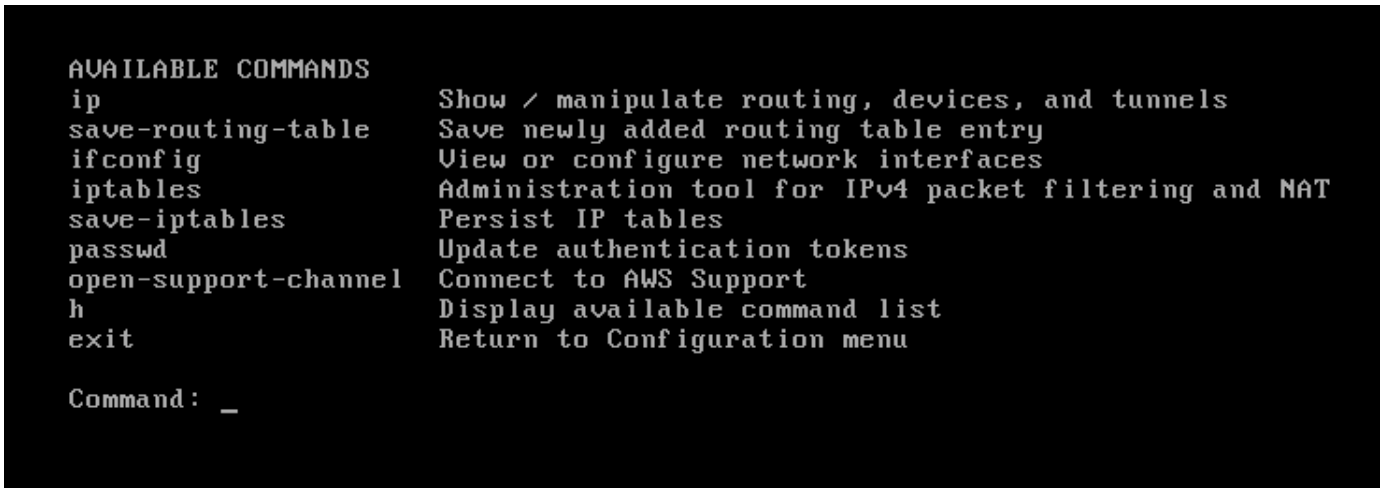
Para ejecutar un comando de configuración o diagnóstico

1. Inicie sesión en la consola local de la gateway:
   - Para obtener más información sobre el inicio de sesión en la consola local de VMware ESXi, consulte Acceso a la consola local de la 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 la páginaAWSActivación del dispositivo: configuraciónMenú principal, introduzca**6**paraSímbolo del sistema.



3. En la páginaAWSActivación del dispositivo: símbolo del sistemaconsola, introduzca**h**y, a continuación, pulse laDevoluciónClave.

   La consola muestra el menú AVAILABLE COMMANDS (COMANDOS DISPONIBLES) con una descripción que hacen los comandos, tal como se muestra en la siguiente captura de pantalla.



4. En el símbolo del sistema, introduzca el comando que desea utilizar y siga las instrucciones.

Para obtener información sobre un comando, introduzca el nombre del comando en el símbolo del sistema.

Configuración de adaptadores de red para la gateway

De forma predeterminada, Storage Gateway está configurada para utilizar el tipo de adaptador de red E1000, pero puede reconfigurar la gateway para que utilice el adaptador de red VMXNET3 (10 GbE). También puede configurar Storage Gateway para permitir el acceso por más de una dirección IP. Para ello, configure la gateway para que utilice más de un adaptador de red.

Temas

Configuración de la gateway para que utilice el adaptador de red VMXNET3

Storage Gateway es compatible con el tipo de adaptador de red E1000, tanto en hosts de VMware ESXi como de Microsoft Hyper-V Hypervisor. Sin embargo, el tipo de adaptador de red VMXNET3 (10 GbE) solo es compatible con el hipervisor de VMware ESXi. Si la gateway está alojada en un hipervisor VMware ESXi, puede reconfigurar la gateway para que utilice el adaptador VMXNET3 (10 GbE). Para obtener más información sobre este adaptador, consulte el sitio web de VMware.

Para hosts de hipervisor KVM, Storage Gateway admite el uso de`virtio`controladores de dispositivos de red. No se admite el uso del tipo de adaptador de red E1000 para hosts KVM.

> **Important**
>
> Para seleccionar VMXNET3, el tipo de sistema operativo invitado debe ser Other Linux64 (Otro Linux64).

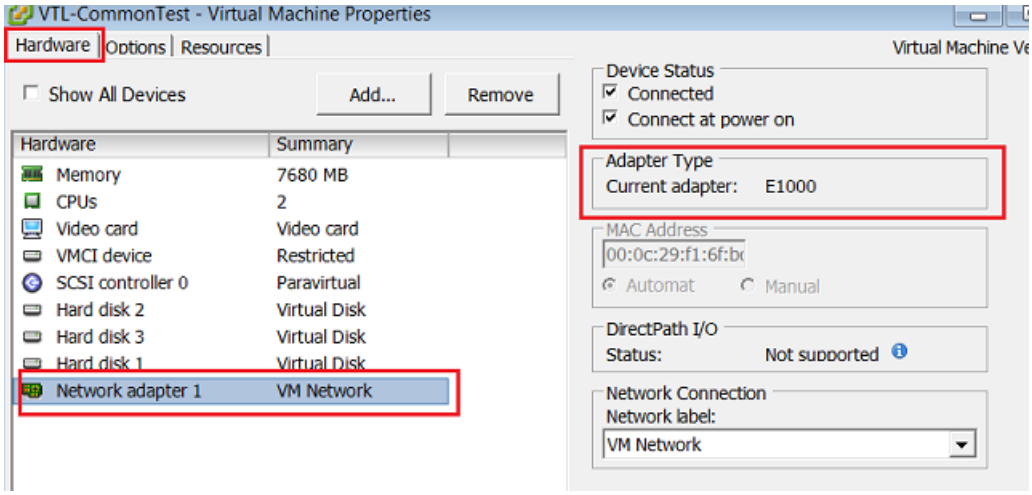
A continuación se muestran los pasos que debe seguir para configurar la gateway de modo que utilice el adaptador VMXNET3:

1. Elimine el adaptador E1000 predeterminado.
2. Agregue el adaptador VMXNET3.
3. Reinicie la gateway.
4. Configure el adaptador para la red.

A continuación se muestra información detallada sobre cómo realizar cada paso.

Para eliminar el adaptador E1000 predeterminado y configurar la gateway para que utilice el adaptador VMXNET3

1. En VMware, abra el menú contextual (haga clic con el botón derecho) de la gateway y elija Edit Settings (Editar configuración).
2. En la ventana Virtual Machine Properties (Propiedades de la máquina virtual), elija la pestaña Hardware.
3. En Hardware, elija Network adapter (Adaptador de red). Tenga en cuenta que el adaptador actual es E1000 en la sección Adapter Type (Tipo de adaptador). Sustituya este adaptador por el adaptador VMXNET3.



4. Elija el adaptador de red E1000 y, a continuación, elija Remove (Eliminar). En este ejemplo, el adaptador de red E1000 es Network adapter 1 (Adaptador de red 1).

> **Note**
>
> Aunque puede ejecutar los adaptadores de red E1000 y VMXNET3 en la gateway al mismo tiempo, no le recomendamos que lo haga, porque puede provocar problemas de red.

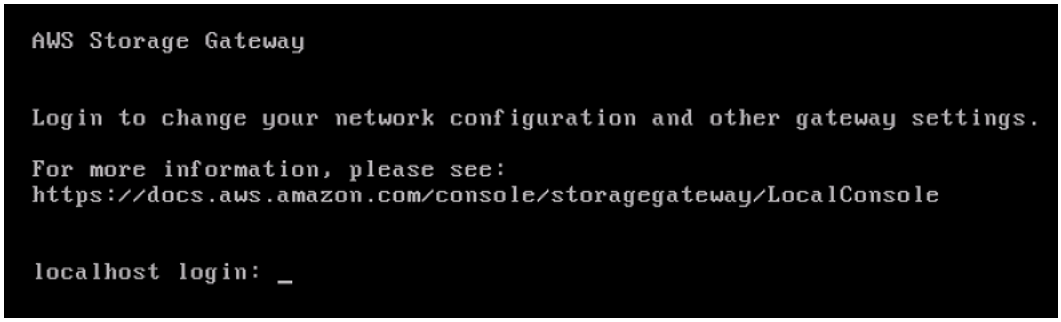
5. Elija Add (Añadir) para abrir el asistente para agregar hardware.
6. Elija Ethernet Adapter (Adaptador Ethernet) y, a continuación, seleccione Next (Siguiente).
7. En el asistente de tipo de red, seleccione **`VMXNET3`** para Adapter Type (Tipo de adaptador) y, a continuación, elija Next (Siguiente).

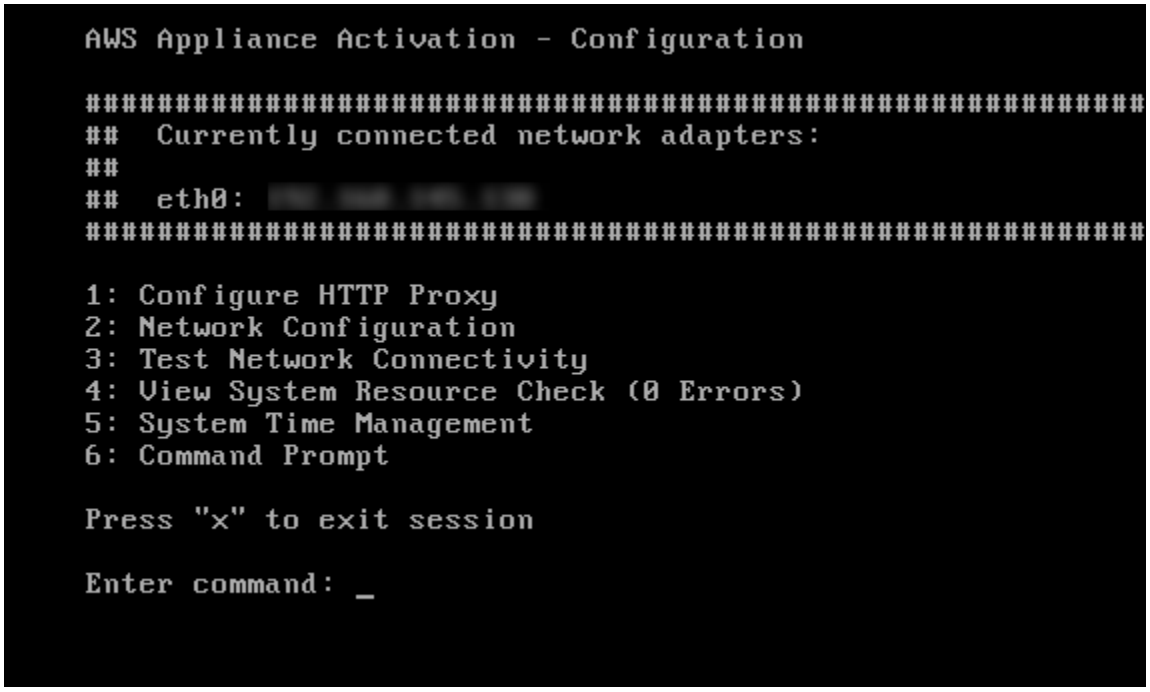
8. En el asistente de propiedades de máquina virtual, verifique en la sección Adapter Type (Tipo de adaptador) que Current Adapter (Adaptador actual) se haya establecido en VMXNET3 y, a continuación, elija OK (Aceptar).
9. En el cliente de VMware vSphere, cierre la gateway.
10. En el cliente de VMware VSphere, reinicie la gateway.

Una vez que se reinicie la gateway, reconfigure el adaptador que acaba de añadir para asegurarse de que se establezca la conectividad de red a Internet.

Para configurar el adaptador para la red

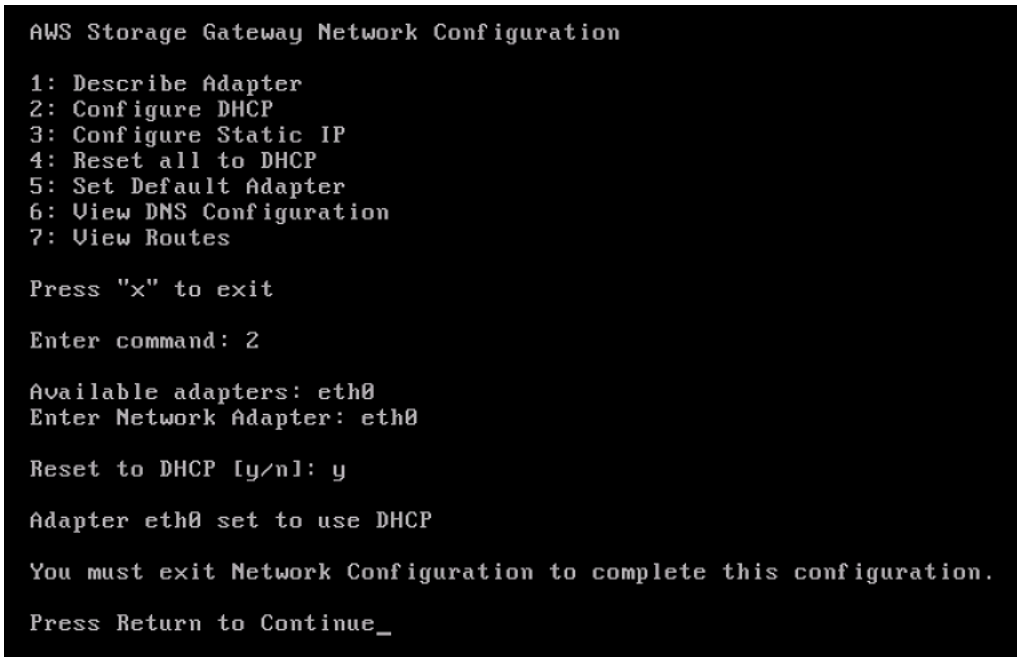
1. En el cliente de VSphere, elija la pestaña Console (Consola) para iniciar la consola local. Para esta tarea de configuración, utilice las credenciales de inicio de sesión predeterminadas para iniciar sesión en la consola local de la gateway. Para obtener información sobre cómo iniciar sesión con las credenciales predeterminadas, consulte Inicio de sesión en la consola local de la gateway de archivos.





2. Cuando se le solicite, introduzca **2** para seleccionar Network Configuration (Configuración de red) y, a continuación, pulse **Enter** (Intro) para abrir el menú de configuración de red

3. Cuando se le solicite, introduzca **4** para seleccionar Reset all to DHCP (Restablecer todo a DHCP) y, a continuación, introduzca **y** (para Sí) en el símbolo del sistema para establecer todos los adaptadores de modo que utilicen DHCP (Dynamic Host Configuration Protocol). Todos los adaptadores disponibles se establecen para utilizar DHCP.



Si la gateway ya está activada, debe cerrarla y reiniciarla desde la consola de administración de Storage Gateway. Una vez que se reinicie la gateway, debe probar la conectividad de red a Internet. Para obtener más información sobre cómo probar la conectividad de red, consulte Probar la conectividad de red de su gateway.

Realización de tareas en la consola local de Amazon EC2 (puerta de enlace de archivos)

Algunas tareas de mantenimiento requieren que inicie sesión en la consola local cuando ejecute una gateway implementada en una instancia de Amazon EC2. En esta sección, puede encontrar información acerca de cómo iniciar sesión en la consola local y llevar a cabo tareas de mantenimiento.

Temas

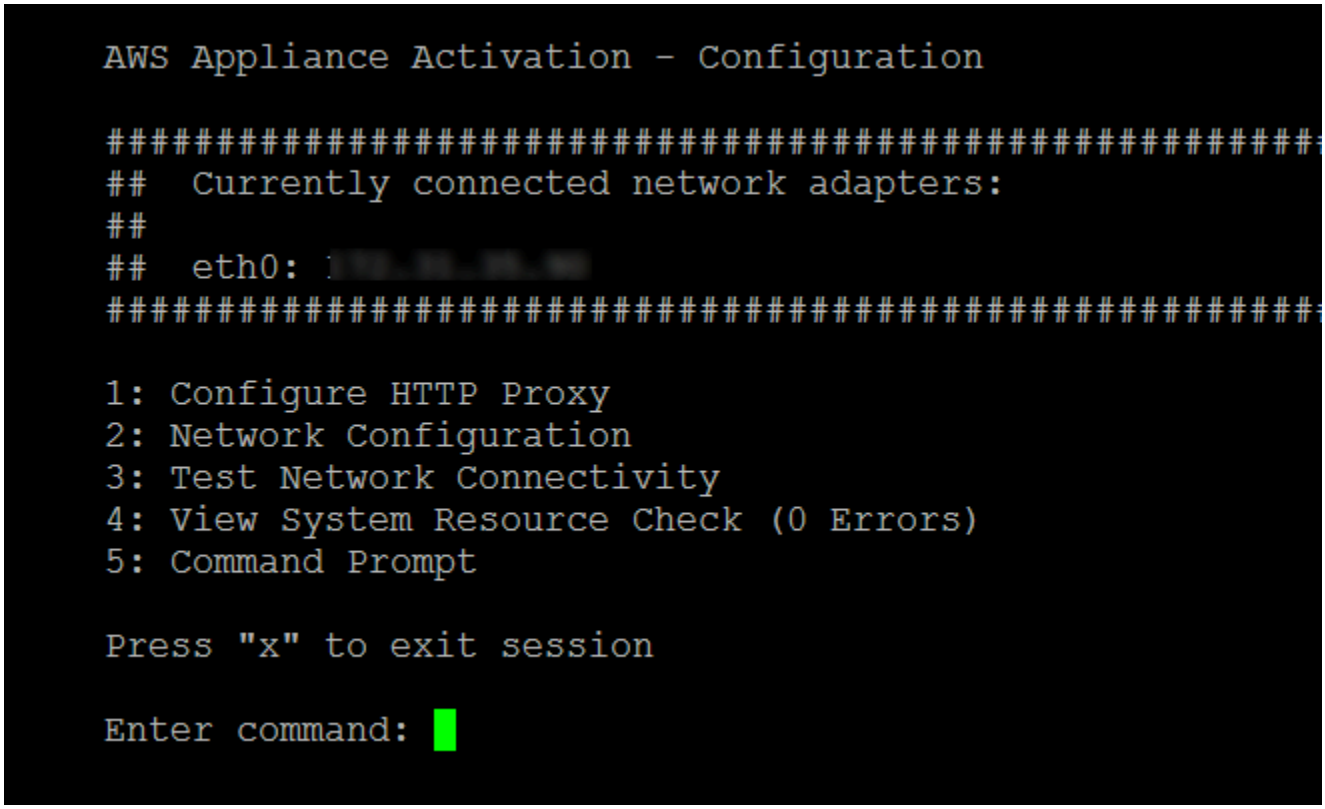
- Inicio de sesión en la consola local de la puerta de enlace Amazon EC2
- Enrutamiento de la puerta de enlace implementada en EC2 a través de un proxy HTTP
- Configuración de la red de la puerta de enlace
- Probar la conectividad de red de su gateway
- Ver el estado de los recursos del sistema de gateway
- Ejecución de comandos de Storage Gateway en la consola local

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

Puede conectarse a la instancia de Amazon EC2 mediante la utilización de un cliente Secure Shell (SSH). Para obtener información detallada, consulteConéctese a la instanciaen laGuía del usuario de Amazon EC2. Para conectarse de esta manera, necesitará el par de claves SSH que ha especificado al lanzar la instancia. Para obtener más información acerca de los pares de claves de Amazon EC2, consultePares de claves de Amazon EC2en laGuía del usuario de Amazon EC2.

Para iniciar sesión en la consola local de la gateway

1. Inicie sesión en la consola local. Si se conecta a la instancia EC2 desde un equipo Windows, inicie sesión como admin.
2. Después de iniciar sesión, verá lasAWSActivación del dispositivo: configuraciónmenú principal, como se muestra en la siguiente captura de pantalla.



Para obtener información sobre	Consulte este tema
Configurar un proxy HTTP para la gateway	Enrutamiento de la puerta de enlace implementada en EC2 a través de un proxy HTTP
Configurar la red para la gateway	Probar la conectividad de red de su gateway
Probar la conectividad de red	Probar la conectividad de red de su gateway
Ver una comprobación de recursos del sistema	Inicio de sesión en la consola local de la puerta de enlace Amazon EC2.
Ejecutar comandos de la consola de Storage	Ejecución de comandos de Storage Gateway en la consola local

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

Para salir de la sesión de configuración, introduzca **x** para salir del menú.

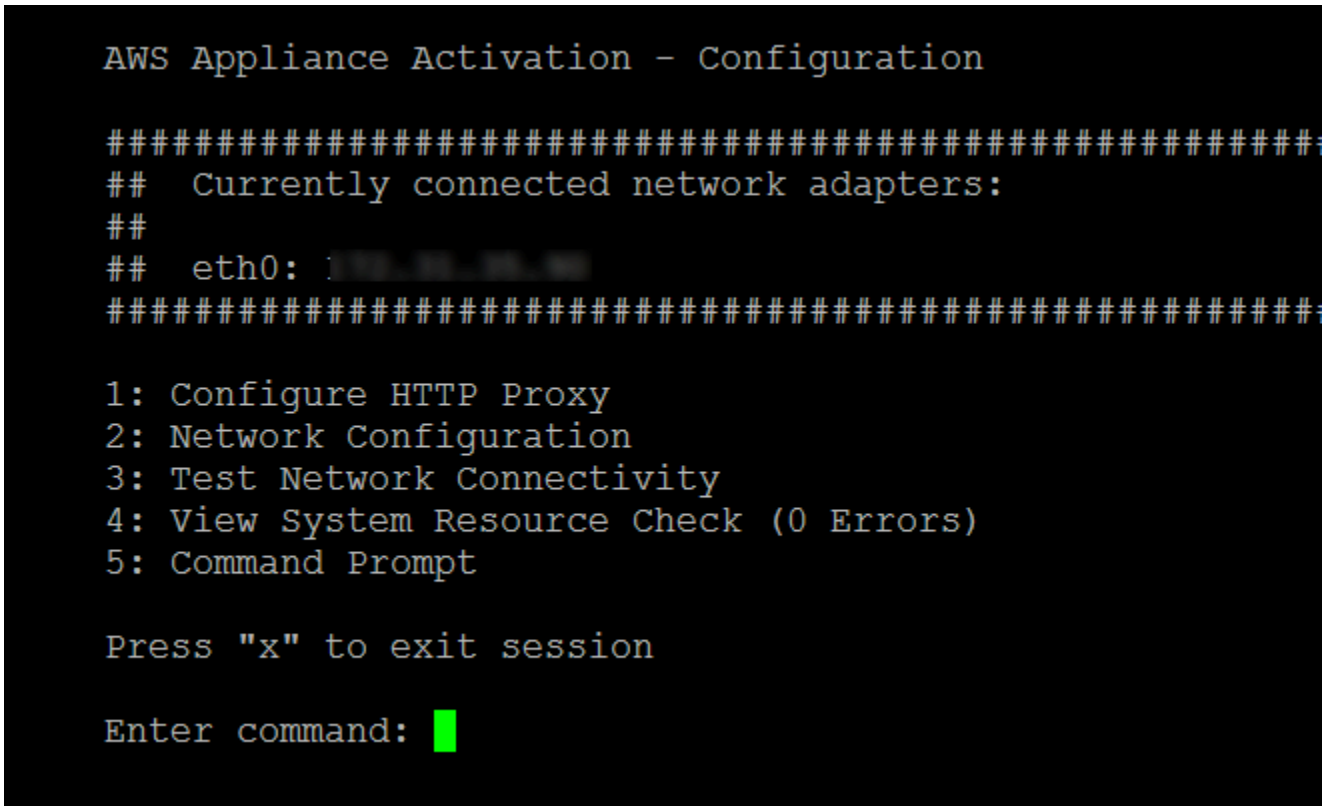
Enrutamiento de la puerta de enlace implementada en EC2 a través de un proxy HTTP

Storage Gateway es compatible con la configuración de un proxy Socket Secure versión 5 (SOCKS5) entre la gateway implementada en Amazon EC2 yAWS.

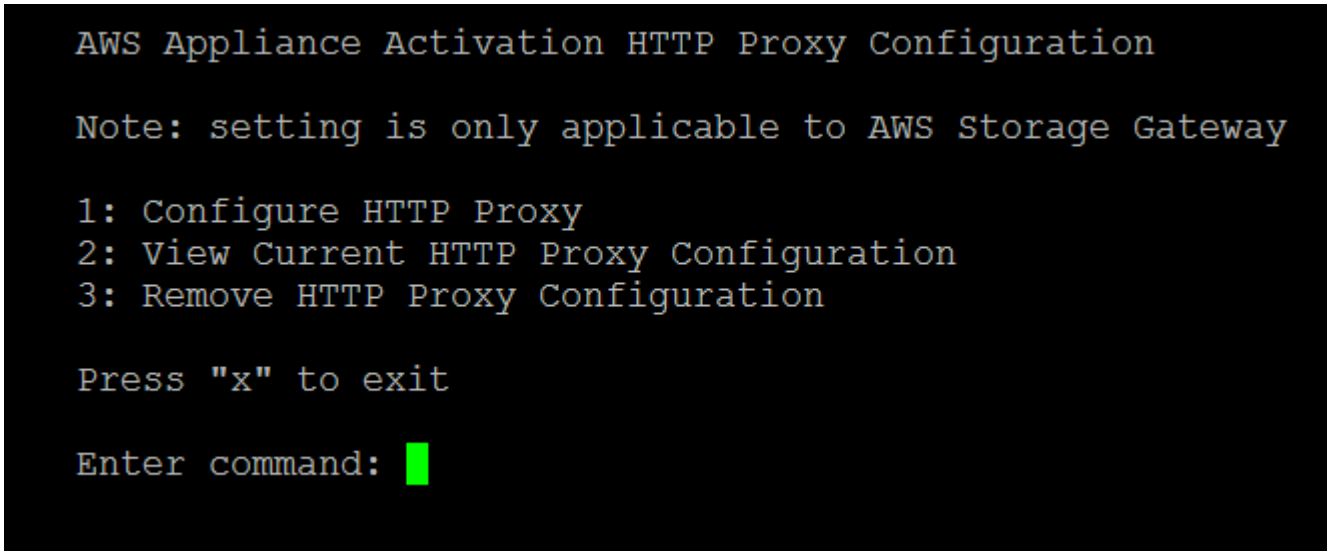
Si la gateway debe utilizar un servidor proxy para comunicarse con Internet, debe configurar los ajustes del proxy HTTP para la gateway. Para ello, especifique una dirección IP y un número de puerto para el host en el que se ejecuta el proxy. Después de hacerlo, Storage Gateway rutea todosAWStráfico de endpoint a través del servidor proxy. Las comunicaciones entre la puerta de enlace y los endpoints se cifran, 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 la puerta de enlace Amazon EC2.
2. En la páginaAWSActivación del dispositivo: configuraciónMenú principal, introduzca**1**para empezar a configurar el proxy HTTP.



3. Elija una de las siguientes opciones en laAWSActivación del dispositivo: configuraciónConfiguración de proxy HTTPmenú.



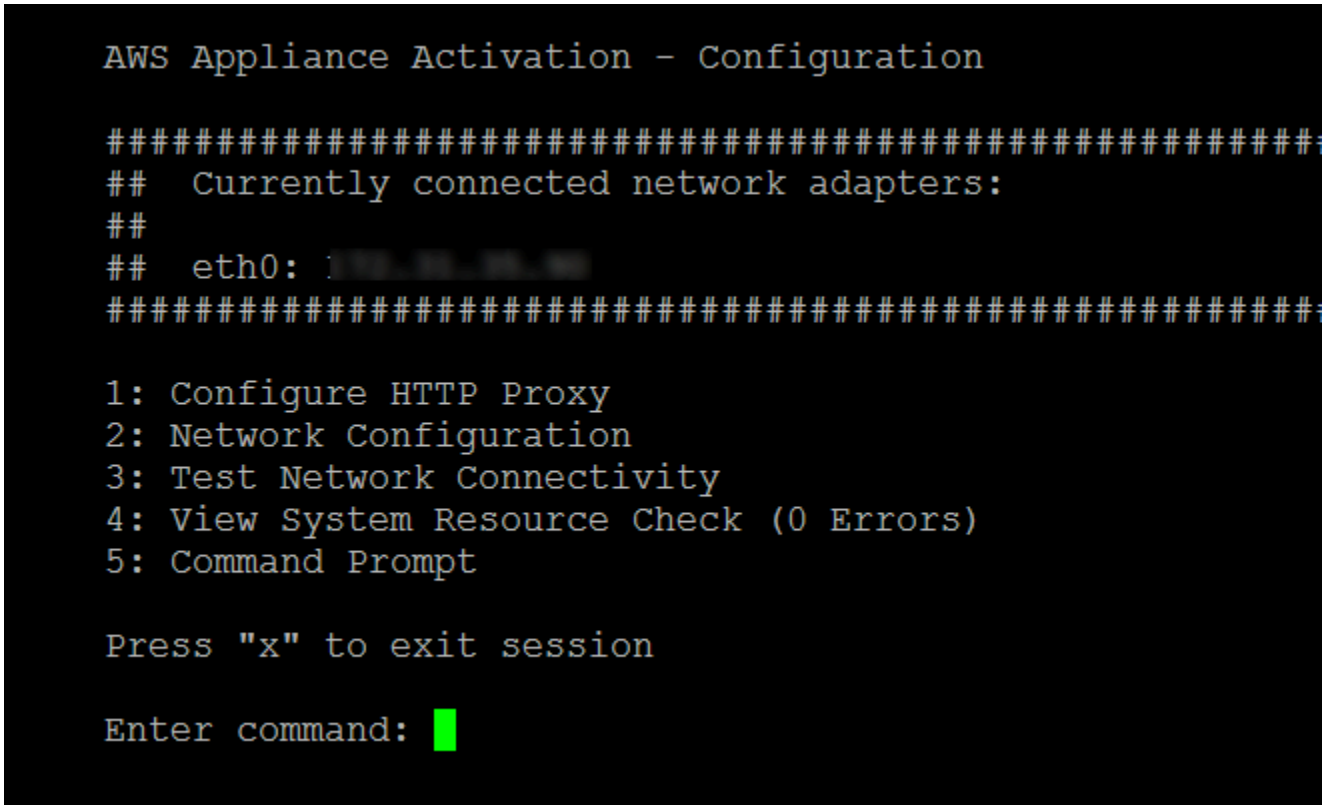
Para	Haga lo siguiente
Configurar un proxy HTTP	Escriba **1**. Debe proporcionar un nombre de host y un puerto para completar la configuración.
Ver la configuración del proxy HTTP actual	Escriba **2**. Si no se ha configurado un proxy HTTP, se muestra el mensaje `HTTP Proxy not configured` . Si se ha configurado un proxy HTTP, se muestran el nombre de host y el puerto del proxy.
Eliminar la configuración de un proxy HTTP	Escriba **3**. Se muestra el mensaje `HTTP Proxy Configuration Removed` .

Configuración de la red de la puerta de enlace

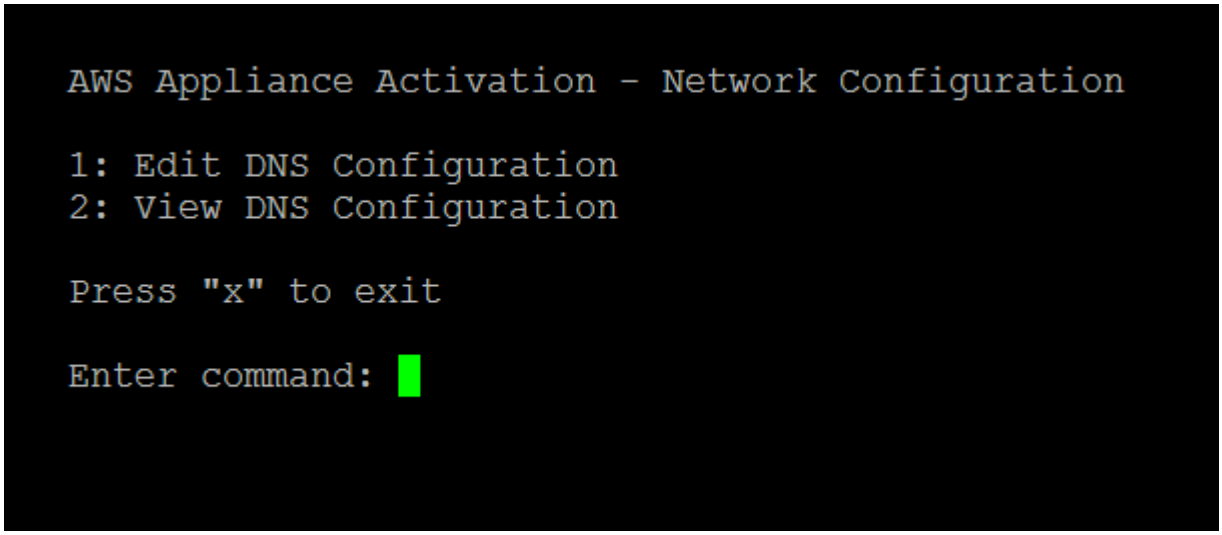
Puede ver y configurar los ajustes del servidor de nombres de dominio (DNS) mediante la consola local.

Para configurar la gateway para que utilice direcciones IP estáticas

1. Inicie sesión en la consola local de la gateway. Para obtener instrucciones, consulte Inicio de sesión en la consola local de la puerta de enlace Amazon EC2.
2. En la páginaAWSActivación del dispositivo: configuraciónMenú principal, introduzca**2**para empezar a configurar el servidor DNS.



3. Elija una de las siguientes opciones en el menú Network Configuration (Configuración de red).



Para	Haga lo siguiente
Editar la configuración de DNS de la gateway	Escriba **1**. Se muestran los adaptadores disponibles de los servidores DNS primario y secundario. Se le pedirá que proporcione la dirección IP nueva.
Ver la configuración de DNS de la ruta de enlace	Escriba **2**. Se muestran los adaptadores disponibles de los servidores DNS primario y secundario.

Probar la conectividad de red de su gateway

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

Para probar la conectividad de la gateway

1. Inicie sesión en la consola local de la gateway. Para obtener instrucciones, consulte Inicio de sesión en la consola local de la puerta de enlace Amazon EC2.
2. Desde lasAWSActivación del dispositivo: configuraciónmenú principal, introduzca el número correspondiente para seleccionarPrueba de conectividad de red.

Si la puerta de enlace ya se ha activado, la prueba de conectividad comienza inmediatamente. Para las puertas de enlace que aún no se han activado, debe especificar el tipo de punto final yRegión de AWStal y 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 final de la puerta de enlace.
4. Si ha seleccionado el tipo de punto final público, introduzca el número correspondiente para seleccionar laRegión de AWSque quieres probar. Para admitidoRegiones de AWSy una lista deAWSendpoints de servicio que puede utilizar con Storage Gateway, consulteAWS Storage GatewayCuotas y puntos de enlace deen laAWSReferencia general de.

A medida que avanza la prueba, cada punto final se muestra[PASSED]o[FAILED], indicando el estado de la conexión de la siguiente manera:

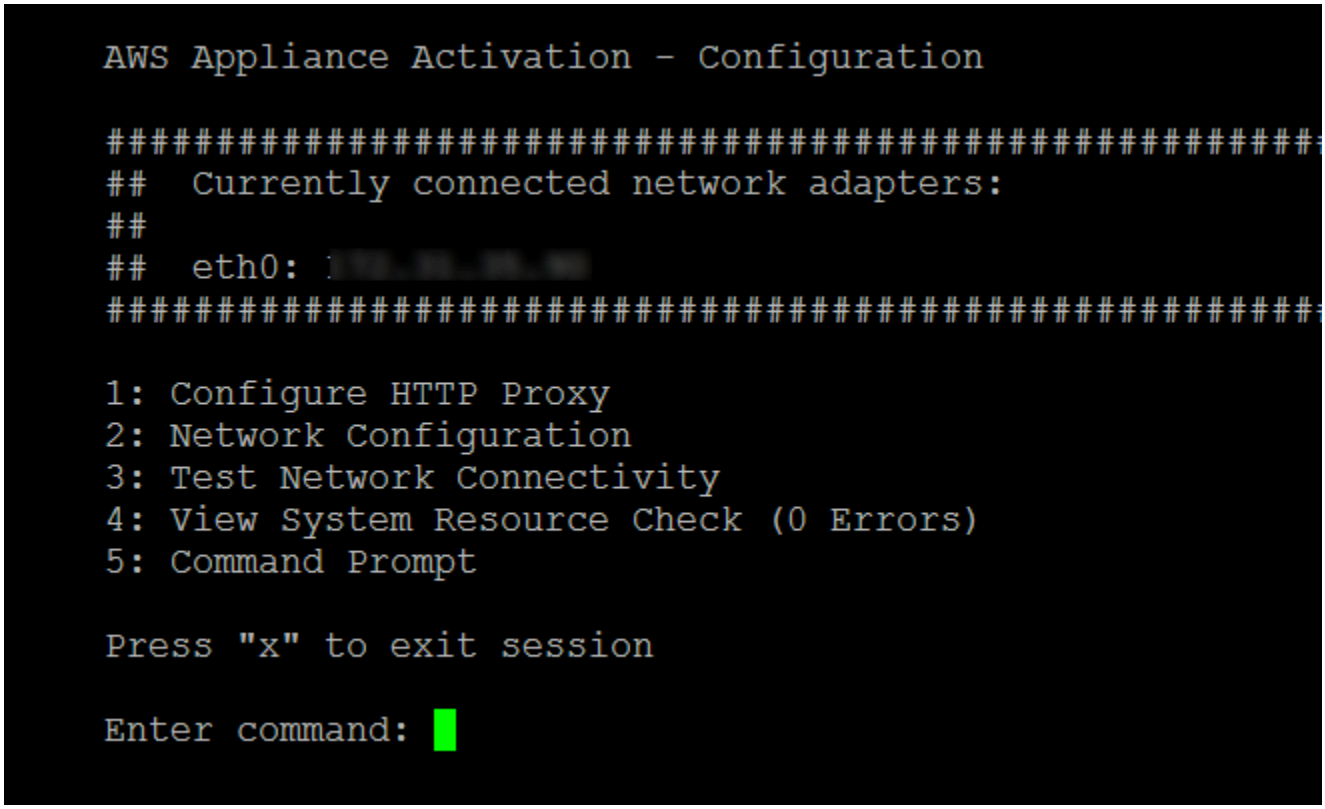
Mensaje	Description (Descripción)
[PASSED]	Storage Gateway tiene conectividad de red
[FAILED]	Storage Gateway no tiene conectividad de red.

Ver el estado de los recursos del sistema de gateway

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 instrucciones, consulte Inicio de sesión en la consola local de la puerta de enlace Amazon EC2.
2. En el navegadorConfiguración Storage GatewayMenú principal, introduzca**4**Para ver los resultados de una comprobación de recursos del sistema.



La consola muestra un mensaje [OK], [WARNING] o [FAIL] para cada recurso, como se describe en la tabla siguiente.

Mensaje	Description (Descripción)
[OK]	El recurso ha superado la comprobación de recursos del sistema.
[WARNING]	El recurso no satisface los requisitos recomendados, pero la gateway puede continuar 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 gateway no funcione correctamente. Storage Gateway muestra un mensaje en el que se describen los resultados de la comprobación de recursos.

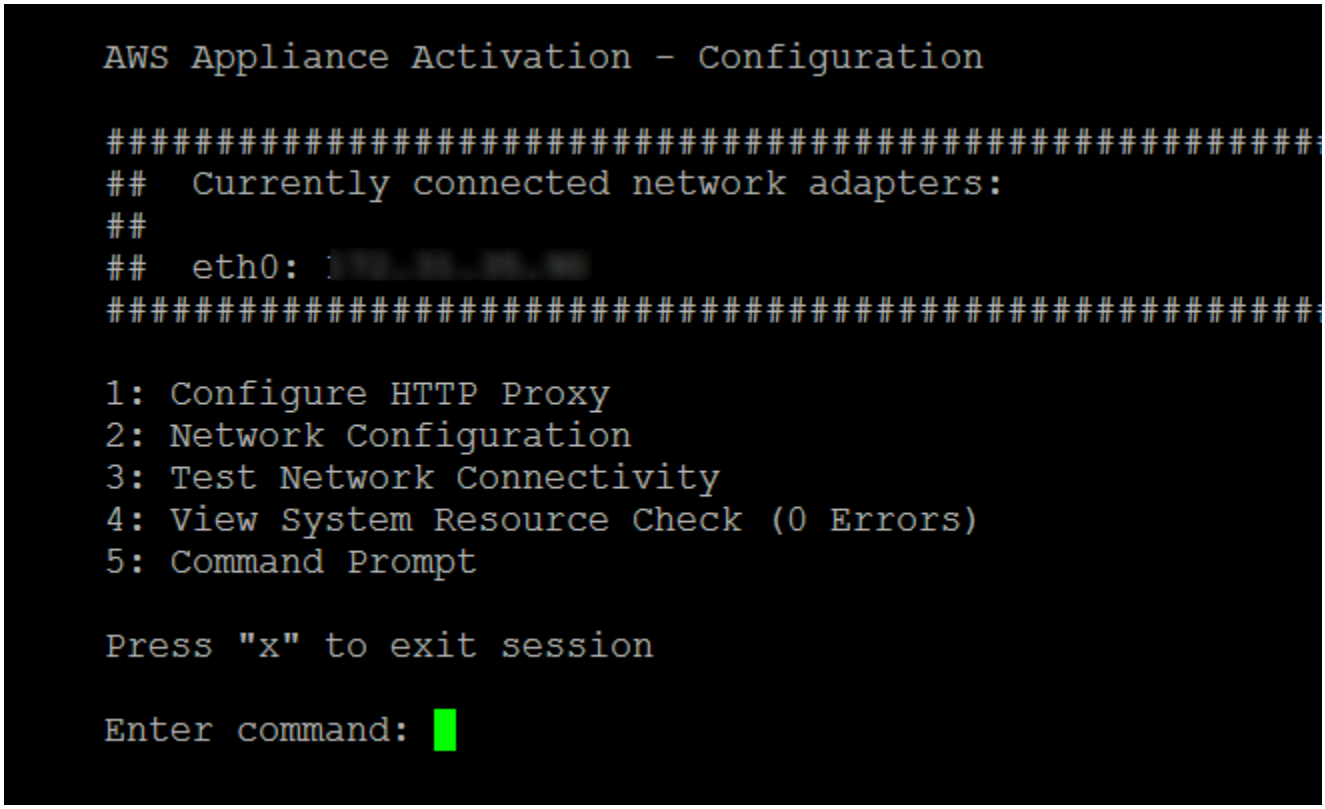
La consola también muestra el número de errores y advertencias junto a la opción de menú de comprobación de recursos.

Ejecución de comandos de Storage Gateway en la consola local

La consola AWS Storage Gateway contribuye a proporcionar un entorno seguro para la configuración y el diagnóstico de problemas con la gateway. Puede utilizar los comandos de la consola para realizar tareas de mantenimiento, tales como guardar tablas de enrutamiento o conectarse a Amazon Web Services Support.

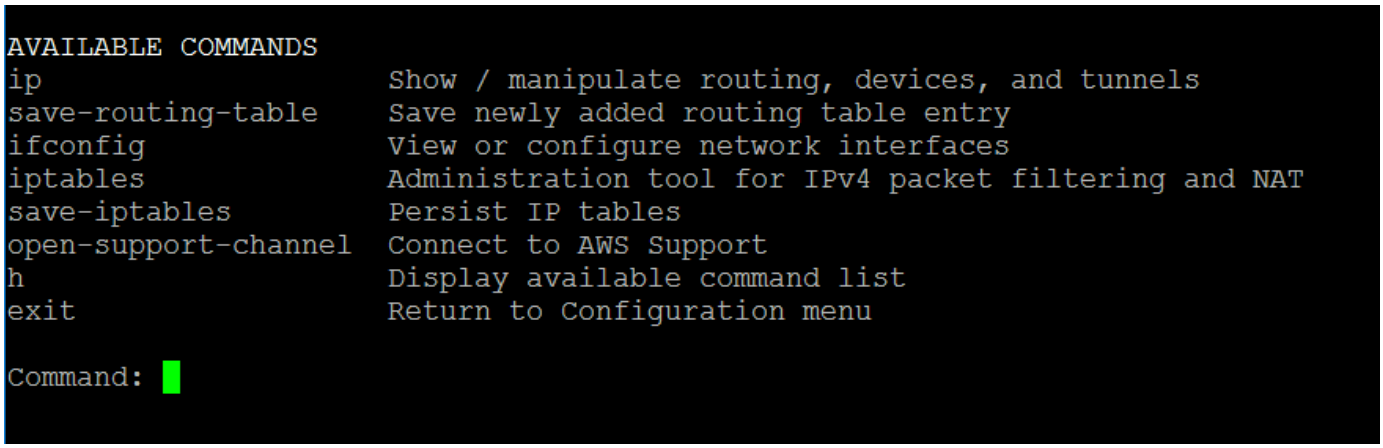
Para ejecutar un comando de configuración o diagnóstico

1. Inicie sesión en la consola local de la gateway. Para obtener instrucciones, consulte Inicio de sesión en la consola local de la puerta de enlace Amazon EC2.
2. En el navegadorAWSConfiguración de activación del dispositivoMenú principal, introduzca**5**paraConsola de gateway.



3. Introduzca **h** en el símbolo de sistema y, a continuación, pulse la tecla Intro.

La consola muestra el menú AVAILABLE COMMANDS (COMANDOS DISPONIBLES) con los comandos disponibles. Tras el menú, aparece el símbolo de la consola de la gateway, tal y como se muestra en la siguiente captura de pantalla.



4. En el símbolo del sistema, introduzca el comando que desea utilizar y siga las instrucciones.

Para obtener información sobre un comando, introduzca el nombre del comando en el símbolo del sistema.

Acceso a la consola local de la gateway

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, puede encontrar información sobre cómo acceder a la consola local de VM mediante la máquina virtual de Linux basada en el kernel (KVM), VMware ESXi y Microsoft Hyper-V Manager.

Temas

- Acceso a la consola local de la gateway con Linux KVM
- Acceso a la consola local de la 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 las máquinas virtuales que están actualmente disponibles en KVM.

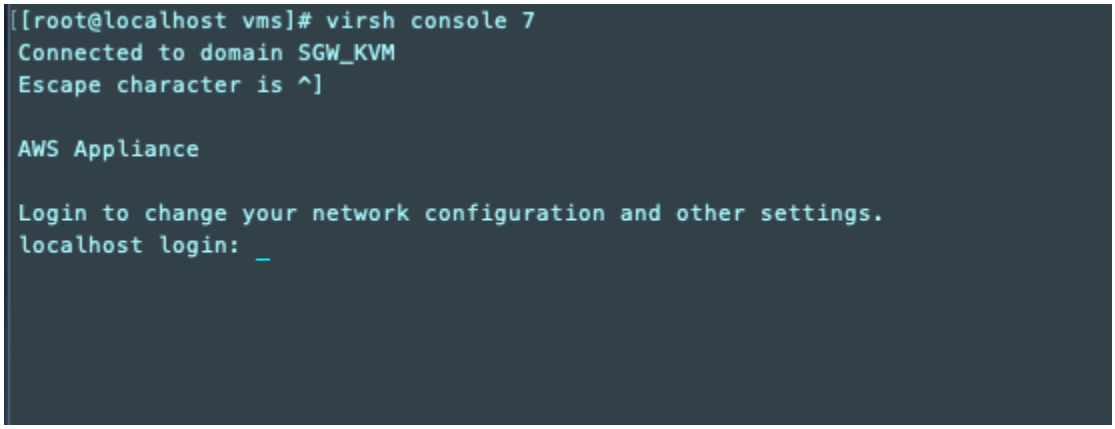
   ```
   # virsh list
   ```

   Puede elegir las máquinas virtuales disponibles por `Id`.

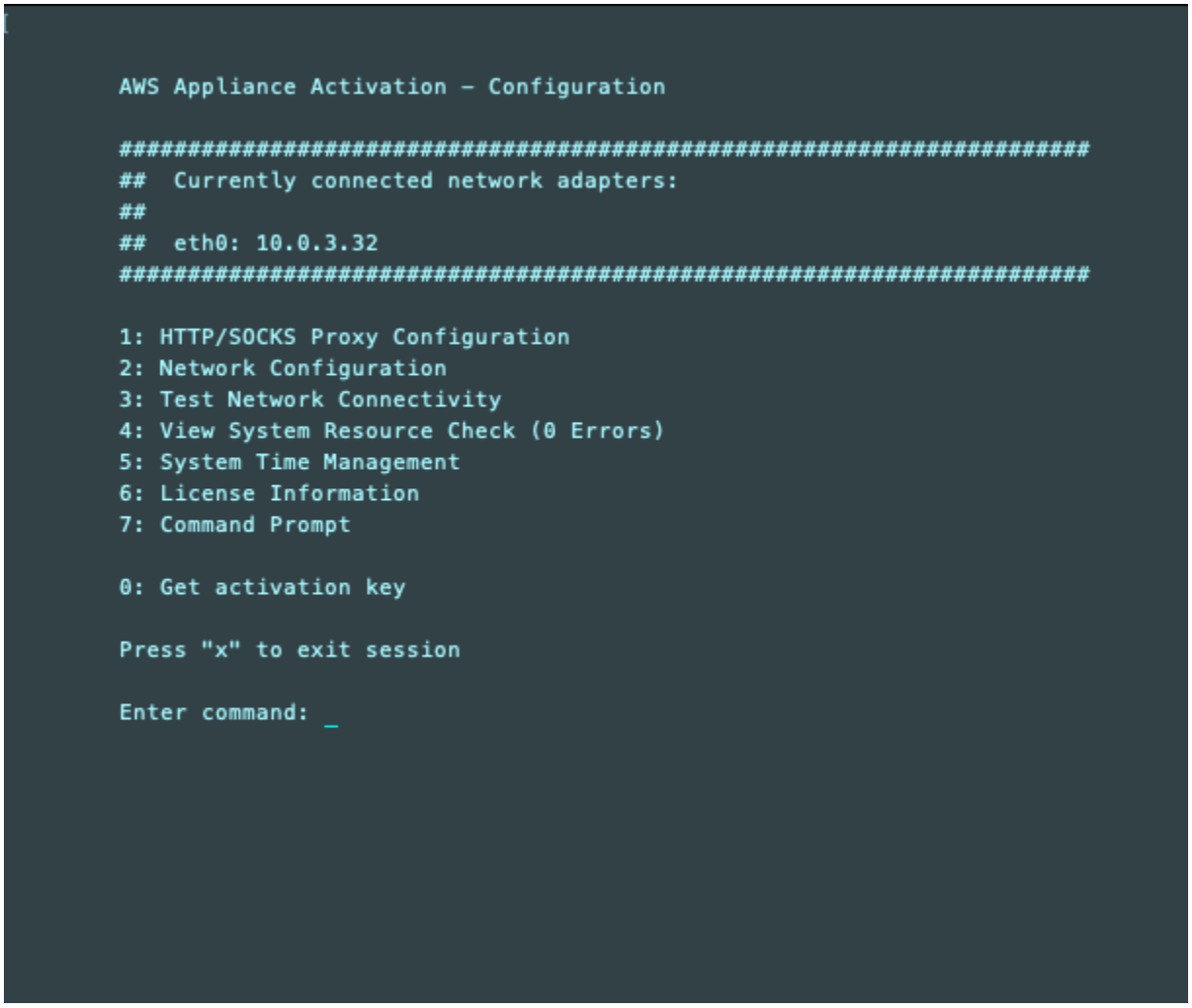
   

2. Utilice el siguiente comando para acceder a la consola local.

   ```
   # virsh console VM_Id
   ```

3. Para obtener las credenciales predeterminadas para iniciar sesión en la consola local, consulte Inicio de sesión en la consola local de la gateway de archivos.
4. Después de haber iniciado sesión, puede activar y configurar su gateway.

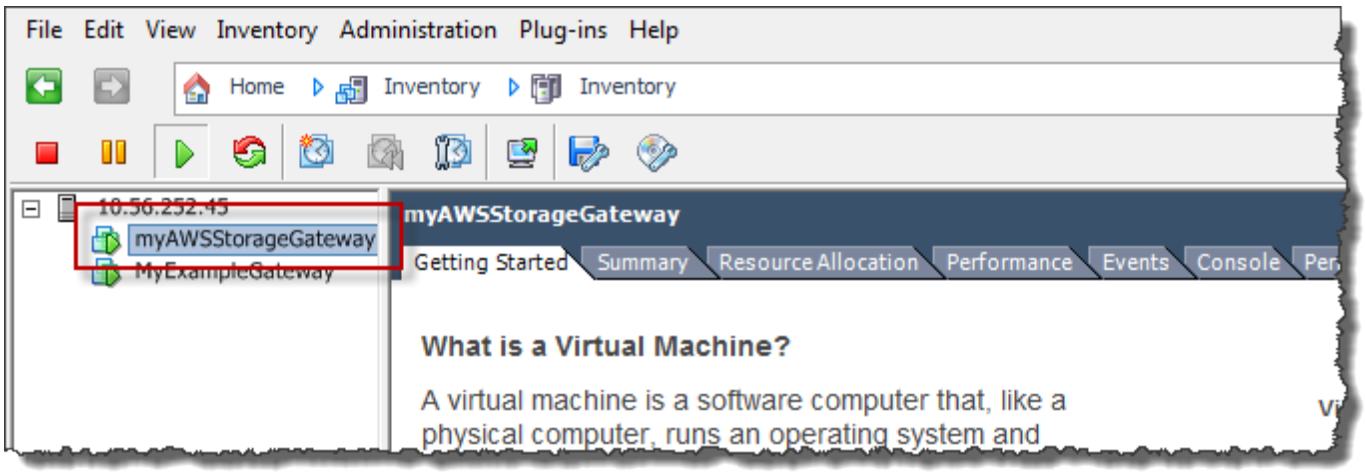


Acceso a la consola local de la gateway con VMware ESXi

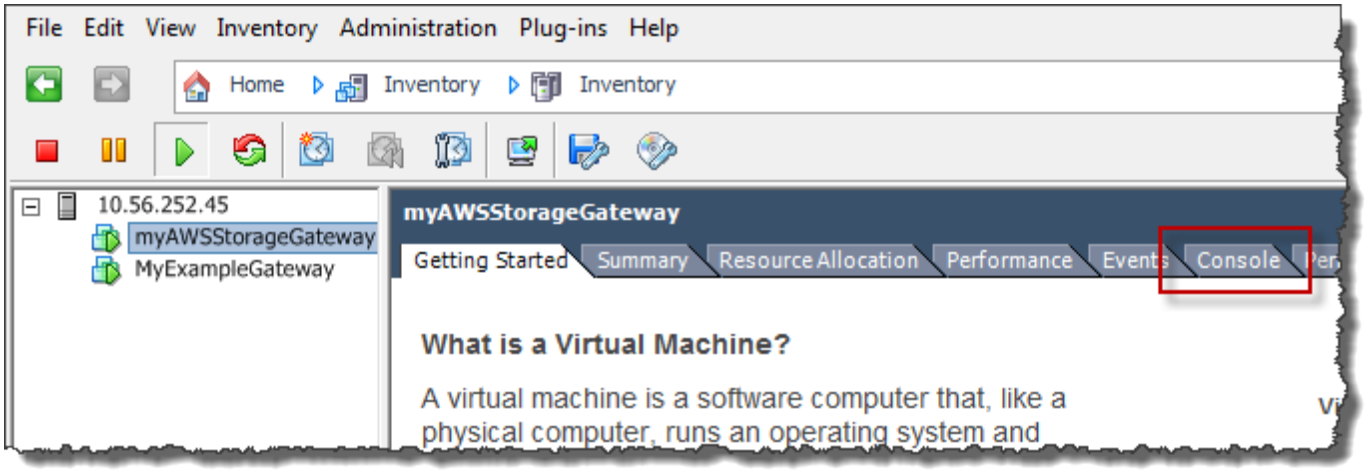
Para obtener acceso a la consola local de la gateway con VMware ESXi

1. En el cliente de VMware vSphere, seleccione la máquina virtual de la gateway.
2. Asegúrese de que la gateway esté activada.

> **Note**
>
> Si la MV de la gateway está activada, aparecerá un icono de flecha verde con el icono de la MV, como se muestra en la siguiente captura de pantalla. Si la MV de la gateway no está activada, puede activarla eligiendo el icono Power On (Encender) verde en el menú Toolbar (Barra de herramientas).

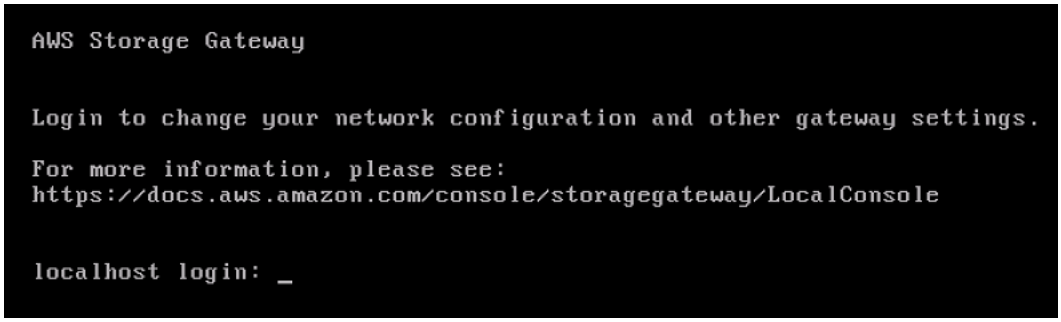


3. Elija la pestaña Console (Consola).



Después de unos minutos, la MV está lista para iniciar sesión.

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



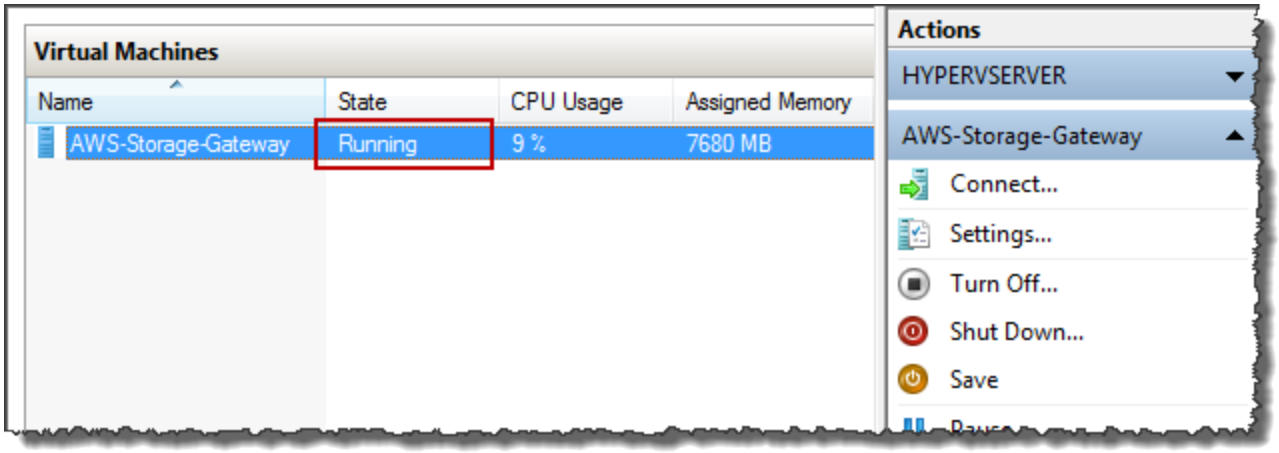
4. Para iniciar sesión con las credenciales predeterminadas, siga el procedimiento Inicio de sesión en la consola local de la gateway de archivos.

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)

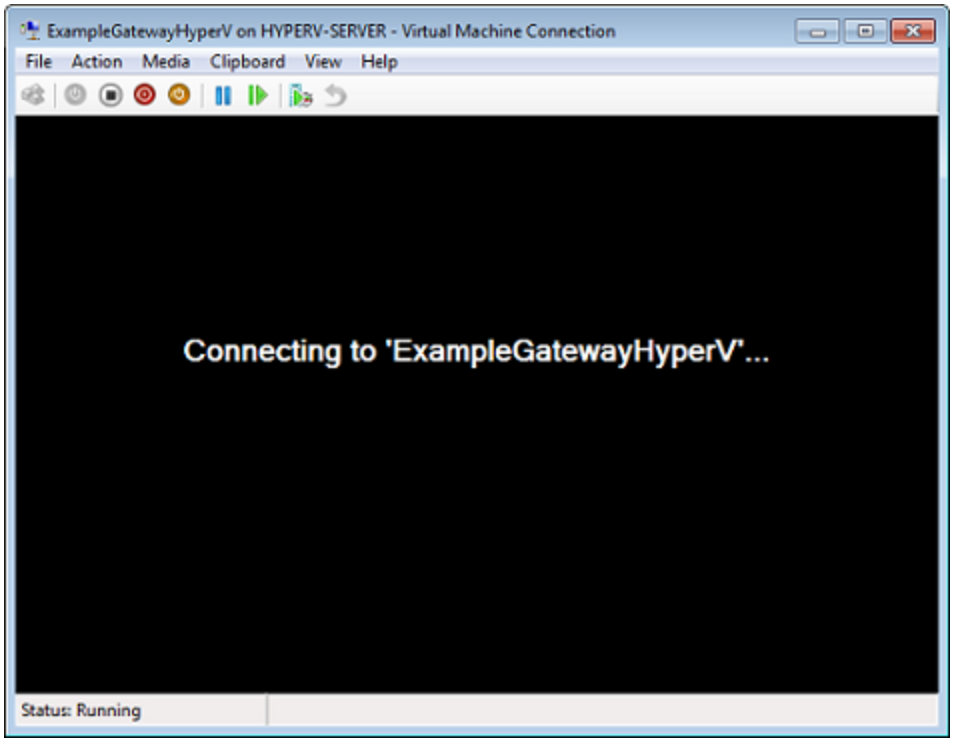
1. En la lista Virtual Machines de Microsoft Hyper-V Manager, seleccione la MV de la gateway.
2. Asegúrese de que la gateway esté activada.

> **Note**
>
> Si la MV de la gateway está activada, se mostrará `Running` como State de la MV, tal como se muestra en la siguiente captura de pantalla. Si la MV de la gateway no está activada, puede activarla eligiendo Start en el panel Actions.

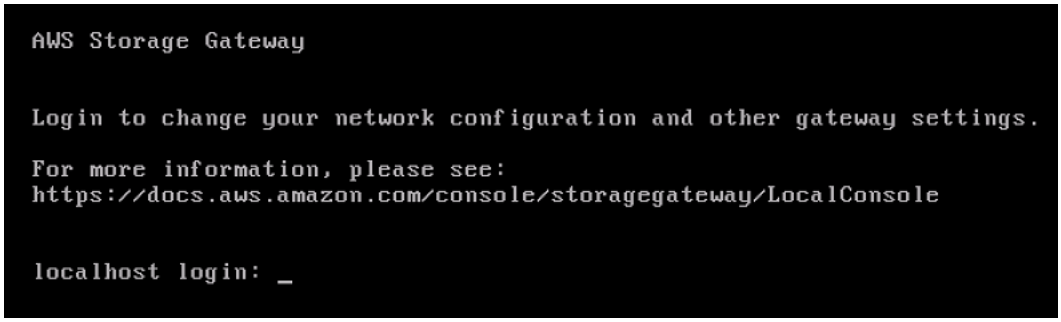


3. En el panel Actions, elija Connect.

Aparece la ventana Virtual Machine Connection. Si aparece una ventana de autenticación, escriba el nombre de usuario y la contraseña proporcionados por el administrador del hipervisor.



Después de unos minutos, la MV está lista para iniciar sesión.



4. Para iniciar sesión con las credenciales predeterminadas, siga el procedimiento Inicio de sesión en la consola local de la gateway de archivos.

Configuración de adaptadores de red para la gateway

En esta sección, encontrará información sobre el modo de configurar varios adaptadores de red para la gateway.

Temas

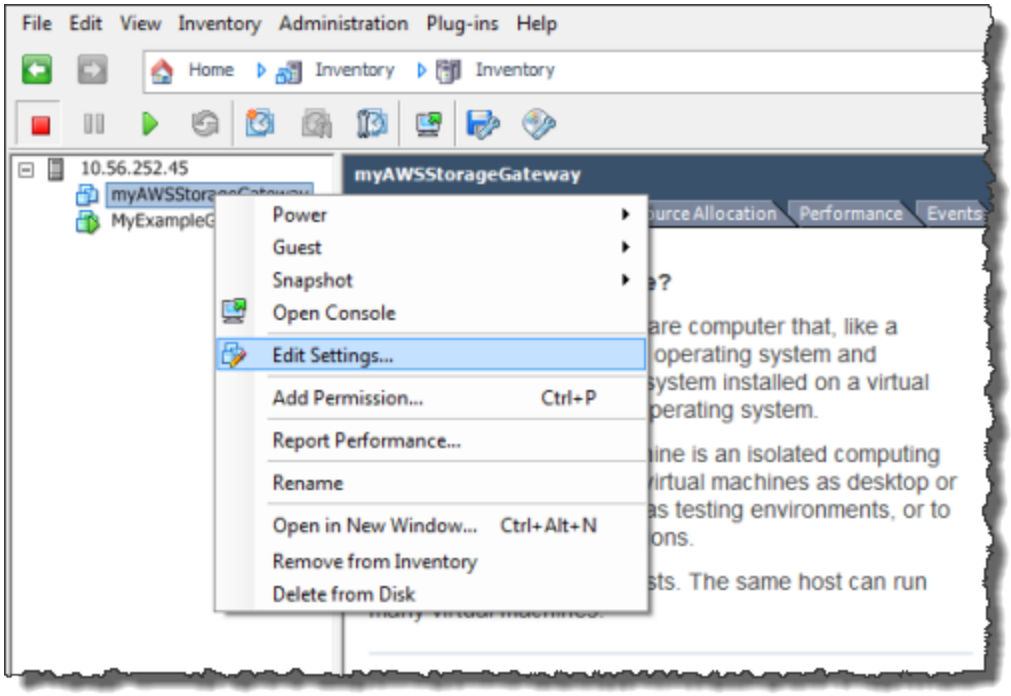
Configuración de la gateway para varios NIC en un host VMware ESXi

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. En el siguiente procedimiento se muestra cómo añadir un adaptador para VMware ESXi.

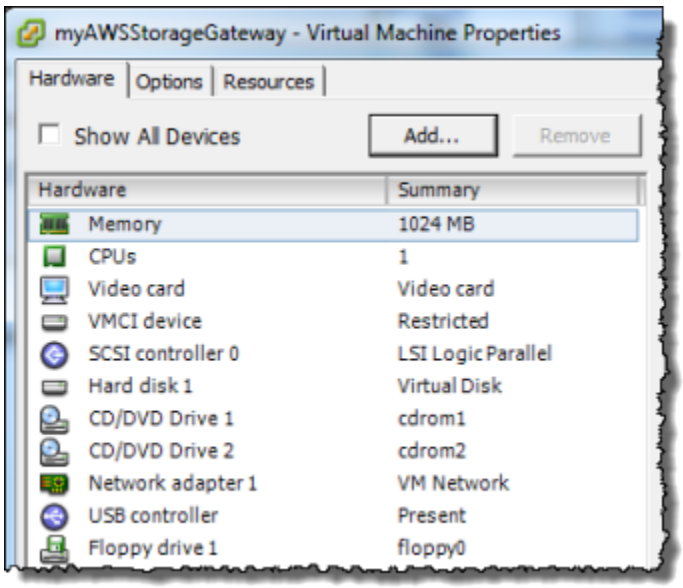
Para configurar la gateway para que utilice un adaptador de red adicional en el host VMware ESXi

1. Apague la gateway.
2. En el cliente de VMware vSphere, seleccione la máquina virtual de la gateway.

   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).

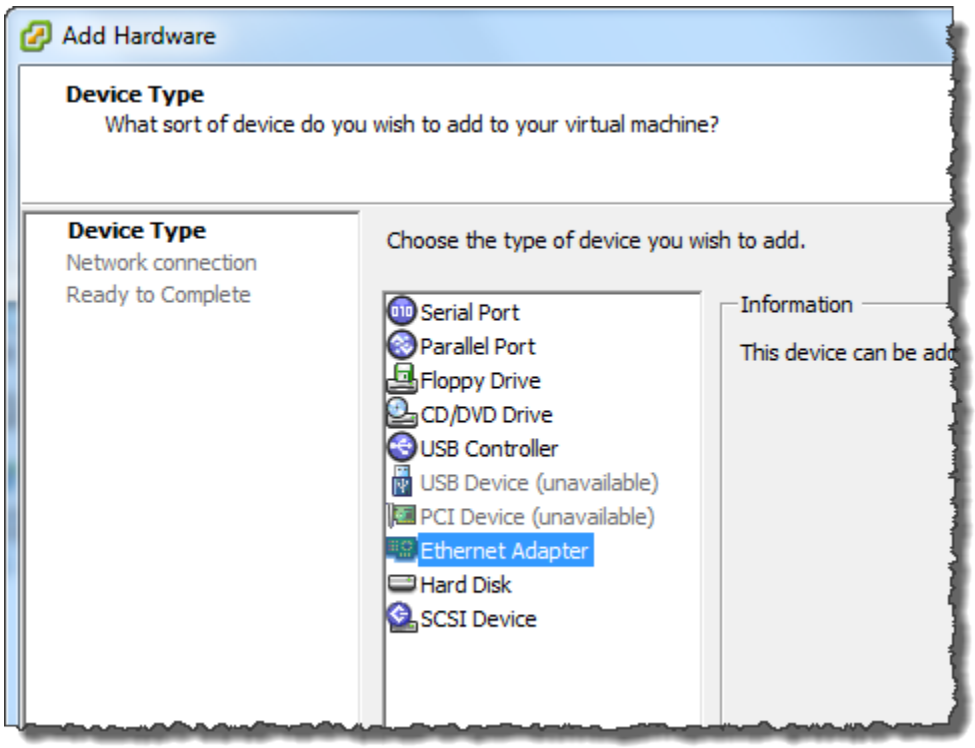


4. En la pestaña Hardware del cuadro de diálogo Virtual Machine Properties (Propiedades de la MV), elija Add (Agregar) para agregar un dispositivo.



5. Siga el asistente para agregar hardware para agregar un adaptador de red.

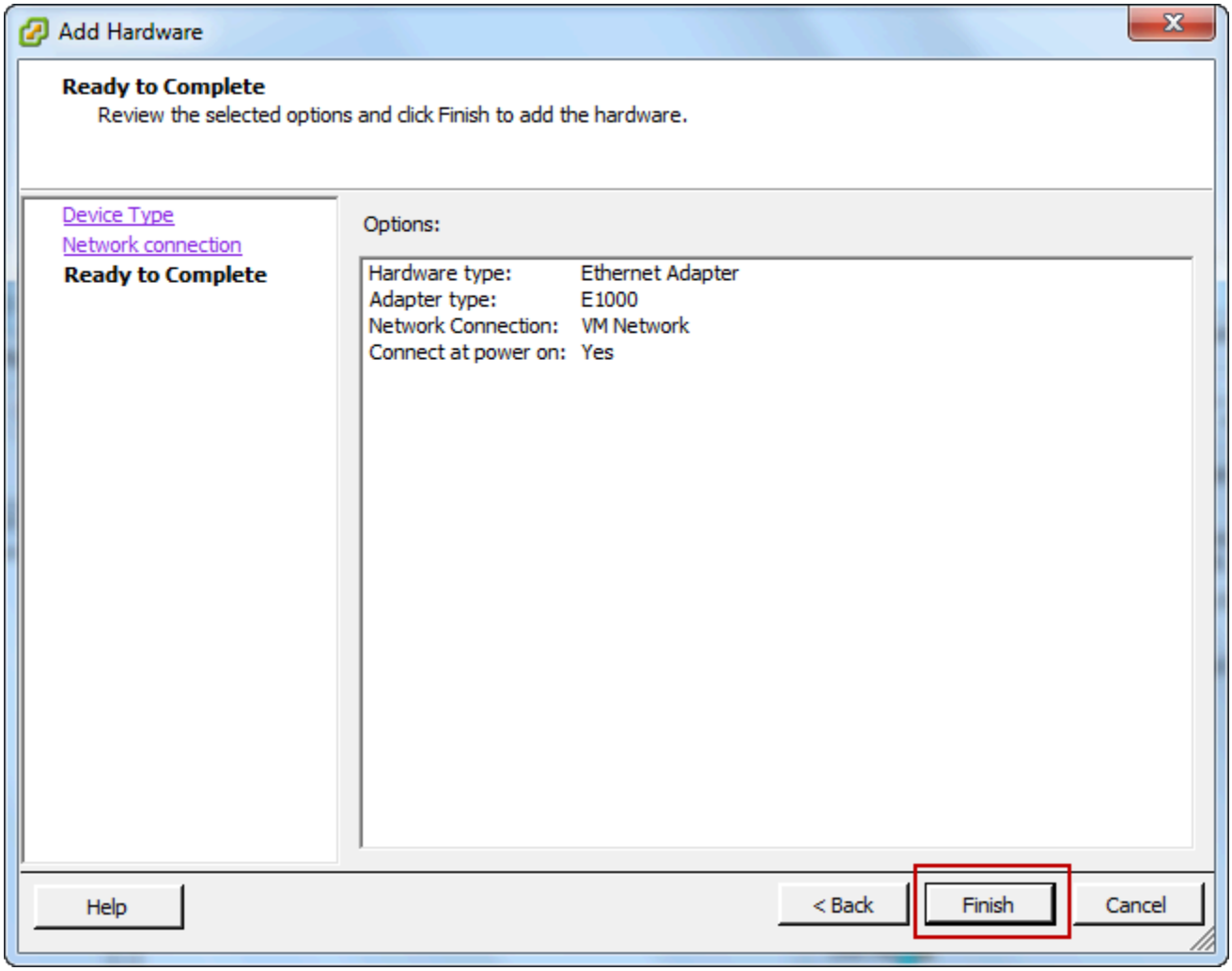
   a. En el panel Device Type (Tipo de dispositivo), elija Ethernet Adapter (Adaptador de Ethernet) para agregar un adaptador y, a continuación, elija Next (Siguiente).



   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).

Le recomendamos que utilice el adaptador de red E1000 con Storage Gateway. Para obtener más información acerca de los tipos de adaptador que pueden aparecer en la lista de adaptadores, consulte Network Adapter Types (Tipos de adaptador de red) en Documentación del servidor de ESXi y vCenter.

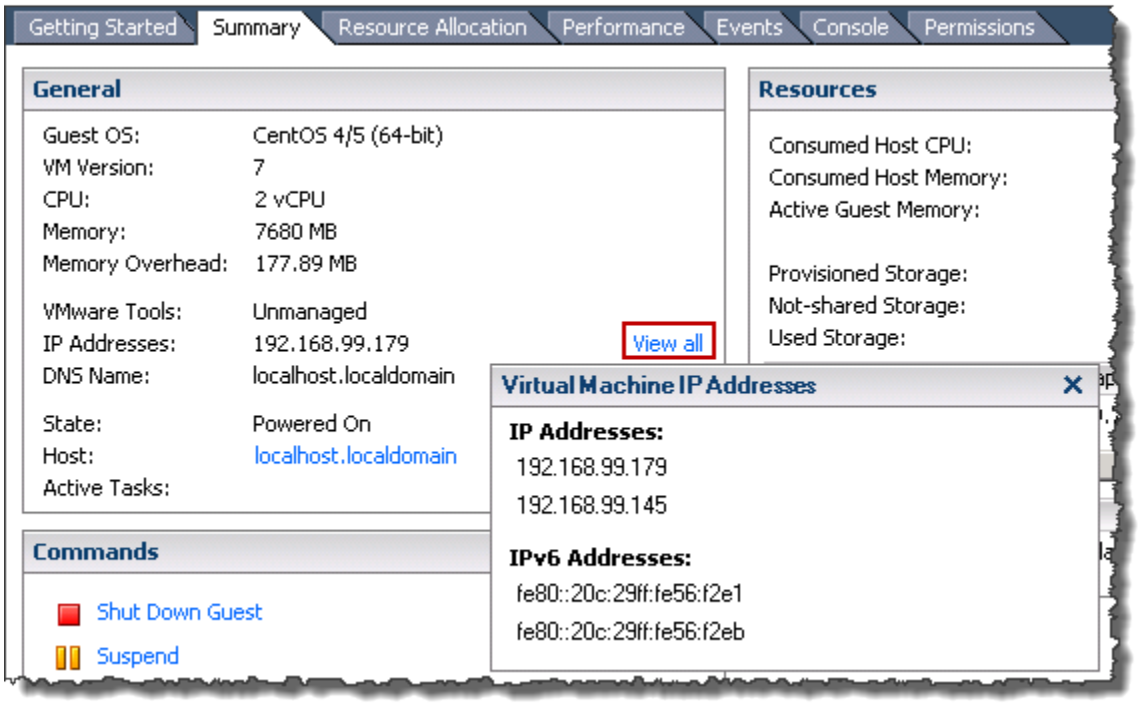
c. En el panel Ready to Complete (Listo para completar), revise la información y, a continuación, elija Finish (Finalizar).



6. Elija la pestaña Summary (Resumen) de la MV y elija View All (Ver todo) junto al cuadro IP Address (Dirección IP). En una ventana Virtual Machine IP Addresses (Direcciones IP de la MV) se muestran todas las direcciones IP que se pueden utilizar para obtener acceso a la gateway. 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.

La imagen siguiente solo tiene un propósito ilustrativo. En la práctica, una de las direcciones IP será la dirección mediante la cual la gateway se comunica con AWS y la otra será una dirección de otra subred.



7. En la consola de Storage Gateway, active la gateway.
8. En el navegadorAeronavegaciónpanel de la consola de Storage Gateway, elijaGateways dey elija la gateway a la que ha agregado el adaptador. Confirme que la segunda dirección IP aparece en la pestaña Details.

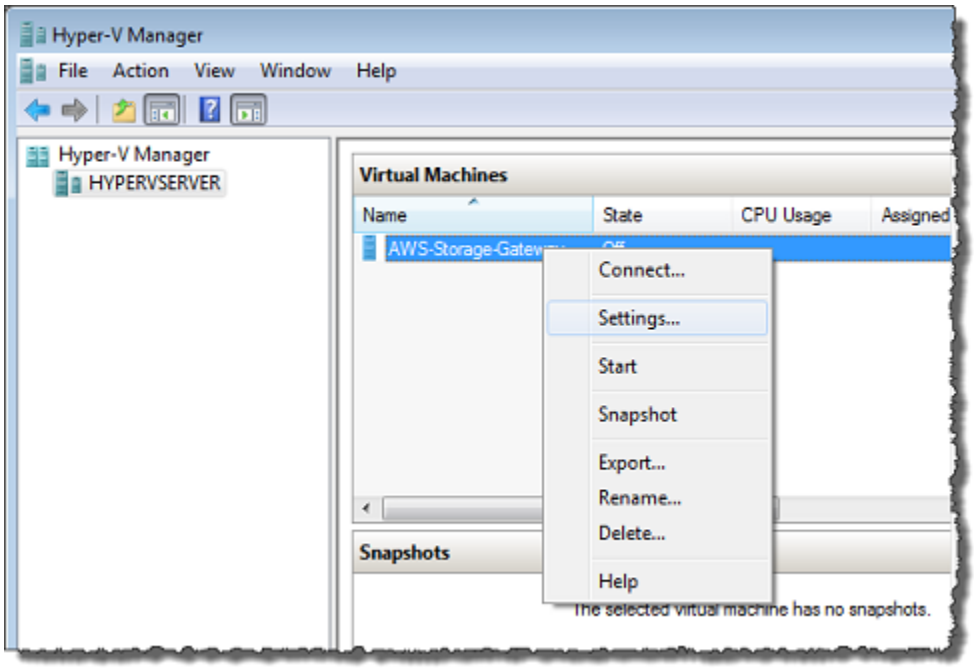
Para obtener más información acerca de tareas de consola comunes a los hosts VMware, Hyper-V y KVM, consulte Realización de tareas en la consola local de la máquina virtual (gateway de archivos)

Configuración de la gateway para varios NIC en un host 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.

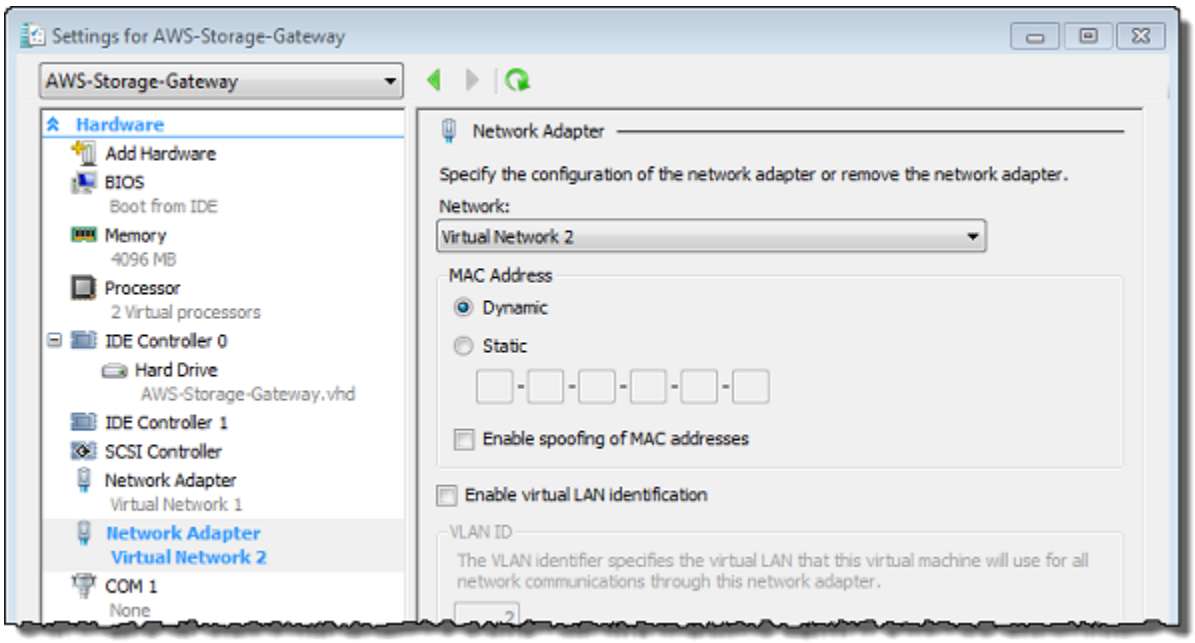
Para configurar la gateway de modo que utilice un adaptador de red adicional en un host Microsoft Hyper-V

1. En la consola de Storage Gateway, desactive la gateway.
2. En Microsoft Hyper-V Manager,seleccione la MV de la gateway.
3. Si la MV no está ya desactivada, abra el menú contextual (haga clic con el botón secundario) y elija Turn Off.
4. En el cliente, abra el menú contextual de la MV de la gateway y elija Edit Settings.



5. En el cuadro de diálogo Settings de la MV, para Hardware, elija Add Hardware.
6. En el panel Add Hardware, elija Network Adapter y, a continuación, elija Add para agregar un dispositivo.
7. Configure el adaptador de red y, a continuación, elija Apply para aplicar la configuración.

   En el siguiente ejemplo, se selecciona Virtual Network 2 para el nuevo adaptador.



8. En el cuadro de diálogo Settings, para Hardware, confirme que se ha agregado el segundo adaptador y, a continuación, elija OK.
9. En la consola de Storage Gateway, active la gateway.
10. En el panel Navigation, elija Gateways y, a continuación, seleccione la gateway a la que ha agregado el adaptador. Confirme que la segunda dirección IP aparece en la pestaña Details.

Para obtener más información acerca de tareas de consola comunes a los hosts VMware, Hyper-V y KVM, consulte Realización de tareas en la consola local de la máquina virtual (gateway de archivos)

Eliminación de la gateway mediante el uso de la consola de AWS Storage Gateway 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.

Cuando se elimina una gateway, deja de aparecer en la consola de administración de AWS Storage Gateway y su conexión iSCSI al iniciador se cierra. 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 gateway mediante la consola de Storage Gateway o mediante programación. A continuación puede encontrar información sobre cómo eliminar una gateway mediante la consola de Storage Gateway. Si desea eliminar la gateway mediante programación, consulteAWS Storage GatewayReferencia de la API.

Temas

Eliminación de la gateway mediante la consola de Storage Gateway

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

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

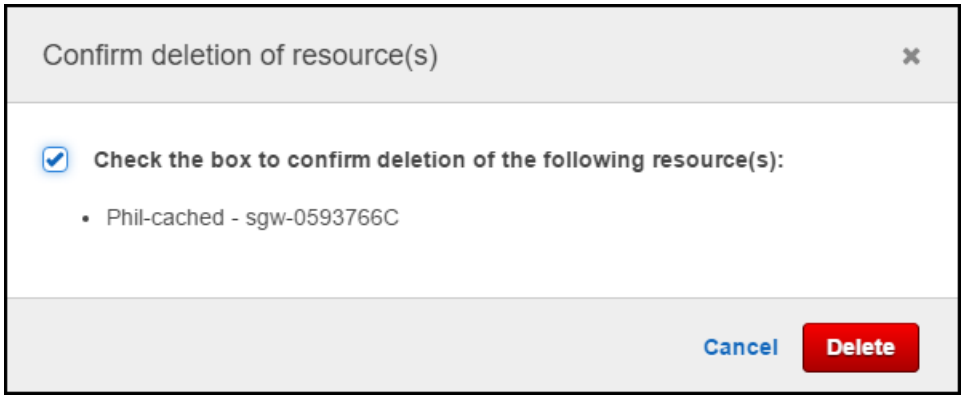
Para eliminar una gateway

1. Abrir la consola de Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
2. En el panel de navegación, elija Gateways y, a continuación, seleccione la gateway que desea eliminar.
3. En Actions (Acciones), elija Delete gateway (Eliminar la gateway).

4.

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

En el cuadro de diálogo de confirmación que aparece, active la casilla de verificación para confirmar la eliminación. Asegúrese de que el ID de la gateway que aparece especifica la gateway que desea eliminar y, a continuación, elija Delete (Eliminar).



> **Important**
>
> Después de eliminar una gateway dejará de pagar cargos por el software, pero persistirán recursos tales como cintas virtuales, instantáneas de Amazon Elastic Block Store (Amazon EBS) e instancias de Amazon EC2. Estos recursos se le seguirán facturando. Puede optar por eliminar las instancias de Amazon EC2 y las instantáneas de Amazon EBS mediante la cancelación de la suscripción a Amazon EC2. Si desea mantener la suscripción a Amazon EC2, puede eliminar las instantáneas de Amazon EBS mediante la consola de Amazon EC2.

Eliminación de recursos de una gateway implementada on-premises

Puede utilizar las instrucciones siguientes para eliminar recursos de una gateway implementada on-premises.

Eliminación de recursos de una gateway de volúmenes implementada en una MV

Si la gateway que desea eliminar está implementada en una máquina virtual (MV), le sugerimos que realice las acciones siguientes para limpiar los recursos:

- Elimine la gateway.

Eliminación de recursos de una gateway implementada en una instancia de Amazon EC2

Si desea eliminar una gateway implementada en una instancia de Amazon EC2, le recomendamos que limpie laAWSrecursos que se hayan utilizado con la gateway, así contribuirá a evitar cargos por uso no deseados.

Eliminación de recursos de los volúmenes almacenados en caché implementados en Amazon EC2

Si ha implementado una gateway con volúmenes almacenados en caché en EC2, le sugerimos que haga lo siguiente para eliminar la gateway y limpiar los recursos:

1. En la consola de Storage Gateway, elimine la gateway como se muestra enEliminación de la gateway mediante la consola de Storage Gateway.
2. En la consola de Amazon EC2, detenga la instancia EC2 si piensa utilizar la instancia de nuevo. De lo contrario, finalice la instancia. Si piensa eliminar volúmenes, anote los dispositivos de bloques asociados a la instancia y los identificadores de los dispositivos antes de finalizar la instancia. Los necesitará para identificar los volúmenes que desee eliminar.
3. En la consola de Amazon EC2, elimine todos los volúmenes de Amazon EBS asociados a la instancia si no planea utilizarlos de nuevo. Para obtener más información, consulteElimine la instancia y el volumenen laGuía del usuario de Amazon EC2 para instancias de Linux.

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

Puede reemplazar un File Gateway existente por una nueva instancia a medida que aumentan sus necesidades de datos y rendimiento, o si recibe unAWSnotificación para migrar la gateway. Es posible que tenga que hacerlo si desea mover la puerta de enlace a una mejor plataforma de host o a instancias Amazon EC2 más recientes, o bien actualizar el hardware del servidor subyacente.

Existen dos métodos para reemplazar una puerta de enlace de archivos existente. En la siguiente tabla se describen los beneficios y los inconvenientes de cada método. Con esta información, seleccione el método más adecuado para su entorno de puerta de enlace y, a continuación, consulte los pasos del procedimiento de la sección correspondiente a continuación.

	Método 1: Migración de disco de caché y ID de puerta de enlace a instancia de reemplazo	Método 2: Instancia de reemplazo con disco de caché vacío y nuevo ID de puerta de enlace
Datos del disco en caché	Los datos del disco de caché se conservan. Este método resulta útil si la puerta de enlace tiene un disco de caché grande o si las aplicacio nes son sensibles al retraso causado por las operaciones de lectura fuera de la caché.	Los datos de la caché se descargan desde elAWSnube . Este método es óptimo para cargas de trabajo de gran cantidad de escritura, si las aplicaciones pueden tolerar el retraso causado por las lecturas fuera de la memoria caché.
Tiempo de inactividad	La puerta de enlace permanecerá desconectada durante 1 o 2 horas durante el proceso de migración.	Sin tiempo de inactividad. La puerta de enlace existente se puede utilizar simultáne amente con la puerta de enlace de reemplazo hasta que elija eliminarla. No se admiten varios escritores

	Método 1: Migración de disco de caché y ID de puerta de enlace a instancia de reemplazo	Método 2: Instancia de reemplazo con disco de caché vacío y nuevo ID de puerta de enlace
		mientras se utilizan ambas puertas de enlace.
ID de gateway	La nueva puerta de enlace hereda el ID de puerta de enlace de la puerta de enlace que reemplaza.	La puerta de enlace y la puerta de enlace de reemplazo existentes tienen ID de puerta de enlace independientes y únicos

> **Note**
>
> Los datos se pueden mover solo entre gateways del mismo tipo.

Método 1: Migración de disco de caché y ID de puerta de enlace a instancia de reemplazo

Para migrar el disco caché y el ID de puerta de enlace de File Gateway a una instancia de reemplazo:

1. Detenga las aplicaciones que escriban en la gateway de archivos existente.
2. Verificar que la`CachePercentDirty`Métrica en laMonitoreopara la puerta de enlace de archivos existente es`0`.
3. Apague la puerta de enlace de archivos existente apagando la máquina virtual host (VM) mediante sus controles de hipervisor.

   Para obtener más información acerca del cierre de una instancia Amazon EC2, consulteDetener e iniciar la instanciaen laGuía del usuario de Amazon EC2.

   Para obtener más información sobre cómo apagar una máquina virtual KVM, VMware o Hyper-V, consulte la documentación de su hipervisor.

4. Desconecte todos los discos, incluidos el disco raíz, los discos de caché y los discos de búfer de carga de la antigua máquina virtual de puerta de enlace.

   > **Note**
   >
   > Anote el ID de volumen del disco raíz, así como del ID de puerta de enlace asociado a ese disco raíz. Tendrá que separar este disco del nuevo hipervisor de puerta de enlace de almacenamiento en un paso posterior.

   Si utiliza una instancia de Amazon EC2 como máquina virtual para la puerta de enlace de archivos, consulteSeparar un volumen de Amazon EBS de una instancia de WindowsoSeparar un volumen de Amazon EBS de una instancia de Linuxen laGuía del usuario de Amazon EC2.

   Para obtener información acerca de la separación de discos de una máquina virtual KVM, VMware o Hyper-V, consulte la documentación de su hipervisor.

5. Creación de un nuevoAWSInstancia de máquina virtual hipervisor de Storage Gateway, 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 acerca de la creación de una nueva máquina virtual hipervisor de Storage Gateway, consulteSelección de una plataforma host y descarga de la máquina virtual.

   > **Note**
   >
   > No agregue discos de caché para la nueva máquina virtual. Esta máquina virtual utilizará los mismos discos de caché que usaba la máquina virtual anterior.

6. Configure su nueva máquina virtual de Storage Gateway para que use la misma configuración de red que la antigua máquina virtual.

   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 la máquina virtual de gateway, consulteConfiguración de red de la gateway.

   Si la máquina virtual de gateway debe utilizar un proxy Socket Secure versión 5 (SOCKS5) para conectarse a Internet, consulteRuteo de la gateway on-premises a través de un proxy.

7. Inicie la nueva máquina virtual de Storage Gateway.
8. Conecte los discos que separó de la antigua máquina virtual de puerta de enlace a la nueva máquina virtual de puerta de enlace. No desconecte el disco raíz existente de la nueva máquina virtual de puerta de enlace.

   > **Note**
   >
   > Para migrar correctamente, todos los discos deben permanecer sin cambios. Cambiar el tamaño del disco u otros valores provoca incoherencias en los metadatos que impiden la migración correcta.

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 utilizar la misma dirección IP para la nueva máquina virtual de puerta de enlace que utilizó para la antigua máquina virtual de puerta de enlace. La URL debe parecerse a los siguientes ejemplos:

   http://*198.51.100.123*/migrate?gatewayId=*sgw-12345678*

   Utilice 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 gateway seaEn ejecuciónen laAWSconsola Storage Gateway. En función del ancho de banda disponible, puede tardar hasta 10 minutos.
11. Detenga la nueva máquina virtual de Storage Gateway.
12. Desconecte el disco raíz de la puerta de enlace anterior, cuyo ID de volumen ha indicado anteriormente, de la nueva puerta de enlace.
13. Inicie la nueva máquina virtual de Storage Gateway.
14. Si la gateway se ha unido a un dominio de Active Directory, vuelva a unirse al dominio. Para obtener instrucciones, consulteConfiguración del acceso a Microsoft Active Directory.

> **Note**
>
> Debe completar este paso incluso si el estado de la puerta de enlace de archivos aparece comoJoined (Se unió).

15. Confirme que los recursos compartidos están disponibles en la dirección IP de la nueva máquina virtual de puerta de enlace y, a continuación, elimine la antigua máquina virtual de puerta de enlace.

> **Warning**
>
> Cuando se elimina una gateway, no se puede recuperar.

Para obtener más información acerca de cómo eliminar una instancia Amazon EC2, consulteTerminar una instanciaen laGuía del usuario de Amazon EC2. Para obtener más información acerca de cómo eliminar una máquina virtual KVM, VMware o Hyper-V, consulte la documentación de su hipervisor.

Método 2: Instancia de reemplazo con disco de caché vacío y nuevo ID de puerta de enlace

Para configurar una instancia de File Gateway de reemplazo con un disco de caché vacío y un nuevo ID de puerta de enlace:

1. Detenga las aplicaciones que escriban en la gateway de archivos existente. Verificar que la`CachePercentDirty`Métrica en laMonitoreoLa pestaña es`0`antes de configurar los recursos compartidos de archivos en la nueva puerta de enlace.
2. UsarAWS Command Line Interface(AWS CLI) para recopilar y guardar la información de configuración sobre la puerta de enlace de archivos y los recursos compartidos de archivos existentes mediante lo siguiente:

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

```
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 los metadatos de la gateway, por ejemplo, su nombre, las interfaces de red, la zona horaria configurada y su estado (si la gateway se está ejecutando).

b. Guarde la configuración del bloque de mensajes del servidor (SMB) de la gateway de archivos.

```
aws storagegateway describe-smb-setting --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, estado de Microsoft Active Directory, si se ha establecido la contraseña de invitado y el tipo de estrategia de seguridad.

c. Guarde la información del recurso compartido de archivos para cada recurso compartido de archivos SMB y Network File System (NFS) de la puerta de enlace de archivos:

- Utilice el siguiente comando para los recursos compartidos de 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 NFS, como su nombre, clase de almacenamiento, estado, rol de IAM Amazon Resource Name (ARN), una lista de clientes a los que se les permite acceder a la puerta de enlace de archivos 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 de rol de IAM, una lista de clientes a los que se les permite acceder a la puerta de enlace de archivos y la ruta utilizada por el cliente NFS para identificar el punto de montaje.

3. Detenga la puerta de enlace de archivos existente haciendo lo siguiente:

a. Detenga las aplicaciones que escriban en la gateway de archivos existente. Verificar que la`CachePercentDirty`Métrica en laMonitoreoLa pestaña es`0`antes de configurar los recursos compartidos de archivos en la nueva puerta de enlace.

b. Detenga la puerta de enlace de archivos existente apagando la máquina virtual (VM) que aloja la puerta de enlace.

4. Cree una nueva puerta de enlace de archivos.
5. Monte los recursos compartidos de archivos configurados en la puerta de enlace anterior.
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 gateway, asegúrese de que no haya aplicaciones escribiendo en la caché de la gateway de archivos. Si elimina una gateway de archivos mientras se esté utilizando, puede producirse pérdida de datos.

> **Warning**
>
> Cuando se elimina una gateway, no se puede recuperar.

7. Elimine la antigua máquina virtual gateway o la instancia EC2.

Desempeño

En esta sección, encontrará información sobre el rendimiento de Storage Gateway.

Temas

- Guía de desempeño de las gateways de archivos
- Optimización del rendimiento de la gateway
- Uso de la alta disponibilidad de VMware vSphere con Storage Gateway

Guía de desempeño de las gateways de archivos

En esta sección, encontrará directrices de configuración para aprovisionar hardware para su máquina virtual de gateway de archivos. Los tamaños y tipos de instancias de Amazon EC2 que se indican en la tabla son ejemplos y se proporcionan como referencia.

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

En los cuadros siguientes,acierto en cachélas operaciones de lectura son lecturas de los recursos compartidos de archivos que se obtienen desde la caché. Falta el cachélas operaciones de lectura son lecturas de los recursos compartidos de archivos que se obtienen desde Amazon S3.

> **Note**
>
> No recomendamos el uso del almacenamiento efímero. Para obtener información sobre el uso del almacenamiento efímero, consulte Uso del almacenamiento efímero con puertas de enlace EC2.

A continuación se presentan ejemplos de configuraciones de puerta de enlace de archivos.

Rendimiento de S3 File Gateway en clientes Linux

Ejemplo de configuraciones	Protocolo	Rendimiento de escritura (tamaños de archivo 1 GB)	Rendimiento de lectura de aciertos de caché	Rendimiento de lectura de errores de la caché
Disco raíz: 80 GB io1, 4.000 IOPS Disco en caché: Caché de 512 GiB, io1, 1 500 IOPS provision adas Rendimiento mínimo de red: 10 Gbps CPU: 16 vCPU | RAM: 32 GB Protocolo NFS recomendado para Linux	NFSv3 - 1 hilo	110 MIB/seg (0,92 Gbps)	590 MiB/s (4,9 Gbps)	310 MIB/seg (2,6 Gbps)
	NFSv3 - 8 hilos	160 MiB/s (1,3 Gbps)	590 MiB/s (4,9 Gbps)	335 MiB/s (2,8 Gbps)
	NFSv4 - 1 hilo	130 MIB/seg (1,1 Gbps)	590 MiB/s (4,9 Gbps)	295 MiB/s (2,5 Gbps)
	NFSv4 - 8 hilos	160 MiB/s (1,3 Gbps)	590 MiB/s (4,9 Gbps)	335 MiB/s (2,8 Gbps)
	SMBV3 - 1 hilo	115 MiB/s (1,0 Gbps)	325 MIB/seg (2,7 Gbps)	255 MIB/seg (2,1 Gbps)
	SMBV3 - 8 hilos	190 MIB/seg (1,6 Gbps)	590 MiB/s (4,9 Gbps)	335 MiB/s (2,8 Gbps)
Dispositivo de hardware de Storage Gateway Rendimiento mínimo de red: 10 Gbps	NFSv3 - 1 hilo	265 MiB/s (2,2 Gbps)	590 MiB/s (4,9 Gbps)	310 MIB/seg (2,6 Gbps)
	NFSv3 - 8 hilos	385 MIB/seg (3,1 Gbps)	590 MiB/s (4,9 Gbps)	335 MiB/s (2,8 Gbps)
	NFSv4 - 1 hilo	310 MIB/seg (2,6 Gbps)	590 MiB/s (4,9 Gbps)	295 MiB/s (2,5 Gbps)
	NFSv4 - 8 hilos	385 MIB/seg (3,1 Gbps)	590 MiB/s (4,9 Gbps)	335 MiB/s (2,8 Gbps)

Ejemplo de configuraciones	Protocolo	Rendimiento de escritura (tamaños de archivo 1 GB)	Rendimiento de lectura de aciertos de caché	Rendimiento de lectura de errores de la caché
Disco raíz: 80 GB, io1 SSD, 4 000 IOPS Disco caché: 4 discos de caché NVME de 2 TB Rendimiento mínimo de red: 10 Gbps CPU: 32 vCPU | RAM: 244 GB Protocolo NFS recomendado para Linux	SMBV3 - 1 hilo	275 MIB/seg (2,4 Gbps)	325 MIB/seg (2,7 Gbps)	255 MIB/seg (2,1 Gbps)
	SMBV3 - 8 hilos	455 MiB/s (3,8 Gbps)	590 MiB/s (4,9 Gbps)	335 MiB/s (2,8 Gbps)
	NFSv3 - 1 hilo	300 MiB/s (2,5 Gbps)	590 MiB/s (4,9 Gbps)	325 MIB/seg (2,7 Gbps)
	NFSv3 - 8 hilos	585 MiB/s (4,9 Gbps)	590 MiB/s (4,9 Gbps)	580 MiB/s (4,8 Gbps)
	NFSv4 - 1 hilo	355 MiB/s (3,0 Gbps)	590 MiB/s (4,9 Gbps)	340 MiB/s (2,9 Gbps)
	NFSv4 - 8 hilos	575 MiB/s (4,8 Gbps)	590 MiB/s (4,9 Gbps)	575 MiB/s (4,8 Gbps)
	SMBV3 - 1 hilo	230 MiB/s (1,9 Gbps)	325 MIB/seg (2,7 Gbps)	245 MiB/s (2,0 Gbps)
	SMBV3 - 8 hilos	585 MiB/s (4,9 Gbps)	590 MiB/s (4,9 Gbps)	580 MiB/s (4,8 Gbps)

Rendimiento de gateway de archivos en clientes Windows

Ejemplo de configuraciones	Protocolo	Rendimiento de escritura (tamaños de archivo 1 GB)	Rendimiento de lectura de aciertos de caché	Rendimiento de lectura de errores de la caché
Disco raíz: 80, GB io1, 4 000 IOPS Disco en caché: Caché de 512 GiB, io1, 1 500 IOPS provision adas Rendimiento mínimo de red: 10 Gbps CPU: 16 vCPU | RAM: 32 GB Protocolo SMB recomendado para Windows	SMBV3 - 1 hilo	150 MiB/s (1,3 Gbps)	180 MiB/s (1,5 Gbps)	20 MiB/s (0,2 Gbps)
	SMBV3 - 8 hilos	190 MIB/seg (1,6 Gbps)	335 MiB/s (2,8 Gbps)	195 MIB/seg (1,6 Gbps)
	NFSv3 - 1 hilo	95 MiB/s (0,8 Gbps)	130 MIB/seg (1,1 Gbps)	20 MiB/s (0,2 Gbps)
	NFSv3 - 8 hilos	190 MIB/seg (1,6 Gbps)	330 MiB/s (2,8 Gbps)	190 MIB/seg (1,6 Gbps)
Dispositivo de hardware de Storage Gateway Rendimiento mínimo de red: 10 Gbps	SMBV3 - 1 hilo	230 MiB/s (1,9 Gbps)	255 MIB/seg (2,1 Gbps)	20 MiB/s (0,2 Gbps)
	SMBV3 - 8 hilos	835 MiB/s (7,0 Gbps)	475 MiB/s (4,0 Gbps)	195 MIB/seg (1,6 Gbps)
	NFSv3 - 1 hilo	135 MIB/seg (1,1 Gbps)	185 MIB/seg (1,6 Gbps)	20 MiB/s (0,2 Gbps)
	NFSv3 - 8 hilos	545 MIB/seg (4,6 Gbps)	470 MiB/s (4,0 Gbps)	190 MIB/seg (1,6 Gbps)

Ejemplo de configuraciones	Protocolo	Rendimiento de escritura (tamaños de archivo 1 GB)	Rendimiento de lectura de aciertos de caché	Rendimiento de lectura de errores de la caché
Disco raíz: 80 GB, io1 SSD, 4 000 IOPS Disco caché: 4 discos de caché NVME de 2 TB Rendimiento mínimo de red: 10 Gbps CPU: 32 vCPU | RAM: 244 GB Protocolo SMB recomendado para Windows	SMBV3 - 1 hilo	230 MiB/s (1,9 Gbps)	265 MiB/s (2,2 Gbps)	30 MiB/s (0,3 Gbps)
	SMBV3 - 8 hilos	835 MiB/s (7,0 Gbps)	780 MiB/s (6,5 Gbps)	250 MIB/seg (2,1 Gbps)
	NFSv3 - 1 hilo	135 MIB/seg (1,1. Gbps)	220 MiB/s (1,8 Gbps)	30 MiB/s (0,3 Gbps)
	NFSv3 - 8 hilos	545 MIB/seg (4,6 Gbps)	570 MiB/s (4,8 Gbps)	240 MiB/s (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.

Optimización del rendimiento de la gateway

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

Añada recursos a la gateway

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

Utilice discos de mayor rendimiento

Para optimizar el rendimiento de la gateway, puede añadir discos de alto rendimiento, como unidades de estado sólido (SSD) y un controlador NVMe. También puede asociar discos virtuales a la MV directamente desde una red de área de almacenamiento (SAN) en lugar de Microsoft Hyper-V NTFS. La mejora del rendimiento del disco suele producir un mejor rendimiento y más operaciones de entrada/salida por segundo (IOPS). Para obtener información sobre la adición de discos, consulte.Agregar almacenamiento en caché.

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

> **Note**
>
> Las métricas de CloudWatch no están disponibles para todas las gateways. Para obtener información sobre métricas de puertas de enlace, consulte Supervisión de la gateway de archivos.

Añada recursos de CPU al host de la gateway

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

Cuando se añaden CPU adicionales al servidor de alojamiento de la gateway, se aumenta la capacidad de procesamiento de la gateway. De este modo, la gateway le permite que, en paralelo, almacene datos de la aplicación al almacenamiento local y cargue estos datos en Amazon S3. Las CPU adicionales también contribuyen a garantizar que la gateway obtenga

suficientes recursos de CPU cuando el host se comparta con otras MV. Proporcionar suficientes recursos de CPU tiene el efecto general de mejorar el rendimiento.

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

- 24 CPU.
- 16 GiB de RAM reservada para las gateways de archivos
  - 16 GiB de RAM reservada para puertas de enlace con un tamaño de caché de hasta 16 TiB
  - 32 GiB de RAM reservada para puertas de enlace con un tamaño de caché de 16 TiB a 32 TiB
  - 48 GiB de RAM reservada para puertas de enlace con un tamaño de caché de 32 TiB a 64 TiB
- Disco 1 asociado a controlador paravirtual 1, que se utiliza como caché de la gateway de la manera siguiente:
  - SSD que utiliza un controlador NVMe.
- Disco 2 asociado a controlador paravirtual 1, que se utiliza como búfer de carga de la gateway de la manera siguiente:
  - SSD que utiliza un controlador NVMe.
- Disco 3 asociado a controlador paravirtual 2, que se utiliza como búfer de carga de la gateway de la manera siguiente:
  - SSD que utiliza un controlador NVMe.
- Adaptador de red 1 configurado en red de MV 1:
  - Utilice la red de VM 1 y añada una VMXnet3 (de 10 Gbps) para su uso en la adquisición.
- Adaptador de red 2 configurado en red de MV 2:
  - Utilice la red de MV 2 y añada una VMXnet3 (de 10 Gbps) para su uso en la conexión a AWS.

Respalde los discos virtuales de la gateway con discos físicos independientes

Cuando aprovisione discos de gateway, le recomendamos encarecidamente que no aprovisione discos locales para el almacenamiento local que utilicen el mismo disco de almacenamiento físico subyacente. Por ejemplo, para VMware ESXi, los recursos de almacenamiento físico subyacente se representan como un almacén de datos. Al implementar la máquina virtual de gateway, debe elegir el almacén de datos en el que se almacenarán los archivos de la máquina virtual. Cuando

aprovisione un disco virtual (por ejemplo, como búfer de carga), puede almacenar el disco virtual en el mismo almacén de datos que la máquina virtual o en un almacén de datos diferente.

Si tiene más de un almacén de datos, le recomendamos encarecidamente que elija un almacén de datos para cada tipo de almacenamiento local que esté creando. Un almacén de datos respaldado por un único disco físico subyacente puede dar lugar a un bajo rendimiento. Por ejemplo, cuando se utiliza el mismo disco para respaldar tanto el almacenamiento en caché como para el búfer de carga en una configuración de gateway. Del mismo modo, un almacén de datos respaldado por una configuración RAID que no sea de alto rendimiento, como RAID 1, puede dar lugar a un bajo rendimiento.

Añada recursos al entorno de aplicaciones

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

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

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

Añada recursos de CPU al entorno de aplicaciones

Si la aplicación puede utilizar más recursos de CPU, la adición de más CPU puede ayudar a la aplicación a escalar la carga de E/S.

Uso de la alta disponibilidad de VMware vSphere con Storage Gateway

Storage Gateway proporciona alta disponibilidad en VMware a través de un conjunto de comprobaciones de estado en el nivel de aplicación integradas con la alta disponibilidad de VMware vSphere (HA de 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 gateway implementada en un entorno de VMware en las instalaciones o en una nube de VMware en AWS se recupera automáticamente de la mayoría de interrupciones de servicio. Esta operación se suele realizar en menos de 60 segundos sin pérdidas de datos.

Para utilizar VMware HA con Storage Gateway, realice los pasos que se indican a continuación.

Temas

Configurar el clúster de HA de vSphere VMware

En primer lugar, si aún no ha creado un clúster de VMware, cree uno. Para obtener información acerca de cómo crear un clúster de VMware, consulte Crear un clúster de HA de vSphere en la documentación de VMware.

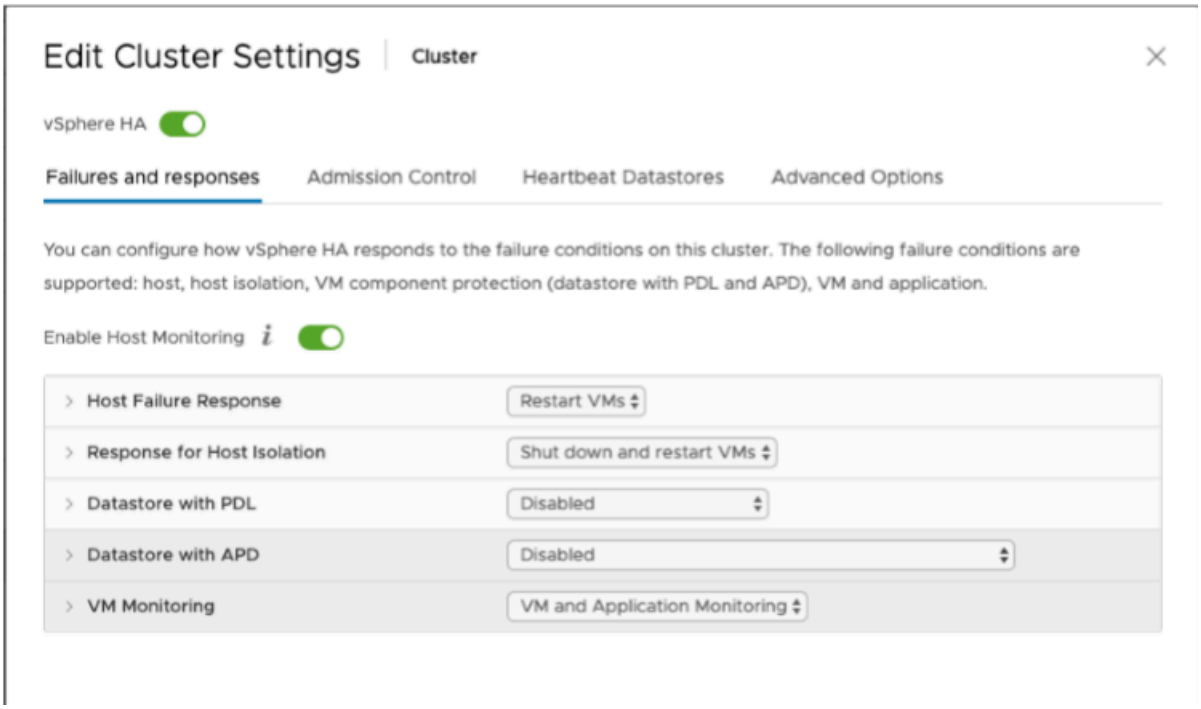
A continuación, configure el clúster de VMware para que funcione con Storage Gateway.

Para configurar el clúster de VMware

1. En la página Edit Cluster Settings (Editar configuración de clúster) de VMware vSphere, asegúrese de que la monitorización de MV se configure para la monitorización de aplicaciones y MV. Para ello, configure las siguientes opciones como se indica a continuación:

   - Respuesta de error de host: Reiniciar MV
   - Respuesta para aislamiento de host: Apagar y reiniciar MV
   - Almacén de datos con PDL: Deshabilitada
   - Almacén de datos con APD: Deshabilitada
   - Monitorización de máquinas virtuales: VM and Application Monitorización de

Para ver un ejemplo, consulte las siguientes capturas de pantalla.



2. Ajuste la sensibilidad del clúster mediante la configuración de los siguientes valores:

   - Intervalo de error— Después de este intervalo, la máquina virtual se reinicia si no se recibe el latido del corazón de una máquina virtual.
   - Tiempo de actividad mínimo— El clúster espera tanto tiempo después de que una máquina virtual comience a supervisar los latidos de las herramientas de VM.
   - Máximo de restablecimientos por MV— El clúster reinicia la máquina virtual un máximo de esta cantidad de veces dentro de la ventana de tiempo máximo de restablecimientos.
   - Periodo de tiempo máximo de restablecimientos— El periodo de tiempo en el que se contabilizan los restablecimientos máximos por VM.

   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 otras MV en ejecución en el clúster, es posible que desee establecer estos valores específicamente para la MV. 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) Añadir opciones de anulación para otras MV del clúster.

Descargar la imagen .ova según el tipo de gateway

Utilice el siguiente procedimiento para descargar la imagen .ova.

Para descargar la imagen .ova según el tipo de gateway

- Descargue la imagen .ova según el tipo de gateway desde:
  - Gateway de archivos —

Implementar la gateway

En el clúster configurado, implemente la imagen .ova en uno de los hosts del clúster.

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.

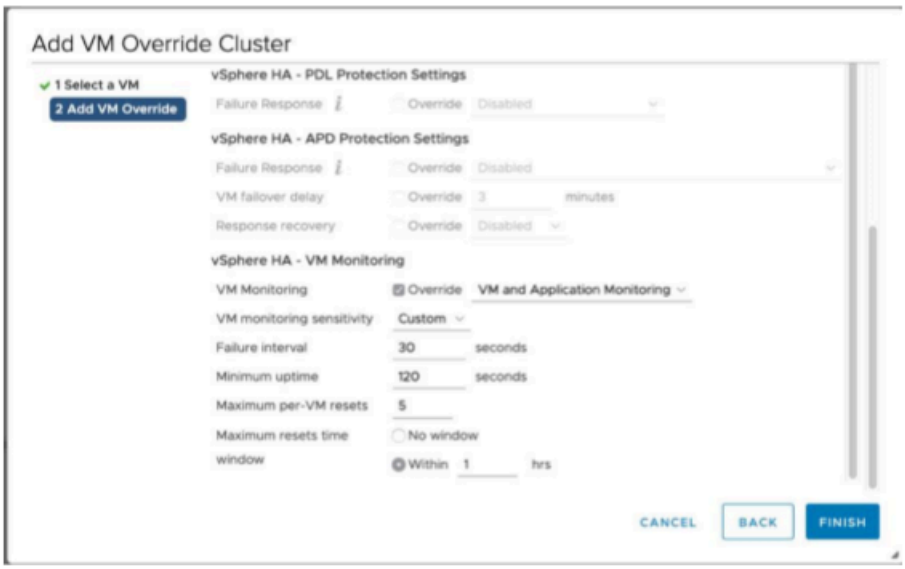
(Opcional) Añadir opciones de anulación para otras MV del clúster

Si tiene otras MV en ejecución en el clúster, es posible que desee establecer los valores del clúster específicamente para cada MV.

Para añadir opciones de anulación para otras MV del clúster

1. En la página Summary (Resumen) de VMware vSphere, seleccione el clúster para abrir la página del clúster y, a continuación, seleccione Configure (Configurar).
2. Seleccione la pestaña Configuration (Configuración) y, a continuación, seleccione VM Overrides (Anulaciones de MV).
3. Añada una nueva opción de anulación de MV para cambiar cada valor.

Para obtener información sobre las opciones de anulación, consulte la siguiente captura de pantalla.



Activar la gateway

Cuando implemente la imagen .ova de la gateway, active la gateway. Las instrucciones acerca de cómo hacerlo son diferentes para cada tipo de gateway.

Para activar la gateway

- Seleccione las instrucciones de activación en función del tipo de gateway:
  - Gateway de archivos —

Probar la configuración de alta disponibilidad de VMware

Después de activar la gateway, pruebe la configuración.

Para probar la configuración de HA de VMware

1. Abrir la consola de Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
2. En el panel de navegación, seleccione Gateways y, a continuación, seleccione la gateway en la que desea probar la HA de VMware.
3. En Actions (Acciones), seleccione Verify VMware HA (Verificar HA de VMware).

4. En el cuadro Verify VMware High Availability Configuration (Verificar configuración de alta disponibilidad de VMware) que aparece, seleccione OK (Aceptar).

   > **Note**
   >
   > Al probar la configuración de HA de VMware, la MV de la gateway se reinicia y se interrumpe la conectividad con la gateway. 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 Exit (Salir).

Puede encontrar información sobre eventos de HA de VMware en los grupos de registros de Amazon CloudWatch. Para obtener más información, consulte Obtener registros de estado de puerta de enlace de archivos con grupos de registros de CloudWatch.

Seguridad enAWSStorage Gateway

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficia de una arquitectura de red y un centro de datos que se han diseñado para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre 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 los servicios de AWS en la nube de AWS. AWS también proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWSProgramas de conformidad de . Para obtener más información acerca de los programas de conformidad que se aplican aAWSStorage Gateway, consulteAWSServicios en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad se determina según el servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo 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 aprende cómo utilizar otrosAWSservicios de que le ayudan a monitorizar y proteger los recursos de Storage Gateway.

Temas

Protección de los datos enAWSStorage Gateway

LaAWS modelo de responsabilidad compartidase aplica a la protección de datos enAWSStorage Gateway. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Este contenido incluye la configuración de seguridad y las tareas de administración de los servicios de AWS que usted utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog AWSShared Responsability Model and GDPR en el Blog de seguridad de AWS.

Para fines de protección de datos, recomendamos proteger las credenciales de Cuenta de AWS y configurar cuentas de usuario individuales con AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir con sus obligaciones laborales. También recomendamos proteger sus datos de las siguientes formas:

- Utilice Multi-Factor Authentication (MFA) con cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos de AWS. Recomendamos TLS 1.2 o una versión posterior.
- Configure la API y el registro de actividad del usuario con AWS CloudTrail.
- Utilice las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los servicios de AWS.
- Utilice avanzados servicios de seguridad administrados, como Amazon Macie, que lo ayuden a detectar y proteger los datos personales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-2 al acceder a AWS a través de una interfaz de línea de comandos o una API, utilice un punto de enlace de FIPS. Para obtener más información sobre los puntos de enlace de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Recomendamos encarecidamente que nunca introduzca información de identificación confidencial, como, por ejemplo, direcciones de email de sus clientes, en etiquetas o en los campos de formato libre, como el campo Name (Nombre). Esto incluye cuando trabaje con Storage Gateway u otroAWSservicios que utilizan la consola, API,AWS CLI, o bienAWSSDK. Los datos que ingresa en etiquetas o campos de formato libre utilizados para los nombres se pueden utilizar 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 medianteAWS KMS

Storage Gateway utiliza SSL/TLS (capas de conexión segura/seguridad de la capa de transporte) para cifrar los datos que se transfieren entre el dispositivo de gateway yAWSAlmacenamiento de. De forma predeterminada, Storage Gateway utiliza claves de cifrado administradas por Amazon S3 (SSE-S3) para cifrar en el lado del servidor todos los datos que almacena en Amazon S3. Tiene la opción de utilizar la API de Storage Gateway para configurar su gateway para cifrar los datos almacenados en la nube mediante el cifrado en el lado del servidor conAWS Key Management Service(SSE-KMS) claves maestras del cliente (CMK).

> **Important**
>
> Cuando utiliza unAWS KMSCMK para el cifrado en el lado del servidor, debe elegir una CMK simétrica. Storage Gateway no admite CMK asimétricas. Para obtener más información, consulte Uso de claves simétricas y asimétricas en la guía para desarrolladores de AWS Key Management Service.

Cifrado de un recurso compartido de archivos

Para un recurso compartido de archivos, puede configurar la puerta de enlace para cifrar los objetos conAWS KMS—claves administradas mediante SSE-KMS. Para obtener información acerca del uso de la API de Storage Gateway para cifrar los datos que se escriben en un recurso compartido de archivos, consulteCreateNFSFileShareen laAWS Storage GatewayReferencia de la API.

Cifrado de un sistema de archivos

Para obtener información, consulte:Cifrado de datos en Amazon FSxen laGuía del usuario de Amazon FSx for Windows File Server.

Cuando utilice AWS KMS para cifrar datos, tenga 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 alAWS KMSOperaciones de la API. Para obtener más información, consulteUso de políticas de IAM conAWS KMSen laAWS Key Management ServiceGuía para desarrolladores.

- Si elimina o deshabilita su CMK o revoca el token de concesión, no podrá tener acceso a los datos del volumen o la cinta. Para obtener más información, consulteEliminar las claves maestras de clienteen laAWS Key Management ServiceGuía para desarrolladores.
- Si crea una instantánea de un volumen cifrado con KMS, la instantánea está cifrada. La instantánea hereda la clave de KMS del volumen.
- Si crea un volumen a partir de una instantánea cifrada con KMS, el volumen está cifrado. Para especificar otra clave de KMS para el volumen nuevo.

> **Note**
>
> Storage Gateway no admite la creación de un volumen sin cifrar a partir de un punto de recuperación de un volumen cifrado con KMS o de una instantánea cifrada con KMS.

Para obtener más información acerca de AWS KMS, consulte ¿Qué es AWS Key Management Service?

Autenticación y control de acceso para Storage Gateway

El acceso a AWS Storage Gateway requiere credenciales que AWS puede utilizar para autenticar las solicitudes. Estas credenciales deben tener permisos para obtener acceso aAWSrecursos, como una gateway, un recurso compartido de archivos, un volumen o una cinta. En las siguientes secciones, se incluye información detallada sobre cómo usarAWS Identity and Access Management(IAM)y Storage Gateway para ayudar a proteger sus recursos controlando quién puede obtener acceso a ellos:

- Autenticación
- Control de acceso

Autenticación

Puede obtener acceso a AWS con los siguientes tipos de identidades:

- root user (usuario raíz)Cuenta de AWS: cuando se crea una Cuenta de AWS por primera vez, comienza con una única identidad de inicio de sesión que tiene acceso total a todos los servicios y recursos de AWS en la cuenta. Esta identidad recibe el nombre de usuario raíz de Cuenta de AWS y se accede a ella al iniciar sesión con la dirección de email y la contraseña que utilizó para

crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz en sus tareas cotidianas, ni siquiera en las tareas administrativas. En lugar de ello, es mejor ceñirse a la práctica recomendada de utilizar el usuario final exclusivamente para crear al primer usuario de IAM. A continuación, guarde las credenciales del usuario raíz en un lugar seguro y utilícelas tan solo para algunas tareas de administración de cuentas y servicios.

- Usuario de IAM— UnUsuario de IAMes una identidad dentro de tuCuenta de AWSque tiene permisos personalizados específicos (por ejemplo, permisos para crear una gateway en Storage Gateway). Puede utilizar un nombre de usuario y una contraseña de IAM para iniciar sesión en páginas web seguras de AWS tales como AWS Management Console, Foros de discusión de AWS o el Centro de AWS Support.

  Además de un nombre de usuario y una contraseña, también puede generar claves de acceso para cada usuario. Puede utilizar estas claves al acceder a los servicios de AWS de manera programática, ya sea a través de uno de los varios SDK o mediante la (CLI) de AWS Command Line Interface. El SDK y las herramientas de CLI utilizan claves de acceso para firmar criptográficamente una solicitud. Si no utiliza las herramientas de AWS debe firmar usted mismo la solicitud. Storage GatewaySignature Version 4, un protocolo para autenticar solicitudes de API de entrada. Para obtener más información sobre cómo autenticar solicitudes, consulte Proceso de firma de Signature Version 4 en la Referencia general de AWS.

- IAM role (Rol de IAM): un rol de IAM es una identidad de IAM que puede crear en la cuenta y que tiene permisos específicos. Un rol de IAM es similar a un usuario de IAM en que se trata de una identidad de AWS con políticas de permisos que determinan lo que la identidad puede hacer y lo que no en AWS. Sin embargo, en lugar de asociarse exclusivamente a una persona, la intención es que cualquier usuario pueda asumir un rol que necesite. Además, un rol no tiene asociadas credenciales a largo plazo estándar, como una contraseña o claves de acceso. En su lugar, cuando se asume un rol, este proporciona credenciales de seguridad temporales para la sesión de rol. Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

  - Acceso de usuarios federados: en lugar de crear un usuario de IAM, puede utilizar identidades existentes de AWS Directory Service, del directorio de usuarios de la compañía o de un proveedor de identidades web. A estas identidades se les llama usuarios federados. AWS asigna una función a un usuario federado cuando se solicita acceso a través de un proveedor

de identidad. Para obtener más información sobre los usuarios federados, consulte Usuarios federados y roles en la Guía del usuario de IAM.

- Acceso a los servicios de AWS: un rol de servicio es un rol de IAM que un servicio asume 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.

- Aplicaciones que se ejecutan en Amazon EC2: puede utilizar un rol de IAM que le permita administrar credenciales temporales para las aplicaciones que se ejecutan en una instancia EC2 y realizan solicitudes AWS CLI o AWS a la API. Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar un rol de AWS a una instancia EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia asociado a la misma. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para obtener más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Control de acceso

Puede tener credenciales válidas para autenticar las solicitudes, pero a menos que tenga permisos no podrá crear ni obtener acceso a los recursos de Storage Gateway. Por ejemplo, debe tener permisos para crear una gateway en Storage Gateway.

En las secciones siguientes se describe cómo administrar los permisos de Storage Gateway. Recomendamos que lea primero la información general.

- Información general sobre la administración de permisos de acceso a Storage Gateway
- Políticas basadas en identidad (políticas de IAM)

Información general sobre la administración de permisos de acceso a Storage Gateway

CadaAWSrecurso de es propiedad de una cuenta de Amazon Web Services y los permisos para crear un recurso o tener acceso a él se rigen por las políticas de permisos. Los administradores de cuentas pueden asociar políticas de permisos a identidades de IAM (es decir, usuarios, grupos y funciones). Algunos servicios (como AWS Lambda) también permiten asociar políticas de permisos con los recursos.

> **Note**
>
> Un administrador de la cuenta (o usuario administrador) es un usuario con privilegios de administrador. Para obtener más información, consulte Prácticas recomendadas de IAM en la Guía del usuario de IAM.

Cuando concede permisos, decide quién debe obtener los permisos, para qué recursos se obtienen permisos y qué acciones específicas desea permitir en esos recursos.

Temas

Recursos y operaciones de Storage Gateway

En Storage Gateway, el recurso principal esGateway de. Storage Gateway también admite los siguientes tipos de recursos adicionales: recurso compartido de archivos, volumen, cinta virtual, destino de iSCSI and dispositivo de biblioteca de cintas virtuales (VTL). Se conocen como subrecursos y no existen a menos que estén asociados a una gateway.

Estos recursos y subrecursos tienen nombres de recursos de Amazon (ARN) únicos asociados a ellos, tal y como se muestra en la siguiente tabla:

Tipo de recurso	Formato de ARN
ARN de gateway	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`*
ARN compartido de archivos	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:share/`*`share-id`*

> **Note**
>
> Los ID de recursos de Storage Gateway se indican en mayúscula. Cuando estos ID de recursos se utilizan con la API de Amazon EC2, Amazon EC2 espera que los ID de recursos estén en minúsculas. Debe cambiar los ID de recursos a minúsculas para utilizarlos con la API de EC2. Por ejemplo, en Storage Gateway el ID para un volumen podría ser `vol-1122AABB`. Cuando utilice este ID con la API de EC2, debe cambiarlo a `vol-1122aabb`. De lo contrario, la API de EC2 podría no comportarse según lo previsto. Los ARN de las gateways activados antes del 2 de septiembre de 2015 contienen el nombre de la gateway, en lugar de su ID Para obtener el ARN de la gateway, utilice la operación `DescribeGatewayInformation` de la API.

Para conceder permisos para operaciones de API específicas, como, por ejemplo, crear una cinta, Storage Gateway proporciona un conjunto de acciones de API que le permiten crear y administrar estos recursos y subresources. Para ver la lista de las acciones de la API, consulteActionsen laAWS Storage GatewayReferencia de la API.

Para conceder permisos para operaciones de API específicas, como, por ejemplo, crear una cinta, Storage Gateway define un conjunto de acciones que puede especificar en una política de permisos. Una operación de la API puede requerir permisos para más de una acción. Para ver una tabla con todas las acciones de API de Storage Gateway y los recursos a los que se aplican, consultePermisos API de Storage Gateway Referencia de acciones, recursos y condiciones.

Titularidad de los recursos

UNApropietario del recursoes la cuenta de Amazon Web Services que creó el recurso. Es decir, el propietario del recurso es la cuenta de Amazon Web Services delentidad principal(cuenta raíz, usuario de IAM o rol de IAM) que autentica la solicitud que crea el recurso. Los siguientes ejemplos ilustran cómo funciona:

- Si usa las credenciales de cuenta raíz de su cuenta de Amazon Web Services para activar una gateway, su cuenta de Amazon Web Services es la propietaria del recurso (en Storage Gateway, el recurso es la gateway).
- Si crea un usuario de IAM en su cuenta de Amazon Web Services y concede permisos a`ActivateGateway`acción para ese usuario, el usuario puede activar una gateway. Sin embargo, la cuenta de Amazon Web Services, a la que pertenece el usuario, es la propietaria del recurso de gateway.
- Si crea un rol de IAM en su cuenta de Amazon Web Services con permisos para activar una gateway, cualquier persona que pueda asumir el rol podrá activar una gateway. La cuenta de Amazon Web Services, a la que pertenece el rol, es la propietaria del recurso de gateway.

Administración del acceso a los recursos

Una política de permisos describe quién tiene acceso a qué. En la siguiente sección se explican las opciones disponibles para crear políticas de permisos.

> **Note**
>
> En esta sección se explica cómo se utiliza IAM en el contexto de Storage Gateway. No se proporciona información detallada sobre el servicio de IAM. Para ver la documentación completa de IAM, consulteQué es IAMen laIAM User Guide.Para obtener más información acerca de la sintaxis y las descripciones de las políticas del IAM, consulte Referencia de políticas de IAM de AWS en la Guía del usuario de IAM.

Las políticas asociadas a una identidad de IAM se denominan políticas basadas en identidad (políticas de IAM) y las políticas asociadas a un recurso se denominan políticas basadas en recursos. Storage Gateway solo admite políticas basadas en identidad (políticas de IAM).

Temas

- Políticas basadas en identidad (políticas de IAM)
- Políticas con base en recursos

Políticas basadas en identidad (políticas de IAM)

Puede asociar políticas a identidades de IAM. Por ejemplo, puede hacer lo siguiente:

- Asociar una política de permisos a un usuario o grupo de su cuenta: un administrador de la cuenta puede utilizar una política de permisos asociada a un usuario determinado para concederle permisos para crear un recurso de Storage Gateway, como una gateway, un volumen o una cinta.
- Adjuntar una política de permisos a un rol (conceder permisos para cuentas cruzadas): Puede adjuntar una política de permisos basada en identidades a un rol de IAM para conceder permisos para cuentas cruzadas. Por ejemplo, el administrador de la Cuenta A puede crear un rol para conceder permisos entre cuentas a otra cuenta de Amazon Web Services (por ejemplo, a la Cuenta B) o aAWSservicio de la siguiente manera:
  1. El administrador de la Cuenta A crea un rol de IAM y asocia una política de permisos a dicho rol, que concede permisos sobre los recursos de la Cuenta A.
  2. El administrador de la Cuenta A asocia una política de confianza al rol que identifica la Cuenta B como la entidad principal que puede asumir el rol.
  3. A continuación, el administrador de la Cuenta B puede delegar permisos para asumir el rol a cualquier usuario de la Cuenta B. De este modo, los usuarios de la Cuenta B podrán crear recursos y obtener acceso a ellos en la Cuenta A. La entidad principal de la política de confianza también puede ser la entidad principal de un servicio de AWS si desea conceder permisos para asumir el rol a un servicio de AWS.

  Para obtener más información sobre el uso de IAM para delegar permisos, consulte Administración de accesos en la Guía del usuario de IAM.

A continuación, se muestra un ejemplo de política que concede permisos para todas las acciones `List*` en todos los recursos. Esta acción es de solo lectura. Por lo tanto, la política no permite al usuario cambiar el estado de los recursos.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAllListActionsOnAllResources",
```

```
            "Effect": "Allow",
            "Action": [
                "storagegateway:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obtener más información acerca del uso de políticas basadas en identidad con Storage Gateway, consulteUsar políticas basadas en identidad (políticas de IAM) para Storage Gateway. Para obtener más información sobre usuarios, grupos, roles y permisos, consulte Identidades (usuarios, grupos y roles) en la Guía del usuario de IAM.

Políticas con base en recursos

Otros servicios, como Amazon S3, también admiten políticas de permisos basadas en recursos. Por ejemplo, puede asociar una política a un bucket de S3 para administrar los permisos de acceso a dicho bucket. Storage Gateway no admite políticas basadas en recursos.

Especificación de elementos de la política: Acciones, efectos, recursos y entidades principales

Para cada recurso de Storage Gateway (consultePermisos API de Storage Gateway Referencia de acciones, recursos y condiciones), el servicio define un conjunto de operaciones de API (consulteActions). Para conceder permisos para estas operaciones de API, Storage Gateway define un conjunto de acciones que puede especificar en una política. Por ejemplo, para el recurso gateway de Storage Gateway, se definen las siguientes acciones:`ActivateGateway`,`DeleteGateway`, y`DescribeGatewayInformation`. Tenga en cuenta que la realización de una operación de la API puede requerir permisos para más de una acción.

A continuación se indican los elementos más básicos de la política:

- Recurso: en una política, se usa un nombre de recurso de Amazon (ARN) para identificar el recurso al que se aplica la política. Para los recursos de Storage Gateway, use siempre el carácter comodín(*)en políticas de IAM. Para obtener más información, consulte Recursos y operaciones de Storage Gateway.
- Acción: utilice palabras clave de acción para identificar las operaciones del recurso que desea permitir o denegar. Por ejemplo, en función de la especificación`Effect`,

el`storagegateway:ActivateGateway`permite o deniega los permisos de usuario para realizar Storage Gateway`ActivateGateway`.

- Efecto: especifique el efecto que se producirá cuando el usuario solicite la acción específica; puede ser permitir o denegar. Si no concede acceso de forma explícita (permitir) a un recurso, el acceso se deniega implícitamente. También puede denegar explícitamente el acceso a un recurso para asegurarse de que un usuario no pueda obtener acceso a él, aunque otra política le conceda acceso.
- Entidad principal: en las políticas basadas en identidades (políticas de IAM), el usuario al que se asocia esta política es la entidad principal implícita. Para las políticas basadas en recursos, debe especificar el usuario, la cuenta, el servicio u otra entidad que desee que reciba permisos (se aplica solo a las políticas basadas en recursos). Storage Gateway no admite políticas basadas en recursos.

Para obtener más información sobre la sintaxis y descripciones de las políticas de IAM consulte Referencia de la política de IAM de AWS de la Guía del usuario de IAM.

Para ver una tabla con todas las acciones de API de Storage Gateway, consultePermisos API de Storage Gateway Referencia de acciones, recursos y condiciones.

Especificación de las condiciones de una política

Al conceder permisos, puede utilizar el lenguaje de la política de IAM para especificar las condiciones en las que se debe aplicar una política. Por ejemplo, es posible que desee que solo se aplique una política después de una fecha específica. Para obtener más información sobre cómo especificar condiciones en un lenguaje de política, consulte Condition en la Guía del usuario de IAM.

Para expresar condiciones, se usan claves de condición predefinidas. No hay claves de condición específicas para Storage Gateway. No obstante, existen claves de condición que se aplican a todo AWS que puede utilizar cuando corresponda. Para ver una lista completa de claves generales de AWS, consulte Claves disponibles en la Guía del usuario de IAM.

Usar políticas basadas en identidad (políticas de IAM) para Storage Gateway

Este tema contiene ejemplos de políticas basadas en identidades, donde los administradores de cuentas pueden asociar políticas de permisos a identidades de IAM (es decir, a usuarios, grupos y funciones).

> **Important**
>
> Le recomendamos que consulte primero los temas de introducción en los que se explican los conceptos básicos y las opciones disponibles para administrar el acceso a los recursos de Storage Gateway. Para obtener más información, consulte Información general sobre la administración de permisos de acceso a Storage Gateway.

En las secciones de este tema se explica lo siguiente:

- Permisos necesarios para usar la consola de Storage Gateway
- AWSpolíticas administradas para Storage Gateway
- Ejemplos de políticas administradas por el cliente

A continuación se muestra un ejemplo de una política de permisos.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsSpecifiedActionsOnAllGateways",
            "Effect": "Allow",
            "Action": [
                "storagegateway:ActivateGateway",
                "storagegateway:ListGateways"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowsSpecifiedEC2ActionsOnAllGateways",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSnapshots",
                "ec2:DeleteSnapshot"
            ],
            "Resource": "*"
        }
    ]
}
```

La política tiene dos instrucciones (fíjese en los elementos `Action` y en los elementos `Resource` de ambas):

- La primera instrucción concede permisos para dos acciones de Storage Gateway (`storagegateway:ActivateGatewaystoragegateway:ListGateways`) en un recurso de puerta de enlace.

  El carácter comodín (*) significa que esta instrucción puede coincidir con cualquier recurso. En este caso, la declaración permite la`storagegateway:ActivateGatewaystoragegateway:ListGateways`acciones en cualquier puerta de enlace. El comodín se utiliza aquí porque no conoce el ID del recurso hasta después de que haya creado la gateway. Para obtener información sobre cómo utilizar un comodín (*) en una política, consulte Ejemplo 2: Permitir acceso de solo lectura a una puerta de enlace.

  > **Note**
  >
  > Los ARN identifican de forma exclusivaAWSde AWS. Para obtener más información, consulte Nombres de recursos de Amazon (ARN) y espacios de nombres de servicios de AWS en la Referencia general de AWS.

  Para limitar los permisos de una determinada acción a una sola gateway concreta, cree una instrucción independiente para esa acción en la política y especifique el ID de la gateway en esa instrucción.

- La segunda instrucción concede permisos para las acciones `ec2:DescribeSnapshots` y `ec2:DeleteSnapshot`. Estas acciones de Amazon Elastic Compute Cloud (Amazon EC2) requieren permisos porque las instantáneas generadas en Storage Gateway se almacenan en Amazon Elastic Block Store (Amazon EBS) y se administran como recursos de Amazon EC2. Por consiguiente, requieren las acciones de EC2 correspondientes. Para obtener más información, consulteActionsen laReferencia de la API de Amazon EC2. Dado que estas acciones de Amazon EC2 no admiten permisos en el nivel de recursos, la política especifica el carácter comodín (*) como`Resource`valor en lugar de especificar un ARN de puerta de enlace.

Para ver una tabla con todas las acciones de API de Storage Gateway y los recursos a los que se aplican, consultePermisos API de Storage Gateway Referencia de acciones, recursos y condiciones.

Permisos necesarios para usar la consola de Storage Gateway

Para utilizar la consola de Storage Gateway, debe conceder permisos de solo lectura. Si ha previsto describir instantáneas, también deberá conceder permisos para realizar acciones adicionales, tal y como se muestra en la política de permisos siguiente:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsSpecifiedEC2ActionOnAllGateways",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        }
    ]
}
```

Este permiso adicional se requiere porque las instantáneas de Amazon EBS generadas en Storage Gateway se administran como recursos de Amazon EC2.

Para configurar los permisos mínimos necesarios para navegar por la consola de Storage Gateway, consulteEjemplo 2: Permitir acceso de solo lectura a una puerta de enlace.

AWSpolíticas administradas para Storage Gateway

Amazon Web Services aborda muchos casos de uso comunes proporcionando políticas de IAM independientes creadas y administradas porAWS. Las políticas administradas conceden los permisos necesarios para casos de uso comunes, lo que le evita tener que investigar los permisos que se necesitan. Para obtener más información acerca deAWSPolíticas administradas, consulteAWSPolíticas administradas deen laIAM User Guide.

Los siguientes ejemplos deAWSLas políticas administradas por, que puede asociar a los usuarios de su cuenta de, son específicas de Storage Gateway:

- AWSStorageGatewayReadOnlyAccess: concede acceso de solo lectura a los recursos de AWS Storage Gateway.
- AWSStorageGatewayFullAccess: concede acceso pleno a los recursos de AWS Storage Gateway.

> **Note**
>
> Para consultar estas políticas de permisos, inicie sesión en la consola de IAM y busque las políticas específicas.

También puede crear sus propias políticas de IAM personalizadas con el fin de conceder permisos para realizar acciones de la API de AWS Storage Gateway. Puede asociar estas políticas personalizadas a los usuarios o grupos de IAM que requieran esos permisos.

Ejemplos de políticas administradas por el cliente

En esta sección, encontrará ejemplos de políticas de usuario que conceden permisos para varias acciones de Storage Gateway. Estas políticas funcionan cuando se utilizanAWSSDK y elAWS CLI. Cuando se utiliza la consola, debe conceder permisos adicionales específicos a la consola, tal y como se explica en Permisos necesarios para usar la consola de Storage Gateway.

> **Note**
>
> Todos los ejemplos utilizan la región EE. UU. Oeste (Oregón) (`us-west-2`) y contienen identificadores de cuenta ficticios.

Temas

- Ejemplo 1: Permitir acciones de Storage Gateway en todas las puertas de enlace
- Ejemplo 2: Permitir acceso de solo lectura a una puerta de enlace
- Ejemplo 3: Permitir acceso a una puerta de enlace específica
- Ejemplo 4: Permitir a un usuario acceder a un volumen específico
- Ejemplo 5: Permitir todas las acciones en puertas de enlace con un prefijo específico

Ejemplo 1: Permitir acciones de Storage Gateway en todas las puertas de enlace

La siguiente política permite a un usuario realizar todas las acciones de Storage Gateway. La política también permite al usuario realizar acciones de Amazon EC2 (DescribeSnapshotsyDeleteSnapshot) en las instantáneas de Amazon EBS generadas desde Storage Gateway.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllAWSStorageGatewayActions",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {You can use Windows ACLs only with file shares that are enabled for Active
 Directory.
            "Sid": "AllowsSpecifiedEC2Actions",
            "Action": [
                "ec2:DescribeSnapshots",
                "ec2:DeleteSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Ejemplo 2: Permitir acceso de solo lectura a una puerta de enlace

La siguiente política permite todas las acciones `List*` y `Describe*` en todos los recursos. Tenga en cuenta que estas acciones son de solo lectura. Por lo tanto, la política no permite al usuario modificar el estado de ningún recurso; es decir, la política no permite al usuario realizar acciones tales como `DeleteGateway`, `ActivateGateway` o `ShutdownGateway`.

La política también permite la acción `DescribeSnapshots` de Amazon EC2. Para obtener más información, consulteDescribeSnapshotsen laReferencia de la API de Amazon EC2.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowReadOnlyAccessToAllGateways",
            "Action": [
                "storagegateway:List*",
                "storagegateway:Describe*"
            ],
            "Effect": "Allow",
```

```
            "Resource": "*"
        },
        {
            "Sid": "AllowsUserToDescribeSnapshotsOnAllGateways",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

En la política anterior, en lugar de utilizar un comodín (*), puede ajustar el ámbito de los recursos cubiertos por la política a una gateway concreta, como se muestra en el siguiente ejemplo. En este caso, la política solo permitirá acciones en esa gateway.

```
"Resource": [
              "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
              "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
            ]
```

Dentro de una gateway, puede restringir aún más el alcance de los recursos y limitarlos exclusivamente a los volúmenes de gateway, como se muestra en el ejemplo siguiente:

```
"Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/volume/
*"
```

Ejemplo 3: Permitir acceso a una puerta de enlace específica

La siguiente política permite todas las acciones en una gateway concreta. Se impide al usuario obtener acceso a otras gateways que se hayan implementado.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowReadOnlyAccessToAllGateways",
            "Action": [
                "storagegateway:List*",
```

```
                "storagegateway:Describe*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "AllowsUserToDescribeSnapshotsOnAllGateways",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "AllowsAllActionsOnSpecificGateway",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
            ]
        }
    ]
}
```

La política anterior funciona si el usuario al que se asocia la política utiliza el API o unAWSSDK para acceder a la puerta de enlace. Sin embargo, si el usuario va a utilizar la consola de Storage Gateway, además deberá concederle permisos para permitir el`ListGateways`acción, como se muestra en el ejemplo siguiente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllActionsOnSpecificGateway",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": [
```

```
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
            ]
        },
        {
            "Sid": "AllowsUserToUseAWSConsole",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Ejemplo 4: Permitir a un usuario acceder a un volumen específico

La siguiente política permite a un usuario realizar todas las acciones en un volumen específico de una gateway. Dado que ningún usuario obtiene permisos de forma predeterminada, la política limita el acceso del usuario a un volumen concreto.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantsPermissionsToSpecificVolume",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-
id/volume/volume-id"
        },
        {
            "Sid": "GrantsPermissionsToUseStorageGatewayConsole",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

La política anterior funciona si el usuario a quien se asocia la política utiliza el API o unAWSSDK para acceder al volumen. Sin embargo, si este usuario va a utilizar elAWS Storage Gateway, también debe conceder permisos para permitir la`ListGateways`acción, como se muestra en el ejemplo siguiente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantsPermissionsToSpecificVolume",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/volume/volume-id"
        },
        {
            "Sid": "GrantsPermissionsToUseStorageGatewayConsole",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Ejemplo 5: Permitir todas las acciones en puertas de enlace con un prefijo específico

La siguiente política permite a un usuario realizar todas las acciones de Storage Gateway en las gateways cuyo nombre comience por`DeptX`. La política también permite el`DescribeSnapshots`Acción de Amazon EC2, que es necesaria para poder describir instantáneas.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsActionsGatewayWithPrefixDeptX",
            "Action": [
```

```
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/DeptX"
        },
        {
            "Sid": "GrantsPermissionsToSpecifiedAction",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

La política anterior funciona si el usuario a quien se asocia la política utiliza el API o unAWSSDK para acceder a la puerta de enlace. Sin embargo, si este usuario planea utilizar elAWS Storage Gateway, debe conceder permisos adicionales, como se describe enEjemplo 3: Permitir acceso a una puerta de enlace específica.

Uso de etiquetas para controlar el acceso a la gateway y los recursos de

Para controlar el acceso a los recursos y las acciones de gateway, puede utilizar políticas de 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 en función de las etiquetas de un recurso

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`.

```
{
  "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:region:account-id:*/*"
      }
  ]
}
```

Control del acceso en función de las etiquetas de una solicitud de IAM

Para controlar lo que un usuario de IAM puede hacer en un recurso de gateway, puede utilizar condiciones en una política de IAM basada en etiquetas. Por ejemplo, puede escribir una política que permite o deniega a un usuario de IAM la posibilidad de realizar operaciones de la API específicas en función de la etiqueta que se proporcionó al crear el recurso.

En el siguiente ejemplo, la primera instrucción permite a un usuario crear una gateway únicamente si el par clave-valor de la etiqueta que se proporcionó al crear la gateway es **`Department`** y **`Finance`**. Al utilizar la operación de la API, tendrá que añadir esta etiqueta a la solicitud de activación.

La segunda instrucción permite al usuario crear un recurso compartido de archivos Network File System (NFS) o Server Message Block (SMB) en una gateway solo si el par clave-valor de la etiqueta de la gateway coincide**`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.

```
{
   "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 las ACL de Microsoft Windows para controlar el acceso a un recurso compartido de archivos SMB

Amazon S3 File Gateway admite dos métodos diferentes para controlar el acceso a los archivos y directorios almacenados en un recurso compartido de archivos SMB: Permisos POSIX o ACL de Windows.

En esta sección, puede encontrar información sobre cómo utilizar las listas de control de acceso (ACL) de Microsoft Windows en recursos compartidos de archivos SMB habilitados con Microsoft Active Directory (AD). Mediante el uso de las ACL de Windows, puede establecer permisos específicos en los archivos y carpetas de un recurso compartido de archivos SMB.

A continuación, se muestran algunas características importantes de las ACL de Windows para los recursos compartidos de archivos SMB:

- Las ACL de Windows se seleccionan 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 las ACL están habilitadas, la información de la ACL se conserva en los metadatos de los objetos de Amazon S3.
- La gateway conserva hasta 10 ACL por archivo o carpeta.
- Cuando se utiliza un recurso compartido de archivos SMB que tiene ACL habilitadas para obtener acceso a objetos de S3 creados fuera de la gateway, los objetos heredan la información de las ACL de la carpeta principal.
- 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 emplear ACL raíz 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 habilitar las ACL de Windows al crear un recurso compartido de archivos SMB mediante la operación CreateSMBFileShare de la API. También puede habilitar las ACL de Windows en un recurso compartido de archivos SMB existente utilizando la operación UpdateSMBFileShare de la API.

Cómo habilitar las ACL de Windows en un recurso compartido de archivos SMB nuevo

Realice los pasos siguientes para habilitar las ACL de Windows en un recurso compartido de archivos SMB nuevo.

Para habilitar las ACL de Windows al crear un recurso compartido de archivos SMB

1. Cree una gateway de archivos si todavía no tiene una. Para obtener más información, consulte .
2. Si la gateway no se ha unido a un dominio, añádala a un dominio. Para obtener más información, consulte .
3. Cree un recurso compartido de archivos SMB.
4. Habilite la ACL de Windows en el archivo compartido desde la consola de Storage Gateway.

   Para usar la consola de 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) Añada un usuario administrador a AdminUsersList si desea que dicho usuario tenga privilegios para actualizar las ACL de todos los archivos y carpetas del recurso compartido de archivos.
6. Actualice las ACL de las carpetas principales de la carpeta raíz. Para ello, utilice el explorador de archivos de Windows para configurar las ACL de las carpetas del recurso compartido de archivos SMB.

   > **Note**
   >
   > Si configura las ACL en la carpeta raíz en lugar de la carpeta principal situada bajo la carpeta raíz, los permisos de las ACL no se conservan en Amazon S3.

   Le recomendamos que configure las ACL en la carpeta de nivel superior situada debajo de la carpeta raíz del recurso compartido de archivos, en lugar de configurarlas directamente en la carpeta raíz del recurso compartido de archivos. Este método hace que se conserve la información como metadatos de los objetos de Amazon S3.
7. Habilite la herencia si es necesario.

> **Note**
>
> Puede habilitar la herencia para los recursos compartidos de archivos creados después del 8 de mayo de 2019.

Si habilita la herencia y actualiza 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.

Cómo habilitar las ACL de Windows en un recurso compartido de archivos SMB existente

Realice los pasos siguientes para habilitar las ACL de Windows en un recurso compartido de archivos SMB existente que tiene permisos de POSIX.

Para habilitar las ACL de Windows en un recurso compartido de archivos SMB existente mediante la consola de 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. Habilite la herencia si es necesario.

> **Note**
>
> No le recomendamos que configure las ACL en el nivel raíz, ya que, si lo hace y elimina la gateway, tendrá que restablecerlas de nuevo.

Si habilita la herencia y actualiza 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 al usar ACL de Windows

Tenga en cuenta los límites siguientes cuando utilice las ACL de Windows para controlar el acceso a los recursos compartidos de archivos SMB:

- Las ACL de Windows solo se admiten en recursos compartidos de archivos habilitados para Active Directory cuando se utilizan clientes SMB de Windows para tener acceso 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 son compatibles con`AudityAlarm`entradas, que son entradas de la lista de control de acceso del sistema (SACL). Las gateways de archivos admiten las entradas `Allow` y `Deny`, que son entradas de lista de control de acceso (DACL) discrecionales.
- 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 las ACL en la carpeta raíz en lugar de la carpeta principal situada bajo la carpeta raíz, los permisos de las ACL no se conservan en Amazon S3.

Teniendo en cuenta estas condiciones, asegúrese de hacer lo siguiente:

- Si configura varias gateways para tener acceso al mismo bucket de Amazon S3, configure la ACL raíz en cada una de las gateways para mantener los permisos coherentes.
- Si elimina un recurso compartido de archivos y vuelve a crearlo en el mismo bucket de Amazon S3, asegúrese de que utiliza el mismo conjunto de ACL raíz.

Permisos API de Storage Gateway Referencia de acciones, recursos y condiciones

Cuando configure el control de acceso y escriba políticas de permisos que puede asociar a una identidad de IAM (políticas basadas en identidad), puede utilizar la siguiente tabla como referencia. En la tabla figuran las operaciones de las API de Storage Gateway, las acciones correspondientes para las que puede conceder permisos para realizar la acción yAWSrecurso para el que puede

conceder los permisos. Las acciones se especifican en el campo `Action` de la política y el valor del recurso se especifica en el campo `Resource` de la política.

Puede usarAWSClaves de condiciones generales de en sus políticas de Storage Gateway para expresar condiciones. Para ver una lista completa de claves generales de AWS, consulte Claves disponibles en la Guía del usuario de IAM.

> **Note**
>
> Para especificar una acción, use el prefijo `storagegateway:` seguido del nombre de operación de la API (por ejemplo, `storagegateway:ActivateGateway`). Para cada acción de Storage Gateway, puede especificar un comodín (*) como recurso.

Para obtener una lista de recursos de Storage Gateway con sus formatos de ARN, consulteRecursos y operaciones de Storage Gateway.

La API de Storage Gateway y los permisos necesarios para las acciones son los siguientes.

ActivateGateway

Acciones: `storagegateway:ActivateGateway`

Recurso: *

AddCache

Acciones: `storagegateway:AddCache`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

AddTagsToResource

Acciones: `storagegateway:AddTagsToResource`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

o bien

`arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/volume/`*`volume-id`*

o bien

arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

AddUploadBuffer

Acciones: storagegateway:AddUploadBuffer

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

AddWorkingStorage

Acciones: storagegateway:AddWorkingStorage

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

CancelArchival

Acciones: storagegateway:CancelArchival

Recurso: arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

CancelRetrieval

Acciones: storagegateway:CancelRetrieval

Recurso: arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

CreateCachediSCSIVolume

Acciones: storagegateway:CreateCachediSCSIVolume

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

CreateSnapshot

Acciones: storagegateway:CreateSnapshot

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

CreateSnapshotFromVolumeRecoveryPoint

Acciones: storagegateway:CreateSnapshotFromVolumeRecoveryPoint

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

CreateStorediSCSIVolume

Acciones: storagegateway:CreateStorediSCSIVolume

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

CreateTapes

Acciones: storagegateway:CreateTapes

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteBandwidthRateLimit

Acciones: storagegateway:DeleteBandwidthRateLimit

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteChapCredentials

Acciones: storagegateway:DeleteChapCredentials

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/target/*iSCSItarget*

DeleteGateway

Acciones: storagegateway:DeleteGateway

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteSnapshotSchedule

Acciones: storagegateway:DeleteSnapshotSchedule

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DeleteTape

Acciones: storagegateway:DeleteTape

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteTapeArchive

Acciones: storagegateway:DeleteTapeArchive

Recurso: *

DeleteVolume

Acciones: storagegateway:DeleteVolume

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DescribeBandwidthRateLimit

Acciones: storagegateway:DescribeBandwidthRateLimit

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeCache

Acciones: storagegateway:DescribeCache

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeCachediSCSIVolumes

Acciones: storagegateway:DescribeCachediSCSIVolumes

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DescribeChapCredentials

Acciones: storagegateway:DescribeChapCredentials

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/target/*iSCSItarget*

DescribeGatewayInformation

Acciones: storagegateway:DescribeGatewayInformation

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeMaintenanceStartTime

Acciones: storagegateway:DescribeMaintenanceStartTime

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeSnapshotSchedule

Acciones: storagegateway:DescribeSnapshotSchedule

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DescribeStorediSCSIVolumes

Acciones: `storagegateway:DescribeStorediSCSIVolumes`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/volume/`*`volume-id`*

DescribeTapeArchives

Acciones: `storagegateway:DescribeTapeArchives`

Recurso: *

DescribeTapeRecoveryPoints

Acciones: `storagegateway:DescribeTapeRecoveryPoints`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DescribeTapes

Acciones: `storagegateway:DescribeTapes`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DescribeUploadBuffer

Acciones: `storagegateway:DescribeUploadBuffer`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DescribeVTLDevices

Acciones: `storagegateway:DescribeVTLDevices`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DescribeWorkingStorage

Acciones: `storagegateway:DescribeWorkingStorage`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DisableGateway

Acciones: `storagegateway:DisableGateway`

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ListGateways

Acciones: storagegateway:ListGateways

Recurso: *

ListLocalDisks

Acciones: storagegateway:ListLocalDisks

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ListTagsForResource

Acciones: storagegateway:ListTagsForResource

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

o bien

arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

o bien

arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

ListTapes

Acciones: storagegateway:ListTapes

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ListVolumeInitiators

Acciones: storagegateway:ListVolumeInitiators

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

ListVolumeRecoveryPoints

Acciones: storagegateway:ListVolumeRecoveryPoints

Recurso: `arn:aws:storagegateway:region:account-id:gateway/gateway-id`

ListVolumes

Acciones: `storagegateway:ListVolumes`

Recurso: `arn:aws:storagegateway:region:account-id:gateway/gateway-id`

RemoveTagsFromResource

Acciones: `storagegateway:RemoveTagsFromResource`

Recurso: `arn:aws:storagegateway:region:account-id:gateway/gateway-id`

o bien

`arn:aws:storagegateway:region:account-id:gateway/gateway-id/volume/volume-id`

o bien

arn:aws:storagegateway:`region`:`account-id`:tape/`tapebarcode`

ResetCache

Acciones: `storagegateway:ResetCache`

Recurso: `arn:aws:storagegateway:region:account-id:gateway/gateway-id`

RetrieveTapeArchive

Acciones: `storagegateway:RetrieveTapeArchive`

Recurso: `arn:aws:storagegateway:region:account-id:gateway/gateway-id`

RetrieveTapeRecoveryPoint

Acciones: `storagegateway:RetrieveTapeRecoveryPoint`

Recurso: `arn:aws:storagegateway:region:account-id:gateway/gateway-id`

ShutdownGateway

Acciones: `storagegateway:ShutdownGateway`

Recurso: `arn:aws:storagegateway:region:account-id:gateway/gateway-id`

StartGateway

Acciones: `storagegateway:StartGateway`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

UpdateBandwidthRateLimit

Acciones: `storagegateway:UpdateBandwidthRateLimit`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

UpdateChapCredentials

Acciones: `storagegateway:UpdateChapCredentials`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/target/`*`iSCSItarget`*

UpdateGatewayInformation

Acciones: `storagegateway:UpdateGatewayInformation`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

UpdateGatewaySoftwareNow

Acciones: `storagegateway:UpdateGatewaySoftwareNow`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

UpdateMaintenanceStartTime

Acciones: `storagegateway:UpdateMaintenanceStartTime`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

UpdateSnapshotSchedule

Acciones: `storagegateway:UpdateSnapshotSchedule`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/volume/`*`volume-id`*

UpdateVTLDeviceType

Acciones: `storagegateway:UpdateVTLDeviceType`

Recurso: `arn:aws:storagegateway:region:account-id:gateway/gateway-id/device/vtldevice`

Temas relacionados

- Control de acceso
- Ejemplos de políticas administradas por el cliente

Uso de roles vinculados a servicios para Storage Gateway

Storage Gateway utilizaAWS Identity and Access Management(IAM)roles vinculados a servicios. Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Storage Gateway. Los roles vinculados a servicios están predefinidos por Storage Gateway e incluyen todos los permisos que el servicio requiere para llamar a otrosAWSservicios en su nombre.

Un rol vinculado a un servicio simplifica la configuración de Storage Gateway porque ya no tendrá que agregar manualmente los permisos necesarios. Storage Gateway define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo Storage Gateway puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Para obtener información acerca de otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Yes (Sí) en la columna Service Linked Role (Rol vinculado a servicios). Seleccione una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de roles vinculados a servicios para Storage Gateway

Storage Gateway usa el rol vinculado al servicio denominadoFunción de servicio de AWS para Storage Gateway— Función de servicio de AWS para Storage Gateway.

El rol vinculado al servicio AWSServiceRoleForStorageGateway confía en que los siguientes servicios asuman el rol:

- `storagegateway.amazonaws.com`

La política de permisos del rol permite que Storage Gateway realice las siguientes acciones en los recursos especificados:

- Acción: `fsx:ListTagsForResource` en `arn:aws:fsx:*:*:backup/*`

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear y editar un rol vinculado a servicio. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a un servicio para Storage Gateway

No necesita crear manualmente un rol vinculado a servicios. Cuando crea un Storage Gateway`AssociateFileSystem`Llamada a la API en elAWS Management Console, elAWS CLI, o elAWSAPI de, Storage Gateway crea automáticamente el rol vinculado al servicio.

> **Important**
>
> Este rol vinculado al servicio puede aparecer en su cuenta si se ha completado una acción en otro servicio que utilice las características compatibles con este rol. Además, si utilizaba el servicio Storage Gateway antes del 31 de marzo de 2021, fecha en que comenzó a admitir los roles vinculados a servicios, Storage Gateway creó el rol AWSServiceRoleForStorageGateway creó el rol AWSServiceRoleForStorageGateway en su cuenta. Para obtener más información, consulte Un nuevo rol ha aparecido en mi cuenta de IAM.

Si elimina este rol vinculado al servicio y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando crea un Storage Gateway`AssociateFileSystem`Llamada a la API de, Storage Gateway vuelve a crear automáticamente el rol vinculado al servicio.

También puede utilizar la consola de IAM para crear un rol vinculado a un servicio conFunción de servicio de AWS para Storage Gatewaycaso de uso. En la AWS CLI o la API de AWS, cree un rol vinculado al servicio con el nombre de servicio `storagegateway.amazonaws.com`. Para obtener más información, consulte Crear un rol vinculado a un servicio en la Guía del usuario de IAM. Si elimina este rol vinculado al servicio, puede utilizar este mismo proceso para volver a crear el rol.

Modificación de un rol vinculado a un servicio en Storage Gateway

Storage Gateway no permite editar el rol vinculado al servicio AWSServiceRoleForStorageGateway. Después de crear un rol vinculado a servicios, no puede cambiarle el nombre, ya que varias

entidades pueden hacer referencia al mismo. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminación de un rol vinculado a un servicio para Storage Gateway

Storage Gateway no elimina automáticamente el rol AWSServiceRoleForStorageGateway. Para eliminar la función AWSServiceRoleForStorageGateway, debe invocar el`iam:DeleteSLR`API. Si no hay recursos de puerta de enlace de almacenamiento que dependan del rol vinculado al servicio, la eliminación se realizará correctamente; de lo contrario, la eliminación fallará. Si desea eliminar el rol vinculado al servicio, debe utilizar las API de IAM`iam:DeleteRole`o`iam:DeleteServiceLinkedRole`. En este caso, debe utilizar las API de Storage Gateway para eliminar primero cualquier puerta de enlace o asociación del sistema de archivos de la cuenta y, a continuación, eliminar la función vinculada al servicio mediante`iam:DeleteRole`o`iam:DeleteServiceLinkedRole`API. Cuando elimina el rol vinculado al servicio mediante IAM, debe utilizar Storage Gateway`DisassociateFileSystemAssociation`API primero para eliminar todas las asociaciones de sistemas de archivos de la cuenta. De lo contrario, la operación de eliminación producirá un error.

> **Note**
>
> Si el servicio Storage Gateway utiliza el rol cuando intenta eliminar los recursos, la eliminación podría producir un error. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos de Storage Gateway utilizados por AWSServiceRoleForStorageGateway

1. Utilice nuestra consola de servicio, CLI o API para realizar una llamada que limpie los recursos y elimine el rol o utilice la consola, la CLI o la API de IAM para realizar la eliminación. En este caso, debe utilizar las API de Storage Gateway para eliminar primero cualquier puerta de enlace y asociación de sistemas de archivos de la cuenta.
2. Si utiliza la consola de IAM, la CLI o la API de, elimine el rol vinculado al servicio mediante IAM`DeleteRole`o`DeleteServiceLinkedRole`API.

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM, elAWS CLI, o elAWSAPI de para eliminar el rol vinculado al servicio AWSServiceRoleForStorageGateway. Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario de IAM.

Regiones que admiten roles vinculados a servicios de Storage Gateway

Storage Gateway admite el uso de roles vinculados a servicios en todas las regiones en las que el servicio está disponible. Para obtener más información, consulte puntos de enlace de servicio de AWS.

Storage Gateway no admite el uso de roles vinculados a servicios en todas las regiones en las que el servicio está disponible. Puede utilizar el rol AWSServiceRoleForStorageGateway en las siguientes regiones.

Nombre de la región de	Identidad de la región	Support en Storage Gateway
US East (N. Virginia)	us-east-1	Sí
US East (Ohio)	us-east-2	Sí
EE. UU Oeste (Norte de California)	us-west-1	Sí
EE. UU. Oeste (Oregón)	us-west-2	Sí
Asia Pacífico (Mumbai)	ap-south-1	Sí
Asia Pacífico (Osaka)	ap-northeast-3	Sí
Asia Pacífico (Seúl)	ap-northeast-2	Sí
Asia Pacífico (Singapur)	ap-southeast-1	Sí
Asia Pacífico (Sídney)	ap-southeast-2	Sí
Asia Pacífico (Tokio)	ap-northeast-1	Sí
Canada (Central)	ca-central-1	Sí
Europa (Fráncfort)	eu-central-1	Sí

Nombre de la región de	Identidad de la región	Support en Storage Gateway
Europa (Irlanda)	eu-west-1	Sí
Europa (Londres)	eu-west-2	Sí
Europa (París)	eu-west-3	Sí
South America (São Paulo)	sa-east-1	Sí
AWS GovCloud (US)	us-gov-west-2	Sí

Registro y monitoreo en AWS Storage Gateway

Storage Gateway está integrado conAWS CloudTrail, un servicio que proporciona un registro de las acciones que realiza un usuario, un rol o unAWSservicio en Storage Gateway. CloudTrail captura todas las llamadas a la API de Storage Gateway como eventos. Las llamadas capturadas incluyen las llamadas realizadas desde la consola de Storage Gateway y las llamadas de código a las operaciones de API de Storage Gateway. Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos de Storage Gateway. Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Event history (Historial de eventos). Mediante 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 acerca de CloudTrail, consulte la AWS CloudTrailGuía del usuario de .

Información de Storage Gateway en CloudTrail

CloudTrail se habilita en su cuenta de AWS cuando la crea. Cuando se produce una actividad en Storage Gateway, dicha actividad se registra en un evento de CloudTrail junto con los demásAWSeventos de servicios enHistorial de eventos. Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte Ver eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de los eventos deAWScuenta, incluidos los eventos de Storage Gateway, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS. 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. También es posible configurar otros servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- Servicios e integraciones compatibles con CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de registro de CloudTrail de varias regiones y Recibir archivos de registro de CloudTrail de varias cuentas

Todas las acciones de Storage Gateway están registradas y documentadas en laActionstema. Por ejemplo, las llamadas a las acciones `ActivateGateway`, `ListGateways` y `ShutdownGateway` generan entradas en los archivos de log de CloudTrail.

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 AWS Identity and Access Management (IAM) o credenciales de usuario raíz.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte el Elemento userIdentity de CloudTrail.

Descripción de las entradas de archivos de registro de Stor

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros en un bucket de Amazon S3 que especifique. Los archivos log de CloudTrail pueden contener una o varias entradas de log. Un evento representa una solicitud específica realizada

desde un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

En el ejemplo siguiente, se muestra una entrada de registro de CloudTrail que ilustra 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"
             }]
}
```

En el ejemplo siguiente se muestra una entrada de registro de CloudTrail que ilustra la acción ListGateways.

```
{
 "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"
             }]
}
```

Validación de la conformidad enAWSStorage Gateway

Auditores externos evalúan la seguridad y la conformidad deAWSStorage Gateway como parte de variosAWSprogramas de conformidad. Estos incluyen SOC, PCI, ISO, FedRAMP, HIPAA, MTCS, C5, K-ISMS, ENS High, OSPAR y HITRUST CSF.

Para obtener una lista de los servicios de AWS en el ámbito de programas de conformidad específicos, consulte AWS Services in Scope by Compliance Program (Servicios en el ámbito de programas de conformidad). Para obtener información general, consulte Programas de conformidad de AWS.

Puede descargar los informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact.

La responsabilidad de conformidad al utilizar Storage Gateway se determina en función de la confidencialidad de los datos, los objetivos de conformidad de la empresa y la legislación y normativa aplicables.AWSproporciona los siguientes recursos para ayudar con la conformidad:

- Security and Compliance Quick Start Guides (Guías de inicio rápido de seguridad y conformidad) (Guías de inicio rápido de seguridad y conformidad): Estas guías de implementación analizan consideraciones sobre arquitectura y proporcionan los pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- Documento técnico sobre arquitectura para seguridad y conformidad de HIPAA : en este documento técnico, se describe cómo las empresas pueden utilizar AWS para crear aplicaciones conformes con HIPAA.
- Recursos de conformidad de AWS: este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- Evaluación de recursos con reglas en la Guía para desarrolladores de AWS Config: el servicio AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub: este servicio de AWS proporciona una vista integral de su estado de seguridad en AWS que lo ayuda a verificar la conformidad con los estándares y las prácticas recomendadas del sector de seguridad.

Resiliencia enAWSStorage Gateway

La infraestructura global de AWS se compone de regiones y zonas de disponibilidad de AWS. AWS Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre las regiones y zonas de disponibilidad de AWS, consulte Infraestructura global de AWS.

Además delAWSinfraestructura global, Storage Gateway ofrece varias características que le ayudan con sus necesidades de resiliencia y copia de seguridad de los datos.

- Utilice VMware vSphere High Availability (VMware HA) para ayudar a proteger las cargas de trabajo de almacenamiento frente a fallos de hardware, hipervisor o red. Para obtener más información, consulteUso de VMware vSphere High Avability with Storage Gateway.
- Utilice AWS Backup para realizar una copia de seguridad de los volúmenes. Para obtener más información, consulteUso deAWS Backuppara realizar una copia de seguridad de los volúmenes.
- Clone el volumen desde un punto de recuperación. Para obtener más información, consulteClonación de un volumen.
- Archivar cintas virtuales en Amazon S3 Glacier. Para obtener más información, consulteArchivado de cintas virtuales.

Seguridad de la infraestructura enAWSStorage Gateway

Como servicio administrado,AWSStorage Gateway está protegido por elAWSprocedimientos de seguridad de red globales que se describen en laAmazon Web Services: Información general de los procesos de seguridaddocumento técnico.

UsasAWSLas llamadas a la API publicadas en para obtener acceso a Storage Gateway a Los clientes deben ser compatibles con Transport Layer Security (TLS) 1.0 o una versión posterior. Recomendamos TLS 1.2 o una versión posterior. 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 de seguridad de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Prácticas recomendadas de seguridad para Storage Gateway

AWSStorage Gateway proporciona un número de características de seguridad que debe tener en cuenta a la hora de desarrollar e implementar sus propias políticas de seguridad. Las siguientes prácticas recomendadas son directrices generales y no suponen una solución de seguridad completa. Puesto que es posible que estas prácticas recomendadas no sean adecuadas o suficientes para el entorno, considérelas como consideraciones útiles en lugar de como normas. Para obtener más información, consulteAWSPrácticas recomendadas de seguridad.

Solución de problemas de la gateway

A continuación, encontrará información sobre la solución de problemas relacionados con gateways, recursos compartidos de archivos, volúmenes, cintas virtuales y snapshots. La información de solución de problemas de gateways locales abarca tanto las gateways implementadas en clientes VMware ESXi como Microsoft Hyper-V. La información de resolución de problemas para recursos compartidos de archivos también se aplica al tipo de Amazon S3 File Gateway. La información de solución de problemas para volúmenes es aplicable a los tipos de gateway de volúmenes. La información de resolución de problemas para cintas se aplica al tipo de gateway de cintas. La información de resolución de problemas de gateway se aplica al uso de métricas de CloudWatch. La información de resolución de problemas de alta disponibilidad abarca a las gateways que se ejecutan en una plataforma de alta disponibilidad (HA) de VMware vSphere.

Temas

Resolución de problemas de gateways on-premises

A continuación encontrará información sobre los problemas habituales que podría encontrar al trabajar con gateways on-premises y cómo habilitarAWS Supportpara ayudar a solucionar problemas de la gateway de.

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 vSphere en la pestaña Summary (Resumen). • Para Microsoft Hyper-V, la dirección IP de la MV puede encontrar se al iniciar sesión en la consola local. 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 configurarlos para dar permiso a los puntos de enlace de servicio para mantener comunicaciones de salida enAWS. Para obtener más información sobre los requisitos de red y firewall, consulte Requisitos de red y firewall.
La activación de la gateway produce un error al hacer clic en laContinúe en la activaciónen 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 conectividad de red de su gateway. • 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

Problema	Acción que ejecutar
	gateway tenga la hora correcta. Para obtener información sobre la sincronización de la hora de los hosts del hipervisor y las MV, consulte Configuración de un servidor NTP (Network Time Protocol) para la gateway. • Tras realizar estos pasos, puede reintentar la implementación de la gateway mediante la consola de Storage Gateway y laConfiguración y activación de gatewaysasistente. • Compruebe que la MV tenga al menos 7,5 GB de RAM. La asignación de la gateway produce un error si hay menos de 7,5 GB de RAM. Para obtener más información, consulte Requisitos de configuración de gateway.
Debe eliminar un disco asignado como espacio de búfer de carga. Por ejemplo, es posible que desee reducir la cantidad de espacio del búfer de carga para una gateway o sustituir un disco utilizado como búfer de carga que ha producido un error.	

Problema	Acción que ejecutar
Debe mejorar el ancho de banda entre la gateway yAWS.	Puede mejorar el ancho de banda entre la gateway y AWS mediante la configuración de la conexión a Internet a AWS en un adaptador de red (NIC) independiente del que conecta las aplicaciones y la MV de la gateway. Este enfoque es útil si tiene una conexión de alto ancho de banda a AWS y desea evitar la contención de ancho de banda, especialmente durante la restauración de una instantánea. Para necesidades de cargas de trabajo de alto rendimiento, puede utilizarAWS Direct Connectpara establecer una conexión de red dedicada entre la gateway on-premise yAWS. Para medir el ancho de banda de la conexión de la gateway a AWS utilice las métricas `CloudBytesDownloaded` y `CloudBytesUploaded` de la gateway. Para obtener más información sobre este tema, consulte Desempeño. 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 páginaPortalde la consola de Storage Gateway, verifique que las direcciones IP de la MV de la gateway sean las mismas que ve al usar el software cliente del hipervisor (es decir, el cliente VMware vSphere o Microsoft Hyper-V Manager). Si encuentra una discrepancia, reinicie la gateway desde la consola de Storage Gateway, como se muestra enApague la MV de la gateway. Después del reinicio, las direcciones delDirecciones IPlista de la consola de Storage GatewayPortaldebe coincidir con las direcciones IP de la gateway, determinadas desde el cliente del hipervisor.
	  • Para VMware ESXi, la dirección IP de la máquina virtual se encuentra en el cliente vSphere en la pestaña Summary (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 gateway a AWS como se describe en Probar la conectividad de red de su gateway.
	• Compruebe la configuración del adaptador de red de la gateway y asegúrese de que todas las interfaces que desee habilitar para la gateway estén habilitadas. Para ver la configuración del adaptador de red para la gateway, siga las instrucciones de Configuración de adaptadores de red para la gateway y seleccione la opción para ver la configuración de red de la gateway.
	
	Puede ver el rendimiento a y desde la gateway desde la consola de Amazon CloudWatch. Para ver más información sobre la medición del rendimiento a y desde la gateway a AWS, consulte Desempeño.

Tiene problemas para importar (implementar) Storage Gateway en Microsoft Hyper-V.	Consulte Resolución de problemas de configuración de Microsoft Hyper-V, donde se explican algunos de los problemas comunes de implementar una gateway en Microsoft Hyper-V.

Problema	Acción que ejecutar
Recibes un mensaje que dice: «Los datos que se han escrito en el volumen de la gateway no se almacenan de forma segura enAWS«.	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 conAWS Support.

HabilitaciónAWS Supportpara ayudar a solucionar problemas de la puerta de enlace alojada en las instalaciones

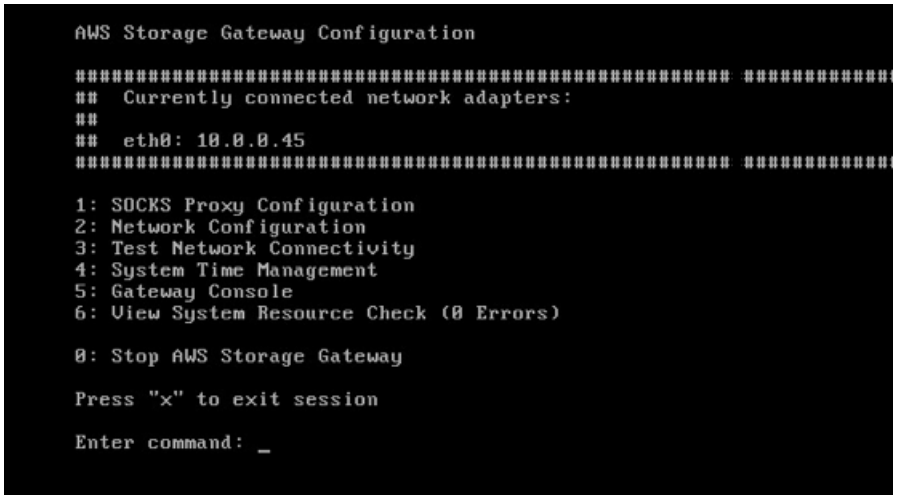
Storage Gateway proporciona una consola local que puede utilizar para realizar varias tareas de mantenimiento, incluida la activaciónAWS SupportPara obtener acceso a la gateway para ayudarle con la solución de problemas de gateway. Por defecto,AWS Supportel acceso a la gateway está deshabilitado. Habilite este acceso mediante la consola local del host. Para darAWS Supportacceso a la gateway, primero inicie sesión en la consola local para el host, vaya a la consola de la gateway de almacenamiento y, a continuación, conecte con el servidor de soporte.

Para habilitarAWS Supportacceso a la gateway

1. Inicie sesión en la consola local del host.

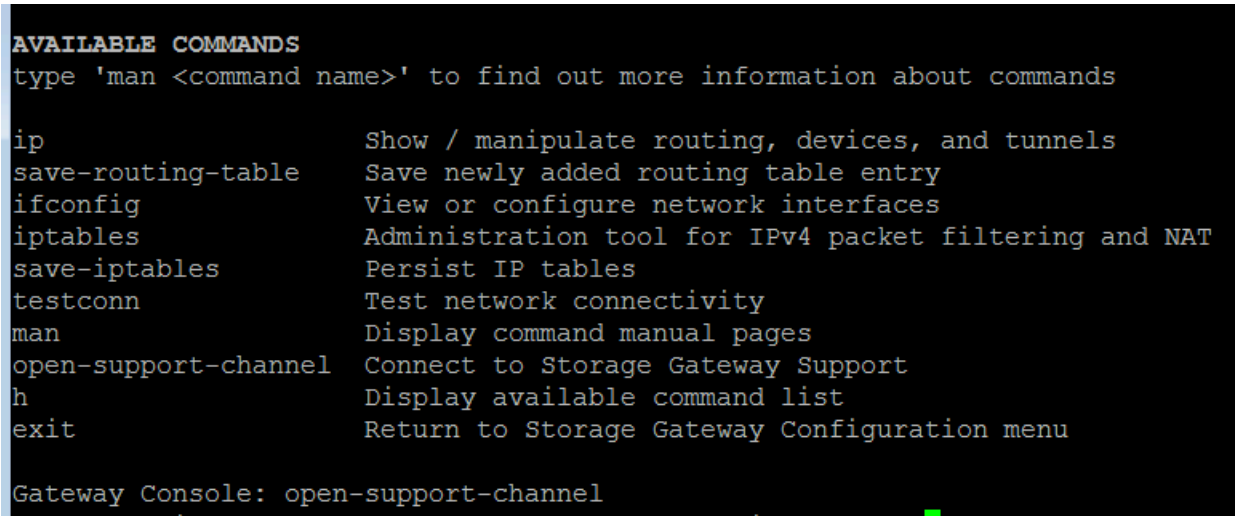
   - VMware ESXi: para obtener más información, consulteAcceso a la consola local de la gateway con VMware ESXi.
   - Microsoft Hyper-V: para obtener más información, consulteAcceso a la consola local de la gateway con Microsoft Hyper-V.

   La consola local tiene un aspecto parecido al siguiente.



2. En el símbolo del sistema, escriba**5**para abrirAWS SupportConsola de canal.
3. Introduzca **h** para abrir la ventana AVAILABLE COMMANDS (COMANDOS DISPONIBLES).
4. Realice una de las siguientes acciones:

   - Si la gateway está utilizando un punto de enlace público, en laCOMANDOS DISPONIBLESventana, introduzca**`open-support-channel`**para conectarse al servicio de atención al cliente de Storage Gateway. Permitir el puerto TCP 22 para poder abrir un canal de soporte enAWS. 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 gateway no está activada, proporcione el punto de enlace de la 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 enAWS. Cuanto conecte con el servicio de atención al cliente, Storage Gateway le asignará un número de soporte. Apunte el número de soporte.



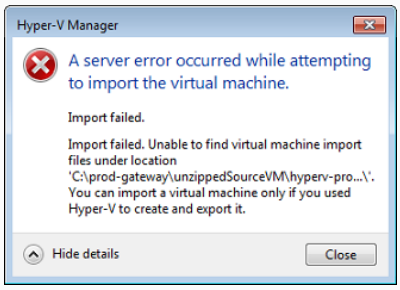
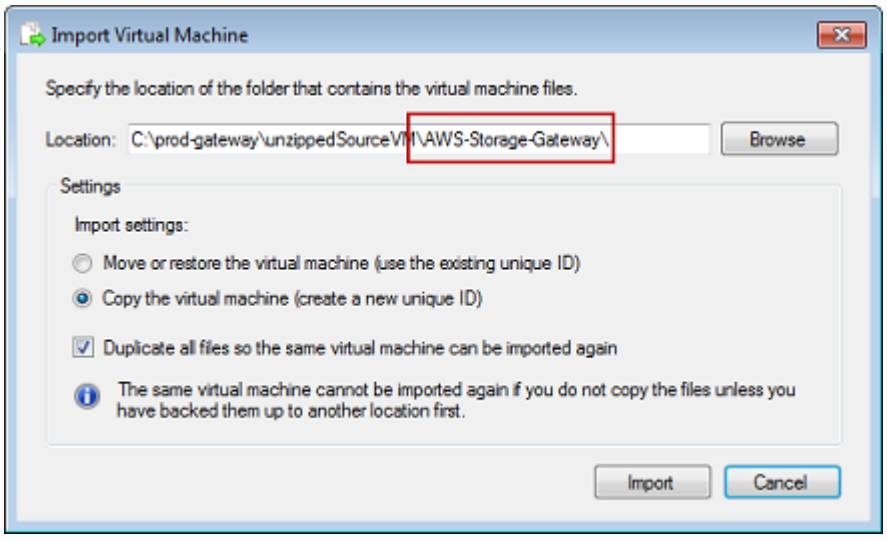
> **Note**
>
> El número de canal no es un número de puerto TCP/UDP (Transmission Control Protocol/User Datagram Protocol). En lugar de ello, la gateway realiza una conexión Secure Shell (SSH) (TCP 22) a los servidores de Storage Gateway y proporciona el canal de soporte para la conexión.

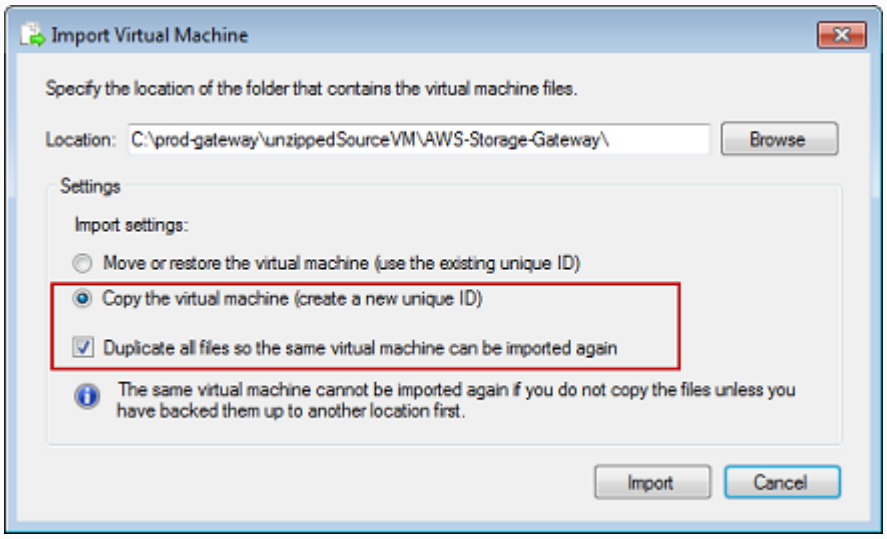
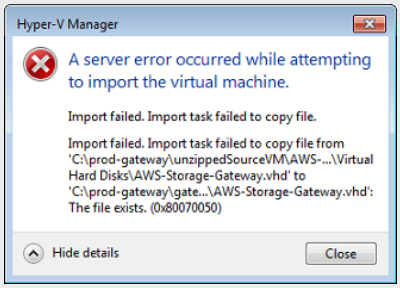
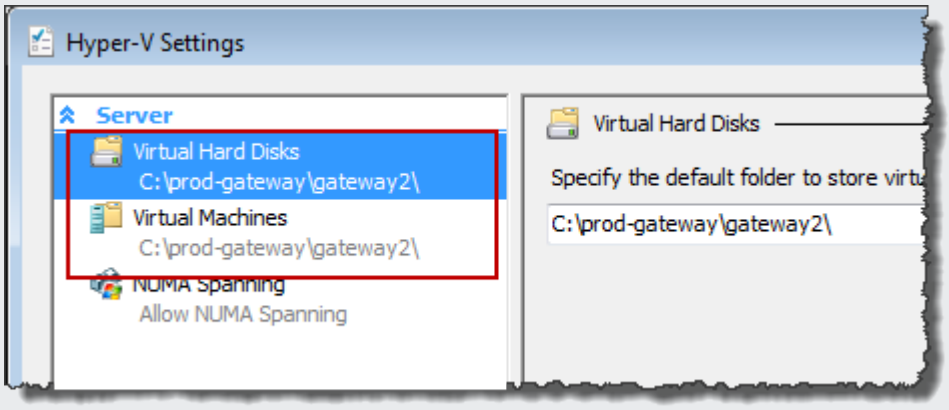
5. Una vez establecido el canal de soporte, proporcione el número de servicio de soporte aAWS Supportasí queAWS Supportpuede proporcionar asistencia para la solución de problemas.
6. Cuando se complete la sesión de soporte, introduzca **q** para finalizarla. No cierre la sesión hasta que Amazon Web Services Support le notifique que la sesión de soporte se ha completado.
7. Entrar**exit**para cerrar sesión en la consola de Storage Gateway.
8. Siga las instrucciones para salir de la consola local.

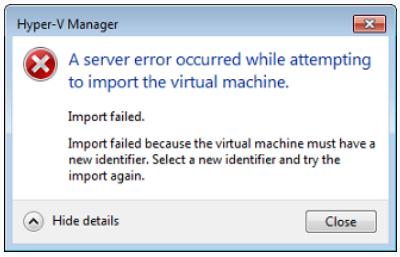
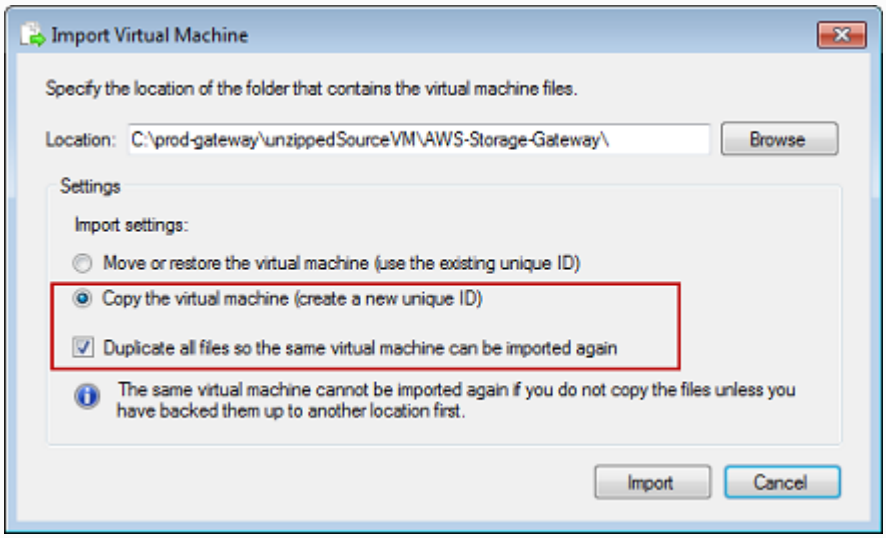
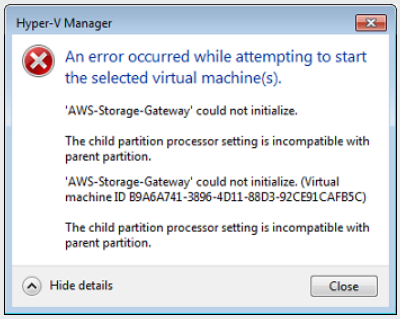
Resolución de problemas de configuración de Microsoft Hyper-V

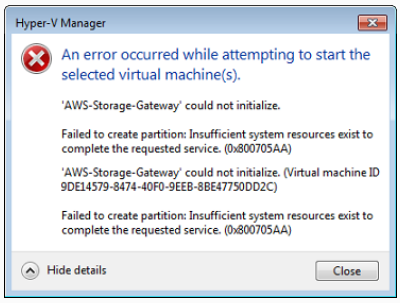
En la siguiente tabla se muestran los problemas habituales que podría encontrar al implementar Storage Gateway en la plataforma de Microsoft Hyper-V.

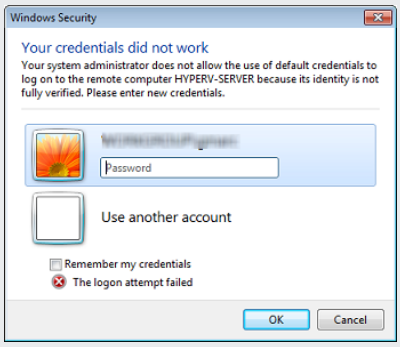
Problema	Acción que ejecutar
Intenta importar una gateway y recibe el	Este error puede producirse por las razones siguientes:

Problema	Acción que ejecutar
mensaje de error: «error en la importación. Unable to find virtual machine import file under location ...". 	• 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 Import Virtual Machine (Importar máquina virtual) debe ser `AWS-Storage-Gateway` , como se muestra en el siguiente ejemplo:  • 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. En el siguiente ejemplo se muestran las opciones que debe comprobar si planea crear varias gateways a partir de una ubicación de archivos de origen sin comprimir.

Problema	Acción que ejecutar
	
Intenta importar una gateway y recibe el mensaje de error: «error en la importación. Import task failed to copy file." 	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, especifiq ue nuevas ubicaciones en el cuadro de diálogo Hyper-V Settings (Configuración de Hyper-V). 

Problema	Acción que ejecutar
Intenta importar una gateway y recibe un mensaje de error: «error en la importación. Import failed because the virtual machine must have a new identifier. Select a new identifier and try the import again." 	Al importar la gateway, asegúrese de que selecciona la opción Copy the virtual machine (Copia la máquina virtual) y de que activa la opción Duplicate all files (Duplicar todos los archivos) en el cuadro de diálogo Import Virtual Machine (Importar máquina virtual) para crear un nuevo ID único para la máquina virtual. En el siguiente ejemplo, se muestran las opciones del cuadro de diálogo Import Virtual Machine (Importar máquina virtual) que debe utilizar. 
Intenta iniciar una MV de gateway y recibe un mensaje de error "The child partition processor setting is incompatible with parent partition." 	Es probable que este error se deba a una discrepancia de CPU entre las CPU requeridas para la gateway y las CPU disponibles en el host. Asegúrese de que el número de CPU de MV sea compatibl e con el hipervisor subyacente. Para obtener más información sobre los requisitos de Storage Gateway, consulteRequisitos de configuración de gateway.

Problema	Acción que ejecutar
Intenta iniciar una MV de gateway y recibe un mensaje de error «Failed to create partition: No existen recursos suficientes para completar el servicio solicitado». 	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, consulteRequisitos de configuración de 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 NTP (Network Time Protocol) para la gateway.
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.

Problema	Acción que ejecutar
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.

Solución de problemas de gateway de Amazon EC2

En las secciones siguientes, encontrará los problemas habituales que podría encontrar al trabajar con la gateway implementada en Amazon EC2. Para obtener más información sobre la diferencia entre una gateway on-premises y una gateway implementada en Amazon EC2, consulteImplementación de una gateway de archivos en un host Amazon EC2.

Para obtener información sobre el uso del almacenamiento efímero, consulte Uso del almacenamiento efímero con puertas de enlace EC2.

Temas

- La activación de la puerta de enlace no se ha producido después de unos instantes
- No encuentra la instancia de la gateway de EC2 en la lista de instancias
- ¿Quieres?AWS Supportpara ayudar a solucionar problemas de la puerta de enlace EC2

La activación de la puerta de enlace no se ha producido después de unos instantes

Compruebe lo siguiente en la consola de Amazon EC2:

- El puerto 80 está habilitado en el grupo de seguridad que ha asociado a la instancia. Para obtener más información acerca de cómo añadir una regla de grupo de seguridad, consulteAdición de una regla de grupo de seguridaden laGuía del usuario de Amazon EC2 para instancias de Linux.

- La instancia de la gateway está marcada como en ejecución. En la consola de Amazon EC2, elEstadoEl valor de la instancia debe ser RUNNING.
- Asegúrese de que el tipo de instancia de Amazon EC2 cumple 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 y elijaImplementación de una nueva gateway en Amazon EC2y vuelva a introducir la dirección IP de la instancia de.

No encuentra la instancia de la gateway de EC2 en la lista de instancias

Si no asignó a la instancia una etiqueta de recurso y tiene muchas instancias en funcionamiento, puede ser difícil saber qué instancia lanzó. En este caso, puede realizar las siguientes acciones para encontrar la instancia de la gateway:

- Compruebe el nombre la Imagen de máquina de Amazon (AMI) en la pestaña Description (Descripción) de la instancia. Una instancia basada en la AMI de Storage Gateway debe empezar con el texto**`aws-storage-gateway-ami`**.
- Si tiene varias instancias basadas en la AMI de Storage Gateway, compruebe el momento de lanzar la instancia para encontrar la instancia correcta.

¿Quieres?AWS Supportpara ayudar a solucionar problemas de la puerta de enlace EC2

Storage Gateway proporciona una consola local que puede utilizar para realizar varias tareas de mantenimiento, incluida la activaciónAWS SupportPara obtener acceso a la gateway para ayudarle con la solución de problemas de gateway. Por defecto,AWS Supportel acceso a la gateway está deshabilitado. Habilite este acceso mediante la consola local de Amazon EC2. Inicie sesión en la consola local de Amazon EC2 mediante Secure Shell (SSH). Para iniciar sesión correctamente mediante SSH, el grupo de seguridad de la instancia debe tener una regla que abra el puerto TCP 22.

> **Note**
>
> Si agrega una nueva regla a un grupo de seguridad existente, la nueva regla se aplicará a todas las instancias que utilicen ese grupo de seguridad. Para obtener más información

sobre los grupos de seguridad y cómo agregar una regla de grupo de seguridad, consulteGrupos de seguridad de Amazon EC2en laGuía del usuario de Amazon EC2.

Para dejarAWS Supportconecte a la gateway, primero inicie sesión en la consola local para la instancia de Amazon EC2, vaya a la consola de la gateway de almacenamiento y, a continuación, proporcione el acceso.

Para habilitarAWS Supportacceso a una gateway implementada en una instancia de Amazon EC2

1. Inicie sesión en la consola local de la instancia de Amazon EC2 de. Para obtener instrucciones, consulteConéctese a la instanciaen laGuía del usuario de Amazon EC2.

   Puede utilizar el siguiente comando para iniciar sesión en la consola local de la instancia EC2.

   ```
   ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
   ```

   > **Note**
   >
   > La*CLAVE PRIVADA*es el`.pem`archivo que contiene el certificado privado del key pair EC2 utilizado para lanzar la instancia de Amazon EC2. Para obtener más información, consulteRecuperar la clave pública de su par de clavesen laGuía del usuario de Amazon EC2.
   >
   > La*INSTANCE-PUBLIC-DNS-NAME*es el nombre público del sistema de nombres de dominio (DNS) de la instancia de Amazon EC2 donde se está ejecutando la gateway. Este DNS público se obtiene seleccionando la instancia de Amazon EC2 en la consola de EC2 y haciendo clic en elDescripciónpestaña.

2. En el símbolo del sistema, escriba**`6 - Command Prompt`**para abrirAWS SupportConsola de canal.
3. Introduzca **h** para abrir la ventana AVAILABLE COMMANDS (COMANDOS DISPONIBLES).
4. Realice una de las siguientes acciones:

   - Si la gateway está utilizando un punto de enlace público, en laCOMANDOS DISPONIBLESventana, introduzca**`open-support-channel`**para conectarse al servicio de atención al cliente de Storage Gateway. Permitir el puerto TCP 22 para poder abrir un canal de soporte enAWS. 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 gateway no está activada, proporcione el punto de enlace de la 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 enAWS. 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 TCP/UDP (Transmission Control Protocol/User Datagram Protocol). En lugar de ello, la gateway 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 el número de servicio de soporte aAWS Supportasí queAWS Supportpuede proporcionar asistencia para la solución de problemas.
6. Cuando se complete la sesión de soporte, introduzca **`q`** para finalizarla. No cierre la sesión hasta que Amazon Web Services Support le notifique que la sesión de soporte se ha completado.
7. Entrar**`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.

Resolución de problemas de dispositivos de hardware

En los siguientes temas, se explican los problemas que puede encontrarse con el dispositivo de hardware de Storage Gateway y las sugerencias sobre cómo solucionarlos.

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 realiza un restablecimiento de fábrica?

Si necesita restablecer la configuración de fábrica en el dispositivo, póngase en contacto con el equipo de dispositivo de hardware de Storage Gateway para obtener Support, como se describe en la siguiente sección de soporte.

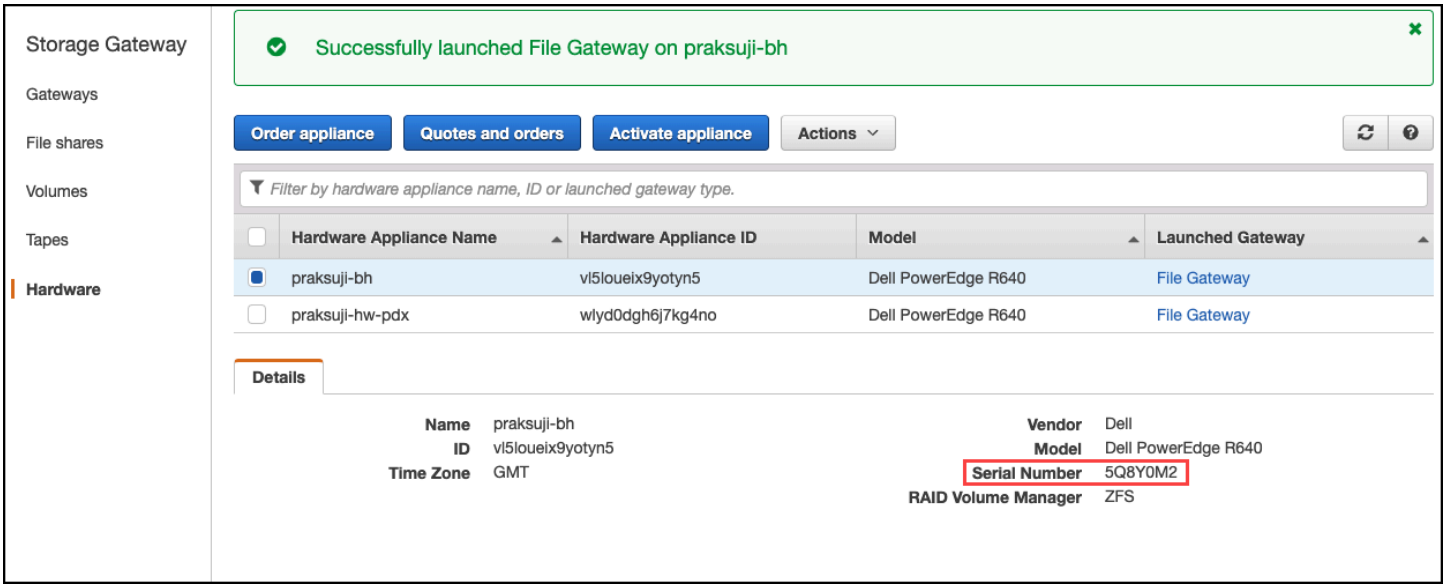
¿Dónde obtiene soporte Dell iDRAC?

El servidor Dell PowerEdge R640 incluye la interfaz de administración iDRAC de Dell. Le recomendamos lo siguiente:

- Si utiliza la interfaz de administración de iDRAC, debe cambiar la contraseña predeterminada. Para obtener más información acerca de las credenciales de iDRAC, consulteDell PowerEdge: ¿Cuál es el nombre de usuario y la contraseña predeterminados de iDRAC?.
- Asegúrese de que el firmware esté actualizado para evitar errores 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 encuentra el número de serie del dispositivo de hardware

Para encontrar el número de serie del dispositivo de hardware, vaya a laHardwareen la consola de Storage Gateway, como se muestra a continuación.



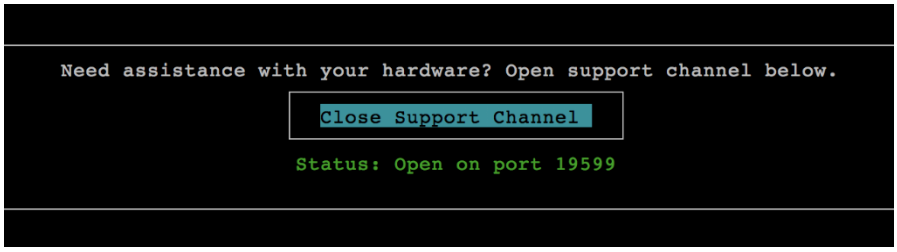
Dónde obtener soporte para dispositivos de hardware

Para contactar con el soporte del dispositivo de hardware de Storage Gateway, consulteAWS Support.

LaAWS SupportEl equipo le pedirá que active el canal de soporte para solucionar de forma remota los problemas de su gateway. 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 paraAWS

1. Abra la consola del hardware.
2. Elija Open Support Channel (Abrir canal de soporte) como se muestra a continuación.



   El número de puerto asignado debe aparecer en 30 segundos si no hay problemas de firewall o de conectividad de red.
3. Anote el número de puerto y proporciónelo aAWS Support.

Resolución de problemas de gateways de archivos

Puede configurar la gateway de archivos con un grupo de registros de Amazon CloudWatch cuando ejecute la alta disponibilidad (HA) de VMware vSphere. Si lo hace, recibirá notificaciones acerca del estado de la gateway de archivos y de los errores que detecta la gateway de archivos. Puede encontrar información sobre estas notificaciones de estado y errores en CloudWatch Logs.

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: InaccessibleStorageClass
- Error: Acceso denegado S3

- Error: InvalidObjectState
- Error: ObjectMissing
- : Notificación: Reinicio
- : Notificación: HardReboot
- : Notificación: HealthCheckFailure
- : Notificación: AvailabilityMonitorTest
- Error: RoleTrustRelationshipInvalid
- Resolución de problemas con métricas de CloudWatch

Error: InaccessibleStorageClass

Puedes obtener un`InaccessibleStorageClass`error cuando un objeto se ha movido fuera de la clase de almacenamiento estándar de Amazon S3.

Normalmente la gateway de archivos detecta el error cuando intenta cargar el objeto especificado en el bucket de S3 o leer el objeto desde el bucket de S3. Con este error, generalmente el objeto se ha trasladado a Amazon S3 Glacier o S3 Glacier Deep Archive.

Para resolver un error de StorageClass InaccessibleStorageClass

- Mueva el objeto de la clase de almacenamiento S3 Glacier o S3 Glacier Deep Archive de nuevo a S3.

  Si mueve el objeto al bucket de S3 para solucionar un error de carga, el archivo se carga al final. Si mueve el objeto al bucket de S3 para solucionar un error de lectura, el cliente SMB o NFS de la gateway de archivos puede leer el archivo.

Error: Acceso denegado S3

Puedes obtener un`S3AccessDenied`error en el acceso al bucket de Amazon S3 de un recurso compartido de archivosAWS Identity and Access Management(IAM). En este caso, el rol de IAM de acceso al bucket de S3 especificado por`roleArn`en el error no permite la operación involucrada. La operación no está permitida debido a los permisos de los objetos del directorio especificado por el prefijo de Amazon S3.

Para resolver un error S3AccessDenied

- Modifique la política de acceso de Amazon S3 asociada `aroleArn`en el registro de estado de la gateway de archivos 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 acerca de los permisos de Amazon S3, consulteEspecificar permisos en una políticaenGuía del usuario de Amazon Simple Storage Service.

  Estas operaciones pueden provocar que se produzca el error `S3AccessDenied`:

  - `S3HeadObject`
  - `S3GetObject`
  - `S3ListObjects`
  - `S3DeleteObject`
  - `S3PutObject`

Error: InvalidObjectState

Puedes obtener un`InvalidObjectState`error cuando un escritor que no sea la gateway de archivos especificada modifica el archivo especificado en el bucket de S3 especificado. Como resultado, el estado del archivo de la gateway de archivos no coincide con el estado en Amazon S3. Cualquier carga posterior del archivo a Amazon S3 o recuperación del archivo desde Amazon S3 fallará.

Para resolver un error de InvalidObjectState

Si la operación que modifica al archivo es`S3Upload`o`S3GetObject`, realice una de las siguientes opciones:

1. Guarde la copia más reciente del archivo en el sistema de archivos local del cliente NFS o SMB (necesita esta copia de archivos en el paso 4). Si la versión del archivo en Amazon S3 es la más reciente, descárguela. Puede hacerlo mediante la AWS Management Console o la AWS CLI.
2. Elimine el archivo de Amazon S3 utilizando laAWS Management ConsoleoAWS CLI.
3. Elimine el archivo de la gateway de archivos mediante el cliente NFS o SMB.
4. Copie la versión más reciente del archivo que ha guardado en el paso 1 en Amazon S3 mediante el cliente NFS o SMB. Haga esto mediante la gateway de archivos.

Error: ObjectMissing

Puedes obtener un`ObjectMissing`error cuando un escritor que no sea la gateway de archivos especificada elimina el archivo especificado del bucket de S3. Cualquier carga posterior a Amazon S3 o recuperación desde Amazon S3 del objeto fallará.

Para resolver un objeto Error que falta

Si la operación que modifica al archivo es`S3Upload`o`S3GetObject`, realice una de las siguientes opciones:

1. Guarde la copia más reciente del archivo en el sistema de archivos local del cliente NFS o SMB (necesita esta copia de archivos en el paso 3).
2. Elimine el archivo de la gateway de archivos mediante el cliente NFS o SMB.
3. Copie la versión más reciente del archivo que ha guardado en el paso 1 mediante el cliente NFS o SMB. Haga esto mediante la gateway de archivos.

: Notificación: Reinicio

Puede recibir una notificación de reinicio cuando la MV de la gateway se reinicia. Puede reiniciar la MV de una gateway mediante la consola de gestión de hipervisor de MV 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.

: 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 las gateways de VMware, un reinicio provocado por la monitorización de aplicaciones de alta disponibilidad de vSphere puede provocar este evento.

Cuando la gateway se ejecuta en dicho entorno, compruebe si hay notificaciones `HealthCheckFailure` y consulte el registro de eventos de VMware para la MV.

: Notificación: HealthCheckFailure

En una gateway de HA de VMware vSphere, puede recibir una notificación `HealthCheckFailure` cuando se produce un error en una comprobación de estado y se solicita un reinicio de la MV. 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 únicamente para las gateways de VMware.

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 asistencia adicional, póngase en contacto conAWS Support.

: Notificación: AvailabilityMonitorTest

Obtienes un`AvailabilityMonitorTest`notificación cuandoejecutar una pruebadelSupervisión de disponibilidad y aplicacionessistema en las gateways que se ejecutan en una plataforma de HA de VMware vSphere.

Error: RoleTrustRelationshipInvalid

Recibe este error cuando el rol de IAM de un recurso compartido de archivos tiene una relación de confianza de IAM mal configurada (es decir, el rol de IAM no confía en la entidad principal de Storage Gateway denominada`storagegateway.amazonaws.com`). Como resultado, la gateway de archivos no podría obtener las credenciales para ejecutar ninguna operación en el bucket de S3 que realiza una copia de seguridad del recurso compartido de archivos.

Para resolver un error RoleTrustRelationshipInvalid

- Utilice la consola de IAM o la API de IAM para incluir`storagegateway.amazonaws.com`como una entidad principal en la que confía el IAMRole de su recurso compartido de archivos. Para obtener información acerca del rol de IAM, consulteTutorial: delegar el acceso a travésAWScuentas que utilizan roles de IAM.

Resolución de problemas con métricas de CloudWatch

A continuación encontrará información sobre las acciones para solucionar los problemas mediante el uso de las métricas de Amazon CloudWatch con Storage Gateway.

Temas

La puerta de enlace reacciona lentamente al navegar por los directorios

Si la gateway de archivos reacciona lentamente al ejecutar lals comando o navegar por directorios, compruebe la`IndexFetch`y`IndexEviction`Métricas de CloudWatch:

- Si el archivo de`IndexFetch`métrica es mayor que 0 cuando ejecuta un`ls`de comandos o de navegación, la gateway de archivos se ha iniciado sin información acerca del contenido del directorio afectado y ha tenido que acceder a Amazon S3. Los esfuerzos posteriores para mostrar el contenido de ese directorio deberían realizarse más rápidamente.
- Si el archivo de`IndexEviction`La métrica es mayor que 0, significa que la gateway de archivos ha alcanzado el límite de lo que puede gestionar en la caché en ese momento. En este caso, la gateway de archivos tiene que liberar espacio de almacenamiento del directorio al que se ha accedido menos recientemente para crear un nuevo directorio. Si esto se produce con frecuencia y tiene un impacto en el rendimiento, póngase en contacto conAWS Support.

  Converse conAWS Supportel contenido del bucket de S3 relacionado y las recomendaciones para mejorar el rendimiento en función del caso de uso.

Tu gateway no responde

Si la gateway de archivos 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 en el que la CPU está inactiva cuando hay una solicitud de E/S del 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 se produzca un efecto embudo en la gateway de archivos a causa de un disco raíz lento, ya que reanuda la caché de índice en la RAM. Puede solucionar este problema mediante el uso de un disco físico más rápido para el disco raíz.
- Si el archivo de`MemUsedBytes`métrica es igual o casi igual que la`MemTotalBytes`métrica, a continuación, la gateway de archivos se está quedando sin RAM disponible. Asegúrese de que la gateway de archivos tenga el menos la RAM mínima requerida. Si ya la tiene, considere añadir más RAM a la gateway de archivos en función de la carga de trabajo y el caso de uso.

  Si el recurso compartido de archivos es SMB, el problema también podría deberse al número de clientes SMB conectados a dicho recurso. Para ver el número de clientes que están conectados en cualquier momento, compruebe la métrica `SMBV(1/2/3)Sessions`. Si hay muchos clientes conectados, es posible que necesite agregar más RAM a la gateway de archivos.

La gateway transfiere datos lentamente a Amazon S3

Si la gateway de archivos transfiere datos lentamente a Amazon S3, haga lo siguiente:

- Si el archivo de`CachePercentDirty`La métrica es 80 o superior, la gateway de archivos escribe los datos en el disco a una velocidad más rápida de la que puede utilizar para cargar los datos en Amazon S3. Considere aumentar el ancho de banda de carga de la gateway de archivos, ya sea mediante la adición de uno o varios discos en caché o mediante la ralentización de las escrituras de los clientes.
- Si el archivo de`CachePercentDirty`Métrica es baja, compruebe la`IoWaitPercent`Métrica de. Si`IoWaitPercent`es mayor que 10, es posible que se produzca un efecto embudo en la gateway de archivos por la velocidad del disco en caché local. Recomendamos el uso de discos locales de unidades de estado sólido (SSD) para la 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`,`S3UploadPartRequestTime`, o bien`S3GetObjectRequestTime`son altos, podría haber un cuello de botella en la red. Intente analizar la red para comprobar que la puerta de enlace tiene el ancho de banda esperado.

La puerta de enlace está realizando más operaciones de Amazon S3 de las esperadas

Si la puerta de enlace de archivos está realizando más operaciones de Amazon S3 de las esperadas, compruebe la`FilesRenamed`Métrica de. Las operaciones de cambio de nombre son costosas de ejecutar en Amazon S3. Optimice su flujo de trabajo para minimizar el número de operaciones de cambio de nombre.

No ve archivos en el bucket de Amazon S3

Si observa que los archivos de la gateway no se reflejan en el bucket de Amazon S3, compruebe la`FilesFailingUpload`Métrica de. Si la métrica informa de que algunos archivos no se han cargado, compruebe las notificaciones de estado. Cuando los archivos no se cargan, la puerta de enlace genera una notificación de estado que contiene más detalles sobre el problema.

El trabajo de copia de seguridad de la gateway falla o se producen errores al escribir en la gateway

Si el trabajo de copia de seguridad de la gateway de archivos falla o se producen errores al escribir en la gateway de archivos, realice las siguientes acciones:

- Si el archivo de`CachePercentDirty`métrica es del 90 por ciento o superior, la gateway de archivos no puede aceptar nuevas escrituras en disco porque no hay suficiente espacio disponible en el disco de caché. Para ver a qué velocidad realiza cargas la gateway de archivos en Amazon FSx o Amazon S3, consulte la`CloudBytesUploaded`Métrica de. Compara esa métrica con la`WriteBytes`métrica, que muestra a qué velocidad escribe archivos el cliente en la gateway de archivos. Si la gateway de archivos escribe más rápido de lo que puede cargar en Amazon FSx o Amazon S3, añada más discos de caché para cubrir el tamaño del trabajo de copia de seguridad como mínimo. También puede aumentar el ancho de banda de carga.
- Si falla un trabajo de copia de seguridad, pero el`CachePercentDirty`La métrica es inferior al 80 por ciento, es posible que la gateway de archivos esté alcanzando el tiempo de espera de la sesión del lado del cliente. Para SMB, puede aumentar este tiempo de espera mediante el comando de 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.

Resolución de problemas de recursos compartidos de archivos

A continuación encontrará información sobre las acciones que debe realizar si experimenta problemas inesperados con recursos compartidos de archivos.

Temas

El recurso compartido de archivos 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 bucket de S3 al que ha asignado el 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 acerca de cómo crear un bucket de S3, consulteCrear un bucketen laGuía del usuario de Amazon Simple Storage Service.

3. Asegúrese de que el nombre del bucket cumple 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.
4. Asegúrese de que la función de IAM que utilizó para acceder al bucket de S3 tiene los permisos adecuados y verifique que el bucket de S3 se muestra como un recurso en la política de IAM. Para obtener más información, consulte Concesión de acceso a un bucket de Amazon S3.

No puede crear un recurso compartido de archivos

1. Si no puede crear un recurso compartido de archivos porque el recurso compartido de archivos se bloquea en el estado CREATING, verifique que el bucket de S3 al que ha asignado el recurso compartido de archivos existe. Para obtener información acerca de cómo hacerlo, consulte El recurso compartido de archivos está bloqueado en el estado CREATING, más arriba.
2. Si existe el bucket S3, compruebe queAWS Security Token Serviceestá activado en la región donde desee crear el recurso compartido de archivos. Si un token de seguridad no está activado, debe activarlo. Para obtener información acerca de cómo habilitar un token medianteAWS Security Token Service, consulteActivación y desactivación deAWSSTS en unAWSRegiónen laIAM User Guide.

Los recursos compartidos de archivos 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 recursos compartidos de archivos no pueden escribir en el bucket de S3 asignado

No le recomendamos configurar el bucket de S3 para permitir que varios recursos compartidos de archivos escriban en un bucket 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 compartir archivos.

No se pueden cargar archivos en el depósito de S3

Si no puede cargar archivos en el bucket de S3, haga lo siguiente:

1. Asegúrese de haber concedido el acceso necesario para que Amazon S3 File Gateway cargue archivos en el 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 Prácticas recomendadas para compartir archivos.
3. Si la puerta de enlace de archivos utiliza SSE-KMS para el cifrado, asegúrese de que la función de IAM asociada al recurso compartido de archivos incluyakms:Encrypt,kms:Decrypt,KMS: volver a cifrar,kms:GenerateDataKey, ykms:DescribeKeypermisos. Para obtener más información, consulteUso de políticas basadas en identidad (políticas de IAM) para Storage Gateway.

No se puede cambiar el cifrado predeterminado para usar SSE-KMS para cifrar los objetos almacenados en mi bucket de S3

Si cambia el cifrado predeterminado y realiza SSE-KMS (cifrado del lado del servidor conAWS KMS—claves administradas) el valor predeterminado de su bucket de S3, los objetos que Amazon S3 File Gateway almacena en el bucket no están cifrados con SSE-KMS. De forma predeterminada, la gateway de archivos S3 utiliza el cifrado del lado del servidor administrado 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 para utilizar SSE-KMS con su propia clave de AWS KMS, debe habilitar el cifrado de 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 medianteAWS KMS.

Los cambios realizados directamente en un bucket de S3 con el control de versiones de objetos habilitado pueden afectar a lo que ve en el recurso compartido de archivos

Si otro cliente ha escrito objetos en el bucket de S3, es posible que la vista del bucket de S3 no esté actualizada como resultado del control de versiones de 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"`. El número de objetos con nombres idénticos y su duración se controla mediante las políticas de ciclo de vida de Amazon S3. Para obtener más información sobre estos conceptos de Amazon S3, consulteUsar el control de versionesyAdministrar el ciclo de vida de los objetosen laGuía 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.

Los archivos que se muestran en la gateway de archivos son las versiones más recientes de los objetos de un bucket de S3 en el momento en que el que se recuperó el objeto o se actualizó la caché. Las gateways de archivos S3 omiten 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 el recurso compartido de archivos, la gateway de archivos de S3 crea una nueva versión de un objeto con nombre con los cambios y esa versión pasa a ser la versión más reciente.

La gateway de archivos de S3 sigue leyendo la versión anterior y las actualizaciones que se realicen estarán basadas en la versión anterior si se añade una versión nueva al bucket de S3 fuera de la aplicación. Para leer la versión más reciente de un objeto, utilice la acción RefreshCache de la API o actualice desde la consola, tal como se indica en Refrescar objetos en el bucket de Amazon S3.

> **Important**
>
> No le recomendamos que se escriban objetos o archivos en el bucket de S3 File Gateway S3 desde fuera del recurso compartido de archivos.

Al escribir en un bucket de S3 con el versionado de objetos habilitado, Amazon S3 File Gateway puede crear varias versiones de un objeto S3

Con el control de versiones de objetos habilitado, puede tener varias versiones de un objeto creadas en Amazon S3 en cada actualización de un archivo desde su cliente NFS o SMB. Estos son los escenarios que pueden dar lugar a la creación de varias versiones de un objeto en el 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 el archivo completo. 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 la puerta de enlace de archivos S3, S3 File Gateway carga los datos del archivo en Amazon S3 seguido de sus metadatos (propiedad, marcas de tiempo, etc.). Al cargar los datos de archivo se crea un objeto Amazon S3 y al cargar los metadatos del archivo se actualizan los metadatos del objeto Amazon S3. Este proceso crea otra versión del objeto, lo que da como resultado dos versiones de un objeto.
- Cuando S3 File Gateway está cargando archivos más grandes, es posible que tenga que cargar fragmentos más pequeños del archivo antes de que el cliente termine de escribir en la puerta de enlace de archivos. Algunas de las razones para ello incluyen liberar espacio en la caché o una alta tasa de escritura en un archivo. Esto puede dar como resultado varias variantes de un objeto en el bucket de S3.

Debe supervisar el bucket de S3 para determinar cuántas versiones de un objeto existen antes de configurar políticas de ciclo de vida para mover objetos a diferentes clases de almacenamiento. Debe configurar la caducidad del ciclo de vida de las versiones anteriores para minimizar el número de versiones que tiene para un objeto del bucket de S3. El uso de replicación en la misma región (SRR) o replicación entre regiones (CRR) entre buckets de S3 aumentará el almacenamiento de información utilizado. Para obtener más información acerca de la replicación, consulteReplicación.

> **Important**
>
> No configure la replicación entre buckets de S3 hasta que comprenda cuánto almacenamiento se utiliza cuando se habilita el versionado de objetos.

El uso de buckets de S3 con control de versiones puede aumentar en gran medida la cantidad de almacenamiento en Amazon S3, ya que cada modificación que se realiza en un archivo crea una versión nueva del objeto S3. De forma predeterminada, Amazon S3 continúa almacenando todas estas versiones a menos que se cree específicamente una política para anular este comportamiento y limitar el número de versiones que se conservan. Si observa un uso del almacenamiento excepcionalmente elevado cuando está habilitado el control de versiones de objetos, compruebe si ha establecido de forma apropiada las políticas de almacenamiento. 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 habilita el control de versiones de objetos tras instalar una gateway de archivos S3 File Gateway, se conservan todos los objetos únicos (`ID="NULL"`) y puede verlas todas 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.

Una vez habilitado el control de versiones de objetos, el bucket de S3 no puede volver a un estado sin control de versiones. 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 de recursos compartidos de archivos automáticamente cuando escribe archivos en la caché localmente mediante el recurso compartido de archivos. Sin embargo, Storage Gateway no actualiza automáticamente la caché cuando carga un archivo directamente en Amazon S3. Cuando lo haga, debe realizar un`RefreshCache`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 caché mediante la consola de Storage Gateway y elAWS Command Line Interface(AWS CLI):

- Para actualizar la caché mediante la consola de Storage Gateway, consulte Actualización de objetos en el depósito de Amazon S3.
- Para actualizar la memoria caché mediante elAWS 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 desea actualizar.
  3. Ejecute la`refresh-cache`con el 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 el icono`RefreshCache`operación, consulte¿Cómo puedo automatizar la operación de RefreshCache en Storage Gateway?

Los permisos de ACL no funcionan según lo previsto

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 la puerta de enlace se redujo tras realizar una operación recursiva

En algunos casos, es posible que realice una operación recurrente, como por ejemplo, cambiar el nombre de un directorio o habilitar la herencia de una ACL y forzar su propagación por el árbol. Si lo hace, la gateway de archivos S3 File Gateway aplica de forma recursiva la operación a todos los objetos del recurso compartido de archivos.

Por ejemplo, supongamos que aplica una herencia a los objetos existentes en un bucket de S3. La S3 File Gateway aplica de forma recursiva la herencia a todos los objetos del bucket. Este tipo de operaciones pueden provocar la degradación del rendimiento de la gateway.

Notificaciones de estado de alta disponibilidad

Al ejecutar la gateway en la plataforma de alta disponibilidad (HA) de VMware vSphere, es posible que reciba notificaciones de estado. Para obtener más información sobre las notificaciones de estado, consulte Resolución de problemas de alta disponibilidad.

Resolución de problemas de alta disponibilidad

A continuación puede encontrar información acerca de las acciones que debe realizar si experimenta problemas de disponibilidad.

Temas

Notificación Health

Cuando ejecuta la gateway en la HA de VMware vSphere, todas las gateways 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

Puede recibir una notificación de reinicio cuando la MV de la gateway se reinicia. Puede reiniciar la MV de una gateway mediante la consola de gestión de hipervisor de MV 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 las gateways de VMware, un reinicio provocado por la monitorización de aplicaciones de alta disponibilidad de vSphere puede provocar este evento.

Acción necesaria

Cuando la gateway se ejecuta en dicho entorno, compruebe si hay notificaciones `HealthCheckFailure` y consulte el registro de eventos de VMware para la MV.

: Notificación: HealthCheckFailure

En una gateway de HA de VMware vSphere, puede recibir una notificación `HealthCheckFailure` cuando se produce un error en una comprobación de estado y se solicita un reinicio de la MV. 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 únicamente para las gateways de VMware.

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 asistencia adicional, póngase en contacto conAWS Support.

: Notificación: AvailabilityMonitorTest

Para una gateway en VMware vSphere, puede obtener una`AvailabilityMonitorTest`notificación cuandoejecutar una pruebadelSupervisión de disponibilidad y aplicacionessistema 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 el grupo de registros de CloudWatch configurado para obtener información acerca de los eventos.

Prácticas recomendadas para la recuperación de datos

Aunque es infrecuente, es posible que su gateway se enfrente a un error irrecuperable. Este error puede producir en la máquina virtual (VM), en la propia gateway, en el almacenamiento local o en otro lugar. Si se produce un error, le recomendamos que siga las instrucciones de la sección adecuada, a continuación, para recuperar los datos.

> **Important**
>
> Storage Gateway no permite recuperar la máquina virtual de una puerta de enlace a partir de una instantánea creada por el hipervisor o desde la Amazon EC2 Amazon Machine Image (AMI). Si la MV de la gateway no funciona correctamente, active una nueva gateway y recupere los datos para esa gateway utilizando las instrucciones siguientes.

Temas

Recuperación de un apagado 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 conectividad de red de su gateway.
- Si la gateway no funciona correctamente y se producen problemas con los volúmenes o las cintas como resultado de un cierre inesperado, puede recuperar los datos. Para obtener información sobre cómo recuperar los datos, consulte las secciones siguientes que se apliquen a su situación.

Recuperación de datos de un disco de caché que funciona mal

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 gateway, vuelva a añadir el disco y reinicie la gateway.
- Si el disco de la caché está dañado o no permite el acceso, cierre la gateway, reinicie el disco de la caché, reconfigure el disco para el almacenamiento en caché y reinicie la gateway.

Para obtener información detallada, consulte Recuperación de datos de un disco de caché que funciona mal.

Recuperación de datos de un centro de datos inaccesible

Si su gateway o centro de datos deja de ser accesible por algún motivo, puede recuperar los datos en otra gateway de un centro de datos diferente o en una gateway alojada en una instancia de Amazon EC2. Si no tiene acceso a otro centro de datos, le recomendamos crear la gateway en una instancia de Amazon EC2. Los pasos que siga dependerán del tipo de gateway cuyos datos intenta recuperar.

Para recuperar datos de una gateway de archivos en un centro de datos inaccesible

En el caso de gateways de archivos, asigne un nuevo recurso compartido de archivos al bucket de Amazon S3 que contiene los datos que desea recuperar.

1. Cree y active una nueva gateway de archivos en un host de Amazon EC2. Para obtener más información, consulte Implementación de una gateway de archivos en un host Amazon EC2.
2. Cree un nuevo recurso compartido de archivos en la gateway de EC2 que ha creado. Para obtener más información, consulteCreación de un recurso compartido de archivos.

3. Monte el recurso compartido de archivos en el cliente y asígnelo al bucket de S3 que contiene los datos que desea recuperar. Para obtener más información, consulteMonte y use el recurso compartido de archivos.

Recursos de Storage Gateway

En esta sección, encontrará información sobreAWSy software, herramientas y recursos de terceros que pueden ayudarle a configurar o administrar la gateway y, también, sobre las cuotas de Storage Gateway.

Temas

Configuración del host

Temas

Configuración de VMware para Storage Gateway

Al configurar VMware para Storage Gateway, asegúrese de sincronizar la hora de la máquina virtual con la hora del host, configurar la máquina virtual para que utilice controladores de disco paravirtualizados al aprovisionar el almacenamiento y proporcionar protección ante errores de la capa de infraestructura en la que se sustenta la máquina virtual de gateway.

Temas

- Sincronización de la hora de la máquina virtual y el host
- Uso de Storage Gateway con VMware High Availability

Sincronización de la hora de la máquina virtual y el host

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).

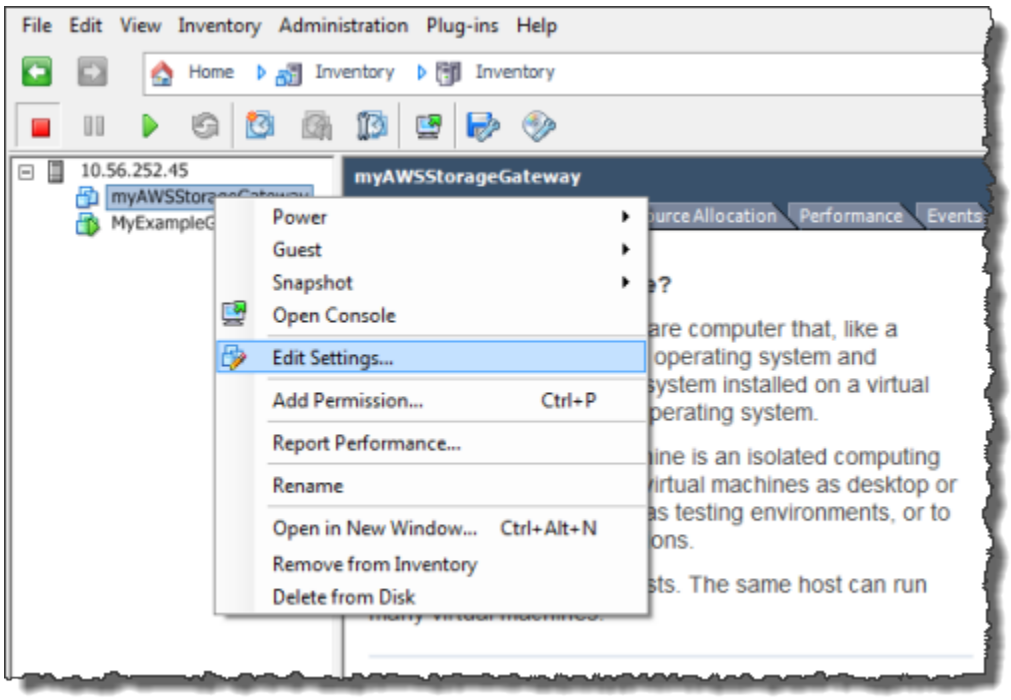
> **Important**
>
> Sincronizar la hora de la máquina virtual con la hora del host es imprescindible para que la gateway se active correctamente.

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, abra el menú contextual (haga clic con el botón derecho) de la máquina virtual de la gateway y elija Edit Settings (Editar configuración).

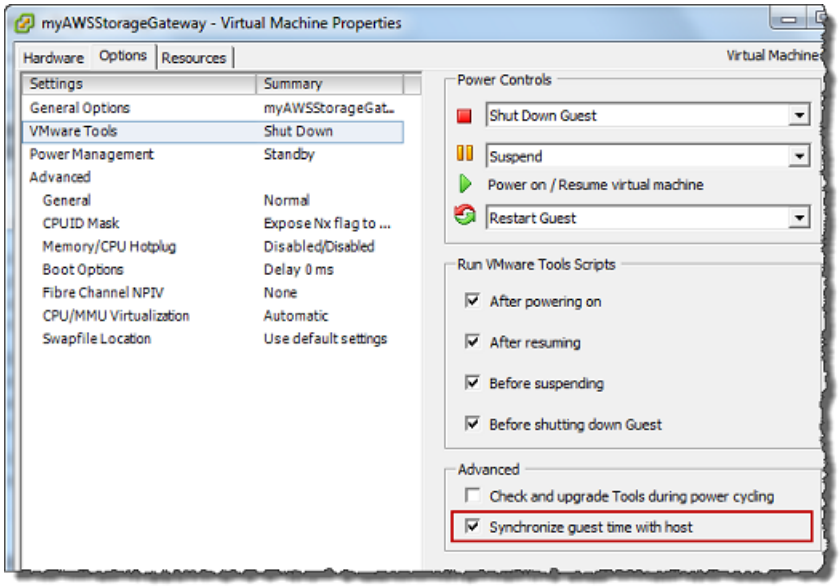
      Se abrirá el cuadro de diálogo Virtual Machine Properties (Propiedades de la máquina virtual).



b. Elija la pestaña Options (Opciones) y seleccione VMware Tools (Herramientas de VMware) en la lista de opciones.

c. Active la opción Synchronize guest time with host (Sincronizar tiempo del invitado con el host) y, a continuación, elija OK (Aceptar).

   La máquina virtual sincronizará su hora con la del host.



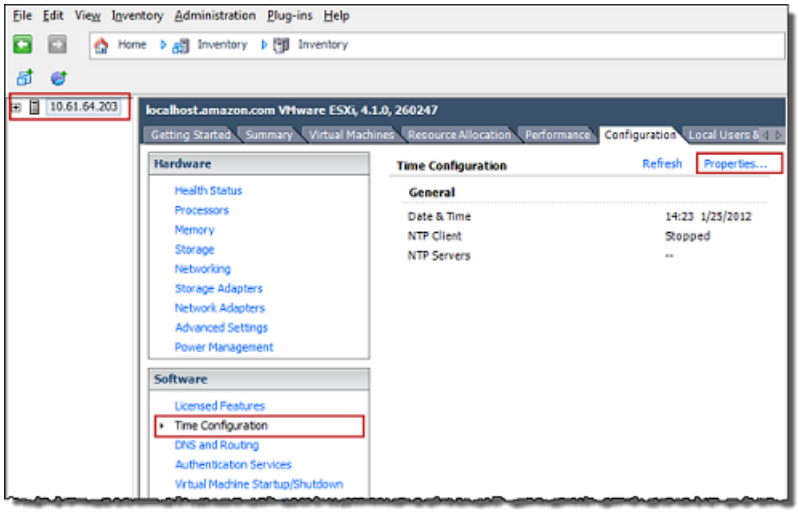
2. Configurar la hora del host.

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.

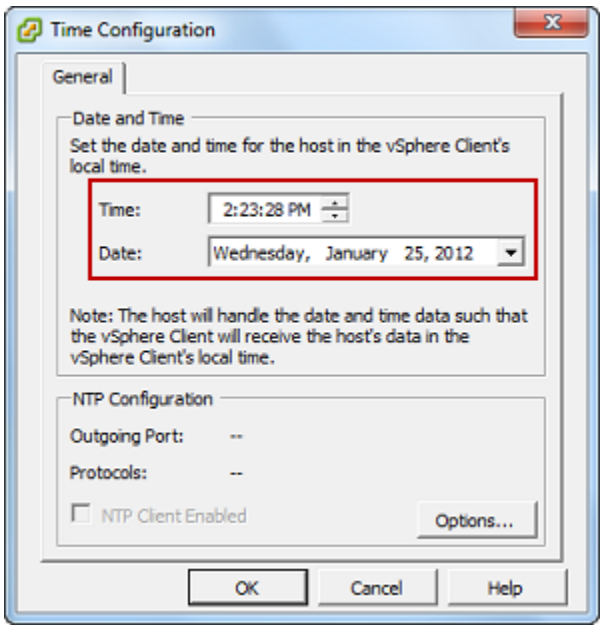
a. En el cliente de VMware vSphere, seleccione el nodo del host de vSphere en el panel izquierdo y, a continuación, elija la pestaña Configuration (Configuración).

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).

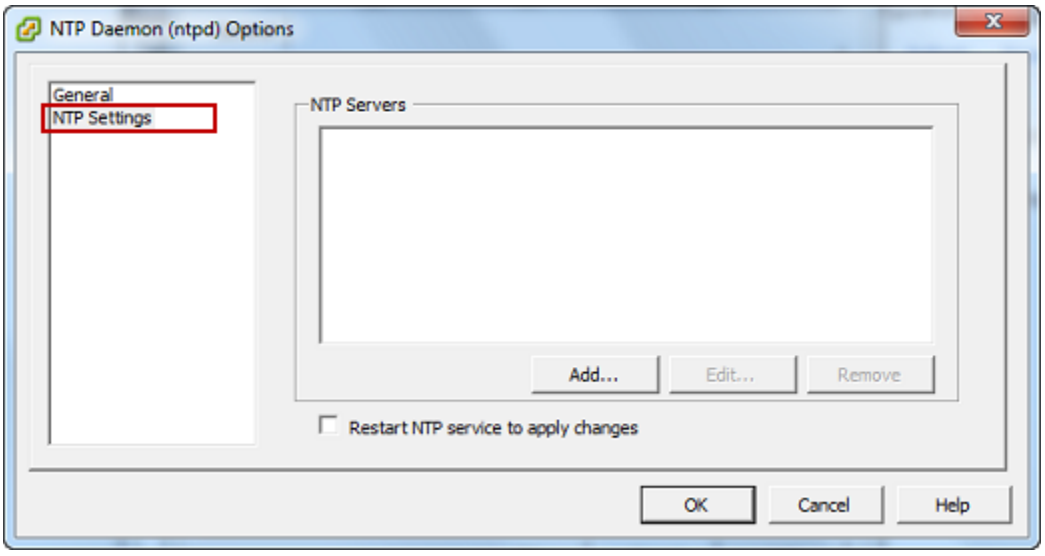


c. En el panel Date and Time (Fecha y hora), establezca la fecha y la hora.



d. Configure el host para que sincronice la hora automáticamente con un servidor de NTP.

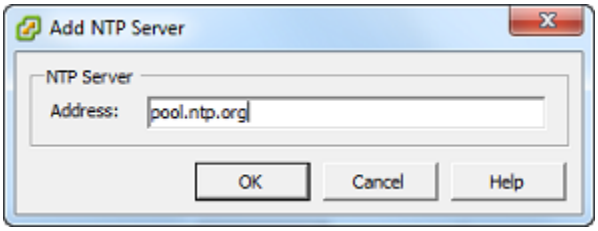
   i. Elija Options (Opciones) en el cuadro de diálogo Time Configuration (Configuración de tiempo). A continuación, en el cuadro de diálogo NTP Daemon (ntpd) Options (Opciones de NTP Daemon (ntpd)), elija NTP Settings (Configuración de NTP) en el panel izquierdo.



   ii. Elija Add (Añadir) para agregar un nuevo servidor NTP.

   iii. En el cuadro de diálogo Add NTP Server (Añadir servidor NTP), escriba la dirección IP o el nombre de dominio completo de un servidor NTP y, a continuación, elija OK (Aceptar).

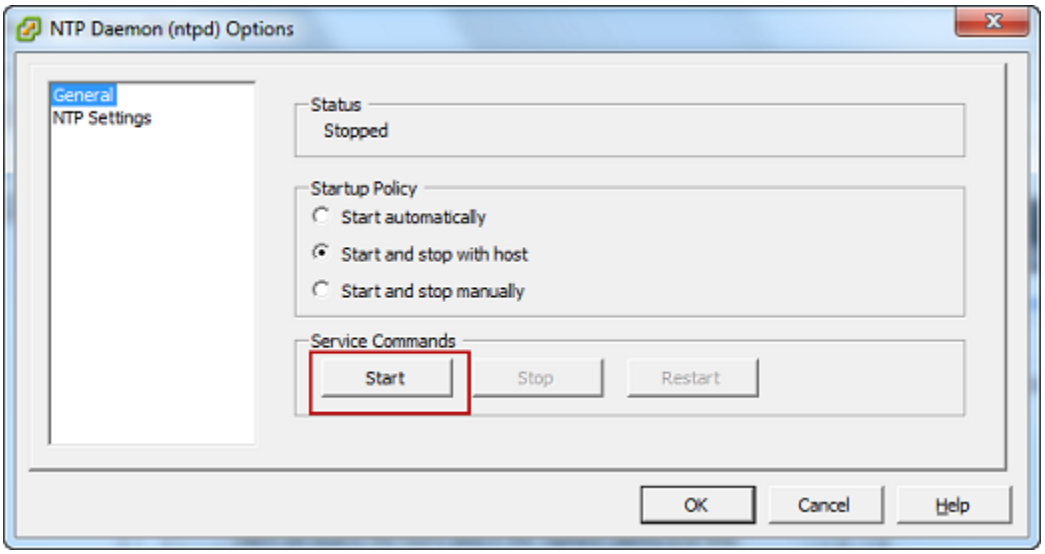
Puede utilizar `pool.ntp.org` como se muestra en el ejemplo siguiente.



iv. En el cuadro de diálogo NTP Daemon (ntpd) Options (Opciones de NTP Daemon (ntpd)), elija General (Generales) en el panel izquierdo.

v. En la sección Service Commands (Comandos de servicio), elija Start (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).

Uso de Storage Gateway con VMware High Availability

VMware High Availability (HA) es un componente de vSphere que puede proporciona protección frente a errores que se produzcan en la capa de infraestructura mediante la compatibilidad con

una MV de gateway. Para ello, VMware HA utiliza varios hosts configurados como un clúster, de modo que si un host en el que se ejecute una MV de gateway produce un error, la MV de la gateway puede reiniciarse automáticamente en otro host del clúster. Para obtener más información acerca de VMware HA, consulteVMware HA: Conceptos y prácticas recomendadasen el sitio web de VMware.

Para utilizar Storage Gateway con VMware HA, le recomendamos que haga lo siguiente:

- Implementación de VMware ESX`.ova`paquete descargable que contiene la MV de Storage Gateway en un solo host de un clúster.
- Cuando implemente el paquete `.ova`, seleccione un almacén de datos que no sea local para un host. En su lugar, utilice un almacén de datos accesible para todos los hosts del clúster. Si selecciona un almacén de datos local para un host y el host produce un error, es posible que la fuente de datos no permita el acceso a otros hosts del clúster y la conmutación por error a otro host no tenga éxito.
- Con clústeres, si implementa el paquete `.ova` en el clúster, seleccione un host cuando se le solicite que lo haga. Además, puede implementar directamente en un host de un clúster.

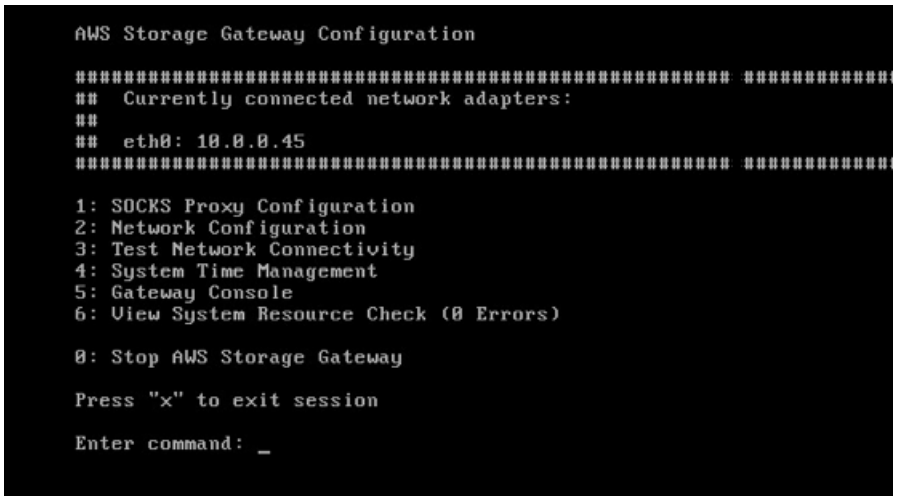
Sincronización de la hora de la MV de la gateway

Para una gateway implementada en VMware ESXi, el ajuste de la hora del host del hipervisor y la sincronización de la hora de la MV con el host es suficiente para evitar desviaciones de tiempo. Para obtener más información, consulte Sincronización de la hora de la máquina virtual y el host. Para una gateway implementada en Microsoft Hyper-V, debe comprobar periódicamente la hora de la MV mediante el procedimiento que se describe a continuación.

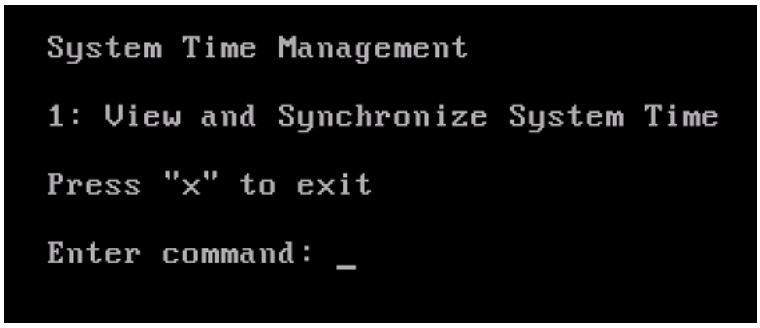
Para ver y sincronizar la hora de la máquina virtual de una gateway de hipervisor con un servidor NTP (Network Time Protocol)

1. Inicie sesión en la consola local de la gateway:
   - Para obtener más información sobre el inicio de sesión en la consola local de VMware ESXi, consulte Acceso a la consola local de la 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 para la máquina virtual de Linux basada en el kernel (KVM), consulte Acceso a la consola local de la gateway con Linux KVM.

2. En la páginaConfiguración Storage Gatewaymenú principal, escriba**4**paraGestión del tiempo del sistema.



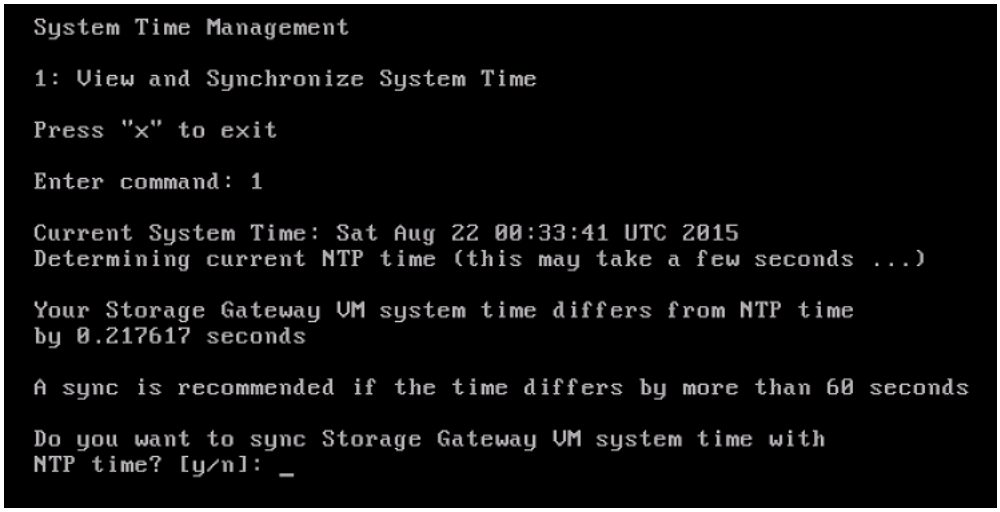
3. En el menú System Time Management (Administración de la hora del sistema), escriba **1** para View and Synchronize System Time (Ver y sincronizar la hora del sistema).



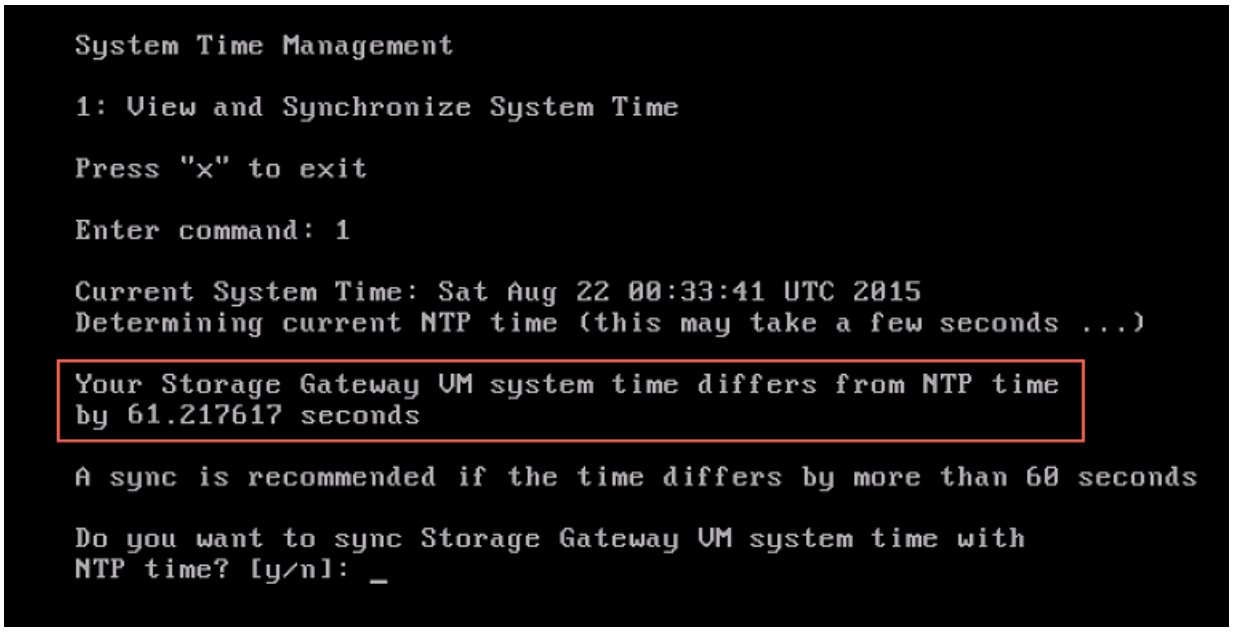
4. Si el resultado indica que debe sincronizar la hora de la máquina virtual con la hora de NTP, escriba **y**. De lo contrario, escriba **n**.

   Si escribe **y** para sincronizar, el proceso puede tardar unos momentos.

   En la siguiente captura de pantalla, se muestra una máquina virtual que no requiere la sincronización de la hora.



En la siguiente captura de pantalla se muestra una MV que requiere la sincronización de la hora.



Implementación de una gateway de archivos en un host Amazon EC2

Puede implementar y activar una gateway de archivos en una instancia de Amazon Elastic Compute Cloud (Amazon EC2). La imagen de Amazon Machine (AMI) de la gateway de archivos está disponible como AMI de la comunidad.

Para implementar una gateway en una instancia Amazon EC2

1. En la página Select host platform, elija Amazon EC2.

2. Elija Launch instance para lanzar la AMI de EC2 de la gateway de almacenamiento. Se abrirá la consola de Amazon EC2, donde puede elegir un tipo de instancia.
3. En la páginaPaso 2: Página Choose an Instance Type, elija la configuración de hardware de la instancia. Storage Gateway es compatible con los tipos de instancias que cumplan determinados requisitos mínimos. Recomendamos comenzar por el tipo de instancia m4.xlarge, que cumple los requisitos mínimos para que la gateway funcione correctamente. Para obtener más información, consulte Requisitos de hardware para las máquinas virtuales locales.

   Puede cambiar el tamaño de la instancia después de lanzarla, si es necesario. Para obtener más información, consulteCambio de tamaño de la instanciaen laGuía del usuario de Amazon EC2 para instancias de Linux.

   > **Note**
   >
   > Algunos tipos de instancias, en especial las i3 EC2, utilizan discos SSD NVMe. Estos pueden causar problemas al iniciar o detener la gateway de archivos; por ejemplo, se pueden perder datos de la caché. Monitorear el`CachePercentDirty`Métrica de Amazon CloudWatch y solo inicie o detenga el sistema cuando ese parámetro sea`0`. Para obtener más información sobre la monitorización de métricas para la gateway, consulteDimensiones y métricas de Storage Gatewayen la documentación de CloudWatch. Para obtener más información sobre los requerimientos del tipo de instancia de Amazon EC2, consultethe section called “Requisitos para los tipos de instancias Amazon EC2”.
4. Seleccione Next (Siguiente): Página Configure Instance Details (Configurar los detalles de la instancia).
5. En la páginaPaso 3: Página Configure Instance Details (Configurar los detalles de la instancia), elija un valor paraAuto-assign Public IP. Si la instancia debe ser accesible públicamente desde Internet, compruebe que la opción Auto-assign Public IP (Asignar IP pública automáticamente) esté establecida en Enable (Habilitar). Si la instancia no debe ser accesible desde Internet, en Auto-assign Public IP (Asignar IP pública automáticamente), seleccione Disable (Deshabilitar).
6. ParaRol de IAM, elige elAWS Identity and Access Management(IAM) que desee utilizar para la gateway.
7. Seleccione Next (Siguiente): Add Storage (Agregar almacenamiento).

8. En la páginaPaso 4: Adición de almacenamientopágina, elijaAdición de nuevo volumenpara añadir almacenamiento a la instancia de la gateway de archivos. Se requiere al menos un volumen de Amazon EBS para configurar para almacenamiento en caché.

   Tamaños de disco recomendados: Caché (mínimo) 150 GiB y caché (máximo) 64 TiB

9. En la páginaPaso 5: Añadir etiquetas, puede añadir una etiqueta opcional a la instancia. A continuación, elija Next (Siguiente): Configure Security Group (Configurar grupo de seguridad).

10. En la páginaPaso 6: Página Configure Security Group (Configurar grupo de seguridad), agregue reglas de firewall para conducir el tráfico específico hacia la instancia. Puede crear un nuevo grupo de seguridad o elegir uno existente.

    > **Important**
    >
    > Además de la activación de Storage Gateway y los puertos de acceso Secure Shell (SSH), los clientes de NFS requieren acceso a puertos adicionales. Para obtener información detallada, consulte Requisitos de red y firewall.

11. Elija Review and Launch para revisar la configuración.

12. En la páginaPaso 7: Página Review Instance Launch (Revisar lanzamiento de instancia)página, elijaLanzamiento.

13. En el cuadro de diálogo Select an existing key pair or create a new key pair, elija Choose an existing key pair y, a continuación, seleccione el par de claves que creó al obtener la configuración. Cuando haya terminado, active la casilla de confirmación y, después, elija Launch Instances.

    Verá una página de confirmación que le indicará que la instancia se está lanzando.

14. Elija View Instances para cerrar la página de confirmación y volver a la consola. En la pantalla Instances se muestra el estado de la instancia. La instancia tarda poco tiempo en lanzarse. Al lanzar una instancia, su estado inicial es pending (pendiente). Una vez iniciada la instancia, el estado cambia a running y recibe un nombre de DNS público.

15. Seleccione la instancia, anote la dirección IP pública enDescripcióny vuelva a laConnect toAWSde la consola de Storage Gateway para continuar la configuración de la puerta de enlace.

Puede determinar el ID de AMI que se utilizará para lanzar una gateway de archivos mediante la consola de Storage Gateway o consultando laAWS Systems Manageralmacén de parámetros.

Para determinar el ID de AMI

1. Inicie sesión en laAWS Management Consoley abra la consola de Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
2. Elija Create gateway (Crear gateway), elija File gateway (Gateway de archivos) y, a continuación, elija Next (Siguiente).
3. En la página Choose host platform, elija Amazon EC2.
4. ElegirLanzar instanciapara lanzar una AMI EC2 de Storage Gateway. Se abrirá la página de la AMI de la comunidad de EC2, donde puede ver el ID de AMI para suAWSRegión en la URL.

   También puede consultar el almacén de parámetros de Systems Manager. Puede utilizar elAWS CLIo la API de Storage Gateway para consultar el parámetro público de Systems Manager en el espacio de nombres`/aws/service/storagegateway/ami/FILE_S3/latest`. Por ejemplo, al utilizar el siguiente comando de la CLI se devuelve el ID de la AMI actual en laAWSRegión .

   ```
   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"
       }
   }
   ```

Cómo obtener una clave de activación para la gateway

Para obtener una clave de activación para su gateway, se realiza una solicitud web a la MV del gateway y devuelve un redireccionamiento que contiene la clave de activación. Esta clave de activación se transfiere como uno de los parámetros a la acción de la API

`ActivateGateway` para especificar la configuración de su gateway. Para obtener más información, consulteActivateGatewayen laReferencia de la API de Storage.

La solicitud que envíe a la MV de la gateway contiene elAWSRegión 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`*.

Temas

- AWS CLI
- Linux (bash/zsh)
- Microsoft Windows PowerShell

AWS CLI

Si aún no lo ha hecho, debe instalar y configurar la AWS CLI. Para ello, siga las siguientes instrucciones en la Guía del usuario de AWS Command Line Interface:

- Instalación deAWS Command Line Interface
- Configuración deAWS Command Line Interface

En el siguiente ejemplo se muestra cómo utilizar elAWS CLIPara recuperar la respuesta HTTP, analizar los encabezados HTTP y obtener la clave de activación.

```
wget 'ec2_instance_ip_address/?activationRegion=eu-west-2' 2>&1 | \
grep -i location | \
grep -i key | \
cut -d'=' -f2 |\
cut -d'&' -f1
```

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 "$activation_region" ]]; then
    echo "Usage: get-activation-key ip_address activation_region"
    return 1
  fi
  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region"); 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

En el siguiente ejemplo se muestra cómo utilizar Microsoft Windows PowerShell para recuperar 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
  )
  PROCESS {
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion" -MaximumRedirection 0 -ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

Uso deAWS Direct Connectcon Storage Gateway

AWS Direct Connectvincula una red interna con Amazon Web Services Cloud. UsandoAWS Direct Connectcon Storage Gateway, puede crear una conexión de red para necesidades de cargas de

trabajo de alto rendimiento, que proporciona una conexión de red dedicada entre la gateway local yAWS.

Storage Gateway utiliza puntos de enlace públicos. Con unAWS Direct Connectconexión en el sitio, puede crear una interfaz virtual pública que permita dirigir el tráfico a los puntos de enlace de Storage Gateway. La interfaz virtual pública omite a los proveedores de Internet en su ruta de acceso a la red. El endpoint público del servicio Storage Gateway puede estar en el mismoAWSRegión como laAWS Direct Connectubicación, o puede estar en otraAWSRegión .

En la siguiente ilustración se muestra un ejemplo de cómoAWS Direct Connectfunciona con Storage Gateway.

En el siguiente procedimiento se supone que ha creado una gateway funcional.

Para utilizarAWS Direct Connectcon Storage Gateway

1. Crear y establecer unAWS Direct Connectconexión entre el centro de datos on-premises y el punto de enlace de Storage Gateway. Para obtener más información acerca de cómo crear una conexión, consulteIntroducción aAWS Direct Connecten laAWS Direct ConnectGuía del usuario de .
2. Connect el dispositivo Storage Gateway en las instalacionesAWS Direct Connectenrutador.
3. Cree una interfaz virtual pública y configure su router local según sea necesario. Para obtener más información, consulteCreación de una interfaz virtualen laAWS Direct ConnectGuía del usuario de .

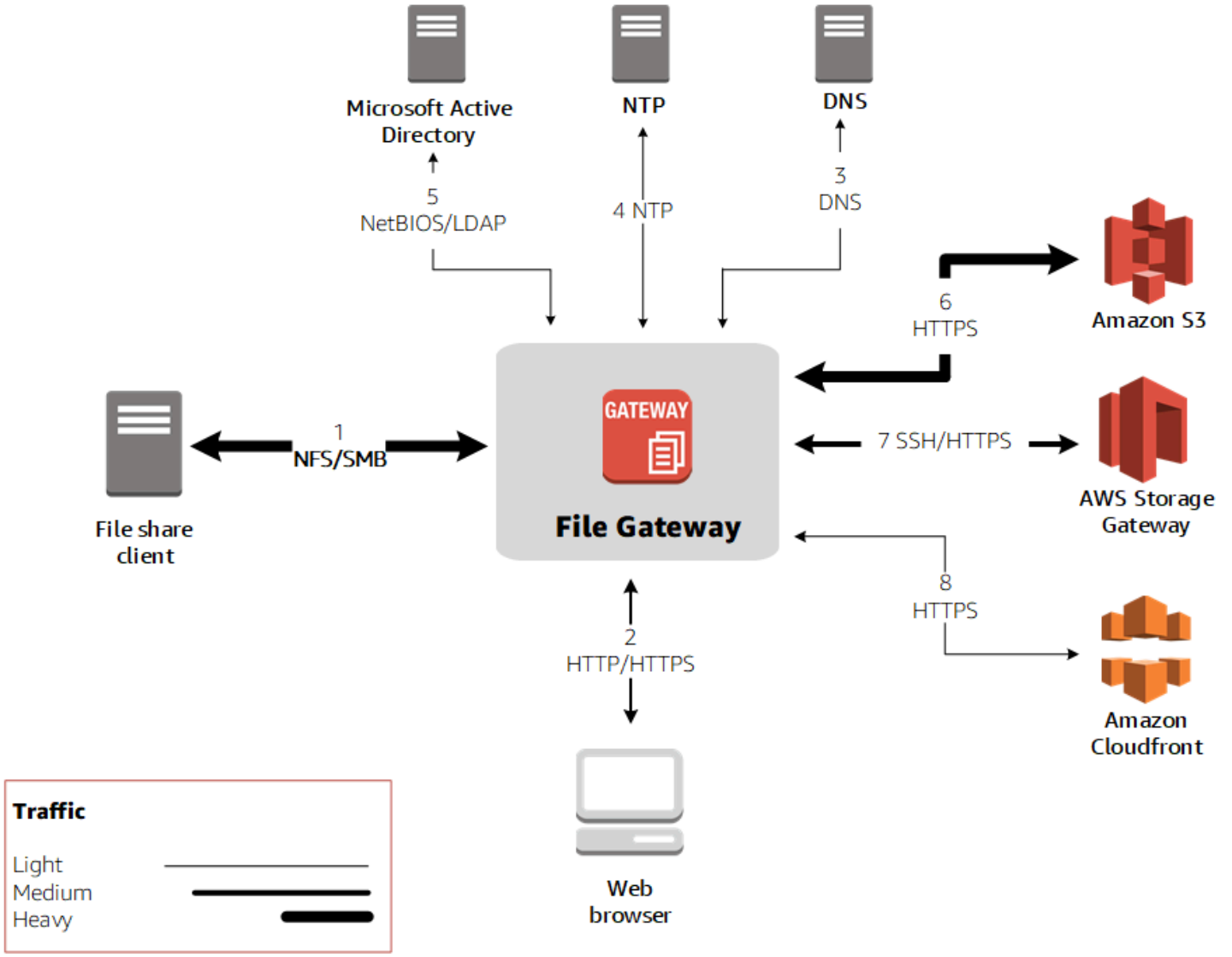
Más información en la documentación deAWS Direct Connect, consulte¿Qué es ?AWS Direct Connect?en laAWS Direct ConnectGuía del usuario de.

Requisitos de los puertos

Storage Gateway requiere los siguientes puertos para su funcionamiento. Algunos puertos son comunes y obligatorios para todos los tipos de gateway. Otros puertos son exigidos por tipos de gateway específicos. En esta sección, encontrará una imagen de los puertos necesarios y una lista los puertos que necesita cada el tipo de gateway.

Gateways de archivos

En la siguiente ilustración se muestran los puertos que se deben abrir para que las gateways de archivos sean operativas.



Los siguientes puertos son comunes y obligatorios para todos los tipos de gateways.

De	Para	Protocolo	Puerto	Cómo se utiliza	
Storage Gateway	Amazon Web Services	Protocolo de control de transmisión (TCP)	443 (HTTPS)	Para la comunicación desde una máquina virtual de Storage Gateway a	

De	Para	Protocolo	Puerto	Cómo se utiliza	
				unAWSpunto de enlace de servicio. Para obtener más información acerca de los puntos de enlace de servicio, consulte Permisos de acceso de AWS Storage Gateway a través de firewalls y routers.	

De	Para	Protocolo	Puerto	Cómo se utiliza	
El navegador web	Storage Gateway	TCP	80 (HTTP)	Los sistemas locales obtienen la clave de activación de Storage Gateway. El puerto 80 solo se utiliza durante la activación de un dispositivo de Storage Gateway. Una 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 red. Si activa la gateway desde la consola de	

De	Para	Protocolo	Puerto	Cómo se utiliza	
				administración Storage Gateway, el host desde el que se conecta a la consola debe tener acceso al puerto 80 de gateway.	
Storage Gateway	Servidor DNS (Domain Name Service)	Protocolo de datagramas de usuario (UDP)/UDP	53 (DNS)	Para comunicarse entre una máquina virtual de Storage Gateway y el servidor DNS.	

De	Para	Protocolo	Puerto	Cómo se utiliza	
Storage Gateway	Amazon Web Services	TCP	22 (canal de soporte)	Permite que el Support de Amazon Web Services obtenga acceso a la gateway para ayudarle con la solución de problemas de gateway. No necesita este puerto abierto para el funcionamiento normal de la gateway, pero se exige para la solución de problemas.	

De	Para	Protocolo	Puerto	Cómo se utiliza	
Storage Gateway	Servidor de Network Time Protocol (NTP)	UDP	123 (NTP)	Lo utilizan los sistemas locales para sincronizar la hora de la VM con la hora del host. Una máquina virtual de Storage Gateway está configurada para utilizar los siguientes servidores NTP: • 0.amazon.pool.ntp.org • 1.amazon.pool.ntp.org • 2.amazon.pool.ntp.org • 3.amazon.pool.ntp.org	

De	Para	Protocolo	Puerto	Cómo se utiliza	
Dispositivo de hardware de Storage Gateway	Proxy HTTP (Hypertext Transfer Protocol)	TCP	8080 (HTTP)	Se necesita brevemente para la activación.	

En la tabla siguiente, se muestran los puertos que deben abrirse para una gateway de archivos mediante el protocolo Network File System (NFS) o Server Message Block (SMB). Estas reglas de puertos forman parte de la definición del grupo de seguridad.

Ru	Elemento de red	Tipo de recurso compartido de archivos	Protocolo	Puert	Entra	Salida	¿Obligrio?	Notas
1	Cliente de recurso compartido de archivos	NFS	Datos TCP/UDP	111	✓	✓	✓	Transferencia de datos de uso compartido de archivos (para NFS únicamente)
			TCP/UDP NFS	2049	✓	✓	✓	Transferencia de datos de uso compartido de archivos (para NFS únicamente)
			TCP/UDP NFSv3	2004	✓	✓	✓	Transferencia de datos de uso compartido de archivos (para NFS únicamente)

Ru	Elemento de red	Tipo de recurso compartido de archivos	Protocolo	Puert	Entra	Salida	¿Obligrio?	Notas
		SMB	TCP/UDP SMBv2	139	✓	✓	✓	Servicio de sesión de transferencia de datos de uso compartido de archivos (solo para SMB); sustituye a los puertos 137—139 para Microsoft Windows NT y posteriores
			TCP/UDP SMBv3	445	✓	✓	✓	Servicio de sesión de transferencia de datos de uso compartido de archivos (solo para SMB); sustituye a los puertos 137—139 para Microsoft Windows NT y posteriores
2	Navegador web	NFS y SMB	TCP HTTP	80	✓	✓	✓	Consola de administración de Amazon Web Services (solo para la activación)

Ru	Elemento de red	Tipo de recurso compartido de archivos	Protocolo	Puert	Entra	Salida	¿Obligrio?	Notas
			TCP HTTPS	443	✓	✓	✓	Consola de administración de Amazon Web Services (todas las demás operaciones)
3	DNS	NFS y SMB	TCP/UDP DNS	53	✓	✓	✓	Resolución de nombres IP
4	NTP	NFS y SMB	UDP NTP	123	✓	✓	✓	Servicio de sincronización de hora
5	Microsoft Active Directory	SMB	UDP NetBIOS	137	✓	✓	✓	Servicio de nombres (no se utiliza para NFS)
			UDP NetBIOS	138	✓	✓	✓	Servicio de datagramas
			TCP LDAP	389	✓	✓		Conexión de cliente de Directory System Agent (DSA)
			TCP LDAPS	636	✓	✓		LDAPS: protocolo ligero de acceso a directorios (LDAP) a través de la capa de conexión segura (SSL)

Ru	Elemento de red	Tipo de recurso compartido de archivos	Protocolo	Puert	Entra	Salida	¿Obligrio?	Notas
6	Amazon S3	NFS y SMB	Datos HTTPS	443	✓	✓	✓	Transferencia de datos de almacenamiento
7	Storage Gatewa	NFS y SMB	TCP SSH	22	✓	✓	✓	canal de soporte
			TCP HTTPS	443	✓	✓	✓	Control de administración
8	Amazon CloudFront	NFS y SMB	TCP HTTPS	443	✓	✓	✓	Para la activación

Conexión a la gateway

Después de elegir un host e implementar la MV de la gateway, conecte y active la gateway. Para ello, necesita la dirección IP de la MV de la gateway. Obtenga la dirección IP de la consola local de la gateway. Inicie sesión en la consola local y obtenga la dirección IP de la parte superior de la página de la consola.

Para las gateways implementadas en las instalaciones, obtenga también la dirección IP del hipervisor. Para gateways de Amazon EC2, también puede obtener la dirección IP de la instancia de Amazon EC2 desde la consola de administración de Amazon EC2. Para encontrar información cómo obtener la dirección IP de la gateway, consulte uno de los siguientes enlaces:

- Host VMware: Acceso a la consola local de la gateway con VMware ESXi
- Host HyperV: Acceso a la consola local de la gateway con Microsoft Hyper-V
- Host de máquina virtual de Linux basada en el kernel (KVM): Acceso a la consola local de la gateway con Linux KVM
- Host EC2: Obtención de una dirección IP de un host Amazon EC2

Cuando encuentre la dirección IP, anótela. A continuación, vuelva a la consola de Storage Gateway y escriba la dirección IP en la consola.

Obtención de una dirección IP de un host Amazon EC2

Para obtener la dirección IP de la instancia de Amazon EC2 donde está implementada la gateway, inicie sesión en la consola local de la instancia EC2. A continuación, obtenga la dirección IP de la parte superior de la página de la consola. Para obtener instrucciones, consulte .

También puede obtener la dirección IP desde la consola de administración de Amazon EC2. Le recomendamos que utilice la dirección IP pública para la activación. Para obtener la dirección IP pública, utilice el procedimiento 1. Si, en su lugar, decide utilizar la dirección IP elástica, consulte el procedimiento 2.

Procedimiento 1: Para conectarse a la gateway mediante la dirección IP pública

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instances y, a continuación, seleccione la instancia EC2 en la que está implementada la gateway.
3. Elija la pestaña Description en la parte inferior y, a continuación, anote la dirección IP pública. Utilice esta dirección IP para conectar con la gateway. Vuelva a la consola de Storage Gateway y escriba la dirección IP.

Si desea utilizar la dirección IP elástica para la activación, utilice el procedimiento siguiente.

Procedimiento 2: Para conectarse a la gateway mediante la dirección IP elástica

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instances y, a continuación, seleccione la instancia EC2 en la que está implementada la gateway.
3. Elija la pestaña Description en la parte inferior y, a continuación, anote el valor de Elastic IP. Utilice esta dirección IP elástica para conectar con la gateway. Vuelva a la consola de Storage Gateway y escriba la dirección IP elástica.
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 gateway está ahora conectada con la dirección IP elástica de la instancia EC2.

Recursos e ID de recursos de Storage Gateway

En Storage Gateway, el recurso principal esGateway depero otros tipos de recursos incluyen:volume,cinta virtual,Destino iSCSI, ydispositivo vtl. Se conocen como subrecursos y no existen a menos que estén asociados a una gateway.

Estos recursos y subrecursos tienen nombres de recursos de Amazon (ARN) únicos asociados a ellos, tal y como se muestra en la siguiente 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*
ARN de volumen	`arn:aws:storagegateway:` *region*`:`*account-id* `:gateway/` *gateway-id* `/volume/`*volume-id*
ARN de cinta	`arn:aws:storagegateway:` *region*`:`*account-id* `:tape/`*tapebarcode*
ARN de destino (destino iSCSI)	`arn:aws:storagegateway:` *region*`:`*account-id* `:gateway/` *gateway-id* `/target/`*iSCSItarget*

Tipo de recurso	Formato de ARN
ARN de dispositivo de biblioteca de cintas virtuales (VTL)	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`* `/device/`*`vtldevice`*

Storage Gateway también admite el uso de instancias EC2 e instantáneas y volúmenes de EBS. Estos recursos son recursos de Amazon EC2 que se utilizan en Storage Gateway.

Trabajo con ID de recurso

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. Un ID de volumen adopta la forma `vol-3344CCDD` donde `vol` es el identificador de recurso para volúmenes.

Para cintas virtuales, puede anteponer un prefijo de hasta cuatro caracteres al ID de código de barra como ayuda para organizar las cintas.

Los ID de recursos de Storage Gateway se indican en mayúscula. No obstante, cuando utilice estos ID de recurso con la API de Amazon EC2, Amazon EC2 espera que los ID de recursos estén en minúsculas. Debe cambiar los ID de recursos a minúsculas para utilizarlos con la API de EC2. Por ejemplo, en Storage Gateway el ID para un volumen podría ser `vol-1122AABB`. Cuando utilice este ID con la API de EC2, debe cambiarlo a `vol-1122aabb`. De lo contrario, la API de EC2 podría no comportarse según lo previsto.

> **Important**
>
> Los ID para volúmenes de Storage Gateway e instantáneas de Amazon EBS creados a partir de volúmenes de gateways van a cambiar 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 utilizar estos ID más largos para poder probar los

sistemas con el nuevo formato. Para obtener más información, consulte ID de recursos más largos para EC2 y EBS.
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, consulteAnuncio: Heads-up — Longer Storage Gateway volume and snapshot IDs coming in 2016.

Etiquetado de recursos de Storage Gateway

En Storage Gateway, puede utilizar etiquetas para administrar los recursos. Las etiquetas permiten agregar metadatos a los recursos y asignarles categorías para facilitar su administración. Cada etiqueta consta de un par clave-valor, que usted define. Puede agregar etiquetas a gateways, volúmenes y cintas virtuales. Puede buscar y filtrar estos recursos en función de las etiquetas que agregue.

Por ejemplo, puede usar etiquetas para identificar recursos de Storage Gateway utilizados por cada departamento de la organización. Podría etiquetar gateways y volúmenes utilizados por el departamento de contabilidad de este tipo: (`key=department` y `value=accounting`). A continuación, puede filtrar por esta etiqueta para identificar todas las gateways y volúmenes utilizados por el departamento de contabilidad y utilizar la información para determinar el costo. Para obtener más información, consulte Uso de etiquetas de asignación de costos y Trabajar con Tag Editor.

Si archiva una cinta virtual etiquetada, la cinta mantiene sus etiquetas en el archivo. Del mismo modo, si recupera una cinta del archivo en otra gateway, las etiquetas se mantienen en la nueva gateway.

Para la gateway de archivos, 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 gateway y los recursos de.

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 paraAWSuso.
- 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 mediante la consola de Storage Gateway, la API de Storage Gateway o laInterfaz de línea de comandos 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 enhttps://console.aws.amazon.com/storagegateway/home.
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 enhttps://console.aws.amazon.com/storagegateway/home.
2. Elija el recurso cuya etiqueta desea editar.
3. Elija Tags (Etiquetas) para abrir el cuadro de diálogo Add/edit tags (Añadir o editar etiquetas).
4. Elija el icono del lápiz que aparece junto a la etiqueta que desea editar y, a continuación, edite la etiqueta.
5. Cuando haya acabado de editar la etiqueta, elija Save (Guardar).

Para eliminar una etiqueta

1. Abra la consola Storage Gateway enhttps://console.aws.amazon.com/storagegateway/home.
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).

Véase también

Uso de etiquetas para controlar el acceso a la gateway y los recursos de

Trabajo con componentes de código abierto paraAWS Storage Gateway

En esta sección, encontrará información sobre las herramientas y licencias de terceros de las que depende la funcionalidad de Storage Gateway.

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 funcionalidad para gateway de volumen, gateway de cinta 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 conAWS Storage Gatewaysoftware:

- Para las gateways implementadas en VMware ESXi:sources.tar que es
- Para las gateways implementadas en Microsoft Hyper-V:sources_hyperv.tar que es
- Para gateways implementadas en la máquina virtual basada en Linux Kernel (KVM):sources_KVM.tar que es

Este producto incluye software desarrollado por OpenSSL para su uso en OpenSSL Toolkit (http://www.openssl.org/). Para obtener las licencias pertinentes para todas las herramientas de terceros dependientes, consulteLicencias 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 OpenSSL para su uso en OpenSSL Toolkit (http://www.openssl.org/). Para obtener las licencias pertinentes para todas las herramientas de terceros dependientes, consulteLicencias de terceros.

Cuotas

Cuotas para los recursos compartidos de archivos

En la siguiente tabla se muestran las cuotas para los recursos compartidos de archivos.

Description (Descripción)	File Gateway
Número máximo de recursos compartidos de archivos por bucket de Amazon S3. Se produce un mapeo de uno a uno entre el recurso de archivos y un bucket de S3.	1
Número máximo de recursos compartidos de archivos por gateway	10
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
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 admitidos por las gateways de archivos, NFS y SMB.	1024 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 requeridos
S3 Gateway de archivos	150 GiB	64 TiB	—

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

Uso de clases de almacenamiento

Storage Gateway es compatible con las clases de almacenamiento Amazon S3 Estándar, Amazon S3 Única zona - Acceso poco frecuente, Amazon S3 One Zone-Infrequent Access, Amazon S3 Intelligent-Tiering y S3 Glacier. Para obtener más información acerca de las clases de almacenamiento, consulteTipos de almacenamiento de Amazon S3en laAmazon Simple Storage Service.

Temas

- Uso de clases de almacenamiento con una puerta de enlace de archivos
- Uso de la clase de almacenamiento GLACIER con la gateway de archivos

Uso de clases de almacenamiento con una puerta de enlace de archivos

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 Estándar o cualquiera de las clases de almacenamiento S3 Estándar - Acceso poco frecuente o S3 Única zona - Acceso poco frecuente o S3 Intelligent-Tiering (Capas inteligentes de S3). Los objetos almacenados en cualquiera de estas clases de almacenamiento pueden pasarse a GLACIER utilizando una política de ciclo de vida.

Clase de almacenamiento de Amazon S3	Consideraciones
Standard	Elija Estándar para almacenar los archivos de acceso frecuente de forma redundant e en varias zonas de disponibilidad que se encuentran distanciadas geográficamente. Es la clase de almacenamiento predeterminada. Consulte 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 almacenados en la clase de almacenamiento Intelligent-Tiering pueden incurrir en cargos adicionales de sobrescri tura, eliminación, solicitud o transición de objetos entre clases de almacenamiento en un plazo de 30 días. Hay una duración mínima de almacenamiento de 30 días y los objetos eliminados antes de 30 días incurren en un cargo prorrateado igual al cargo por almacenamiento durante 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. Los objetos de menos de 128 KB no son aptos para la organización automática en capas en la clase de almacenamiento Intelligent-Tierin g. Estos objetos se cobran según las tarifas de nivel de acceso frecuente y se aplican tarifas por eliminación anticipada.

Clase de almacenamiento de Amazon S3	Consideraciones
	S3 Intelligent-Tiering ahora admite un nivel de acceso a archivos y un nivel de Deep Archive Access. S3 Intelligent-Tiering migra automáticamente los objetos a los que no se haya accedido durante 90 días a la capa de acceso a archivos y después de 180 días sin acceso a ellos, a la capa de acceso a archivo profundo. Cada vez que se restaura un objeto de uno de los niveles de acceso al archivo, el objeto se mueve al nivel de acceso frecuente en unas horas y está listo para recuperarse. 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 archivado. 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 presenta la puerta de enlace de archivos. Cuando las operaciones de archivos que actualizan metadatos (como propietario, marca de hora, permisos y ACL) se realizan en archivos administrados por la puerta de enlace de archivos, se elimina el objeto existente y se crea una nueva versión del objeto en esta clase de almacenamiento de Amazon S3. Debe validar el impacto de las operaciones de archivos en la creación de objetos antes de utilizar esta clase de almacenamiento en producción porque se aplican tarifas de eliminación anticipada. Consulte 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 Estándar - Acceso poco frecuente pueden incurrir en cargos adicional es de sobrescritura, eliminación, solicitud, recuperación o transición de objetos entre clases de almacenamiento en un plazo de 30 días. Hay una duración mínima de almacenam iento de 30 días. Los objetos eliminados antes de 30 días incurren en un cargo prorrateado igual al cargo por almacenamiento durante 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. Los objetos de menos de 128 KB se cobran por 128 KB y se aplican tarifas por eliminación anticipad a. Cuando las operaciones de archivos que actualizan metadatos (como propietario, marca de hora, permisos y ACL) se realizan en archivos administrados por la puerta de enlace de archivos, se elimina el objeto existente y se crea una nueva versión del objeto en esta clase de almacenamiento de Amazon S3. Debe validar el impacto de las operaciones de archivos en la creación de objetos antes de utilizar esta clase de almacenamiento en producción porque se aplican tarifas de

Clase de almacenamiento de Amazon S3	Consideraciones
	eliminación anticipada. Consulte 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 se accede con poca frecuencia en una única zona de disponibilidad. Los objetos almacenados en la clase de almacenamiento Única zona - Acceso poco frecuente pueden incurrir en cargos adicional es de sobrescritura, eliminación, solicitud, recuperación o transición de objetos entre clases de almacenamiento en un plazo de 30 días. Hay una duración mínima de almacenam iento de 30 días y los objetos eliminados antes de 30 días incurren en un cargo prorrateado igual al cargo por almacenamiento durante 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. Los objetos de menos de 128 KB se cobran por 128 KB y se aplican tarifas por eliminación anticipad a. Cuando las operaciones de archivos que actualizan metadatos (como propietario, marca de hora, permisos y ACL) se realizan en archivos administrados por la puerta de enlace de archivos, se elimina el objeto existente y se crea una nueva versión del objeto en esta clase de almacenamiento de Amazon S3. Debe validar el impacto de las operaciones de archivos en la creación de objetos antes de utilizar esta clase de almacenamiento en producción porque se aplican tarifas de eliminación anticipada. Consulte Precios de Amazon S3 para obtener más información.

Aunque puede escribir objetos directamente desde un recurso compartido de archivos en la clase de almacenamiento S3 Estándar - Acceso poco frecuente, S3 Única zona - Acceso poco frecuente o S3 Intelligent-Tiering (Capas inteligentes de S3), le recomendamos que utilice una política de ciclo de vida para realizar la transición de los objetos en lugar de escribir directamente desde el recurso compartido de archivos, especialmente si espera actualizar o eliminar la objeto dentro de los 30 días posteriores a archivarlo. Para obtener información acerca de la política de ciclo de vida, consulteAdministrar el ciclo de vida de los objetos.

Uso de la clase de almacenamiento GLACIER con la gateway de archivos

Si realiza la transición de un archivo a S3 Glacier mediante políticas de ciclo de vida de Amazon S3 y el archivo está visible para los clientes del recurso compartido de archivos a través de la caché, obtendrá errores de E/S al actualizar el archivo. Le recomendamos que configure CloudWatch Events para que reciba notificaciones cuando se produzcan estos errores de E/S y que utilice la notificación para tomar medidas. Por ejemplo, puede 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 acerca de cómo restaurar los objetos archivados, consulteRestaurar objetos archivadosen laAmazon Simple Storage Service.

Referencia de API para Storage Gateway

Además de utilizar la consola, puede utilizar la API de AWS Storage Gateway para configurar y administrar las gateways mediante programación. En esta sección se describen las operaciones de AWS Storage Gateway, la solicitud de formas para la autenticación y la administración de errores. Para obtener más información acerca de las regiones y los puntos de enlace disponibles para Storage Gateway, consulteAWS Storage GatewayCuotas y puntos de enlace deen laAWSReferencia general de.

> **Note**
>
> También puede utilizar laAWSSDK al desarrollar aplicaciones con Storage Gateway. LaAWSLos SDK para Java, .NET y PHP envuelven la API de 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 GatewayEncabezados de solicitud obligatorios

En esta sección se describen los encabezados obligatorios que debe enviar con cada solicitud POST aAWS 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.

En el siguiente ejemplo, se muestran los encabezados que se utilizan en la operación ActivateGateway.

```
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 con las solicitudes POST paraAWS Storage Gateway. Los encabezados siguientes que comienzan con «x-amz» sonAWS-Encabezados específicos. El resto de los encabezados que se muestran son encabezados comunes utilizados en transacciones HTTP.

Encabezado	Description (Descripción)

`Authorization`	El encabezado de autorización contiene varios elementos de informaci ón sobre la solicitud que habilitanAWS Storage Gatewaypara determina r si la solicitud es una acción válida 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/aw`
	`s4_request,`
	`SignedHeaders=content-type;host;x-amz-date;x-amz-targ`
	`et,`
	`Signature= CalculatedSignature`
	
	En la sintaxis anterior, debe especificar el valor de YourAccessKey, el año, el mes y el día (yyyymmdd), la región y el valor de Calculate dSignature. El formato del encabezado de autorización se rige por los requisitos delAWSProceso de firma V4. Los detalles de la firma se tratan en el tema Firma de solicitudes.

`Content-Type`	Usar`application/x-amz-json-1.1` como tipo de canal para todas las solicitudes aAWS Storage Gateway.

Encabezado	Description (Descripción)
	`Content-Type: application/x-amz-json-1.1`
`Host`	Use el encabezado del host para especificar elAWS Storage Gatewaypunto final al que envías tu solicitud. Por ejemplo,`storagegateway.us-east-2.amazonaws.com` es el punto de enlace de la región EE.UU. Este (Ohio). Para obtener más información acerca de los puntos de enlace disponibles paraAWS Storage Gateway, consulteAWS Storage GatewayCuotas y puntos de enlace deen laAWSReferencia general de. `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`x-amz-date` El encabezado está presente, elAWS Storage Gatewayignora cualquier`Date`encabezado durante la autenticación de la solicitud . El formato `x-amz-date` debe ser ISO8601 básico con el formato AAAAMMDD'T'HHMMSS'Z'. Si se utiliza tanto el encabezado `Date` como `x-amz-date` , el formato de encabezado de fecha no tiene que ser ISO8601. `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`
`x-amz-target`	Este encabezado especifica la versión de la API y la operación que se está solicitando. Los valores de encabezado de destino se forman concatenando la versión de la API con el nombre de la API y están en el siguiente formato. `x-amz-target: StorageGateway_ APIversion .operationName` El valor de operationName (p. ej. "ActivateGateway") se encuentra en la lista de la API, Referencia de API para Storage Gateway.

Firma de solicitudes

Storage Gateway requiere que se firmen todas las solicitudes que se envíen, 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 AWSSignature 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: Creación de 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 a partir de la clave de acceso secreta, utilizando el ámbito de credenciales para crear una serie de códigos de autenticación de mensajes basados en hash (HMAC).

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. Encontrará otros cálculos de referencia en Conjunto de pruebas de Signature Version 4, en la Referencia general de Amazon Web Services.

El ejemplo supone lo siguiente:

- La marca temporal de la solicitud es "Mon, 10 Sep 2012 00:00:00" GMT.
- El punto de enlace es la región EE.UU. Este (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 este API (ni para ningún API de Storage Gateway).

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: Creación de 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, entonces 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:

```
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 ofrece información de referencia acerca de errores de AWS Storage Gateway. 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 operación `ActivationKeyInvalid` solamente lo devuelve la API ActivateGateway.

Según el tipo de error, Storage Gateway puede devolver solo 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

La siguiente tabla muestra las excepciones de la API AWS Storage Gateway. Cuando una operación de AWS Storage Gateway 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

Excepción	Mensaje	Código de estado HTTP
`InvalidClientTokenId`	El certificado X.509 oAWSEl ID de clave de acceso proporcionado no existe en nuestros registros.	403: prohibido
`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 suAWSClave de acceso y 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 valor válido (registrado)AWSID de clave de acceso o 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`	LaAWSEl ID de clave de acceso de necesita una suscripción al servicio.	400: solicitud maligna

Excepción	Mensaje	Código de estado HTTP
`ThrottlingException`	Tasa superada.	400: solicitud maligna
`UnknownOperationException`	Se ha especificado una operación desconocida. Las operaciones válidas se muestran en Operaciones en 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 tabla siguiente se muestra el mapeo entre los códigos de error de operación de AWS Storage Gateway y las API que pueden devolver los códigos. 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
Conflicto de configuración de endpoint de asociación de sistemas de archivos	La configuración de endpoint de File System Association existente entra en conflicto con la configuración especificada.	Sistema de archivos asociado
Dirección de punto final de la asociación del sistema de archivos ya en uso	La dirección IP del endpoint especificada ya está en uso.	Sistema de archivos asociado
Falta la dirección IP del punto final de la asociación del sistema de archivos	Falta la dirección IP del endpoint de la asociación del sistema de archivos.	Sistema de archivos asociado

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
No se ha encontrado la asociación del sistema de archivos	La asociación del sistema de archivos especificada no se ha encontrado.	Actualización de la asociación del sistema de archivos Disociar sistema de archivos Descripción de las asociaciones de sistemas de archivos
No se ha encontrado el sistema de archivos	El sistema de archivos especificado no se ha encontrado.	Sistema de archivos asociado

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 especific ada no está conectada.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRec overyPoint 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
`MaximumVolumeCount Exceeded`	El número de volúmenes máximo se ha superado.	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes
`NetworkConfigurati onChanged`	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:

- Content-Type: application/x-amz-json-1.1
- 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.

Type: 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.

Type: Recopilación

errorCode

Uno de los códigos de error de operación .

Type: Cadena

errorDetails

Este campo no se utiliza en la versión actual de la API.

Type: Cadena

message

Uno de los mensajes de código de error de operación.

Type: Cadena

Ejemplos de respuestas de error

El siguiente cuerpo JSON se devuelve si utiliza la API DescribeStorediSCSIVolumes y especifica una entrada de solicitud ARN de gateway que no existe.

```
{
```

```
  "__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."
}
```

Operaciones en Storage Gateway

Para ver la lista de operaciones de Storage Gateway, consulteActionsen laAWS Storage GatewayReferencia de la API.

Historial de revisión deAWSStorage Gateway

- Versión de API: 30-06-2013
- Actualización de documentación más reciente: 12 de octubre de 2021

En la siguiente tabla se describen los cambios importantes en cada versión delAWSStorage Gatewaydespués de abril de 2018. Para obtener notificaciones sobre las actualizaciones de esta documentación, puede suscribirse a una fuente RSS.

update-history-change	update-history-description	update-history-date
Procedimientos de creación de gateway actualizados	El procedimiento para crear una nueva gateway se ha actualizado para reflejar los cambios en la consola de Storage Gateway. Para obtener más información, consulteCrear y activar una puerta de enlace de archivos de Amazon S3.	12 de octubre de 2021
Support archivos de cierre forzado en recursos compartidos de archivos SMB	Ahora puede utilizar la configuración de grupo local para asignar permisos de administrador de puerta de enlace. Los administradores de puerta de enlace pueden utilizar el complemento Carpetas compartidas Microsoft Management Console para cerrar forzosamente los archivos abiertos y bloqueados en los recursos compartidos de archivos SMB. Para obtener más información,	12 de octubre de 2021

	consulteConfigure grupos locales para su gateway.	
Compatibilidad con registros de auditoría para recursos compartidos de archivos NFS	Ahora puede configurar recursos compartidos de archivos NFS para generar registros de auditoría que proporcionan detalles sobre el acceso de los usuarios a archivos y carpetas dentro 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 inapropiados. Para obtener más información, consulteDescripción de los registros de auditoría de file gateway.	12 de octubre de 2021
Compatibilidad con alias de puntos de acceso	Los recursos compartidos de archivos de puerta de enlace de archivos ahora se pueden conectar al almacenamiento de Amazon S3 mediante alias de punto de acceso estilo bucket. Para obtener más información, consulteCreación de un recurso compartido de archivos.	12 de octubre de 2021

Compatibilidad con puntos de acceso y endpoints de VPC	Los recursos compartidos de archivos de puerta de enlace de archivos ahora pueden conectarse a buckets de S3 a través de puntos de acceso o endpoints de interfaz en su VPC con tecnologíaAWS PrivateLink. Para obtener más información, consulteCreación de un recurso compartido de archivos.	7 de julio de 2021
Soporte de bloqueo oportunista	Los recursos compartidos de archivos de gateway de archivos 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 informaci ón, consulteCreación de un recurso compartido de archivos SMB.	7 de julio de 2021
Conformidad con FedRAMP	Storage Gateway cumple ahora con FedRAMP. Para obtener más información, consulteValidación del cumplimiento de Storage Gateway.	24 de noviembre de 2020

Limitación del ancho de banda basada en programación	Storage Gateway ahora permite la limitación del ancho de banda basada en la programación para las gateways de cintas y de volúmenes. Para obtener más información, consulteProgramación de la limitación del ancho de banda mediante la consola de Storage Gateway.	9 de noviembre de 2020
Notificación de carga de archivos para gateway de archivos	File gateway ahora proporcio na una notificación de carga de archivos, que le notifica cuando la puerta de enlace de archivos ha cargado completamente un archivo en Amazon S3. Para obtener más información, consulteObtener notificación de subida de archivos.	9 de noviembre de 2020
Enumeración basada en acceso para puerta de enlace de archivos	File gateway ahora proporcio na una enumeración basada en el acceso, que filtra la enumeración de archivos y carpetas en un recurso compartido de archivos SMB en función de las ACL del recurso compartido. Para obtener más informaci ón, consulteCreación de un recurso compartido de archivos SMB.	9 de noviembre de 2020

Migración de archivos gateway	File gateway ahora proporcio na un proceso documentado para reemplazar una puerta de enlace de archivos existente por una nueva puerta de enlace de archivos. Para obtener más información, consulteSustitución de una puerta de enlace de archivos por una nueva puerta de enlace de archivos.	30 de octubre de 2020
Rendimiento de lectura de caché fría de puerta de enlace de archivos 4x	Storage Gateway ha aumentado el rendimiento de lectura de caché fría 4x. Para obtener más información, consulteGuía de rendimiento de las gateways de archivos.	31 de agosto de 2020
Solicite el dispositivo de hardware a través de la consola	Ahora puede solicitar el dispositivo de hardware a través delAWSConsola Storage Gateway Para obtener más informaci ón, consulteEl dispositivo de hardware de Storage Gateway.	12 de agosto de 2020

Support los puntos de enlace del estándar federal de procesamiento de información (FIPS) en un nuevoAWSRegiones de	Ahora puede activar una gateway con endpoints FIPS en las regiones EE. UU. Este (Ohio), EE. UU. Este (Norte de Virginia), EE. UU. Oeste (Norte de California), EE. UU. Oeste (Oregón) y Canadá (Central). Para obtener más información, consulteAWSCuotas y puntos de enlace de Storage Gatewayen laAWSReferencia general de.	31 de julio de 2020

Support varios recursos compartidos de archivos adjuntos a un único bucket de Amazon S3	File gateway ahora admite la creación de varios recursos compartidos de archivos para un único bucket de S3 y la sincronización de la caché local de la puerta de enlace de archivos con un bucket en función de la frecuencia de acceso al directorio. Puede limitar el número de depósitos necesarios para administr ar los recursos compartidos de archivos que crea en la puerta de enlace de archivos. 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 nombres de recursos compartidos de archivos de puerta de enlace para que sean independientes del nombre del bucket para ajustarse a la convención de nomenclatura de recursos compartidos de archivos local. Para obtener más informaci ón, consulteCreación de un recurso compartido de archivos NFSoCreación de un recurso compartido de archivos SMB.	7 de julio de 2020

Almacenamiento de caché local de puerta de enlace de archivos 4 veces mayor	Storage Gateway ahora admite una caché local de hasta 64 TB para gateway de archivos, 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, consulteTamaños de disco local recomendados para la puerta de enlaceen laStorage Gateway.	7 de julio de 2020
Ver alarmas de Amazon CloudWatch en la consola de Storage Gateway	Ahora puede ver las alarmas de CloudWatch en la consola de Storage Gateway. Para obtener más información, consulteInformación acerca de las alarmas de Cloud.	29 mayo de 2020

Compatibilidad con los puntos de enlace del estándar federal de procesamiento de información (FIPS).	Ahora puede activar una gateway con puntos de enlace de FIPS en las regiones AWS GovCloud (US). Para elegir un punto de enlace de FIPS para una gateway de archivos, consulte Selección de un punto de enlace de servicio. Para elegir un punto de enlace de FIPS para una gateway de volumen, consulte Selección de un punto de enlace de servicio. Para elegir un punto de enlace de FIPS para una gateway de cinta, consulte Selección de un punto de enlace de servicio.	22 de mayo de 2020
NuevoAWSRegiones de	Storage Gateway ahora está disponible en las regiones de África (Ciudad del Cabo) y Europa (Milán). Para obtener más información, consulteAWSCuotas y puntos de enlace de Storage Gatewayen laAWSReferencia general de.	7 de mayo de 2020

Compatibilidad con la clase de almacenamiento S3 Intelligent-Tiering	Storage Gateway ahora es compatible con 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, consulteClase de almacenamiento para optimizar automáticamente los objetos a los que se obtiene acceso con mucha y poca frecuenciaen laGuía del usuario de Amazon Simple Storage Service.	30 de abril de 2020
NuevoAWSRegión	Storage Gateway ya está disponible en laAWSRegión GovCloud (EE. UU. Este). Para obtener más información, consulteAWSCuotas y puntos de enlace de Storage Gatewayen laAWSReferencia general de.	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 gateway on-premise en la plataforma de virtualiz ación Microsoft Hyper-V. Las gateways implementadas en KVM tienen la misma funcional idad y características que las gateways en las instalaciones existentes. Para obtener más información, consulteHiperviso res compatibles y requisitos de hosten laStorage Gateway.	4 de febrero de 2020
Compatibilidad con la alta disponibilidad de VMware vSphere	Storage Gateway ahora admite la alta disponibilidad en VMware para proteger las cargas de trabajo de almacenamiento frente a fallos de hardware, hiperviso r o red. Para obtener más información, consulteUso de la alta disponibilidad de VMware vSphere con Storage Gatewayen laStorage Gateway. Esta versión también incluye mejoras de rendimiento. Para obtener más información, consulteRendimientoen laStorage Gateway.	20 de noviembre de 2019

NuevoRegión de AWSpara Gateway de cinta	La gateway de cinta ahora está disponible en la región América del Sur (São Paulo). Para obtener más informaci ón, consulteAWSCuotas y puntos de enlace de Storage Gatewayen laAWSReferencia general de.	24 de septiembre de 2019
Support para Amazon CloudWatch Logs	Ahora puede configurar las gateways de archivos con los grupos de registros de Amazon CloudWatch para recibir notificaciones de los errores y el estado de la gateway y sus recursos. Para obtener más informaci ón, consulteRecibir notificac iones sobre los errores y el Health gateway con los grupos de registros de Amazon CloudWatchen laGuía del usuario de Storage Gateway	4 de septiembre de 2019
NuevoRegión de AWS	Storage Gateway ahora está disponible en la región Asia Pacífico (Hong Kong). Para obtener más informaci ón, consulteAWSCuotas y puntos de enlace de Storage Gatewayen laAWSReferencia general de.	14 de agosto de 2019

NuevoRegión de AWS	Storage Gateway ahora está disponible en la región de Medio Oriente (Baréin). Para obtener más informaci ón, consulteAWSCuotas y puntos de enlace de Storage Gatewayen laAWSReferencia general de.	29 de julio de 2019
Posibilidad de activar una gateway en una Virtual Private Cloud (VPC)	Ahora puede activar una gateway en una VPC. Puede crear una conexión privada entre su dispositivo de software local y una infraestr uctura de almacenamiento basada en la nube. Para obtener más información, consulte Activación de una gateway en una nube virtual privada.	20 de junio de 2019
Compatibilidad de los recursos compartidos de archivos SMB con las ACL de Microsoft Windows	Para las gateways de archivos, ahora puede utilizar las listas de control de acceso (ACL) de Microsoft Windows para controlar el acceso a los recursos compartidos de archivos Server Message Block (SMB). Para obtener más información, consulte Uso de las ACL de Microsoft Windows para controlar el acceso a un recurso compartid o de archivos SMB.	8 de mayo de 2019

Compatibilidad de la gateway de archivos con la autorización basada en etiquetas	La gateway de archivos ahora es compatible con la autorización basada en etiquetas. Puede controlar el acceso a los recursos de la gateway de archivos basándose en las etiquetas de los 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 de Storage Gateway en Europa	El dispositivo de hardware de Storage Gateway ahora está disponible en Europa. Para obtener más información, consulteAWSRegiones del dispositivo de hardware de Storageen laAWSReferencia general de. Además, ahora puede aumentar el almacenamiento utilizable en el dispositivo de hardware de Storage Gateway de 5 TB a 12 TB y sustituir la tarjeta de red de cobre instalada por una tarjeta de red de fibra óptica de 10 gigabits. Para obtener más información, consulte Configuración del dispositivo de hardware.	25 de febrero de 2019

Support dispositivos de hardware Storage Gateway	El dispositivo de hardware de Storage Gateway incluye el software Storage Gateway preinstalado en un servidor de terceros. Puede administrar el dispositivo desde la AWS Management Console. El dispositivo puede alojar gateways de archivos, cintas y volúmenes. Para obtener más información, consulteEl dispositivo 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 gateways de archivos. 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 en cada versión delAWSStorage Gatewayantes de mayo de 2018.

Cambio	Descripción	Fecha de modificación
Support clase de almacenamiento S3 Única zona	En las gateways de archivos, ahora puede elegir S3 One Zone-IA como clase de almacenamiento predeterminada para recursos compartidos de archivos. El uso de esta clase de almacenamiento le	4 de abril de 2018

Cambio	Descripción	Fecha de modificación
- Acceso poco común	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.	
Nuevo Región de AWS	La gateway de cinta ahora está disponible en la región Asia Pacífico (Singapur). Para obtener información detallada, consulte Regiones de AWS compatibles.	3 de abril de 2018
Support notificaciones de actualización de la caché, pago por solicitante y listas de control de acceso predefinidas para los buckets de Amazon S3	Las gateways de archivos ahora le permiten recibir una notificación cuando la gateway termine de actualizar la caché para el bucket de Amazon S3. Para obtener más información, consulteRefreshCache.html que esen laReferencia de la API de Storage. En las gateways de archivos, ahora puede especificar que el solicitante o el lector pague los cargos de acceso en lugar del propietario del bucket. Las gateways de archivos ahora permiten dar control total al propietario del bucket de S3 que se mapea al recurso compartido de archivos NFS. Para obtener más información, consulte Creación de un recurso compartido de archivos.	1 de marzo de 2018
Nuevo Región de AWS	Storage Gateway ahora está disponible en la región UE (París) Para obtener información detallada, consulte Regiones de AWS compatibles.	18 de diciembre de 2017

Cambio	Descripción	Fecha de modificación
Ayuda con las notificaciones de carga de archivos y la detección del tipo MIME	Las gateways de archivos ahora le permiten recibir una notificación cuando todos los archivos escritos en un recurso compartido de archivos NFS se han cargado en Amazon S3. Para obtener más informaci ón, consulteNotifyWhenUploadeden laReferencia de la API de Storage. Las gateways de archivos ahora permiten adivinar el tipo MIME de los objetos cargados en función de las extensiones de archivo. Para obtener más informaci ón, consulte Creación de un recurso compartido de archivos.	21 de noviembre de 2017
Compatibilidad con VMware ESXi Hypervisor versión 6.5	AWSStorage Gateway ahora es compatible con VMware ESXi Hypervisor versión 6.5. 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 gateway de archivos con el hipervisor Microsoft Hyper-V	A partir de ahora, se puede implementar una gateway de archivos en un hipervisor Microsoft Hyper-V. Para obtener información, consulte Hipervisores compatibl es y requisitos de host.	22 de junio de 2017
Nuevo Región de AWS	Storage Gateway ahora está disponible en la región Asia Pacífico (Mumbai). Para obtener información detallada, consulte Regiones de AWS compatibles.	02 de mayo de 2017

Cambio	Descripción	Fecha de modificación
Actualizaciones en los ajustes de los recursos compartidos de archivos Compatibilidad con la actualización de la caché para recursos compartidos de archivos	Las gateways de archivos 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 gateways de archivos ahora son capaces de encontrar objetos en el bucket de Amazon S3 que se han agregado o quitado después de que la gateway elaborase la última lista del contenido del bucket y almacenase en caché el resultado. Para obtener más información, consulte RefreshCache en la referencia de API.	28 de marzo de 2017
Compatibilidad con las gateways de archivos en Amazon EC2	AWSStorage Gateway ahora permite implementar una gateway de archivos en Amazon EC2. Puede lanzar una gateway de archivos en Amazon EC2 mediante Storage Gateway Amazon Machine Image (AMI) de Amazon, disponible como AMI de la comunidad. Para obtener información sobre cómo crear una gateway de archivos e implementarla en una instancia EC2, consulte Crear y activar una puerta de enlace de archivos de Amazon S3. Para obtener información sobre cómo lanzar una AMI de gateway de archivos, consulte Implementación de una gateway de archivos en un host Amazon EC2. Además, la gateway de archivos ahora admite la configuración de proxy HTTP. Para obtener más información, consulte Enrutamiento de la puerta de enlace implementada en EC2 a través de un proxy HTTP.	08 de febrero de 2017

Cambio	Descripción	Fecha de modificación
Nuevo Región de AWS	Storage Gateway ahora está disponible en la región UE (Londres) Para obtener información detallada, consulte Regiones de AWS compatibles.	13 de diciembre de 2016
Nuevo Región de AWS	Storage Gateway ahora está disponible en la región Canadá (Central) Para obtener información detallada, consulte Regiones de AWS compatibles.	08 de diciembre de 2016
Compatibilidad con las gateways de archivos	Además de la gateway de volumen y la gateway de cinta, Storage Gateway ahora ofrece File Gateway. La puerta de enlace de archivos 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

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.