



Guía del usuario de puerta de enlace de cinta

AWS Storage Gateway



Versión de API 2013-06-30

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Storage Gateway: Guía del usuario de puerta de enlace de cinta

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

.....	x
¿Qué es una puerta de enlace de cinta?	1
Gateway de cinta	1
¿Es la primera vez que utiliza Storage Gateway?	2
Funcionamiento de puerta de enlace de cinta	2
Puertas de enlace de cinta	2
Precios	5
Planee la implementación de la puerta de enlace	6
Empezar con AWS Storage Gateway	7
Inscríbase en AWS Storage Gateway	7
Regiones de AWS compatibles con Storage Gateway	8
Requisitos	8
Requisitos de hardware y almacenamiento	8
Requisitos de red y firewall	11
Hipervisores compatibles y requisitos de host	22
Compatible con iniciadores SCSI	24
Aplicaciones de copia de seguridad de terceros compatibles	25
Acceder AWS Storage Gateway	26
Uso del dispositivo de hardware	27
AWS Regiones compatibles	28
Configuración del dispositivo de hardware	28
Instalación física del dispositivo de hardware	29
Dimensiones del dispositivo de hardware	30
Configuración de parámetros de red	35
Activación del dispositivo de hardware	38
Creación de una puerta de enlace	39
Configuración de una dirección IP para la puerta de enlace	40
Configuración de la puerta de enlace	42
Eliminación de una puerta de enlace	42
Eliminación del dispositivo de hardware	43
Creación de la puerta de enlace	45
Descripción general: activación de una puerta de enlace	45
Configuración de una puerta de enlace	45
Connect to AWS	45

Revisión y activación	45
Descripción general: configuración de la puerta de enlace	46
Descripción general: recursos de almacenamiento	46
Creación de una puerta de enlace de cinta	46
Creación de una gateway	46
Creación de grupos de cintas personalizados	53
Creación de cintas	56
Uso de la puerta de enlace de cinta	62
Activación de una puerta de enlace en una nube virtual privada	153
Creación de un VPC punto final para Storage Gateway	154
Administración de la gateway	156
Administración de la puerta de enlace de cinta	156
Edición de información de la puerta de enlace	157
Adición de cintas	157
Administración de la creación automática de cintas	158
Archivado de cintas	160
Traslado de cintas a S3 Glacier Deep Archive	161
Recuperación de cintas archivadas	162
Visualizar el uso de cintas	163
Eliminación de cintas	164
Eliminación de grupos de cintas personalizados	165
Desactivación de la puerta de enlace de cinta	166
Información sobre el estado de las cintas	167
Transferir los datos a una nueva puerta de enlace	169
Trasladar cintas virtuales a una nueva puerta de enlace de cinta	170
Supervisión de Storage Gateway	175
Información acerca de las métricas de gateway	175
Dimensiones de las métricas de Storage Gateway	179
Supervisión del búfer de carga	179
Supervisión del almacenamiento en caché	182
Entender CloudWatch las alarmas	184
Crear CloudWatch las alarmas recomendadas	186
Crear una CloudWatch alarma personalizada	187
Supervisión de la puerta de enlace de cinta	189
Obtención de los registros del estado de la gateway de cinta	189
Uso de Amazon CloudWatch Metrics	191

Descripción de las métricas de cintas virtuales	192
Medición del rendimiento entre su puerta de enlace de cinta y AWS	195
Mantenimiento de la gateway	199
Como apagar la MV de la gateway	199
Inicio y detención de una puerta de enlace de cinta	200
Administración de discos locales	201
Cálculo de la cantidad de almacenamiento en disco local	201
Optimizar el rendimiento	203
Cálculo del tamaño del búfer de carga	203
Cálculo del tamaño del almacenamiento en caché	205
Adición de búfer de carga o almacenamiento en caché	205
Administración del ancho de banda	206
Cambio de la limitación controlada del ancho de banda mediante la consola de Storage Gateway	207
Programación de la limitación del ancho de banda	208
Usando el AWS SDK for Java	210
Usando el AWS SDK for .NET	212
Usando el AWS Tools for Windows PowerShell	214
Administrar las actualizaciones de la pasarela	215
Frecuencia de actualización y comportamiento esperado	216
Activa o desactiva las actualizaciones de mantenimiento	217
Modifique la programación del período de mantenimiento de la puerta de enlace	218
Realizar tareas de mantenimiento mediante la consola local	219
Realización de tareas en la consola local de la MV de	219
Realización de tareas en la consola EC2 local	239
Acceso a la consola local de la gateway	245
Configuración de adaptadores de red para la gateway	250
Eliminar tu puerta de enlace y eliminar recursos	255
Eliminación de la puerta de enlace mediante la consola de Storage Gateway	255
Eliminación de recursos de una gateway implementada on-premises	257
Eliminar recursos de una puerta de enlace implementada en una EC2 instancia de Amazon	258
Rendimiento y optimización para Tape Gateway	260
Directrices de rendimiento para las puertas de enlace de cinta	260
Optimización del rendimiento de la gateway	263
Configuración recomendada	263

Añada recursos a la gateway	264
Optimiza la configuración de TI SCSI	267
Utilice un tamaño de bloques mayor para las unidades de cinta	267
Optimice el rendimiento de las unidades de cinta virtuales	268
Añada recursos al entorno de aplicaciones	268
Uso de la VMware alta disponibilidad con Storage Gateway	269
Configure su clúster vSphere VMware de alta disponibilidad	270
Descarga de la imagen .ova de la consola de Storage Gateway	272
Implementar la gateway	272
(Opcional) Agregue opciones de anulación para otras opciones VMs del clúster	273
Activar la gateway	273
Pruebe su configuración VMware de alta disponibilidad	274
Seguridad	275
Protección de datos	276
Cifrado de datos	277
Identity and Access Management	278
Público	279
Autenticación con identidades	280
Administración de acceso mediante políticas	283
Cómo funciona AWS Storage Gateway con IAM	286
Ejemplos de políticas basadas en identidades	293
Resolución de problemas	296
Registro y supervisión	298
Información sobre Storage Gateway en CloudTrail	298
Descripción de las entradas de archivos de registro de Storage Gateway	299
Validación de conformidad	301
Resiliencia	302
Seguridad de infraestructuras	303
AWS Mejores prácticas de seguridad	303
Resolución de problemas de puertas de enlace	305
Solución de problemas: problemas de puerta de enlace sin conexión	305
Compruebe el firewall o el proxy asociados	306
Compruebe si hay una inspección continua SSL o exhaustiva del tráfico de su puerta de enlace	306
Compruebe si hay un corte de energía o un fallo de hardware en el host del hipervisor	306
Compruebe si hay problemas con un disco caché asociado	306

Solución de problemas: problemas de activación de la pasarela	307
Resuelva los errores al activar su puerta de enlace mediante un punto final público	308
Resuelva los errores al activar su puerta de enlace mediante un VPC punto de conexión de Amazon	311
Resuelva los errores al activar su puerta de enlace mediante un punto final público y haya un VPC punto final de Storage Gateway en el mismo VPC	316
Solución de problemas de puerta de enlace en las instalaciones	316
Activación AWS Support para ayudar a solucionar los problemas de su puerta de enlace ...	321
Solución de problemas de configuración de Microsoft Hyper-V	322
Solución de problemas de Amazon EC2 Gateway	327
La puerta de enlace no se ha activado poco tiempo después	328
No puedes encontrar la instancia de EC2 puerta de enlace en la lista de instancias	328
No se puede adjuntar un EBS volumen de Amazon a la instancia de EC2 gateway	329
Mensaje que indica que no hay discos disponibles al tratar de agregar volúmenes de almacenamiento	329
Cómo eliminar un disco asignado como espacio del búfer de carga para reducir la cantidad de espacio del búfer de carga	329
El rendimiento hacia o desde la EC2 puerta de enlace se reduce a cero	329
Activarlo AWS Support para ayudar a solucionar los problemas de la puerta de enlace	330
Conéctate a tu Amazon EC2 Gateway mediante la consola serie	332
Solución de problemas del dispositivo de hardware	332
Cómo determinar la dirección IP del servicio	332
Cómo restablecer la configuración de fábrica	332
Cómo realizar un reinicio remoto	332
¿Cómo obtener la DRAC asistencia de Dell i	333
Cómo encontrar el número de serie del dispositivo hardware	333
Cómo obtener soporte para el dispositivo de hardware	334
Solución de problemas con cintas virtuales	334
Recuperar una cinta virtual de una gateway no recuperable	335
Solución problemas de cintas irrecuperables	338
Notificaciones de estado de alta disponibilidad	340
Solución de problemas de alta disponibilidad	340
Notificaciones de estado	340
Métricas	342
Recuperación de datos: prácticas recomendadas	342
Recuperación de un cierre inesperado de una VM	343

Recuperación de datos a partir de una puerta de enlace o VM que no funciona correctamente	343
Recuperación de datos desde una cinta irrecuperable	344
Recuperación de datos a partir de un disco de la caché que no funciona correctamente	344
Recuperación de datos de un centro de datos inaccesible	344
Recursos adicionales	346
Implementación y configuración del host de VM de la puerta de enlace	346
Configuración VMware para Storage Gateway	347
Sincronización de la hora de la MV de la gateway	354
Implemente un EC2 host de Amazon para Tape Gateway	356
Implementación de Amazon EC2 con la configuración predeterminada	360
Modificar las opciones de metadatos de las EC2 instancias de Amazon	363
Información adicional sobre los recursos de almacenamiento de Tape Gateway	364
Retirada de discos de la gateway	364
EBSVolúmenes para gateways EC2	368
Trabajo con VTL dispositivos	369
Trabajo con cintas	374
Obtención de la clave de activación	377
Linux (curl)	378
Linux (bash/zsh)	379
Microsoft Windows PowerShell	379
Mediante la consola local	380
Conexión de los SCSI iniciadores	380
Conexión a VTL dispositivos	382
Conexión de sus volúmenes o VTL dispositivos a un cliente Linux	388
Personalización de los ajustes SCSI	390
Configuración de la autenticación CHAP	399
Uso AWS Direct Connect con Storage Gateway	408
Requisitos de puerto de red para Tape Gateway	408
Conexión a la gateway	415
Obtener una dirección IP de un EC2 host de Amazon	416
Comprensión de los recursos y los recursos IDs	417
Trabajando con un recurso IDs	418
Etiquetado de recursos	418
Trabajo con etiquetas	419
Componentes de código abierto	420

Cuotas de Storage Gateway	421
Cuotas para las cintas	421
Tamaños de disco local recomendados para la puerta de enlace	422
APIReferencia	423
Encabezados de solicitud obligatorios	423
Firmar solicitudes	426
Ejemplo de cálculo de firma	427
Respuestas de error	428
Excepciones	429
Códigos de error de operación	431
Respuestas de error	451
Operaciones	453
Historial de documentos	454
Actualizaciones anteriores	473
Notas de la versión	495

La documentación de puerta de enlace de archivo de Amazon S3 se ha trasladado a [What is Amazon S3 File Gateway?](#)

La documentación de Amazon FSx File Gateway se ha trasladado a [¿Qué es Amazon FSx File Gateway?](#)

La documentación de puerta de enlace de volumen se ha trasladado a [¿Qué es una puerta de enlace de volumen?](#)

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la versión original de inglés, prevalecerá la versión en inglés.

¿Qué es una puerta de enlace de cinta?

AWS Storage Gateway conecta un dispositivo de software local con un almacenamiento basado en la nube para proporcionar una integración perfecta con las funciones de seguridad de datos entre su entorno de TI local y la infraestructura AWS de almacenamiento. Puede utilizar el servicio para almacenar datos en Amazon Web Services Cloud para obtener un almacenamiento escalable y rentable que contribuya a mantener la seguridad de los datos.

AWS Storage Gateway ofrece soluciones de almacenamiento basadas en archivos (Amazon S3 File y Amazon FSx File), basadas en volúmenes (en caché y almacenadas) y en cinta.

Temas

- [Gateway de cinta](#)
- [¿Es la primera vez que utiliza Storage Gateway?](#)
- [Funcionamiento de puerta de enlace de cinta \(arquitectura\)](#)
- [Precios de Storage Gateway](#)
- [Planee la implementación de Storage Gateway](#)

Gateway de cinta

Puerta de enlace de cinta: una puerta de enlace de cinta proporciona almacenamiento de cinta virtual respaldado por la nube.

Con una puerta de enlace de cinta, puede archivar datos de copia de seguridad de manera económica y duradera en S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. Una puerta de enlace de cinta ofrece una infraestructura de cintas virtuales que se escala perfectamente con las necesidades empresariales y elimina la carga operativa que supone el aprovisionamiento, el escalado y el mantenimiento de una infraestructura de cintas físicas.

Puede implementar Storage Gateway de forma local como un dispositivo de máquina virtual que se ejecute en VMware ESXi un hipervisor Microsoft Hyper-V, como un dispositivo de hardware o como AWS una instancia de Amazon. KVM EC2 La puerta de enlace se implementa en una EC2 instancia para aprovisionar volúmenes de almacenamiento. SCSI AWS Puedes usar pasarelas alojadas en EC2 instancias para la recuperación ante desastres, la duplicación de datos y el almacenamiento de las aplicaciones alojadas en Amazon. EC2

Para ver información general sobre la arquitectura, consulte [Funcionamiento de puerta de enlace de cinta \(arquitectura\)](#). Para ver todos los casos de uso posibles que permite AWS Storage Gateway , consulte la [AWS Storage Gateway](#).

Documentación: para ver la documentación de puerta de enlace de cinta, consulte [Creación de una puerta de enlace de cinta](#).

¿Es la primera vez que utiliza Storage Gateway?

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:

- [Creación de una puerta de enlace de cinta](#) proporciona instrucciones sobre cómo crear y usar una puerta de enlace de cinta. Muestra cómo hacer copias de seguridad de los datos en cintas virtuales y archivar las cintas.
- [Administración de la gateway](#) describe cómo realizar tareas de administración para la puerta de enlace y sus recursos.

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

Funcionamiento de puerta de enlace de cinta (arquitectura)

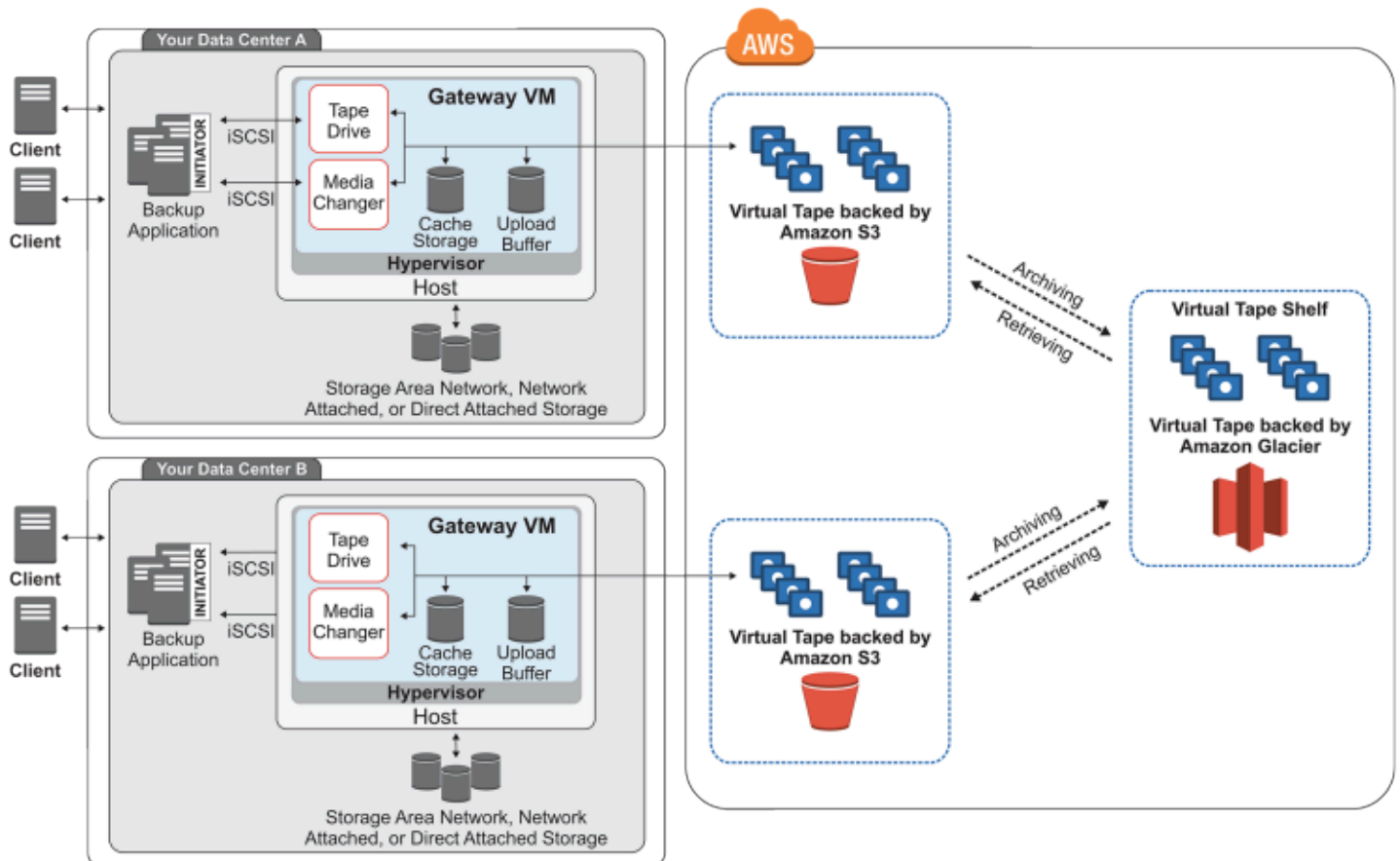
A continuación, encontrará una descripción general de la arquitectura de la solución de puerta de enlace de cinta.

Puertas de enlace de cinta

La puerta de enlace de cinta ofrece una solución duradera y económica para archivar datos en Amazon Web Services Cloud. Con su interfaz de biblioteca de cintas virtuales (VTL), puede utilizar su infraestructura de backup basada en cintas existente para almacenar datos en cartuchos de cinta virtuales que cree en su Tape Gateway. Cada puerta de enlace de cinta está preconfigurada con un

cambiador de medios y unidades de cinta. Están disponibles para las aplicaciones de backup de sus clientes existentes en forma de SCSI dispositivos i. Agregue los cartuchos de cinta que necesite para archivar los datos.

En el diagrama siguiente se proporciona información general de la implementación de la puerta de enlace de cinta.



En el diagrama se identifican los siguientes componentes de la puerta de enlace de cinta:

- **Cinta virtual:** una cinta virtual es como un cartucho de cinta física. Sin embargo, los datos de las cintas virtuales se almacenan en Amazon Web Services Cloud. Al igual que las cintas físicas, las cintas virtuales pueden estar en blanco o contener datos escritos. Puede crear cintas virtuales mediante la consola Storage Gateway o mediante programación mediante Storage Gateway. API Cada gateway puede contener hasta 1500 cintas o hasta 1 PiB de datos de cinta totales a la vez. El tamaño de cada cinta virtual, que puede configurar al crear la cinta, está entre 100 GiB y 15 TiB.
- **Biblioteca de cintas virtuales (VTL):** A VTL es como una biblioteca de cintas física disponible localmente con brazos robóticos y unidades de cinta. VTL incluye la colección de cintas virtuales almacenadas. Cada puerta de enlace de cinta viene con una VTL.

Las cintas virtuales que cree aparecen en la puerta de enlace VTL. Las cintas incluidas VTL están respaldadas por Amazon S3. A medida que el software de backup escribe datos en la puerta de enlace, la puerta de enlace almacena los datos de forma local y, a continuación, los carga de forma asíncrona en cintas virtuales de su servidor, es VTL decir, Amazon S3.

- **Unidad de cinta:** una unidad de VTL cinta es análoga a una unidad de cinta física que puede realizar operaciones de E/S y búsqueda en una cinta. Cada una VTL incluye un conjunto de 10 unidades de cinta, que están disponibles para su aplicación de respaldo en forma de dispositivos iSCSI.
- **Cambiador de soportes:** un cambiador de VTL soportes es análogo a un robot que mueve las cintas por las ranuras de almacenamiento y las unidades de cinta de una biblioteca de cintas físicas. Cada uno VTL viene con un cambiador de soportes, que está disponible para su aplicación de respaldo como un dispositivo i. SCSI
- **Archivo:** el archivo es análogo a una instalación externa donde se almacenan cintas. Puede archivar las cintas de su puerta de enlace VTL al archivo. Si es necesario, puede recuperar las cintas del archivo y devolverlas al de su puerta de enlace VTL.
- **Archivado de cintas:** cuando el software de copia de seguridad expulsa una cinta, la puerta de enlace la traslada al archivo para almacenarla a largo plazo. El archivo de almacenamiento se encuentra en la región de AWS en la que se ha activado la puerta de enlace. Las cintas del archivo se almacenan en la estantería de cintas virtual (VTS). Cuenta con el VTS respaldo de [S3 Glacier Flexible Retrieval](#) o [S3 Glacier Deep Archive](#), un servicio de almacenamiento de bajo costo para archivar datos, realizar copias de seguridad y retenerlos a largo plazo.
- **Recuperación de cintas:** las cintas archivadas no se pueden leer directamente. Para leer una cinta archivada, primero debe recuperarla en su Tape Gateway mediante la consola Storage Gateway o Storage GatewayAPI.

Important

Si archiva una cinta en S3 Glacier Flexible Retrieval, normalmente puede recuperarla en un plazo de entre 3 y 5 horas. Si archiva una cinta en S3 Glacier Deep Archive, normalmente puede recuperarla en un plazo de 12 horas.

Tras implementar y activar una puerta de enlace de cintas, debe montar las unidades de cinta virtuales y el cambiador de medios en los servidores de aplicaciones locales como dispositivos. SCSI Puede crear cintas virtuales según sea necesario. A continuación, puede utilizar la aplicación de

software de copia de seguridad existente para escribir datos en las cintas virtuales. El cambiador de medios carga y descarga las cintas virtuales en las unidades de cinta virtuales para realizar operaciones de lectura y escritura.

Asignación de discos locales para la VM de la puerta de enlace

La máquina virtual de la gateway necesita discos locales, que deberá asignar para los siguientes fines:

- **Almacenamiento en caché:** el almacenamiento en caché funciona como un almacén permanente para los datos que están a la espera de cargarse desde el búfer de carga en Amazon S3.

Si su aplicación lee datos de una cinta virtual, la gateway guarda los datos en el almacenamiento en caché. La gateway almacena datos a los que se ha tenido acceso recientemente en el almacenamiento en caché para un acceso de baja latencia. Si la aplicación solicita datos en cinta, la puerta de enlace comprueba primero los datos en el almacenamiento en caché antes de descargarlos. AWS

- **Búfer de carga:** el búfer de carga proporciona un espacio provisional para la puerta de enlace antes de cargar los datos en una cinta virtual. El búfer de carga también es muy importante para la creación de puntos de recuperación que puede utilizar para recuperar cintas de errores inesperados. Para obtener más información, consulte [Necesita recuperar una cinta virtual desde una puerta de enlace de cinta que no funciona correctamente](#).

Cuando la aplicación de copia de seguridad escribe datos en la gateway, esta copia los datos en el almacenamiento en caché y en el búfer de carga. A continuación, confirma que se ha completado la operación de escritura en la aplicación de copia de seguridad.

Para obtener instrucciones sobre la cantidad de espacio de disco que debe asignar para el almacenamiento en caché y el búfer de carga, consulte [Cálculo de la cantidad de almacenamiento en disco local](#).

Precios de Storage Gateway

Para obtener información actualizada sobre los precios, consulte los [precios](#) en la página de AWS Storage Gateway detalles.

Planee la implementación de Storage Gateway

Con el dispositivo de software Storage Gateway, puede conectar su infraestructura de aplicaciones local existente con un almacenamiento en la AWS nube escalable y rentable que proporciona funciones de seguridad de datos.

Para implementar Storage Gateway, primero debe decidir sobre estas dos cosas:

1. El tipo de puerta de enlace: en esta guía se describen los siguientes tipos de puerta de enlace:
 - Puerta de enlace de cinta: si busca una alternativa económica, duradera, a largo plazo y fuera de las instalaciones para archivar datos, implemente una puerta de enlace de cinta. Con su interfaz de biblioteca de cintas virtuales (VTL), puede utilizar su infraestructura de software de backup basada en cintas existente para almacenar datos en cartuchos de cinta virtuales que cree. Para obtener más información, consulte [Aplicaciones de copia de seguridad de terceros compatibles con una puerta de enlace de cinta](#). Al archivar cintas, no hay que preocuparse por la administración de las cintas localmente ni por organizar envíos de cintas fuera de las instalaciones. Para obtener una descripción general de la arquitectura, consulte [Funcionamiento de puerta de enlace de cinta \(arquitectura\)](#).
2. Opción de alojamiento: puede ejecutar Storage Gateway de forma local como un dispositivo de máquina virtual o un dispositivo de hardware, o AWS como una EC2 instancia de Amazon. Para obtener más información, consulte [Requisitos para configurar Tape Gateway](#). Si tu centro de datos se desconecta y no tienes un host disponible, puedes implementar una puerta de enlace en una EC2 instancia. Storage Gateway proporciona una Amazon Machine Image (AMI) que contiene la imagen de máquina virtual de la puerta de enlace.

Además, cuando configure un host para implementar un dispositivo de software de gateway, debe asignar suficiente almacenamiento para la máquina virtual de la gateway.

Antes de continuar con el paso siguiente, asegúrese de que ha hecho lo siguiente:

1. Para una puerta de enlace implementada en las instalaciones, debe elegir el tipo de host de VM y configurarlo. Sus opciones son VMware ESXi Hypervisor, Microsoft Hyper-V y Máquina virtual basada en el núcleo de Linux (). KVM Si implementa la gateway detrás de un firewall, asegúrese de que los puertos estén accesibles a la máquina virtual de la gateway. Para obtener más información, consulte [Requisitos para configurar Tape Gateway](#).
2. Instale el software de copia de seguridad del cliente. Para obtener más información, consulte [Aplicaciones de copia de seguridad de terceros compatibles con una puerta de enlace de cinta](#).

Empezar con AWS Storage Gateway

En esta sección, encontrará instrucciones sobre cómo comenzar a utilizar Storage Gateway. Para empezar, primero debe registrarse en AWS. Si es la primera vez que lo utiliza, le recomendamos que lea las secciones sobre regiones y requisitos.

Temas

- [Inscríbase en AWS Storage Gateway](#)
- [Regiones de AWS compatibles con Storage Gateway](#)
- [Requisitos para configurar Tape Gateway](#)
- [Acceder AWS Storage Gateway](#)

Inscríbase en AWS Storage Gateway

Para utilizar Storage Gateway, se requiere una cuenta de Amazon Web Services, que proporciona acceso a todos los recursos, foros, servicios de soporte e informes de uso de AWS. No se le cobrará ninguno de los servicios si no los utiliza. Si ya tiene una cuenta de Amazon Web Services, puede omitir este paso.

Para inscribirse en una cuenta de Amazon Web Services

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

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

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

Para obtener información sobre los precios, consulte [Precios](#) en la página de información detallada de Storage Gateway.

Regiones de AWS compatibles con Storage Gateway

Storage Gateway almacena datos de volumen, instantáneas, cintas y archivos en la AWS región en la que está activada la puerta de enlace. Los datos de los archivos se almacenan en la AWS región en la que se encuentra el bucket de Amazon S3. Seleccione una AWS región en la parte superior derecha de la consola de administración de Storage Gateway antes de empezar a implementar la puerta de enlace.

- Storage Gateway: para ver AWS las regiones compatibles y una lista de los puntos de enlace de AWS servicio que puede usar con Storage Gateway, consulte [AWS Storage Gateway Puntos de conexión y cuotas](#) en. Referencia general de AWS
- Dispositivo de hardware Storage Gateway: para conocer AWS las regiones compatibles que puede utilizar con el dispositivo de hardware, consulte [las regiones del dispositivo de AWS Storage Gateway hardware](#) en. Referencia general de AWS

Requisitos para configurar Tape Gateway

A menos que se especifique lo contrario, los siguientes requisitos son comunes a todas las configuraciones de gateway.

Temas

- [Requisitos de hardware y almacenamiento](#)
- [Requisitos de red y firewall](#)
- [Hipervisores compatibles y requisitos de host](#)
- [Compatible con SCSI iniciadores](#)
- [Aplicaciones de copia de seguridad de terceros compatibles con una puerta de enlace de cinta](#)

Requisitos de hardware y almacenamiento

En esta sección se describen los requisitos mínimos de hardware y la configuración de la puerta de enlace y la cantidad mínima de espacio en disco que se debe asignar para el almacenamiento necesario.

Requisitos de hardware para VMs

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

- Cuatro procesadores virtuales asignados a la MV.
- Para Tape Gateway, su hardware debe dedicar las siguientes cantidades de RAM:
 - 16 GiB de reserva RAM para pasarelas con un tamaño de caché de hasta 16 TiB
 - 32 GiB de reserva RAM para pasarelas con un tamaño de caché de 16 TiB a 32 TiB
 - 48 GiB de reserva RAM para pasarelas con un tamaño de caché de 32 TiB a 64 TiB
- 80 GiB de espacio de disco para la instalación de los datos del sistema y la imagen de la máquina virtual.

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 [AWS Storage Gateway cuotas](#).

Requisitos para los tipos de EC2 instancias de Amazon

Al implementar la puerta de enlace en Amazon Elastic Compute Cloud (AmazonEC2), el tamaño de la instancia debe ser al menos xlarge para que la puerta de enlace funcione. Sin embargo, para la familia de instancias optimizadas para computación, el tamaño debe ser como mínimo 2xlarge.

En el caso de Tape Gateway, la EC2 instancia de Amazon debe dedicar las siguientes cantidades en RAM función del tamaño de la caché que vaya a utilizar para la puerta de enlace:

- 16 GiB de reserva RAM para pasarelas con un tamaño de caché de hasta 16 TiB
- 32 GiB de reserva RAM para pasarelas con un tamaño de caché de 16 TiB a 32 TiB
- 48 GiB de reserva RAM para pasarelas con un tamaño de caché de 32 TiB a 64 TiB

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

Recomendadas para los volúmenes en caché y los tipos de puerta de enlace de cinta

- Familia de instancias de uso general: tipo de instancia m4, m5 o m6.

Note

No recomendamos utilizar el tipo de instancia m4.16xlarge.

- Familia de instancias optimizadas para la computación: tipos de instancia c4, c5 o c6. Elija un tamaño de instancia de 2 veces grande o superior para cumplir con los requisitos requeridos. RAM
- Familia de instancias optimizadas para memoria: tipos de instancia r3, r5 o r6.
- Familia de instancias optimizadas para el almacenamiento: tipos de instancia i3 o i4.

Requisitos de almacenamiento

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

En la siguiente tabla se recomiendan los tamaños para el almacenamiento en disco local de gateway implementada.

Tipo de gateway	Caché (mínimo)	Caché (máximo)	Búfer de carga (mínimo)	Búfer de carga (máximo)	Otros discos locales necesarios
Gateway de cinta	150 GiB	64 TiB	150 GiB	2 TiB	—

Note

Puede configurar una o más unidades locales para la memoria caché y el búfer de carga hasta la capacidad máxima.

Al añadir caché o búfer de carga a una puerta de enlace existente, es importante crear nuevos discos en el host (hipervisor o EC2 instancia de Amazon). No cambie el tamaño de los discos si se han asignado previamente como caché o como búfer de carga.

Para obtener información acerca de las cuotas de gateway, consulte [AWS Storage Gateway cuotas](#).

Requisitos de red y firewall

La puerta de enlace requiere acceso a Internet, a las redes locales, a los servidores del Servicio de Nombres de Dominio (DNS), a los firewalls, a los enrutadores, etc. A continuación, puede encontrar información sobre los puertos necesarios y cómo permitir el acceso a través de firewalls y routers.

Note

En algunos casos, puede implementar Storage Gateway en Amazon EC2 o usar otros tipos de implementación (incluida la implementación local) con políticas de seguridad de red que restrinjan los rangos de direcciones AWS IP. En estos casos, es posible que la puerta de enlace experimente problemas de conectividad del servicio cuando cambien los valores del rango de AWS IP. Los valores del rango de direcciones AWS IP que debes usar se encuentran en el subconjunto de servicios de Amazon de la AWS región en la que activas tu puerta de enlace. Para obtener los valores actuales de rango de IP, consulte [AWS Rangos de direcciones IP de](#) en la Referencia general de AWS.

Note

Los requisitos de ancho de banda de la red varían en función de la cantidad de datos que carga y descarga la puerta de enlace. Se requiere un mínimo de 100 Mbps para descargar, activar y actualizar correctamente la puerta de enlace. Sus patrones de transferencia de datos determinarán el ancho de banda necesario para soportar su carga de trabajo. En algunos casos, puede implementar Storage Gateway en Amazon EC2 o usar otros tipos de implementación

Temas

- [Requisitos de los puertos](#)
- [Requisitos de red y firewall para el dispositivo de hardware de Storage Gateway](#)
- [Permitir el AWS Storage Gateway acceso a través de firewalls y enrutadores](#)
- [Configuración de grupos de seguridad para su instancia de Amazon EC2 Gateway](#)

Requisitos de los puertos

Storage Gateway requiere que se permita el funcionamiento de determinados puertos. 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 puerto de red para Tape Gateway](#).

Puertos comunes para todos los tipos de gateway

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

Protocolo	Puerto	Dirección	Origen	Destino	Cómo se utiliza
TCP	43 (HTTPS)	Salida	Storage Gateway	AWS	Para la comunicación entre Storage Gateway y el punto final del AWS servicio. Para obtener más información acerca de los puntos de enlace de servicio, consulte Permitir el AWS Storage Gateway acceso a través de firewalls y enrutadores .

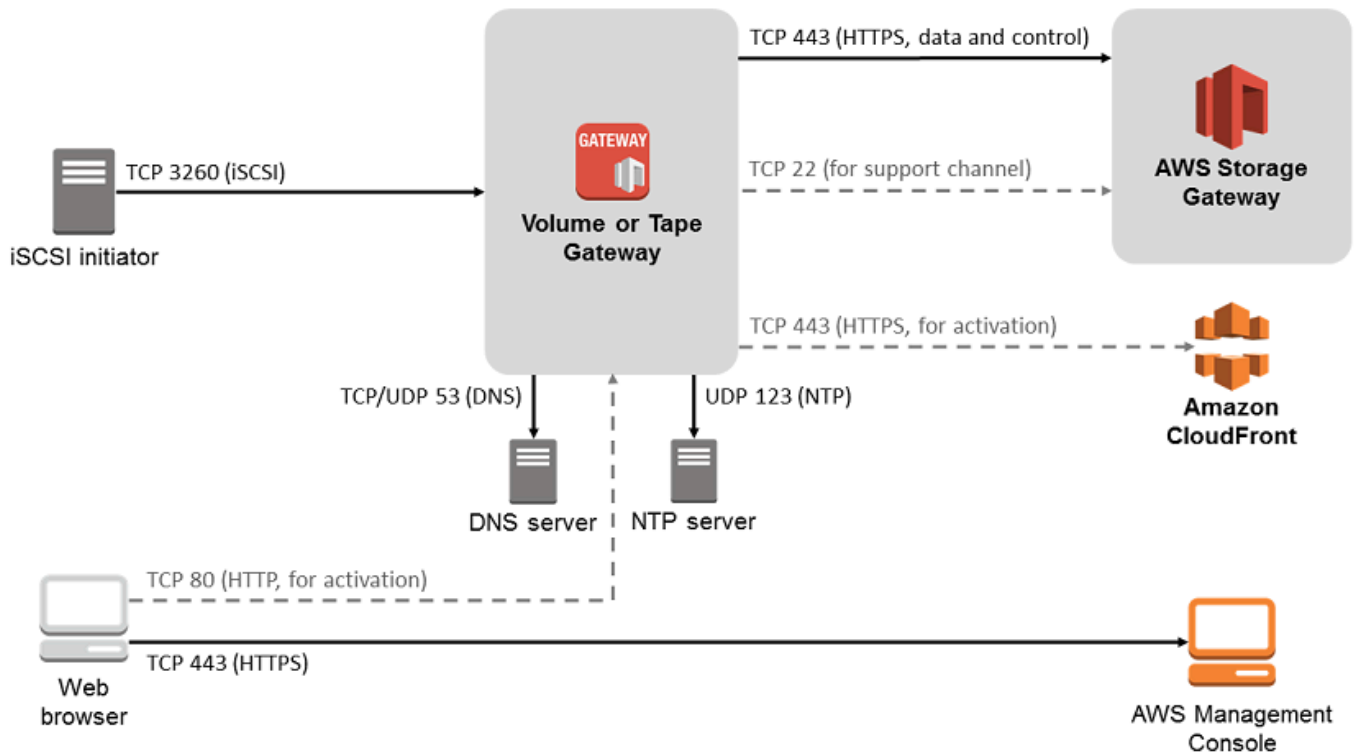
Protocolo	Puerto	Dirección	Origen	Destino	Cómo se utiliza
TCP	80 (HTTP)	Entrada	El host desde el que se conecta a la consola AWS de administración.	Storage Gateway	<p>Por los sistemas locales para obtener la clave de activación de Storage Gateway. El puerto 80 solo se utiliza durante la activación del dispositivo de Storage Gateway.</p> <p>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 puerta de enlace desde la consola de administr</p>

Protocolo	Puerto	Dirección	Origen	Destino	Cómo se utiliza
					ación de Storage Gateway, el host desde el que se conecta a la consola debe tener acceso al puerto 80 de la puerta de enlace.
TCP/UDP	53 (DNS)	Salida	Storage Gateway	Servidor del Servicio de nombres de dominio (DNS)	Para la comunicación entre Storage Gateway y el DNS servidor.

Protocolo	Puerto	Dirección	Origen	Destino	Cómo se utiliza
TCP	22 (canal de soporte)	Salida	Storage Gateway	AWS Support	Permite acceder AWS Support a su puerta de enlace para ayudarlo a solucionar los problemas de la puerta de enlace. No necesita este puerto abierto para el funcionamiento normal de la gateway, pero se exige para la solución de problemas.
UDP	123 (NTP)	Salida	NTPcliente	NTPservidor	Lo utilizan los sistemas locales para sincronizar la hora de la VM con la hora del host.

Puertos para puertas de enlace de volumen y de cinta

En la siguiente ilustración se muestran los puertos que se deben abrir para la puerta de enlace de cinta.



Además de los comunes, la puerta de enlace de cinta requiere el siguiente puerto.

Protocolo	Puerto	Dirección	Origen	Destino	Cómo se utiliza
TCP	3260 (iSCSI)	Entrada	i Inicadores SCSI	Storage Gateway	Mediante sistemas locales para conectarse a los SCSI objetivos expuestos por la puerta de enlace.

Para obtener información detallada sobre los requisitos de los puertos, consulte [Requisitos de puerto de red para Tape Gateway](#) en la sección Recursos adicionales de Storage Gateway.

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

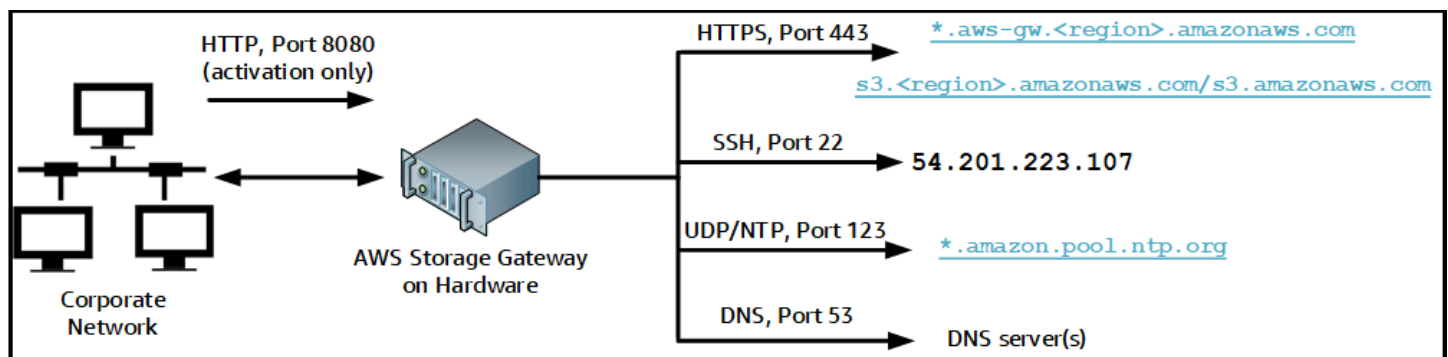
Cada dispositivo de hardware de Storage Gateway requiere los siguientes servicios de red:

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

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

1. i DRAC
2. em1
3. em2
4. em3
5. em4

Puede utilizar el DRAC puerto i para la administración remota del servidor.



Un dispositivo de hardware requiere los siguientes puertos para funcionar.

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

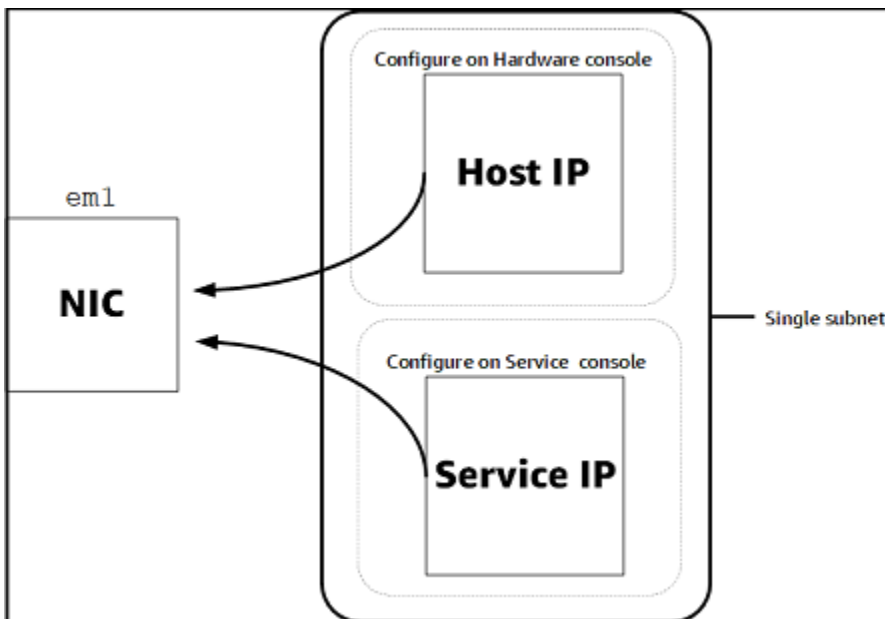
Para rendir de acuerdo con el diseño, un dispositivo de hardware requiere que la configuración de red y de firewall sea como se indica a continuación:

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

Note

Para ver una ilustración que muestra la parte posterior del servidor con sus puertos, consulte [Instalación física del dispositivo de hardware](#)

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



Para obtener más información acerca de la activación y la configuración de un dispositivo de hardware, consulte [Uso del dispositivo de hardware de Storage Gateway](#).

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

Su puerta de enlace requiere acceso a los siguientes puntos finales del servicio para poder comunicarse con ellos. AWS Si utiliza un firewall o un router para filtrar o limitar el tráfico de red, debe configurar el firewall y el router para dar permiso a los puntos de conexión de servicio para mantener comunicaciones de salida con AWS.

Note

Si configura VPC puntos de conexión privados para que Storage Gateway los utilice para la conexión y la transferencia de datos desde y hacia AWS, su puerta de enlace no requiere

acceso a la Internet pública. Para obtener más información, consulte [Activación de una puerta de enlace en una nube virtual privada](#).

 Important

En función de la AWS región de su puerta de enlace, sustitúyala *region* en el punto final del servicio con la cadena de región correcta.

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

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

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

```
anon-cp.storagegateway.region.amazonaws.com:443  
client-cp.storagegateway.region.amazonaws.com:443  
proxy-app.storagegateway.region.amazonaws.com:443  
dp-1.storagegateway.region.amazonaws.com:443
```

Se requiere el siguiente punto final del servicio de puerta de enlace para realizar API llamadas.

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

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


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

El punto de conexión de servicio de Amazon S3, que se muestra a continuación, únicamente lo utilizan las puertas de enlace de archivo. Una puerta de enlace de archivo requiere este punto de conexión para obtener acceso al bucket S3 al que se asigna un recurso compartido de archivos.

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

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

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

 Note

Si su puerta de enlace no puede determinar la AWS región en la que se encuentra su depósito de S3, este punto de enlace de servicio se establece de forma predeterminada. `s3.us-east-1.amazonaws.com` Le recomendamos que permita el acceso a la región Este de EE. UU. (Norte de Virginia) (us-east-1), además de a las regiones de AWS en las que se active su puerta de enlace y en las que se encuentre el bucket de S3.

Los siguientes son los puntos de enlace de servicio de S3 para las regiones AWS GovCloud (US) .

```
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 FIPS de servicio para un bucket de S3 en la región AWS GovCloud (EE. UU. Oeste).

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

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

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

- Storage Gateway: para ver AWS las regiones compatibles y una lista de los puntos de enlace de AWS servicio que puede usar con Storage Gateway, consulte los [AWS Storage Gateway puntos de enlace y las cuotas](#) en. Referencia general de AWS

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

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

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

- El grupo de seguridad no debe permitir conexiones entrantes procedentes de Internet. Solamente debe permitir que se comuniquen con la gateway las instancias que se encuentren dentro del grupo de seguridad de la gateway. Si necesitas permitir que las instancias se conecten a la puerta de enlace desde fuera de su grupo de seguridad, te recomendamos que permitas las conexiones solo en los puertos 3260 (para SCSI las conexiones i) y 80 (para la activación).
- Si quieres activar tu puerta de enlace desde un EC2 host de Amazon ajeno al grupo de seguridad de la puerta de enlace, permite las conexiones entrantes en el puerto 80 desde la dirección IP de ese host. Si no puede determinar la dirección IP del host de activación, puede abrir el puerto 80, activar la gateway y, a continuación, cerrar el acceso en el puerto 80 tras completar la activación.
- Permita el acceso al puerto 22 solo si lo utiliza AWS Support para solucionar problemas. Para obtener más información, consulte [¿Desea ayudar AWS Support a solucionar los problemas de su puerta de enlace EC2?](#)

En algunos casos, puedes usar una EC2 instancia de Amazon como iniciador (es decir, para conectarte a SCSI destinos i) en una puerta de enlace que hayas implementado en AmazonEC2. 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 puerto de red para Tape Gateway](#).

Hipervisores compatibles y requisitos de host


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

 Note

Cuando un fabricante ponga fin a la compatibilidad general con una versión del hipervisor, Storage Gateway también lo hará. Para obtener información detallada sobre la compatibilidad con versiones específicas de un hipervisor, consulte la documentación del fabricante.

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

- VMware ESXi Hipervisor (versión 7.0 u 8.0): para esta configuración, también necesita un VMware vSphere cliente para conectarse al host.
- Microsoft Hyper-V Hypervisor (2012 R2, 2016, 2019 o 2022): hay una versión gratuita independiente de Hyper-V disponible en el [Centro de descarga de Microsoft](#). Para esta configuración, necesitará Microsoft Hyper-V Manager en un equipo cliente Microsoft Windows para conectarse al host.
- Máquina virtual basada en el núcleo de Linux (KVM): una tecnología de virtualización gratuita y de código abierto. KVM se incluye en todas las versiones de Linux 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 KVM entorno en funcionamiento y ya está familiarizado con su funcionamiento. KVM
- EC2 Instancia de Amazon: Storage Gateway proporciona una imagen de máquina de Amazon (AMI) que contiene la imagen de máquina virtual de la puerta de enlace. Solo los tipos de archivos, volúmenes en caché y Tape Gateway se pueden implementar en Amazon EC2. Para obtener información sobre cómo implementar una puerta de enlace en Amazon EC2, consulte [Implementación de una EC2 instancia de Amazon para alojar su Tape Gateway](#).
- Dispositivo de hardware de Storage Gateway: Storage Gateway proporciona un dispositivo de hardware físico como opción de implementación en las instalaciones para ubicaciones con una infraestructura de máquina virtual limitada.

 Note

Storage Gateway no admite la recuperación de una puerta de enlace de una máquina virtual que se creó a partir de una instantánea o un clon de otra máquina virtual de puerta de enlace o de Amazon EC2 AMI. Si la MV de la gateway no funciona correctamente, active una nueva

gateway y recupere los datos para esa gateway. Para obtener más información, consulte [Recuperación de un cierre inesperado de una máquina virtual](#).

Storage Gateway no es compatible con la memoria dinámica ni con la asignación dinámica (ballooning) de memoria virtual.

Compatible con SCSI iniciadores

Al implementar una puerta de enlace de cinta, la puerta de enlace está preconfigurada con un cambiador de medios y 10 unidades de cinta. Estas unidades de cinta y el cambiador de medios están disponibles para las aplicaciones de backup de sus clientes existentes en forma de dispositivos i. SCSI

Para conectarse a estos SCSI dispositivos i, Storage Gateway admite los siguientes SCSI iniciadores i:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows 10
- Windows 8.1
- Red Hat Enterprise Linux 5
- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7
- VMwareESXInitiator, que ofrece una alternativa al uso de iniciadores en los sistemas operativos invitados de su VMs

Important


Storage Gateway no admite Microsoft Multipath I/O (MPIO) desde clientes Windows. Storage Gateway admite la conexión de varios hosts al mismo volumen si los hosts coordinan el acceso mediante el clúster de conmutación por error de Windows Server (WSFC). Sin embargo, no puede conectar varios hosts al mismo volumen (por ejemplo, si comparten un sistema de archivos NTFS /ext4 que no esté agrupado en clústeres) sin usar WSFC

Aplicaciones de copia de seguridad de terceros compatibles con una puerta de enlace de cinta

Utilice una aplicación de copia de seguridad para leer, escribir y administrar cintas con una puerta de enlace de cinta. Las siguientes aplicaciones de copia de seguridad de terceros son compatibles con las puertas de enlace de cinta.

El tipo de cambiador de medio que elija depende de la aplicación de copia de seguridad que vaya a utilizar. En la siguiente tabla se enumeran las aplicaciones de copia de seguridad de terceros que se han probado y que han demostrado ser compatibles con puertas de enlace de cinta. Esta tabla incluye el tipo de cambiador de medio recomendado para cada aplicación de copia de seguridad.

Aplicación de copia de seguridad	Tipo de cambiador de medio
Backup Arcserve	AWS-Gateway-VTL
Bacula Enterprise V10.x	AWS-Gateway-VTL o STK-L700
Commvault V11	STK-L700
Dell 19.5 EMC NetWorker	AWS-Gateway-VTL
IBMSpectrum Protect v8.1.10	IBM-03584L32-0402
Protector de datos Micro Focus (HPE) 9 o 11.x	AWS-Gateway-VTL
Microsoft System Center 2012 R2 o 2016 Data Protection Manager	STK-L700
NovaStor DataCenter/Network 6.4 o 7.1	STK-L700
Quest NetVault Backup 12.4 o 13.x	STK-L700
Veeam Backup & Replication 11A	AWS-Gateway-VTL
Veritas Backup Exec 2014, 15, 16, 20 o 22.x	AWS-Gateway-VTL
Veritas Backup Exec 2012	STK-L700

Aplicación de copia de seguridad	Tipo de cambiador de medio
<p> Note</p> <p>Veritas ha finalizado el soporte para Backup Exec 2012.</p>	
Veritas, NetBackup versión 7.x u 8.x	AWS-Gateway-VTL

Important

Le recomendamos encarecidamente que elija el cambiador de medio que aparece en la lista para su aplicación de copia de seguridad. Es posible que otros cambiadores de medio no funcionen correctamente. Una vez que la puerta de enlace está activada, puede elegir otro tipo de cambiador de medio. Para obtener más información, consulte [Selección de un cambiador de medios después de activar la puerta de enlace](#).

Acceder AWS Storage Gateway

Puede utilizar la [consola de administración de Storage Gateway](#) para 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.

Para permitir el acceso del navegador a la consola de Storage Gateway, asegúrese de que el navegador tenga acceso al API punto final de Storage Gateway. Para obtener más información, consulte [Puntos de conexión y cuotas de Storage Gateway](#) en la Referencia general de AWS .

Además, puede utilizarla AWS Storage Gateway API para configurar y administrar sus puertas de enlace mediante programación. Para obtener más información acerca de, consulte. API [APIReferencia para Storage Gateway](#)

También puede utilizarla AWS SDKs para desarrollar aplicaciones que interactúen con Storage Gateway. El AWS SDKs para Java,. NETy PHP empaquetar el Storage Gateway subyacente API para simplificar las tareas de programación. Para obtener información sobre la descarga de las SDK bibliotecas, consulte [Ejemplos de bibliotecas de códigos](#).

Uso del dispositivo de hardware de Storage Gateway

El dispositivo de hardware de Storage Gateway es un dispositivo de hardware físico con el software Storage Gateway preinstalado en una configuración de servidor validada. Puede administrar los dispositivos de hardware desde la página Información general sobre el dispositivo de hardware de la consola de AWS Storage Gateway .

El dispositivo de hardware es un servidor 1U de alto rendimiento que puede implementar en su centro de datos o en las instalaciones, dentro de su firewall corporativo. Cuando active el dispositivo de hardware, el proceso de activación asocia su dispositivo de hardware a su cuenta de Amazon Web Services. Después de la activación, el dispositivo de hardware aparece en la consola como una puerta de enlace en la página Información general sobre el dispositivo de hardware. Puede configurar el dispositivo de hardware como una puerta de enlace de archivo, una puerta de enlace de cinta o una puerta de enlace 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.

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

Temas

- [AWS Regiones compatibles](#)
- [Configuración del dispositivo de hardware](#)
- [Instalación física del dispositivo de hardware](#)
- [Configuración de parámetros de red](#)
- [Activación del dispositivo de hardware](#)
- [Creación de una puerta de enlace](#)
- [Configuración de una dirección IP para la puerta de enlace](#)
- [Configuración de la puerta de enlace](#)
- [Eliminación de una puerta de enlace del dispositivo de hardware](#)
- [Eliminación del dispositivo de hardware](#)

AWS Regiones compatibles

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

Configuración del dispositivo de hardware

Tras recibir el dispositivo de hardware Storage Gateway, utiliza la consola del dispositivo de hardware para configurar las redes a fin de proporcionar una conexión permanente AWS y activar el dispositivo. La activación asocia su dispositivo a la cuenta de Amazon Web Services que ha utilizado durante el proceso de activación. Después de la activación del dispositivo, puede lanzar un archivo, volumen o la puerta de enlace de cinta desde la consola de Storage Gateway.

Note

Es su responsabilidad asegurarse de que el firmware del dispositivo de hardware lo sea. up-to-date

Para instalar y configurar su dispositivo de hardware

1. Monte el bastidor del dispositivo y conecte la alimentación y las conexiones de red. Para obtener más información, consulte [Instalación física del dispositivo de hardware](#).
2. Establezca las direcciones del Protocolo de Internet versión 4 (IPv4) tanto para el dispositivo de hardware (el host) como para Storage Gateway (el servicio). Para obtener más información, consulte [Configuración de parámetros de red](#).
3. Active el dispositivo de hardware en la página de información general del dispositivo de hardware de la consola en la AWS región que elija. Para obtener más información, consulte [Activación del dispositivo de hardware](#).
4. Instale Storage Gateway en su dispositivo de hardware. Para obtener más información, consulte [Configuración de la puerta de enlace](#).

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

Como aumentar el almacenamiento en caché utilizable

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

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

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

Opciones de tarjeta interfaz de red

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

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

Instalación física del dispositivo de hardware

Cuando abra el dispositivo de hardware de Storage Gateway, siga las instrucciones que se encuentran en la caja para montar el servidor en un bastidor. Su electrodoméstico tiene un formato de 1U y cabe en un rack de 19 pulgadas estándar que cumple con las normas de la Comisión Electrotécnica Internacional (IEC).

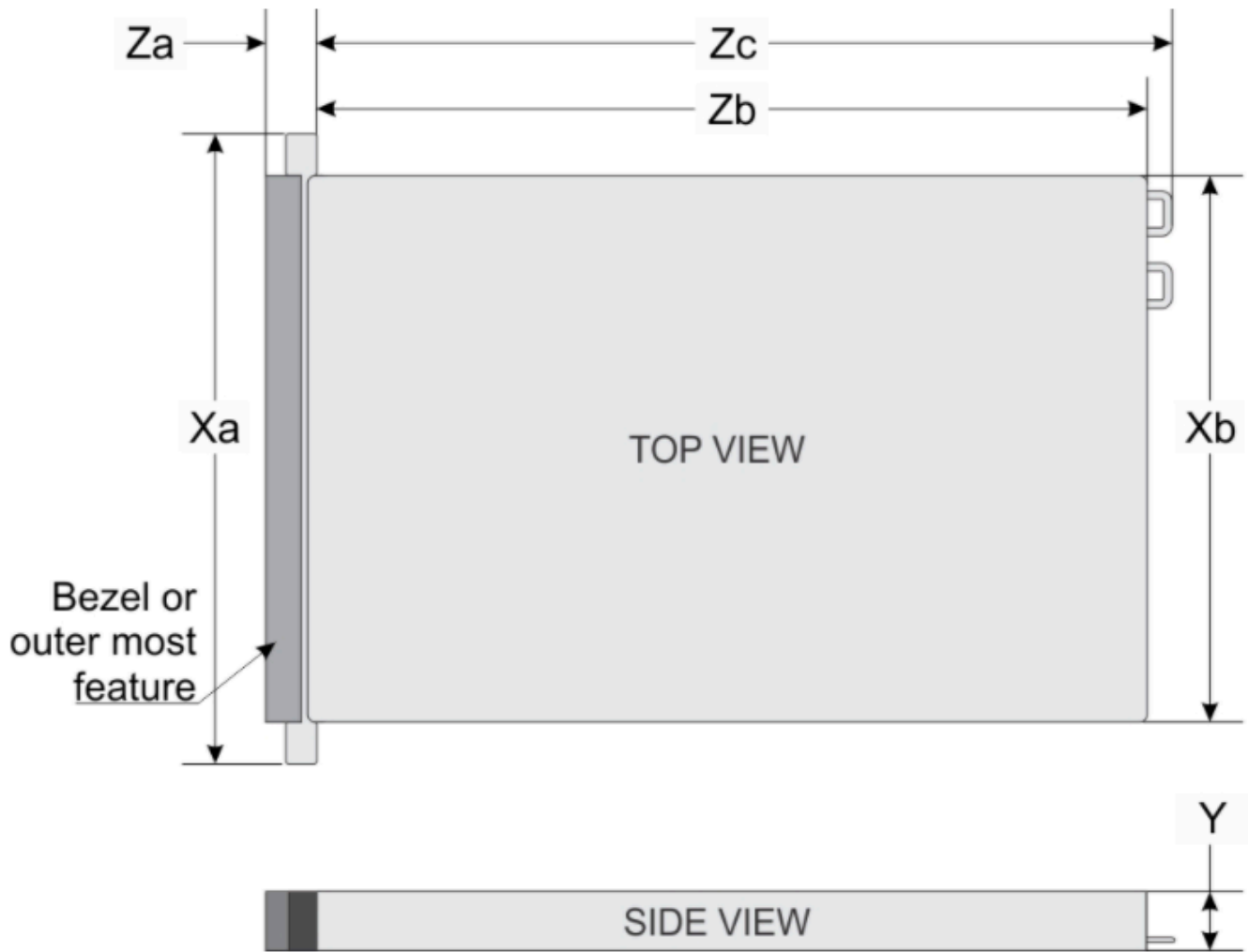
Para instalar su dispositivo de hardware, necesita los siguientes componentes:

- Cables de alimentación: se necesita uno pero se recomienda tener dos.

- Cableado de red compatible (en función de la tarjeta de interfaz de red (NIC) que se incluya en el dispositivo de hardware). Módulo óptico Twinax Copper DAC SFP + (compatible con Intel) o transceptor de cobre SFP Base-T.
- Solución de conmutación de teclado y monitor o teclado, vídeo y ratón (). KVM

Dimensiones del dispositivo de hardware

dimensiones del dispositivo de hardware, incluidos los soportes de montaje y el bisel.



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)

dimensiones del dispositivo de hardware, incluidos los soportes de montaje y el bisel.

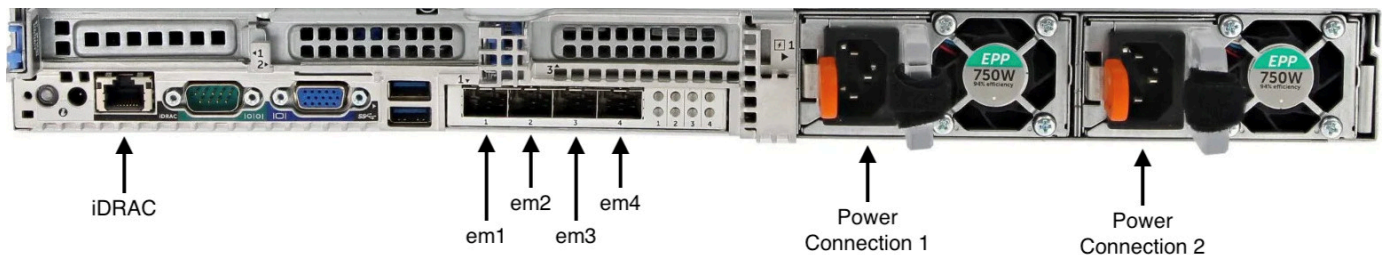
Para conectar el dispositivo de hardware a la alimentación

Note

Antes de realizar el siguiente procedimiento, asegúrese de que cumple todos los requisitos del dispositivo de hardware de Storage Gateway como se describe en [Requisitos de red y firewall para el dispositivo de hardware de 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. parte trasera del dispositivo de hardware con etiquetas de conectores de red y alimentación.



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

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 admite el VLAN enlace troncal. Configure el puerto del conmutador al que va a conectar el dispositivo de hardware como un puerto no troncalVLAN.

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



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

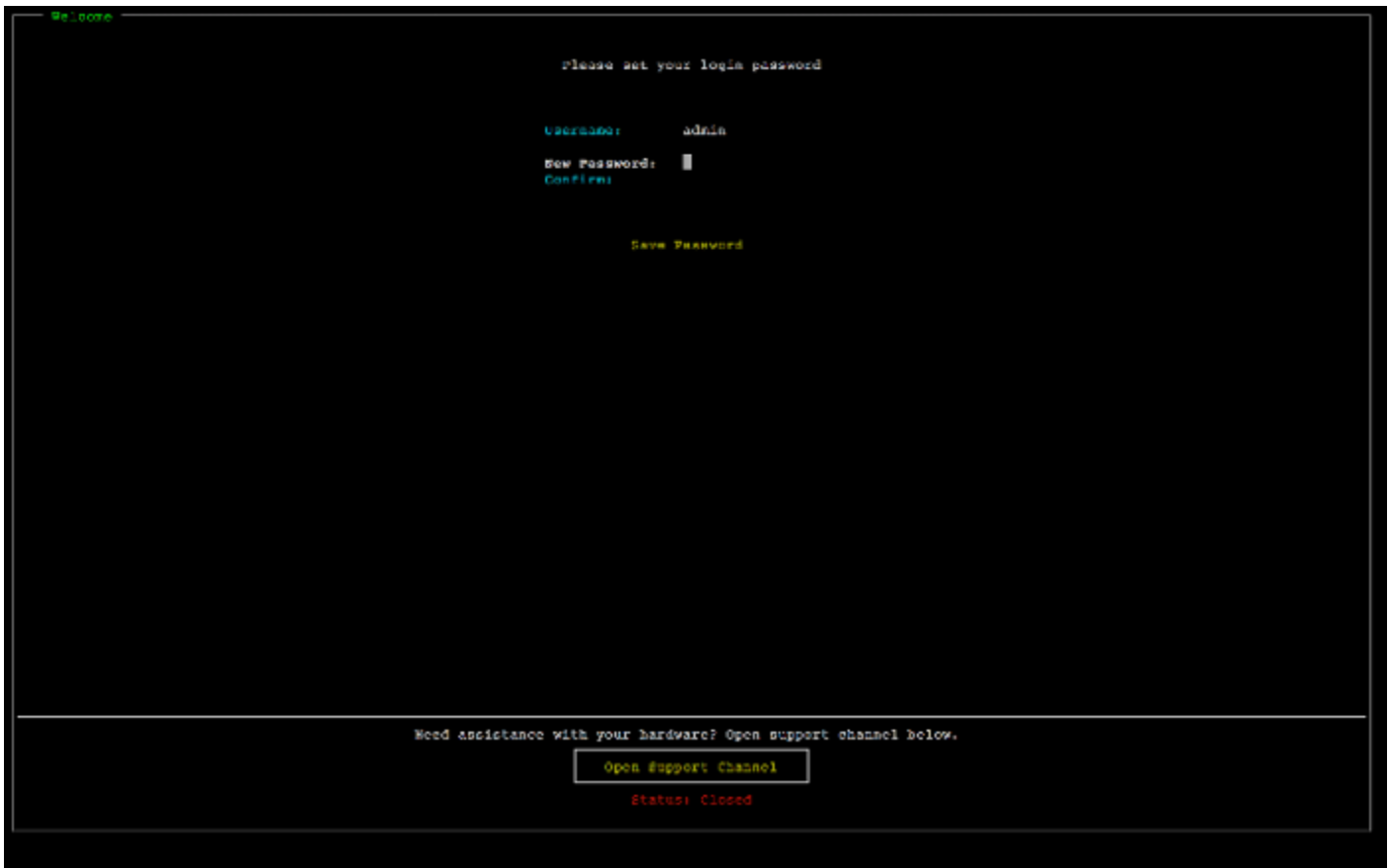
Después de que el servidor se inicie, la consola de hardware aparecerá en el monitor. La consola de hardware presenta una interfaz de usuario específica AWS que puede utilizar para configurar los parámetros de red iniciales. Puede configurar estos parámetros para conectar el dispositivo a AWS y abrir un canal de soporte para la solución de problemas del servicio técnico de Amazon Web Services.

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.

pantalla de diálogo de configuración de contraseña de la consola del dispositivo de hardware.



pantalla de diálogo de configuración de contraseña de la consola del dispositivo de hardware.

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

menú principal de la consola del dispositivo de hardware que muestra las conexiones y las opciones del menú.



menú principal de la consola del dispositivo de hardware que muestra las conexiones y las opciones del menú.

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 [Instalación física del dispositivo de hardware](#).

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 a AWS.

Para establecer una dirección de red

1. Seleccione **Configure Network** y pulse la tecla **Enter**. La pantalla **Configure Network** aparece a continuación.
pantalla de configuración de red de la consola del dispositivo de hardware.



pantalla de configuración de red de la consola del dispositivo de hardware.

2. Para la dirección IP, introduzca una IPv4 dirección válida de una de las siguientes fuentes:
 - Utilice la IPv4 dirección asignada por el servidor del Protocolo de configuración dinámica de host (DHCP) al puerto de red físico.

Si lo hace, anote esta IPv4 dirección para usarla más adelante en el paso de activación.

- Asigne una IPv4 dirección 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.

Tras introducir una IPv4 dirección válida, pulse la tecla `Down arrow` o `Tab`.

Note

Puede usar este procedimiento para configurar otras interfaces de red además de la em1 para obtener redundancia. Si configura otras interfaces, deben proporcionar la misma conexión permanente a los AWS puntos finales enumerados en los requisitos.

El dispositivo de hardware ni Storage Gateway no admiten la vinculación de redes ni el Protocolo de control de agregación de enlaces (LACP).
No recomendamos configurar varias interfaces de red en la subred, ya que esto a veces puede provocar problemas de enrutamiento.

la consola del dispositivo de hardware está configurada NIC para una pantalla IP estática.



la consola del dispositivo de hardware está configurada NIC para una pantalla IP estática.

3. En Subnet, introduzca una máscara de subred válida y, a continuación, pulse `Down arrow`.
4. Para Gateway, introduzca la IPv4 dirección de la puerta de enlace de red y, a continuación, pulse `Down arrow`.
5. Para DNS1, introduzca la IPv4 dirección de su servidor del Servicio de nombres de dominio (DNS) y, a continuación, pulse `Down arrow`.
6. (Opcional) Para DNS2, introduzca una segunda IPv4 dirección y, a continuación, pulse `Down arrow`. Una segunda asignación de DNS servidor proporcionaría redundancia adicional en caso de que el primer DNS servidor no estuviera disponible.

7. Seleccione Guardar y, a continuación, pulse Enter para guardar la configuración de IPv4 direcciones estáticas del 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

Tras configurar la dirección IP, introduzca esta dirección IP en la página Hardware de la AWS Storage Gateway consola para activar el dispositivo de hardware. El proceso de activación valida que su dispositivo de hardware tenga las credenciales de seguridad apropiadas y registra el dispositivo en su cuenta de AWS .

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

Para activar el dispositivo de hardware de Storage Gateway

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

Note

Únicamente para la activación, deben cumplirse las siguientes condiciones:

- Su navegador debe estar en la misma red que su dispositivo de hardware.
- El firewall debe permitir el HTTP acceso al dispositivo por el puerto 8080 para el tráfico entrante.

2. Elija Hardware en el menú de navegación del lado izquierdo de la página.

3. Seleccione Activar dispositivo.
4. En Dirección IP, introduzca la dirección IP que configuró para el dispositivo de hardware y, a continuación, seleccione Conectar.

Para obtener más información sobre la configuración de la dirección IP, consulte [Configuración de parámetros de red](#).

5. En Nombre, escriba un nombre para su dispositivo de hardware. Los nombres pueden tener una longitud máxima de 225 caracteres y no pueden incluir barras inclinadas.
6. En Zona horaria del dispositivo de hardware, introduzca la zona horaria local desde la que se generará la mayor parte de la carga de trabajo de la puerta de enlace y, a continuación, seleccione Siguiente.

La zona horaria controla cuándo se realizan las actualizaciones de hardware y se utilizan las 2:00 h como hora programada predeterminada para realizar las actualizaciones. Lo ideal es que, si la zona horaria está configurada correctamente, las actualizaciones se realicen de forma predeterminada fuera del horario laboral local.

7. Revise los parámetros de activación en la sección de detalles del dispositivo de hardware. Puede seleccionar Anterior para volver atrás y realizar los cambios necesarios. De lo contrario, seleccione Activar para finalizar la activación.

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

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

Paso siguiente

[Creación de una puerta de enlace](#)

Creación de una puerta de enlace

Puede crear una puerta de enlace de archivos S3, una puerta de enlace de FSx archivos, una puerta de enlace de cinta o una puerta de enlace de volumen en el dispositivo de hardware.

Para crear una puerta de enlace en su dispositivo de hardware

1. Inicie sesión en la consola Storage Gateway de su <https://console.aws.amazon.com/storagegateway/casa> AWS Management Console y ábrala.
2. Seleccione Hardware.
3. Seleccione el dispositivo de hardware activado en el que desea crear la puerta de enlace y, a continuación, seleccione Crear puerta de enlace.
4. Siga los procedimientos que se describen en [Creación de la puerta de enlace](#) para instalar, conectar y configurar el tipo de puerta de enlace elegido.

Cuando termine de crear la puerta de enlace en la consola de Storage Gateway, el software Storage Gateway comenzará a instalarse automáticamente en el dispositivo de hardware. Una puerta de enlace puede tardar entre 5 y 10 minutos en mostrarse como si estuviera en línea en la consola.

Para asignar una dirección IP estática a la 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 puerta de enlace](#)

Configuración de una dirección IP para la puerta de enlace

Antes de activar el dispositivo de hardware, asignó una dirección IP a su interfaz de red física. Ahora que ha activado el dispositivo e iniciado el Storage Gateway en él, debe asignar otra dirección IP a la máquina virtual de Storage Gateway que se ejecuta en el dispositivo de hardware. Para asignar una dirección IP estática a una puerta de enlace instalada en su dispositivo de hardware, configure la dirección IP desde la consola local para esa puerta de enlace. Sus aplicaciones (como su SMB cliente NFS o, su SCSI iniciador i, 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 [the section called “Ajuste de la contraseña de la consola local desde la consola de Storage Gateway”](#).
5. Vaya a la página Configuración de red de la consola local de la gateway como se muestra a continuación.
 página de configuración de la consola local de la puerta de enlace que muestra las opciones, incluida la configuración de red.

```

AWS Storage Gateway Configuration
#####
## Currently connected network adapters:
##
## eth0: 10.0.0.45
#####

1: SOCKS Proxy Configuration
2: Network Configuration
3: Test Network Connectivity
4: System Time Management
5: Gateway Console
6: View System Resource Check (0 Errors)

0: Stop AWS Storage Gateway

Press "x" to exit session

Enter command: _

```

página de configuración de la consola local de la puerta de enlace que muestra las opciones, incluida la configuración de red.

6. Escriba 2 para ir a la página Network Configuration que se muestra a continuación.
 página de configuración de red de la consola local de la puerta de enlace con DHCP opciones de IP estática.

```

AWS Storage Gateway Network Configuration

1: Describe Adapter
2: Configure DHCP
3: Configure Static IP
4: Reset all to DHCP
5: Set Default Adapter
6: View DNS Configuration
7: View Routes

Press "x" to exit

Enter command: _


```

página de configuración de red de la consola local de la puerta DHCP de enlace con opciones de IP estática.

7. Configure una dirección DHCP IP o estática para el puerto de red de su dispositivo de hardware a fin de incluir un archivo, un volumen y una puerta de enlace de 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 `Ctrl+] (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 puerta de enlace](#)

Configuración de la puerta de enlace

Después de activar y configurar su dispositivo de hardware, este aparece en la consola. Ahora puede crear el tipo de gateway que desee. Continúe con la instalación en la página Configurar puerta de enlace correspondiente a su tipo de puerta de enlace. Para obtener instrucciones, consulte [Configuración de la puerta de enlace de cinta](#).


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. En la página Hardware de la consola de Storage Gateway, elija el dispositivo de hardware que desee eliminar.
2. En Actions, elija Remove gateway. Aparece el cuadro de diálogo de confirmación.

3. Compruebe que desea eliminar el software de la puerta de enlace del dispositivo de hardware especificado, escriba la palabra eliminar en el cuadro de confirmación y seleccione Eliminar.


 Note

Después de eliminar el software de la puerta de enlace, no podrá deshacer la acción. En determinados tipos de gateway, puede perder datos tras su eliminación, sobre todo datos almacenados. Para obtener más información sobre la eliminación de una gateway, consulte [Eliminar la puerta de enlace y eliminar los recursos asociados](#).

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

Eliminación del dispositivo de hardware

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

 Note

Para mover el dispositivo a una AWS cuenta diferente o Región de AWS, primero debe eliminarlo mediante el siguiente procedimiento y, a continuación, abrir el canal de soporte y el contacto de la puerta de enlace AWS Support para realizar un restablecimiento parcial. Para obtener más información, consulte [Activar el AWS Support acceso para ayudar a solucionar los problemas de la puerta de enlace alojada en las instalaciones Cómo las instalaciones](#).

Para eliminar el dispositivo de hardware

1. Si ha instalado una puerta de enlace en el dispositivo de hardware, primero debe eliminar la puerta de enlace antes de eliminar el dispositivo. Para obtener instrucciones sobre cómo eliminar una puerta de enlace de su dispositivo de hardware, consulte [Eliminación de una puerta de enlace del dispositivo de hardware](#).
2. En la página Hardware de la consola de Storage Gateway, elija el dispositivo de hardware que desee eliminar.
3. En Actions (Acciones), elija Delete appliance (Eliminar dispositivo). Aparece el cuadro de diálogo de confirmación.

4. Compruebe que desea eliminar el dispositivo de hardware especificado, escriba la palabra eliminar en el cuadro de confirmación y seleccione Eliminar.

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

Creación de la puerta de enlace

Los temas de información general de esta página proporcionan una sinopsis general de cómo funciona el proceso de creación de Storage Gateway. Para conocer step-by-step los procedimientos para crear un tipo específico de puerta de enlace mediante la consola de Storage Gateway, consulte [Creación de una puerta de enlace de cinta](#).

Descripción general: activación de una puerta de enlace

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

Configuración de una puerta de enlace

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

Connect to AWS

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

Revisión y activación

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

Descripción general: configuración de la puerta de enlace

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

Descripción general: recursos de almacenamiento

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

Creación de una puerta de enlace de cinta

En esta sección, encontrará instrucciones sobre cómo crear y utilizar una puerta de enlace de cinta en AWS Storage Gateway.

Temas

- [Creación de una gateway](#)
- [Creación de un grupo de cintas personalizado](#)
- [Creación de nuevas cintas virtuales para Tape Gateway](#)
- [Uso de la puerta de enlace de cinta](#)

Creación de una gateway

En esta sección, encontrará instrucciones sobre cómo descargar, implementar y activar una puerta de enlace de cinta.

Temas

- [Configuración de una puerta de enlace de cinta](#)
- [Conecte su Tape Gateway a AWS](#)
- [Revisión de la configuración y activación de la puerta de enlace de cinta](#)
- [Configuración de la puerta de enlace de cinta](#)

Configuración de una puerta de enlace de cinta

Para configurar una nueva puerta de enlace de cinta

1. Abre AWS Management Console at <https://console.aws.amazon.com/storagegateway/home/> y elige el Región de AWS lugar donde quieres crear tu puerta de enlace.
2. Seleccione Crear puerta de enlace para abrir la página Configurar puerta de enlace.
3. En la sección Configuración de puerta de enlace, realice lo siguiente:
 - a. En Nombre de la puerta de enlace, introduzca un nombre para la puerta de enlace. Puede buscar este nombre para encontrar la puerta de enlace en las páginas de la lista de la consola de Storage Gateway.
 - b. En Zona horaria de la puerta de enlace, elija la zona horaria local de la parte del mundo en la que desee implementar la puerta de enlace.
4. En la sección Opciones de puerta de enlace, en Tipo de puerta de enlace, elija puerta de enlace de cinta.
5. En la sección Opciones de plataforma, haga lo siguiente:
 - a. En Plataforma host, elija la plataforma en la que desee implementar la puerta de enlace y, 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:
 - VMwareESXi- Descargue, implemente y configure la máquina virtual de puerta de enlace mediante VMwareESXi.
 - Microsoft Hyper-V: descargue, implemente y configure la máquina virtual de puerta de enlace mediante Microsoft Hyper-V.
 - Linux KVM: descargue, implemente y configure la máquina virtual de puerta de enlace mediante LinuxKVM.

- Amazon EC2: configura y lanza una EC2 instancia de Amazon para alojar tu puerta de enlace. Esta opción no está disponible para las puertas de enlace de volumen almacenado.
 - Dispositivo de hardware: solicite un dispositivo de hardware físico dedicado AWS para alojar su puerta de enlace.
- b. En Confirmar la configuración de la puerta de enlace, seleccione la casilla de verificación para confirmar que ha realizado los pasos de implementación de la plataforma host que ha elegido. Este paso no se aplica a la plataforma host del dispositivo de hardware.
6. En la sección Configuración de aplicación de copia de seguridad, en Aplicación de copia de seguridad, elija la aplicación que desee utilizar para hacer copias de seguridad de los datos de cinta en las cintas virtuales asociadas a puerta de enlace de cinta.
 7. Elija Paso siguiente para continuar.

Ahora que su puerta de enlace está configurada, debe elegir cómo desea que se conecte y se comunique AWS. Para obtener instrucciones, consulte [Connect your Tape Gateway a AWS](#).

Conecte su Tape Gateway a AWS

Para conectar una nueva puerta de enlace de cinta a AWS

1. Complete el procedimiento que se describe en [Configuración de una puerta de enlace de cinta](#) si aún no lo ha hecho. Cuando haya terminado, seleccione Siguiente para abrir la página Conectarse a AWS en la consola de Storage Gateway.
2. En la sección Opciones de punto final, para Punto final de servicio, elija el tipo de punto final con el que se comunicará su puerta de enlace AWS. Puede elegir entre las siguientes opciones:
 - Acceso público: su puerta de enlace se comunica AWS a través de la Internet pública. Si selecciona esta opción, utilice la casilla de verificación del punto final FIPS habilitado para especificar si la conexión debe cumplir con las normas federales de procesamiento de información (FIPS).

Note

Si necesita FIPS entre FIPS 140 y 2 módulos criptográficos validados para acceder a AWS través de una interfaz de línea de comandos o un terminal compatibleAPI, utilice un terminal compatible. Para obtener más información, consulte la [Norma Federal de Procesamiento de Información \(\) FIPS 140-2](#).

El punto final del FIPS servicio solo está disponible en algunas AWS regiones. Para obtener más información, consulte [Puntos de conexión y cuotas de Storage Gateway](#) en la Referencia general de AWS.

- VPCalojado: su puerta de enlace se comunica con la suya AWS a través de una conexión privadaVPC, lo que le permite controlar la configuración de la red. Si selecciona esta opción, debe especificar un VPC punto final existente eligiendo su ID de VPC punto final en el menú desplegable o proporcionando su VPC DNS nombre o dirección IP.
3. En la sección Opciones de conexión de puerta de enlace, en Opciones de conexión, elija cómo identificar la puerta de enlace en AWS. Puede elegir entre las siguientes opciones:
- Dirección IP: indique la dirección IP de la puerta de enlace en el campo correspondiente. Esta dirección IP debe ser pública o accesible desde su red actual y debe poder conectarse a ella desde su navegador web.
- Puedes obtener la dirección IP de la puerta de enlace iniciando sesión en la consola local de la puerta de enlace desde tu cliente hipervisor o copiándola desde la página de detalles de tu EC2 instancia de Amazon.
- Clave de activación: proporcione la clave de activación de la puerta de enlace en el campo correspondiente. Puede generar una clave de activación mediante la consola local de la puerta de enlace. Elija esta opción si la dirección IP de la puerta de enlace no está disponible.
4. Elija Paso siguiente para continuar.

Ahora que ha elegido cómo quiere que se conecte su puerta de enlace AWS, debe activarla. Para obtener instrucciones, consulte [Revisión de la configuración y activación de la puerta de enlace de cinta](#).


Revisión de la configuración y activación de la puerta de enlace de cinta

Para activar una nueva puerta de enlace de cinta

1. Complete los procedimientos que se describen en los siguientes temas si aún no lo ha hecho:
 - [Configuración de una puerta de enlace de cinta](#)
 - [Conecte su Tape Gateway a AWS](#)

Cuando haya terminado, seleccione **Siguiente** para abrir la página **Revisar y activar** en la consola de Storage Gateway.

2. Revise los detalles iniciales de la puerta de enlace de cada sección de la página.
3. Si una sección contiene errores, elija **Editar** para volver a la página de configuración correspondiente y realizar los cambios.

 **Note**

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

4. Seleccione **Activar puerta de enlace** para continuar.

Ahora que ha activado la puerta de enlace, debe realizar la primera configuración para asignar los discos de almacenamiento local y configurar el registro. Para obtener instrucciones, consulte [Configuración de la puerta de enlace de cinta](#).

Configuración de la puerta de enlace de cinta

Para realizar la primera configuración en una nueva puerta de enlace de cinta

1. Complete los procedimientos que se describen en los siguientes temas si aún no lo ha hecho:
 - [Configuración de una puerta de enlace de cinta](#)
 - [Conecte su Tape Gateway a AWS](#)
 - [Revisión de la configuración y activación de la puerta de enlace de cinta](#)

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

2. En la sección **Configurar almacenamiento**, utilice los menús desplegables para asignar al menos un disco con una capacidad mínima de 165 GiB y un disco con una capacidad mínima de 150 GiB para **CACHESTORAGE**. **UPLOADBUFFER** Los discos locales que se enumeran en esta sección corresponden al almacenamiento físico que aprovisionó en su plataforma host.

3. En la sección del grupo de CloudWatch registros, elige cómo configurar Amazon CloudWatch Logs para supervisar el estado de tu puerta de enlace. Puede elegir entre las siguientes opciones:
 - Crear un nuevo grupo de registro: configure un nuevo grupo de registro para supervisar la puerta de enlace.
 - Utilizar un grupo de registro existente: elija un grupo de registro existente en el menú desplegable correspondiente.
 - Desactiva el registro: no utilices Amazon CloudWatch Logs para supervisar tu puerta de enlace.

 Note


Para recibir los registros de estado de Storage Gateway, los siguientes permisos deben estar presentes en la política de recursos del grupo de registros. Sustituya el *highlighted section* con la resourceArn información del grupo de registros específico para su implementación.

```
"Sid": "AWSLogDeliveryWrite20150319",
  "Effect": "Allow",
  "Principal": {
    "Service": [
      "delivery.logs.amazonaws.com"
    ]
  },
  "Action": [
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource": "arn:aws:logs:eu-west-1:1234567890:log-group:/foo/bar:log-stream:*"
```

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

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

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

 Note

Esta función requiere permisos CloudWatch de política, que no se otorgan automáticamente como parte de la política de acceso total preconfigurada de Storage Gateway. Asegúrese de que su política de seguridad conceda los siguientes permisos antes de intentar crear CloudWatch las alarmas recomendadas:

- `cloudwatch:PutMetricAlarm`: crear alarmas
- `cloudwatch:DisableAlarmActions`: desactivar acciones de alarma
- `cloudwatch:EnableAlarmActions`: activar acciones de alarma
- `cloudwatch>DeleteAlarms`: eliminar alarmas

- Cree una alarma personalizada: configure una nueva CloudWatch alarma para que le notifique las métricas de su puerta de enlace. Seleccione Crear alarma para definir las métricas y especificar las acciones de alarma en la CloudWatch consola de Amazon. Para obtener instrucciones, consulta [Uso de CloudWatch alarmas de Amazon](#) en la Guía del CloudWatch usuario de Amazon.
 - Sin alarma: no reciba CloudWatch notificaciones sobre las métricas de su pasarela.
5. (Opcional) En la sección Etiquetas, seleccione Agregar etiqueta nueva y, a continuación, introduzca un par clave-valor que distinga mayúsculas de minúsculas para ayudarle a buscar y filtrar la puerta de enlace en las páginas de la lista de la consola de Storage Gateway. Repita este paso para agregar todas las etiquetas que necesite.
 6. Elija Configurar para terminar de crear la puerta de enlace.

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

Ahora que ha creado la puerta de enlace, debe crear cintas virtuales para utilizarla. Para obtener instrucciones, consulte [Creación de cintas](#).

Creación de un grupo de cintas personalizado

En esta sección se describe cómo crear un nuevo grupo de cintas personalizado en AWS Storage Gateway.

Temas

- [Elección de un tipo de grupo de cintas](#)
- [Uso de un bloqueo de retención de cintas](#)
- [Creación de un grupo de cintas personalizado](#)

Elección de un tipo de grupo de cintas

AWS Storage Gateway utiliza grupos de cintas para determinar la clase de almacenamiento en la que desea que se archiven las cintas cuando se expulsan. Storage Gateway ofrece dos grupos de cintas estándar:

- Grupo de Glacier: archiva la cinta en la clase de almacenamiento S3 Glacier Flexible Retrieval. Cuando el software de copia de seguridad expulsa la cinta, se archiva automáticamente en S3 Glacier Flexible Retrieval. S3 Glacier Flexible Retrieval se utiliza para archivos más activos en los que se pueden recuperar las cintas en un plazo que suele ser de entre 3 y 5 horas. Para más información sobre las clases de almacenamiento, consulte [Clases de almacenamiento para el archivado de objetos](#) en la Guía del usuario de Amazon Simple Storage Service.
- Grupo de Deep Archive: archiva la cinta en la clase de almacenamiento S3 Glacier Deep Archive. Cuando el software de copia de seguridad expulsa la cinta, esta se archiva automáticamente en S3 Glacier Deep Archive. S3 Glacier Deep Archive se utiliza para la retención de datos y la conservación digital a largo plazo en las que se tiene acceso a los datos una o dos veces al año. Por lo general, puede recuperar las cintas archivadas en S3 Glacier Deep Archive en un plazo de 12 horas. Para obtener información detallada, consulte [Clases de almacenamiento para el archivado de objetos](#) en la Guía del usuario de Amazon Simple Storage Service.

Si archiva una cinta en S3 Glacier Flexible Retrieval, puede trasladarla a S3 Glacier Deep Archive más adelante. Para obtener más información, consulte [Traslado de cintas a la clase de almacenamiento S3 Glacier Deep Archive](#).

Storage Gateway también admite la creación de grupos de cintas personalizados, lo que le permite activar el bloqueo de retención de cintas para evitar que las cintas archivadas se eliminen o se

muevan a otro grupo durante un período de tiempo fijo de hasta 100 años. Esto incluye controles de permisos de bloqueo sobre quién puede eliminar las cintas o modificar la configuración de retención.

Uso de un bloqueo de retención de cintas

Con el bloqueo de retención de cintas, puede bloquear las cintas archivadas. El bloqueo de retención de cintas es una opción para las cintas de un grupo de cintas personalizado. Las cintas con el bloqueo de retención de cinta activado no se pueden eliminar ni mover a otro grupo durante un período de tiempo fijo de hasta 100 años.

Puede configurar el bloqueo de retención de la cintas en uno de los siguientes dos modos:

- **Modo de gobierno:** cuando se configura en el modo de gobierno, solo AWS Identity and Access Management (IAM) los usuarios con los permisos para actuar `storagegateway:BypassGovernanceRetention` pueden eliminar las cintas del grupo. Si va a utilizar el AWS Storage Gateway API para quitar la cinta, también debe `BypassGovernanceRetention` configurarlo `true`.
- **Modo de cumplimiento:** cuando se configura en el modo de cumplimiento, ningún usuario, ni siquiera el usuario Cuenta de AWS raíz, puede eliminar la protección.

Una vez que se bloquea un objeto en el modo de cumplimiento, no es posible cambiar el tipo de bloqueo de retención ni acortar su periodo de retención. El tipo de bloqueo en modo de cumplimiento evita que la cinta se pueda sobrescribir o eliminar durante la duración del periodo de retención.

Important

La configuración de un grupo personalizado no puede cambiarse una vez creada.

Puede activar el bloqueo de retención de cintas cuando cree un grupo de cintas personalizado. Todas las cintas nuevas que se adjunten a un grupo personalizado heredan el tipo de bloqueo de retención, el período y la clase de almacenamiento de ese grupo.

También puede activar el bloqueo de retención de cintas en las cintas que se archivaron antes del lanzamiento de esta característica al mover las cintas entre el grupo predeterminado y el grupo personalizado que cree. Si la cinta se archiva, el bloqueo de retención de cintas se activa de forma inmediata.

Note

Si va a mover cintas archivadas entre las clases de almacenamiento S3 Glacier Flexible Retrieval y S3 Glacier Deep Archive, se le cobrará una tarifa por ello. No se cobra ninguna tarifa adicional por mover una cinta de un grupo predeterminado a uno personalizado si la clase de almacenamiento sigue siendo la misma.

Creación de un grupo de cintas personalizado

Siga los pasos siguientes para crear un grupo de cintas personalizado mediante la consola de AWS Storage Gateway .

Para crear un grupo de cintas personalizado

1. Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa>.
2. En el panel de navegación izquierdo, elija la pestaña Biblioteca de cintas y, a continuación, elija la pestaña Grupos.
3. Seleccione Crear grupo para abrir el panel Crear grupo.
4. En Nombre, introduzca un nombre único para identificar el grupo de cintas personalizado. El nombre debe tener entre 2y 100 caracteres.
5. En Clase de almacenamiento, elija Glacier o Glacier Deep Archive.
6. En Tipo de bloqueo de retención, elija Ninguno, Conformidad o Gobernanza.

Note

Si selecciona Conformidad, ningún usuario, ni siquiera el usuario de Cuenta de AWS raíz, podrá eliminar el bloqueo de retención de cintas.

7. Si elige un tipo de bloqueo de retención de cintas, introduzca el Período de retención en días. El período máximo de retención es de 36 500 días (100 años).
8. (Opcional) En Etiquetas, elija Agregar nueva etiqueta para agregar una etiqueta a su grupo de cintas personalizado. Una etiqueta es un par clave-valor con distinción entre mayúsculas y minúsculas, que le ayuda a administrar, filtrar y buscar cintas.

Escriba una Clave y, opcionalmente, un Valor para la etiqueta. Puede agregar hasta 50 etiquetas al grupo de cintas.

9. Elija Crear grupo para crear el nuevo grupo de cintas personalizado.

Creación de nuevas cintas virtuales para Tape Gateway

En esta sección se describe cómo crear nuevas cintas virtuales mediante AWS Storage Gateway. Puede crear nuevas cintas virtuales manualmente mediante la AWS Storage Gateway consola o Storage GatewayAPI. También puede configurar la puerta de enlace de cinta para crearlas automáticamente, lo que reduce la necesidad de administrar las cintas manualmente, simplifica las implementaciones de gran tamaño y ayuda a escalar las necesidades de almacenamiento de archivado y en las instalaciones.

Tape Gateway admite la escritura única, la lectura múltiple (WORM) y el bloqueo de retención de cintas en las cintas virtuales. WORM-las cintas virtuales activadas ayudan a garantizar que los datos de las cintas activas de la biblioteca de cintas virtuales no se puedan sobrescribir ni borrar. Para obtener más información sobre WORM la protección de las cintas virtuales, consulte la siguiente sección, [the section called “WORMProtección de cinta”](#).

Con el bloqueo de retención de cintas, puede especificar el modo y el período de retención de las cintas virtuales archivadas, lo que evita que se eliminen durante un período fijo de tiempo de hasta 100 años. Incluye controles de permisos sobre quién puede eliminar las cintas o modificar la configuración de retención. Para obtener más información sobre el bloqueo de retención de cintas, consulte [the section called “Bloqueo de retención de cintas”](#).

Note

Solo se le cobrará por la cantidad de datos que grabe en la cinta, no por la capacidad de la cinta.

Puede utilizar AWS Key Management Service (AWS KMS) para cifrar los datos escritos en una cinta virtual almacenada en Amazon Simple Storage Service (Amazon S3). Actualmente, puede hacerlo utilizando AWS Storage Gateway API o AWS Command Line Interface (AWS CLI). Para obtener más información, consulte [CreateTapeso cree cintas](#).

Temas

- [Protección de cinta para escribir una vez, leer muchas \(WORM\)](#)
- [Creación manual de cintas](#)
- [Permitir la creación automática de cintas](#)

Protección de cinta para escribir una vez, leer muchas (WORM)

Puede evitar que las cintas virtuales se sobrescriban o borren activando la WORM protección para las cintas virtuales en su interior. AWS Storage Gateway WORM la protección de las cintas virtuales se activa al crear las cintas.

Los datos que se escriben en cintas WORM virtuales no se pueden sobrescribir. Solo los datos nuevos se pueden adjuntar a las cintas WORM virtuales y los datos existentes no se pueden borrar. La activación de la WORM protección de las cintas virtuales ayuda a proteger esas cintas mientras están en uso activo, antes de expulsarlas y archivarlas.

WORM la configuración solo se puede establecer cuando se crean las cintas y esa configuración no se puede cambiar una vez creadas las cintas.


Creación manual de cintas

Puede crear nuevas cintas virtuales manualmente mediante la AWS Storage Gateway consola o Storage GatewayAPI. La consola ofrece una interfaz práctica para la creación de cintas con la flexibilidad de especificar un prefijo para un código de barras de cinta generado aleatoriamente. Si necesita personalizar completamente los códigos de barras de las cintas (por ejemplo, para que coincidan con el número de serie de la cinta física correspondiente), debe utilizar elAPI. Para obtener más información sobre la creación de cintas mediante Storage GatewayAPI, consulte [CreateTapeWithBarcode](#) la API referencia de Storage Gateway.

Creación de cintas virtuales manualmente mediante la consola de Storage Gateway

1. Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa>.
2. En el panel de navegación, elija la pestaña Gateways.
3. Elija Crear cintas para abrir el cuadro de diálogo Crear cintas.
4. En Gateway, elija una gateway. Se crea la cinta para esta gateway.
5. En el Tipo de cinta, elija Estándar para crear cintas virtuales estándar. Elija WORM crear cintas virtuales, escribir una vez y leer muchas (WORM).
6. En Number of tapes (Número de cintas), elija el número de cintas que desee crear. Para obtener más información acerca de las cuotas de cintas, consulte [AWS Storage Gateway cuotas](#).
7. En Capacity (Capacidad), escriba el tamaño de la cinta virtual que desea crear. Las cintas deben tener más de 100 GiB. Para obtener información sobre las cuotas de capacidad, consulte [AWS Storage Gateway cuotas](#).


8. En Barcode prefix (Prefijo de código de barras), escriba el prefijo que desee anteponer al código de barras de las cintas virtuales.

 Note

Las cintas virtuales se identifican de forma única mediante un código de barras y puede agregar un prefijo al código de barras. El prefijo es opcional, pero puede utilizarlo para identificar las cintas virtuales. El prefijo debe constar de letras mayúsculas (A - Z) y tener entre uno y cuatro caracteres.

9. En Grupo, elija Grupo de Glacier, Grupo de Deep Archive o un grupo personalizado que haya creado. El grupo representa la clase de almacenamiento en la que se almacena la cinta cuando el software de copia de seguridad la expulsa.
 - Elija Grupo de Glacier si desea archivar la cinta en la clase de almacenamiento S3 Glacier Flexible Retrieval. Cuando el software de copia de seguridad expulsa la cinta, se archiva automáticamente en S3 Glacier Flexible Retrieval. S3 Glacier Flexible Retrieval se utiliza para archivos más activos en los que se pueden recuperar la cinta en un plazo que suele ser de entre 3 y 5 horas. Para más información sobre las clases de almacenamiento, consulte [Clases de almacenamiento para el archivado de objetos](#) en la Guía del usuario de Amazon Simple Storage Service.
 - Elija Grupo de Deep Archive si desea archivar la cinta en la clase de almacenamiento S3 Glacier Deep Archive. Cuando el software de copia de seguridad expulsa la cinta, esta se archiva automáticamente en S3 Glacier Deep Archive. S3 Glacier Deep Archive se utiliza para la retención de datos y la conservación digital a largo plazo en las que se tiene acceso a los datos una o dos veces al año. Por lo general, puede recuperar una cinta archivada en S3 Glacier Deep Archive en un plazo de 12 horas. Para más información sobre las clases de almacenamiento, consulte [Clases de almacenamiento para el archivado de objetos](#) en la Guía del usuario de Amazon Simple Storage Service.
 - Elija un grupo personalizado, si hay alguno disponible. Los grupos de cintas personalizados se configuran para utilizar Grupo de Deep Archive o Grupo de Glacier. Las cintas se archivan en la clase de almacenamiento configurada cuando el software de copia de seguridad las expulsa.

Si archiva una cinta en S3 Glacier Flexible Retrieval, puede trasladarla a S3 Glacier Deep Archive más adelante. Para obtener más información, consulte [Traslado de cintas a la clase de almacenamiento S3 Glacier Deep Archive](#).

 Note

Las cintas creadas antes del 27 de marzo de 2019 se archivan directamente en S3 Glacier Deep Archive cuando el software de copia de seguridad las expulsa.

10. (Opcional) En Etiquetas, elija Agregar nueva etiqueta e introduzca una clave y un valor para agregar etiquetas a la cinta. Una etiqueta es un par clave-valor que distingue entre mayúsculas y minúsculas, y que le ayuda a administrar, filtrar y buscar cintas.
11. Elija Create tapes (Crear cintas).
12. En el panel de navegación, elija Biblioteca de cintas > Cintas para ver las cintas. De forma predeterminada, esta lista muestra hasta 1000 cintas a la vez, pero las búsquedas que realice se aplican a todas las cintas. Puede utilizar la barra de búsqueda para buscar cintas que coincidan con un criterio específico o para reducir la lista a menos de 1000 cintas. Si la lista contiene 1000 cintas o menos, puede ordenarlas en orden ascendente o descendente según una serie de propiedades.

El estado de las cintas virtuales se establece inicialmente en el CREATING momento en que se crean las cintas virtuales. Una vez creadas las cintas, su estado cambia a AVAILABLE. Para obtener más información, consulte [Administración de la puerta de enlace de cinta](#).

Permitir la creación automática de cintas

El puerto de enlace de cinta puede crear automáticamente nuevas cintas virtuales para mantener el número mínimo de cintas disponibles que configure. A continuación, hace que estas cintas estén disponibles para importación en la aplicación de copia de seguridad para que los trabajos de copia de seguridad puedan ejecutarse sin interrupción. Al permitir la creación automática de cintas, elimina la necesidad de crear secuencias de comandos personalizadas, además del proceso manual para crear nuevas cintas virtuales.

La puerta de enlace de cinta genera automáticamente una nueva cinta cuando tiene menos cintas que el número mínimo de cintas disponibles especificado para la creación automática de cintas. Se genera una cinta nueva cuando:

- Se importa una cinta desde una ranura de importación/exportación.
- Se importa una cinta a la unidad de cinta.

La puerta de enlace mantiene un número mínimo de cintas con el prefijo de código de barras especificado en la política de creación automática de cintas. Si hay menos cintas que el número mínimo de cintas con el prefijo de código de barras, la puerta de enlace crea automáticamente las cintas nuevas necesarias para igualar el número mínimo de cintas especificado en la política de creación automática de cintas.

Al expulsar una cinta y pasarla a la ranura de importación o exportación, esa cinta no se tiene en cuenta para el número mínimo de cintas especificado en la política de creación automática de cintas. Solo las cintas en la ranura de importación o exportación se consideran “disponibles”. La exportación de una cinta no inicia la creación automática de cintas. Solo las importaciones afectan a la cantidad de cintas disponibles.

Al mover una cinta de la ranura de importación o exportación a una unidad de cinta o ranura de almacenamiento, se reduce la cantidad de cintas en la ranura de importación o exportación con el mismo prefijo de código de barras. La puerta de enlace crea nuevas cintas para mantener la cantidad mínima de cintas disponibles para ese prefijo de código de barras.


Para permitir la creación automática de cintas

1. Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa>.
2. En el panel de navegación, elija la pestaña Gateways.
3. Elija la gateway para la que desea crear cintas automáticamente.
4. En el menú Actions (Acciones), elija Configure tape auto-create (Configurar creación automática de cintas).

Aparece la página Creación automática de cintas. Aquí puede agregar, cambiar o eliminar las opciones de creación automática de cintas.

5. Para permitir la creación automática de cintas, elija Agregar nuevo elemento y, a continuación, configure los ajustes para la creación automática de cintas.
6. En el Tipo de cinta, elija Estándar para crear cintas virtuales estándar. Elija WORMcrear write-once-read-many(WORM) cintas virtuales.
7. En Cantidad mínima de cintas, escriba la cantidad mínima de cintas virtuales que deben estar disponibles en la puerta de enlace de cinta en todo momento. El intervalo válido para este valor es 1 como mínimo y 10 como máximo.
8. En Capacity (Capacidad), introduzca el tamaño, en bytes, de la capacidad de la cinta virtual. El intervalo válido es 100 Gib como mínimo y 15 TiB como máximo.

9. En Barcode prefix (Prefijo de código de barras), escriba el prefijo que desee anteponer al código de barras de las cintas virtuales.

 Note

Las cintas virtuales se identifican de forma única mediante un código de barras y puede agregar un prefijo al código de barras. El prefijo es opcional, pero puede utilizarlo para ayudar a identificar las cintas virtuales. El prefijo debe constar de letras mayúsculas (A - Z) y tener entre uno y cuatro caracteres.

10. En Grupo, elija Grupo de Glacier, Grupo de Deep Archive o un grupo personalizado que haya creado. El grupo representa la clase de almacenamiento en la que se almacena la cinta cuando el software de copia de seguridad la expulsa.
 - Elija Grupo de Glacier si desea archivar la cinta en la clase de almacenamiento S3 Glacier Flexible Retrieval. Cuando el software de copia de seguridad expulsa la cinta, se archiva automáticamente en S3 Glacier Flexible Retrieval. S3 Glacier Flexible Retrieval se utiliza para archivos más activos en los que se pueden recuperar la cinta en un plazo que suele ser de entre 3 y 5 horas. Para más información sobre las clases de almacenamiento, consulte [Clases de almacenamiento para el archivado de objetos](#) en la Guía del usuario de Amazon Simple Storage Service.
 - Elija Grupo de Deep Archive si desea archivar la cinta en la clase de almacenamiento S3 Glacier Deep Archive. Cuando el software de copia de seguridad expulsa la cinta, esta se archiva automáticamente en S3 Glacier Deep Archive. S3 Glacier Deep Archive se utiliza para la retención de datos y la conservación digital a largo plazo en las que se tiene acceso a los datos una o dos veces al año. Por lo general, puede recuperar una cinta archivada en S3 Glacier Deep Archive en un plazo de 12 horas. Para más información sobre las clases de almacenamiento, consulte [Clases de almacenamiento para el archivado de objetos](#) en la Guía del usuario de Amazon Simple Storage Service.
 - Elija un grupo personalizado, si hay alguno disponible. Los grupos de cintas personalizados se configuran para utilizar Grupo de Deep Archive o Grupo de Glacier. Las cintas se archivan en la clase de almacenamiento configurada cuando el software de copia de seguridad las expulsa.

Si archiva una cinta en S3 Glacier Flexible Retrieval, puede trasladarla a S3 Glacier Deep Archive más adelante. Para obtener más información, consulte [Traslado de cintas a la clase de almacenamiento S3 Glacier Deep Archive](#).

Note

Las cintas creadas antes del 27 de marzo de 2019 se archivan directamente en S3 Glacier Deep Archive cuando el software de copia de seguridad las expulsa.

11. Cuando termine de configurar los ajustes, elija Guardar cambios.
12. En el panel de navegación, elija Biblioteca de cintas > Cintas para ver las cintas. De forma predeterminada, esta lista muestra hasta 1000 cintas a la vez, pero las búsquedas que realice se aplican a todas las cintas. Puede utilizar la barra de búsqueda para buscar cintas que coincidan con un criterio específico o para reducir la lista a menos de 1000 cintas. Si la lista contiene 1000 cintas o menos, puede ordenarlas en orden ascendente o descendente según una serie de propiedades.

El estado de las cintas virtuales disponibles se establece inicialmente en el CREATING momento en que se crean las cintas. Una vez creadas las cintas, su estado cambia a AVAILABLE. Para obtener más información, consulte [Administración de la puerta de enlace de cinta](#).

Para obtener más información sobre cómo cambiar las políticas de creación automática de cintas o eliminar la creación automática de cintas de una puerta de enlace de cinta, consulte [Administración de la creación automática de cintas](#).

Paso siguiente

[Uso de la puerta de enlace de cinta](#)

Uso de la puerta de enlace de cinta

A continuación, encontrará instrucciones para utilizar la puerta de enlace de cinta.

Temas

- [Conexión de sus VTL dispositivos](#)
- [Uso del software de respaldo para probar la configuración de la puerta de enlace](#)
- [¿Qué tengo que hacer ahora?](#)

Conexión de sus VTL dispositivos

A continuación, encontrará instrucciones sobre cómo conectar los dispositivos de la biblioteca de cintas virtuales (VTL) a su cliente Microsoft Windows o Red Hat Enterprise Linux (RHEL).

Temas

- [Conexión a un cliente Microsoft Windows](#)
- [Conexión a un cliente Linux](#)

Conexión a un cliente Microsoft Windows

El siguiente procedimiento muestra un resumen de los pasos que deberá seguir para conectarse a un cliente Windows.

Para conectar sus VTL dispositivos a un cliente de Windows

1. Inicie `iscsicpl.exe`.

Note

Debe tener derechos de administrador en el equipo cliente para ejecutar el SCSI iniciador i.

2. Inicie el servicio Microsoft i SCSI Initiator.
3. En el cuadro de diálogo Propiedades SCSI del iniciador i, seleccione la pestaña Descubrimiento y, a continuación, elija Discover Portal.
4. Proporcione la dirección IP de su Tape Gateway como dirección IP o DNS nombre.
5. Elija la pestaña Targets y, a continuación, elija Refresh. Las 10 unidades de cinta y el cambiador de medios aparecen en el cuadro Discovered targets. El estado de los destinos es Inactive.
6. Elija el primer dispositivo y conéctelo. Puede conectar los dispositivos de uno en uno.
7. Conecte todos los destinos.

En un cliente de Windows, el proveedor de la unidad de cinta debe ser Microsoft. Utilice el siguiente procedimiento para comprobar cuál es el proveedor de la unidad y actualizarlos si es necesario:

Para verificar y actualizar el controlador y el proveedor

1. En el cliente de Windows, inicie el Administrador de dispositivos.
2. Amplíe Tape drives, abra el menú contextual de una unidad de cinta y elija Properties.
3. En la pestaña Driver del cuadro de diálogo Device Properties, verifique que el Driver Provider es Microsoft.
4. Si el Driver Provider no es Microsoft, establezca el valor de la siguiente manera:
 - a. Elija Actualizar controlador.
 - b. En el cuadro de diálogo Update Driver Software, elija Browse my computer for driver software.
 - c. En el cuadro de diálogo Update Driver Software, elija Let me pick from a list of device drivers on my computer.
 - d. Elija la unidad de LTO cinta y, a continuación, seleccione Siguiente.
5. Elija Close para cerrar la ventana Update Driver Software y verifique que el valor de Driver Provider esté ahora establecido en Microsoft.
6. Repita los pasos para actualizar el controlador y el proveedor para todas las unidades de cinta.

Conexión a un cliente Linux

El siguiente procedimiento muestra un resumen de los pasos que debe seguir para conectarse a un RHEL cliente.

Para conectar un cliente Linux a los VTL dispositivos

1. Instale el `iscsi-initiator-utils` RPM paquete.

Puede utilizar el comando siguiente para instalar el paquete.

```
sudo yum install iscsi-initiator-utils
```

2. Asegúrese de que el SCSI daemon `i` esté en ejecución.

Para RHEL 5 o 6, usa el siguiente comando.

```
sudo /etc/init.d/iscsi status
```

Para RHEL 7, utilice el siguiente comando.

```
sudo service iscsid status
```

3. Descubra los objetivos de volumen o VTL dispositivo definidos para una puerta de enlace. Utilice el comando de detección siguiente.

```
sudo /sbin/iscsiadm --mode discovery --type sendtargets --portal [GATEWAY_IP]:3260
```

El resultado del comando de detección tendrá un aspecto semejante al de este ejemplo.

Para puertas de enlace de volumen: `[GATEWAY_IP]:3260, 1`
`iqn.1997-05.com.amazon:myvolume`

Para puertas de enlace de cinta: `iqn.1997-05.com.amazon:[GATEWAY_IP]-tapedrive-01`

4. Conéctese a un destino.

Asegúrese de especificar el correcto `[GATEWAY_IP]` y IQN en el comando `connect`.

Use el siguiente comando.

```
sudo /sbin/iscsiadm --mode node --targetname  
iqn.1997-05.com.amazon:[ISCSI_TARGET_NAME] --portal [GATEWAY_IP]:3260,1 --login
```

5. Compruebe que el volumen se encuentre asociado a la máquina cliente (el iniciador). Para ello, utilice el siguiente comando.

```
ls -l /dev/disk/by-path
```

El resultado del comando tendrá un aspecto semejante al de este ejemplo.

```
lrwxrwxrwx. 1 root root 9 Apr 16 19:31 ip-[GATEWAY_IP]:3260-iscsi-  
iqn.1997-05.com.amazon:myvolume-lun-0 -> ../../sda
```

En el caso de Volume Gateways, le recomendamos encarecidamente que, después de configurar el iniciador, personalice la SCSI configuración de `i` tal y como se describe en

[Personalización de la configuración de Linux i SCSI](#)

Compruebe que el VTL dispositivo esté conectado a la máquina cliente (el iniciador). Para ello, utilice el siguiente comando.

```
ls -l /dev/tape/by-path
```

El resultado del comando tendrá un aspecto semejante al de este ejemplo.

```
total 0
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-mediachanger-lun-0-changer -> ../../sg20
lrwxrwxrwx 1 root root 9 Sep 8 11:19 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-01-lun-0 -> ../../st6
lrwxrwxrwx 1 root root 10 Sep 8 11:19 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-01-lun-0-nst -> ../../nst6
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-02-lun-0 -> ../../st7
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-02-lun-0-nst -> ../../nst7
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-03-lun-0 -> ../../st8
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-03-lun-0-nst -> ../../nst8
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-04-lun-0 -> ../../st9
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-04-lun-0-nst -> ../../nst9
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-05-lun-0 -> ../../st10
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-05-lun-0-nst -> ../../nst10
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-06-lun-0 -> ../../st11
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-06-lun-0-nst -> ../../nst11
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-07-lun-0 -> ../../st12
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-07-lun-0-nst -> ../../nst12
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-08-lun-0 -> ../../st13
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-08-lun-0-nst -> ../../nst13
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-09-lun-0 -> ../../st14
```

```
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-09-lun-0-nst -> ../../nst14
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-10-lun-0 -> ../../st15
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-10-lun-0-nst -> ../../nst15
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x0000000000000012-lun-0-
changer -> ../../sg6
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001c-lun-0
-> ../../st0
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001c-
lun-0-nst -> ../../nst0
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001f-lun-0
-> ../../st1
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001f-
lun-0-nst -> ../../nst1
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x0000000000000022-lun-0
-> ../../st2
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.0-fc-0x0000000000000022-
lun-0-nst -> ../../nst2
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000025-lun-0
-> ../../st5
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000025-
lun-0-nst -> ../../nst5
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000028-lun-0
-> ../../st3
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000028-
lun-0-nst -> ../../nst3
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.1-fc-0x000000000000002b-lun-0
-> ../../st4
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.1-fc-0x000000000000002b-
lun-0-nst -> ../../nst4
```


Paso siguiente

[Uso del software de copia de seguridad para comprobar la configuración de la puerta de enlace](#)

Uso del software de respaldo para probar la configuración de la puerta de enlace

Para comprobar la configuración de la puerta de enlace de cinta, realice las siguientes tareas mediante la aplicación de copia de seguridad:


1. Configure la aplicación de backup para detectar los dispositivos de almacenamiento.

 Note

Para mejorar el rendimiento de E/S, le recomendamos ajustar el tamaño del bloque de las unidades de cinta en la aplicación de copia de seguridad a 1 MB. Para obtener más información, consulte [Utilice un tamaño de bloques mayor para las unidades de cinta](#).

2. Realice una copia de seguridad de los datos en una cinta.
3. Archive la cinta.
4. Recupere la cinta desde el archivo.
5. Restaurar los datos desde la cinta.

Para probar su configuración, utilice una aplicación de copia de seguridad compatible, tal y como se describe a continuación.

 Note

A menos que se indique lo contrario, todas las aplicaciones de copia de seguridad se permiten en Microsoft Windows.

Temas

- [Probar la configuración mediante Arcserve Backup](#)
- [Comprobación de la configuración mediante Bacula Enterprise](#)
- [Comprobación de la configuración mediante Commvault](#)
- [Probar su configuración con Dell EMC NetWorker](#)
- [Probar su configuración mediante IBM Spectrum Protect](#)
- [Probar la configuración mediante Micro Focus Data Protector](#)
- [Probar la configuración mediante Microsoft System Center DPM](#)
- [Probar la configuración mediante NovaStor DataCenter](#)
- [Probar la configuración mediante Quest NetVault Backup](#)
- [Pruebe su configuración con Veeam Backup and Replication](#)
- [Comprobación de la configuración mediante Veritas Backup Exec](#)

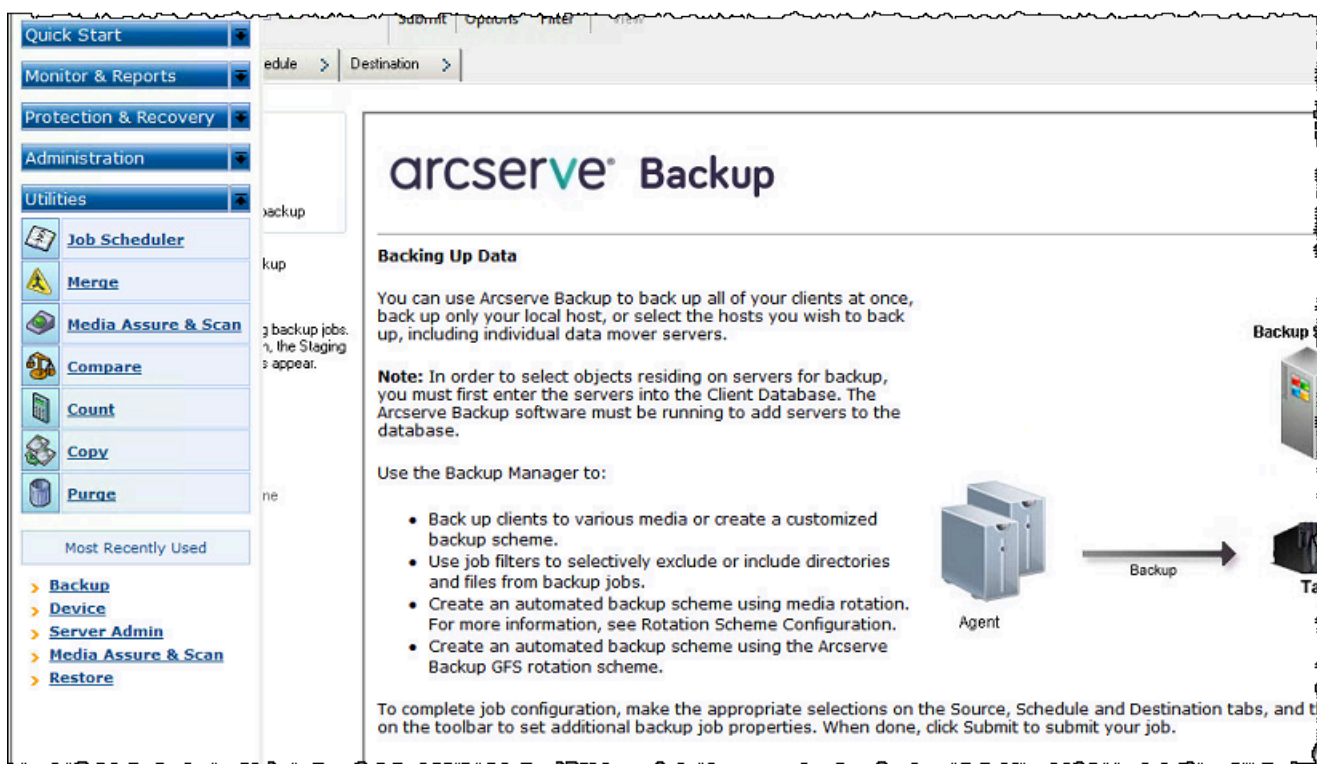
- [Probar su configuración mediante Veritas NetBackup](#)

Para obtener más información sobre aplicaciones de backup compatibles, consulte [Aplicaciones de copia de seguridad de terceros compatibles con una puerta de enlace de cinta](#).

Probar la configuración mediante Arcserve Backup

Puede hacer copias de seguridad de sus datos en cintas virtuales, archivar las cintas y administrar sus dispositivos de biblioteca de cintas virtuales (VTL) mediante Arcserve Backup r17.0. En este tema, encontrará documentación básica acerca de cómo configurar Arcserve Backup con una puerta de enlace de cinta y realizar operaciones de copia de seguridad y restauración. Para obtener información detallada sobre el uso de Arcserve Backup r17.0, consulte la [documentación de Arcserve Backup r17](#) en la Guía de administración de Arcserve.

La siguiente captura de pantalla muestra los menús de Arcserve.



Temas

- [Configurar Arcserve para que funcione con dispositivos VTL](#)
- [Carga de cintas en un grupo de medios](#)
- [Copia de seguridad de datos en una cinta](#)

- [Archivado de una cinta](#)
- [Restauración de datos desde una cinta](#)

Configurar Arcserve para que funcione con dispositivos VTL

Una vez que haya conectado los dispositivos de la biblioteca de cintas virtuales (VTL) al cliente, escanee en busca de sus dispositivos.

Para buscar VTL dispositivos

1. En el administrador de Arcserve Backup, elija el menú Utilities (Utilidades).
2. Elija Media Assure and Scan.

Carga de cintas en un grupo de medios

Cuando el software Arcserve se conecta a la gateway y las cintas están disponibles, Arcserve carga automáticamente las cintas. Si la gateway no se encuentra en el software Arcserve, pruebe a reiniciar el motor de cinta en Arcserve.

Para reiniciar el motor de cinta

1. Elija Quick Start, elija Administration y, a continuación, elija Device.
2. En el menú de navegación, abra el menú contextual (haga clic con el botón derecho) de la gateway y elija una ranura de importación/exportación.
3. Elija Quick Import y asigne una cinta a una ranura vacía.
4. Abra el menú contextual (haga clic con el botón derecho) de la gateway y elija Inventory/Offline Slots.
5. Elija Quick Inventory para recuperar información de medios de la base de datos.

Si agrega nuevas cintas, debe buscarlas en la gateway para que aparezcan en Arcserve. Si las nuevas cintas no aparecen, debe importarlas.

Para importar cintas

1. Elija el menú Quick Start, elija Back up y, a continuación, elija Destination tap.
2. Elija la gateway, abra el menú contextual (haga clic con el botón derecho) de una cinta y elija Import/Export Slot.

3. Abra el menú contextual (haga clic con el botón derecho) de cada cinta nueva y elija Inventory.
4. Abra el menú contextual (haga clic con el botón derecho) de cada cinta nueva y elija Format.

El código de barras de cada cinta aparece ahora en la consola de Storage Gateway y las cintas estarán listas para su uso.

Copia de seguridad de datos en una cinta

Cuando las cintas se hayan cargado en Arcserve, puede realizar un backup de los datos. El proceso de backup es el mismo que para las cintas físicas.

Para realizar un backup de datos en una cinta

1. Desde el menú Quick Start, abra la sesión de restauración de una copia de seguridad.
2. Elija la pestaña Source y, a continuación, elija el sistema de archivos o el sistema de base de datos del que desea realizar una copia de seguridad.
3. Elija la pestaña Schedule y elija el método de repetición que desee utilizar.
4. Elija la pestaña Schedule y elija el método de repetición que desee utilizar. Si el tamaño de los datos que está copiando supera al de la cinta, Arcserve le pedirá que monte una nueva cinta.
5. Elija Submit para hacer una copia de seguridad de los datos.

Note

Si la puerta de enlace de cinta se reinicia por algún motivo durante un trabajo de copia de seguridad en curso, es posible que el trabajo de copia de seguridad se realice incorrectamente. Para completar el trabajo de copia de seguridad incorrecto, debe volver a enviarlo.

Archivado de una cinta

Al archivar una cinta, la puerta de enlace de cinta traslada la cinta desde la biblioteca de cintas al almacenamiento sin conexión. Antes de expulsar y archivar una cinta, es posible que desee comprobar su contenido.

Para archivar una cinta

1. Desde el menú Quick Start, abra la sesión de restauración de una copia de seguridad.

2. Elija la pestaña Source y, a continuación, elija el sistema de archivos o el sistema de base de datos del que desea realizar una copia de seguridad.
3. Elija la pestaña Schedule y elija el método de repetición que desee utilizar.
4. Elija la gateway, abra el menú contextual (haga clic con el botón derecho) de una cinta y elija Import/Export Slot.
5. Asigne una ranura de correo para cargar la cinta. El estado de la consola de Storage Gateway cambia a Archivado. El proceso de archivado puede tardar algún tiempo.

El proceso de archivado puede tardar algún tiempo en completarse. El estado inicial de la cinta aparece como IN TRANSIT TO VTS. Cuando se inicia el archivado, el estado cambia a ARCHIVING. Una vez finalizado el archivado, la cinta ya no aparece en la lista, VTL sino que se archiva en S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive.

Restauración de datos desde una cinta

La restauración de datos archivados se realiza en dos fases.

Para restaurar datos desde una cinta archivada

1. Recupere la cinta archivada en una puerta de enlace de cinta. Para obtener instrucciones, consulte [Recuperación de cintas archivadas](#).
2. Utilice Arcserve para restaurar los datos. Este proceso es el mismo que la restauración de datos desde cintas físicas. Para ver las instrucciones, consulte la [documentación de Arcserve Backup r17](#).

Para restaurar datos desde una cinta, utilice el siguiente procedimiento.

Para restaurar datos desde una cinta

1. Desde el menú Quick Start, abra la sesión de restauración.
2. Elija la pestaña Source y, a continuación, elija el sistema de archivos o el sistema de base de datos que desea restaurar.
3. Elija la pestaña Destination y acepte la configuración predeterminada.
4. Elija la pestaña Schedule, elija el método de repetición que desee utilizar y, a continuación, elija Submit.

Paso siguiente

[Eliminación de recursos innecesarios](#)

Comprobación de la configuración mediante Bacula Enterprise

Puede hacer copias de seguridad de sus datos en cintas virtuales, archivarlas y administrar sus dispositivos de biblioteca de cintas virtuales (VTL) mediante Bacula Enterprise versión 10. En este tema, encontrará documentación básica acerca de cómo configurar la aplicación de copia de seguridad Bacula versión 10 para una puerta de enlace de cinta y realizar operaciones de copias de seguridad y restauración. Para obtener información detallada acerca de cómo utilizar Bacula versión 10, consulte los [manuales y documentación de Bacula Systems](#) o póngase en contacto con Bacula Systems.

Note

Bacula solo se admite en Linux.

Configuración de Bacula Enterprise

Una vez que haya conectado sus dispositivos de biblioteca de cintas virtuales (VTL) a su cliente Linux, configure el software Bacula para que reconozca sus dispositivos. Para obtener información sobre cómo conectar VTL los dispositivos a su cliente, consulte. [Conexión de sus VTL dispositivos](#)

Para instalar Bacula

1. Obtenga una copia con licencia del software Enterprise Bacula de Bacula Systems.
2. Instale el software Bacula Enterprise en su equipo local o en la nube.

Para obtener información acerca de cómo obtener el software de instalación, consulte el tema sobre [Enterprise Backup para Amazon S3 y Storage Gateway](#). Para obtener instrucciones de instalación adicionales, consulte el documento técnico de Bacula que trata sobre el [uso de servicios en la nube y almacenamiento de objetos con Bacula Enterprise Edition](#).

Configuración de Bacula para que funcione con dispositivos VTL

A continuación, configure Bacula para que funcione con sus dispositivos. VTL Seguidamente, encontrará los pasos de configuración básicos.

Para configurar Bacula

1. Instale Bacula Director y el daemon Bacula Storage. Para obtener instrucciones, consulte el capítulo 7 del documento técnico de Bacula que trata sobre el [uso de servicios en la nube y almacenamiento de objetos con Bacula Enterprise Edition](#).
2. Conéctese al sistema que ejecuta Bacula Director y configure el iniciador iSCSI. Para ello, utilice el script proporcionado en el paso 7.4 del documento técnico de Bacula que trata sobre el [uso de servicios en la nube y almacenamiento de objetos con Bacula Enterprise Edition](#).
3. Configure los dispositivos de almacenamiento. Utilice el script proporcionado en el documento técnico de Bacula indicado anteriormente.
4. Configure el Bacula Director local, añada los objetivos de almacenamiento y defina los grupos de medios de sus cintas. Utilice el script proporcionado en el documento técnico de Bacula indicado anteriormente.

Ejecución de backups de datos en cinta

1. Cree cintas desde la consola de Storage Gateway. Para obtener información sobre cómo crear cintas, consulte [Creación de cintas](#).
2. Transfiera las cintas de la ranura I/E a la ranura de almacenamiento mediante el siguiente comando.

```
/opt/bacula/scripts/mtx-changer
```

Por ejemplo, el siguiente comando transfiere las cintas de la ranura I/E 1601 a la ranura de almacenamiento 1.

```
/opt/bacula/scripts/mtx-changer transfer 1601 1
```

3. Inicie la consola de Bacula mediante el siguiente comando.

```
/opt/bacula/bin/bconsole
```

Note

Cuando cree y transfiera cintas a Bacula, utilice el comando de la consola de Bacula (bconsole) `update slots storage=VTL` para que Bacula reconozca las nuevas cintas que ha creado.

- Etiquete la cinta con el código de barras como el nombre o etiqueta del volumen mediante el siguiente comando de la bconsole.

```
label storage=VTL pool=pool.VTL barcodes === label the tapes with the  
barcode as the volume name / label
```

- Monte la cinta con el siguiente comando.

```
mount storage=VTL slot=1 drive=0
```

- Cree un trabajo de copia de seguridad que use los grupos de medios que ha creado y, a continuación, escriba datos en la cinta virtual utilizando los mismos procedimientos que con las cintas físicas.
- Desmonte la cinta desde la consola de Bacula mediante el siguiente comando.

```
umount storage=VTL slot=1 drive=0
```

Note

Si su Tape Gateway se reinicia por cualquier motivo durante un trabajo de backup en curso, el trabajo de backup fallará y el estado de la cinta en Bacula Enterprise cambiará a FULL. Si sabe que la cinta no se ha utilizado por completo, puede volver a cambiar manualmente el estado de la cinta a APPEND y continuar con el trabajo de respaldo con la misma cinta. También puede continuar con el trabajo en una cinta diferente si hay otras cintas en estado APPEND disponibles.

Archivado de una cinta

Cuando hayan terminado todos los trabajos de copia de seguridad de una determinada cinta y pueda archivar la cinta, utilice el script `mtx-changer` para mover la cinta de la ranura de almacenamiento a la ranura I/E. Esta acción es similar a la acción de expulsión en otras aplicaciones de copia de seguridad.

Para archivar una cinta

- Transfiera la cinta de la ranura de almacenamiento a la ranura I/E mediante el siguiente comando `/opt/bacula/scripts/mtx-changer`.

Por ejemplo, el siguiente comando transfiere una cinta de la ranura de almacenamiento 1 a la ranura I/E 1601.

```
/opt/bacula/scripts/mtx-changer transfer 1 1601
```

2. Compruebe que la cinta está archivada en el almacenamiento sin conexión (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive) y que tiene el estado Archivada.

Restauración de datos desde una cinta archivada y recuperada

La restauración de datos archivados se realiza en dos fases.

Para restaurar datos desde una cinta archivada

1. Recupere la cinta archivada desde el archivo a la puerta de enlace de cinta. Para obtener instrucciones, consulte [Recuperación de cintas archivadas](#).
2. Restaure los datos mediante el software Bacula:
 - a. Importe las cintas en la ranura de almacenamiento con el comando `/opt/bacula/scripts/mtx-changer` para transferir cintas desde la ranura I/E.

Por ejemplo, el siguiente comando transfiere las cintas de la ranura I/E 1601 a la ranura de almacenamiento 1.

```
/opt/bacula/scripts/mtx-changer transfer 1601 1
```

- b. Utilice la consola de Bacula para actualizar las ranuras y, a continuación, monte la cinta.
- c. Ejecute el comando de restauración para restaurar los datos. Para obtener instrucciones, consulte la documentación de Bacula.

Comprobación de la configuración mediante Commvault

Puede hacer copias de seguridad de sus datos en cintas virtuales, archivarlas y administrar sus dispositivos de biblioteca de cintas virtuales con la versión 11 de Commvault. VTL En este tema encontrará la documentación básica acerca de cómo configurar la aplicación de copia de seguridad Commvault para una puerta de enlace de cinta, crear un archivo de copia de seguridad y recuperar datos de cintas archivadas. Para obtener información detallada acerca de cómo utilizar Commvault, consulte [Commvault Quick Start Guide](#) en el sitio web de Commvault.

Temas

- [Configuración de Commvault para que funcione con dispositivos VTL](#)
- [Creación de una política de almacenamiento y de un subcliente](#)
- [Backup de datos en una cinta en Commvault](#)
- [Archivado de cintas en Commvault](#)
- [Restauración de datos desde una cinta](#)

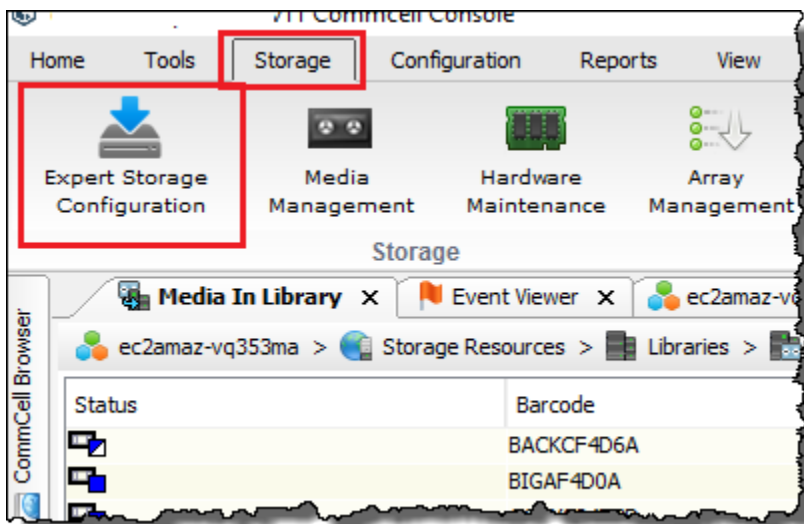
Configuración de Commvault para que funcione con dispositivos VTL

Tras conectar los VTL dispositivos al cliente de Windows, debe configurar Commvault para que los reconozca. Para obtener información sobre cómo conectar VTL los dispositivos al cliente de Windows, consulte [Conexión de sus VTL dispositivos a un cliente de Windows](#).

La aplicación de backup de Commvault no reconoce automáticamente VTL los dispositivos. Debe agregar manualmente los dispositivos para exponerlos a la aplicación de backup Commvault y, a continuación, detectar los dispositivos.

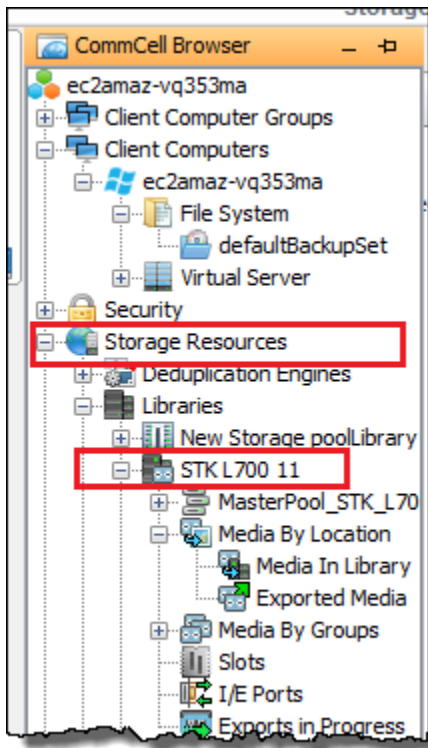
Para configurar Commvault

1. En el menú principal de la CommCell consola, seleccione Almacenamiento y, a continuación, seleccione Configuración de almacenamiento experta para abrir el cuadro de MediaAgents diálogo de selección.



2. Elija el agente de medios disponible que desee utilizar, seleccione Add y, a continuación, elija OK.
3. En el cuadro de diálogo Expert Storage Configuration, elija Start y, a continuación, Detect/Configure Devices.

4. Deje seleccionada la opción Device Type, seleccione primero Exhaustive Detection y, después, OK.
5. En el cuadro de diálogo de confirmación Confirm Exhaustive Detection, seleccione Yes.
6. En el cuadro de diálogo Device Selection, elija la biblioteca y todas sus unidades y, a continuación, elija OK. Espere que los dispositivos sean detectados y, a continuación, elija Close para cerrar el informe de registros.
7. Haga clic con el botón derecho en la biblioteca, seleccione Configure y, a continuación, seleccione Yes. Cierre el cuadro de diálogo de configuración.
8. En la sección ¿Tiene esta biblioteca un lector de códigos de barras? cuadro de diálogo, elija Sí y, a continuación, para el tipo de dispositivo, elija IBMULTRIUMV5.
9. En el CommCell navegador, selecciona Recursos de almacenamiento y, a continuación, selecciona Bibliotecas para ver tu biblioteca de cintas.



10. Para ver las cintas de su biblioteca, abra el menú contextual (haga clic con el botón derecho) de la biblioteca y, a continuación, elija Discover Media, Media location, Media Library.
11. Para montar las cintas, abra el menú contextual (haga clic con el botón derecho) del medio y después elija Load.

Creación de una política de almacenamiento y de un subcliente

Cada trabajo de backup y restauración está asociado con una política de almacenamiento y una política de subcliente.

Una política de almacenamiento asigna la ubicación original de los datos a los medios.

Para crear una política de almacenamiento

1. En el CommCell navegador, elija Políticas.
2. Abra el menú contextual (haga clic con el botón derecho) de Storage Policies y después elija New Storage Policy.
3. En el asistente "Create Storage Policy", seleccione Data Protection and Archiving y, a continuación, Next.
4. Escriba un nombre para la política de almacenamiento en Storage Policy Name y, a continuación, elija Incremental Storage Policy. Para asociar esta política de almacenamiento con cargas incrementales, seleccione una de las opciones. De lo contrario, deje las opciones sin marcar y, a continuación, seleccione Next.
5. En el cuadro de diálogo Do you want to Use Global Deduplication Policy?, elija la opción de Deduplication que prefiera y, a continuación, elija Next.
6. En Biblioteca como Copia principal, selecciona tu VTL biblioteca y, a continuación, selecciona Siguiente.
7. Compruebe que la configuración del agente de medios es la correcta y, a continuación, elija Next.
8. Compruebe que la configuración del grupo de reserva es la correcta y, a continuación, elija Next.
9. Configure sus políticas de retención en los datos de iData Agent Backup y, a continuación, seleccione Siguiente.
10. Revise la configuración del cifrado y, a continuación, elija Next.
11. Para ver la política de almacenamiento, elija Storage Policies.

Cree una política de subcliente y asíciela con su política de almacenamiento. Una política de subcliente le permite configurar clientes de sistemas de archivos similares a partir de una plantilla central, para que no tenga que configurar varios sistemas de archivos similares manualmente.

Para crear una política de subcliente

1. En el CommCell navegador, elija Ordenadores cliente y, a continuación, elija su ordenador cliente. Elija Sistema de archivos y, a continuación, elija defaultBackupSet.
2. Haga clic con defaultBackupSetel botón derecho, elija Todas las tareas y, a continuación, elija Nuevo subcliente.
3. En el cuadro de propiedades del subcliente, escriba un nombre en SubClient Nombre y, a continuación, pulse Aceptar.
4. Elija Browse, diríjase a los archivos cuya copia de seguridad desea realizar, seleccione Add y cierre el cuadro de diálogo.
5. En el cuadro de propiedades Subclient, elija la pestaña Storage Device, una política de almacenamiento en Storage policy y OK.
6. En la ventana de Backup Schedule que aparece, asocie el nuevo subcliente con una programación de copia de seguridad.
7. Elija Do Not Schedule si desea que la copia de seguridad se realice una sola vez o bajo demanda y, a continuación, elija OK.

Ahora debería ver su subcliente en la defaultBackupSetpestaña.

Backup de datos en una cinta en Commvault

Cree un trabajo de backup y escriba datos en una cinta virtual utilizando los mismos procedimientos que con las cintas físicas. Para obtener más información, consulte la [documentación de Commvault](#).

Note

Si la puerta de enlace de cinta se reinicia por algún motivo durante un trabajo de copia de seguridad en curso, es posible que el trabajo de copia de seguridad se realice incorrectamente. En algunos casos, puede seleccionar una opción para reanudar el trabajo incorrecto. De lo contrario, tendrá que enviar un nuevo trabajo. Si Commvault marca la cinta como inutilizable después de un trabajo incorrecto, debe volver a cargar la cinta en la unidad para seguir grabando en ella. Si hay varias cintas disponibles, Commvault podría continuar con el trabajo de copia de seguridad incorrecto en una cinta diferente.

Archivado de cintas en Commvault

Puede iniciar el proceso de archivado expulsando la cinta. Al archivar una cinta, la puerta de enlace de cinta traslada la cinta desde la biblioteca de cintas al almacenamiento sin conexión. Antes de expulsar y archivar una cinta, es posible que primero desee comprobar su contenido.

Para archivar una cinta

1. En el CommCell navegador, selecciona Recursos de almacenamiento, Bibliotecas y, a continuación, selecciona Tu biblioteca. Elija Media By Location y, a continuación, elija Media In Library.
2. Abra el menú contextual (haga clic con el botón derecho) de la cinta que desee archivar, elija All Tasks, Export y, a continuación, OK.

El proceso de archivado puede tardar algún tiempo en completarse. El estado inicial de la cinta aparece como IN TRANSIT TO VTS. Cuando se inicia el archivado, el estado cambia a ARCHIVING. Una vez finalizado el archivado, la cinta ya no aparece en la lista. VTL

En el software Commvault, compruebe que la cinta ya no se encuentra en la ranura de almacenamiento.

En el panel de navegación de la consola de Storage Gateway, elija Cintas. Compruebe que el estado de la cinta archivada sea. ARCHIVED

Restauración de datos desde una cinta

Puede restaurar los datos de una cinta que nunca se ha archivado ni recuperado, o que sí se haya archivado y recuperado. En el caso de cintas que nunca se han archivado ni recuperado (cintas "nonretrieved"), dispone de dos opciones para restaurar los datos:

- Restaurar por subcliente
- Restaurar por ID de trabajo

Para restaurar los datos de una cinta "nonretrieved" por subcliente

1. En el CommCell navegador, elija Ordenadores cliente y, a continuación, elija su ordenador cliente. Elija Sistema de archivos y, a continuación, elija defaultBackupSet.
2. Abra el menú contextual (haga clic con el botón derecho) de su subcliente, elija Browse and Restore y, a continuación, elija View Content.

3. Elija los archivos que desea restaurar y, a continuación, elija Recover All Selected.
4. Seleccione Home y, después, Job Controller para supervisar el estado del trabajo de restauración.

Para restaurar los datos de una cinta "nonretrieved" por ID de trabajo

1. En el CommCell navegador, elija Ordenadores cliente y, a continuación, elija su ordenador cliente. Haga clic con el botón derecho del ratón en File System, seleccione View y, a continuación, seleccione Backup History.
2. En la categoría Backup Type, elija el tipo de trabajo de copia de seguridad que desee y, a continuación, elija OK. Aparecerá una pestaña con el historial de trabajos de backup.
3. Busque el Job ID que desea restaurar, haga clic con el botón derecho del ratón en él y, a continuación, elija Browse and Restore.
4. En el cuadro de diálogo Browse and Restore Options, elija View Content.
5. Elija los archivos que desea restaurar y, a continuación, elija Recover All Selected.
6. Seleccione Home y, después, Job Controller para supervisar el estado del trabajo de restauración.

Para restaurar los datos de una cinta archivada y recuperada

1. En el CommCell navegador, elija Recursos de almacenamiento, Bibliotecas y, a continuación, elija Su biblioteca. Elija Media By Location y, a continuación, elija Media In Library.
2. Haga clic con el botón derecho del ratón en la cinta recuperada, elija All Tasks y, a continuación, elija Catalog.
3. En el cuadro de diálogo Catalog Media, elija Catalog only y, a continuación, OK.
4. Seleccione CommCell Inicio y, a continuación, seleccione Job Controller para supervisar el estado del trabajo de restauración.
5. Una vez que el trabajo finalice correctamente, abra el menú contextual (haga clic con el botón derecho) de la cinta, seleccione View y, a continuación, elija View Catalog Contents. Anote el valor de Job ID para usarlo más adelante.
6. Elija Recatalog/Merge. Asegúrese de que esté seleccionado Merge only en el cuadro de diálogo Catalog Media.
7. Seleccione Home y, después, Job Controller para supervisar el estado del trabajo de restauración.

8. Cuando el trabajo se haya realizado correctamente, selecciona CommCell Inicio, Panel de control y, a continuación, selecciona Navegar/Buscar/Recuperar.
9. Elija Show aged data during browse and recovery, OK y, finalmente, cierre Control Panel.
10. En el CommCell navegador, haga clic con el botón derecho en Computadoras cliente y, a continuación, seleccione su computadora cliente. Elija View y, a continuación, elija Job History.
11. En el cuadro de diálogo Job History Filter, elija Advanced.
12. Elija Incluir Aged Data y, a continuación, elija OK.
13. En el cuadro de diálogo Job History, elija OK para abrir la pestaña history of jobs.
14. Busque el trabajo que desea restaurar, abra el menú contextual (haga clic con el botón derecho) del trabajo y, a continuación, elija Browse and Restore.
15. En el cuadro de diálogo Browse and Restore, elija View Content.
16. Elija los archivos que desea restaurar y, a continuación, elija Recover All Selected.
17. Seleccione Home y, después, Job Controller para supervisar el estado del trabajo de restauración.

Probar su configuración con Dell EMC NetWorker

Con Dell EMC NetWorker 19.5, puede hacer copias de seguridad de sus datos en cintas virtuales, archivarlas y administrar los dispositivos de su biblioteca de cintas virtuales (VTL). En este tema, encontrará documentación básica sobre cómo configurar el EMC NetWorker software de Dell para que funcione con una puerta de enlace en cinta y realizar una copia de seguridad, incluida la forma de configurar los dispositivos de almacenamiento, escribir datos en una cinta, archivar una cinta y restaurar los datos de una cinta.

Para obtener información detallada sobre cómo instalar y usar el EMC NetWorker software de Dell, consulte la [Guía de administración](#).

Para obtener más información sobre aplicaciones de backup compatibles, consulte [Aplicaciones de copia de seguridad de terceros compatibles con una puerta de enlace de cinta](#).

Temas

- [Configuración para que funcione con VTL dispositivos](#)
- [Permitir la importación de WORM cintas a Dell EMC NetWorker](#)
- [Hacer copias de seguridad de los datos en una cinta en Dell EMC NetWorker](#)
- [Archivar una cinta en Dell EMC NetWorker](#)


- [Restauración de datos de una cinta archivada en Dell EMC NetWorker](#)

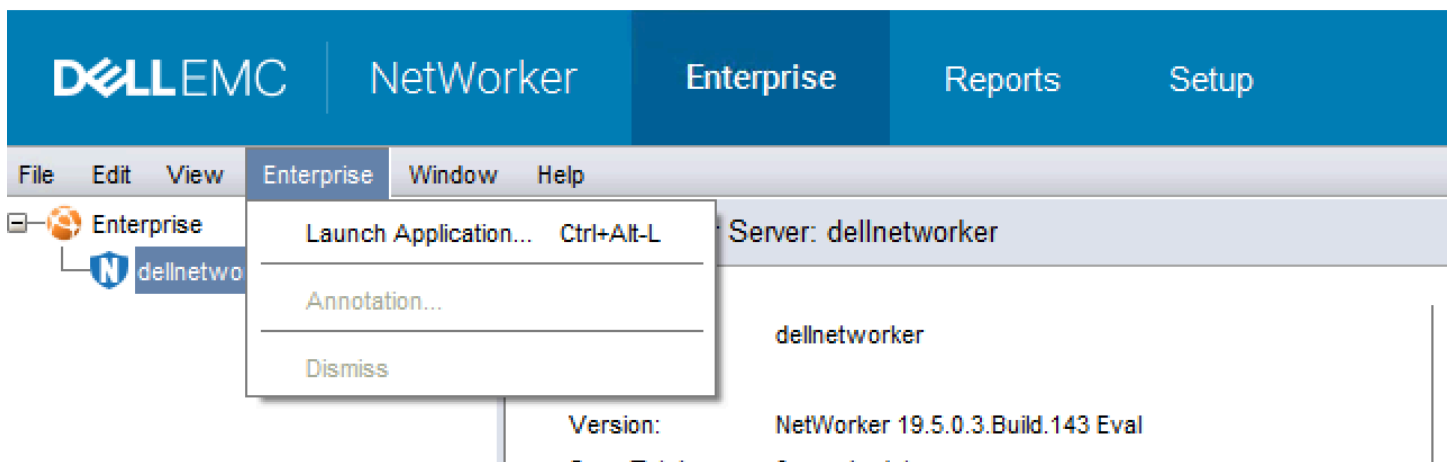
Configuración para que funcione con VTL dispositivos

Después de conectar los dispositivos de la biblioteca de cintas virtuales (VTL) al cliente de Microsoft Windows, debe configurarlos para reconocer los dispositivos. Para obtener información acerca de cómo conectar VTL los dispositivos al cliente de Windows, consulte [Conexión de sus VTL dispositivos](#).

no reconoce automáticamente dispositivos de puerta de enlace de cinta. Para exponer sus VTL dispositivos al NetWorker software y hacer que el software los detecte, debe configurar el software manualmente. En adelante, daremos por hecho que ha instalado correctamente el software y que se ha familiarizado con la consola de administración. Para obtener más información sobre la consola de administración, consulte la sección sobre la interfaz de la consola de NetWorker administración de la [Guía de EMC NetWorker administración de Dell](#).

La siguiente captura de pantalla muestra la versión EMC NetWorker 19.5 de Dell.

 NetWorker Management Console V19.5.0.3 - localhost



Para configurar el EMC NetWorker software de Dell para VTL los dispositivos

1. Inicie la aplicación Dell EMC NetWorker Management Console, seleccione Enterprise en el menú y, a continuación, seleccione localhost en el panel izquierdo.
2. Abra el menú contextual (clic con el botón derecho) para localhost y, a continuación, elija Launch Application.
3. Seleccione la pestaña Devices, abra el menú contextual (clic con el botón derecho) para Libraries y, a continuación, elija Scan for Devices.

4. En el asistente Scan for Devices, elija Start Scan y, a continuación, elija Aceptar en el cuadro de diálogo que aparece.
5. Amplíe el árbol de la carpeta Bibliotecas para ver todas las bibliotecas y pulse F5 para actualizar. Este proceso podría tardar unos segundos en cargar los dispositivos en la biblioteca.
6. Abra una ventana de comandos (CMD.exe) con privilegios de administrador y ejecute la utilidad «jbconfig» que viene instalada en la versión 19.5 de Dell. EMC NetWorker

```
Microsoft Windows [Version 10.0.17763.2366]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>jbconfig

Jbconfig is running on host dellnetworker (Windows Server 2019 Datacenter 10.0),
and is using dellnetworker as the NetWorker server.

    1) Configure an Autodetected SCSI Jukebox.
    2) Configure an Autodetected NDMP SCSI Jukebox.
    3) Configure an SJI Jukebox.
    4) Configure an STL Silo.
    5) Exit.

Which activity do you want to perform? [1]
14484:jbconfig: Scanning SCSI buses; this may take a while ...
Installing 'Standard SCSI Jukebox' jukebox - scsidev@1.0.0.

What name do you want to assign to this jukebox device? AWSVTL
15814:jbconfig: Attempting to detect serial numbers on the jukebox and drives ...

15815:jbconfig: Will try to use SCSI information returned by jukebox to configure drives.

Turn NetWorker auto-cleaning on (yes / no) [yes]? no

The following drive(s) can be auto-configured in this jukebox:
1> LTO Ultrium-5 @ 1.1.0 ==> \\.\Tape0
2> LTO Ultrium-5 @ 1.2.0 ==> \\.\Tape1
3> LTO Ultrium-5 @ 1.3.0 ==> \\.\Tape2
4> LTO Ultrium-5 @ 1.4.0 ==> \\.\Tape3
5> LTO Ultrium-5 @ 1.5.0 ==> \\.\Tape4
6> LTO Ultrium-5 @ 1.6.0 ==> \\.\Tape5
7> LTO Ultrium-5 @ 1.7.0 ==> \\.\Tape6
8> LTO Ultrium-5 @ 1.8.0 ==> \\.\Tape7
9> LTO Ultrium-5 @ 1.9.0 ==> \\.\Tape8
10> LTO Ultrium-5 @ 1.10.0 ==> \\.\Tape9
These are all the drives that this jukebox has reported.
```

```

To change the drive model(s) or configure them as shared or NDMP drives,
you need to bypass auto-configure. Bypass auto-configure? (yes / no) [no]

Jukebox has been added successfully

The following configuration options have been set:

> Jukebox description to the control port and model.
> Autochanger control port to the port at which we found it.
> Autocleaning off.
> Barcode reading to on.
> Volume labels that match the barcodes.

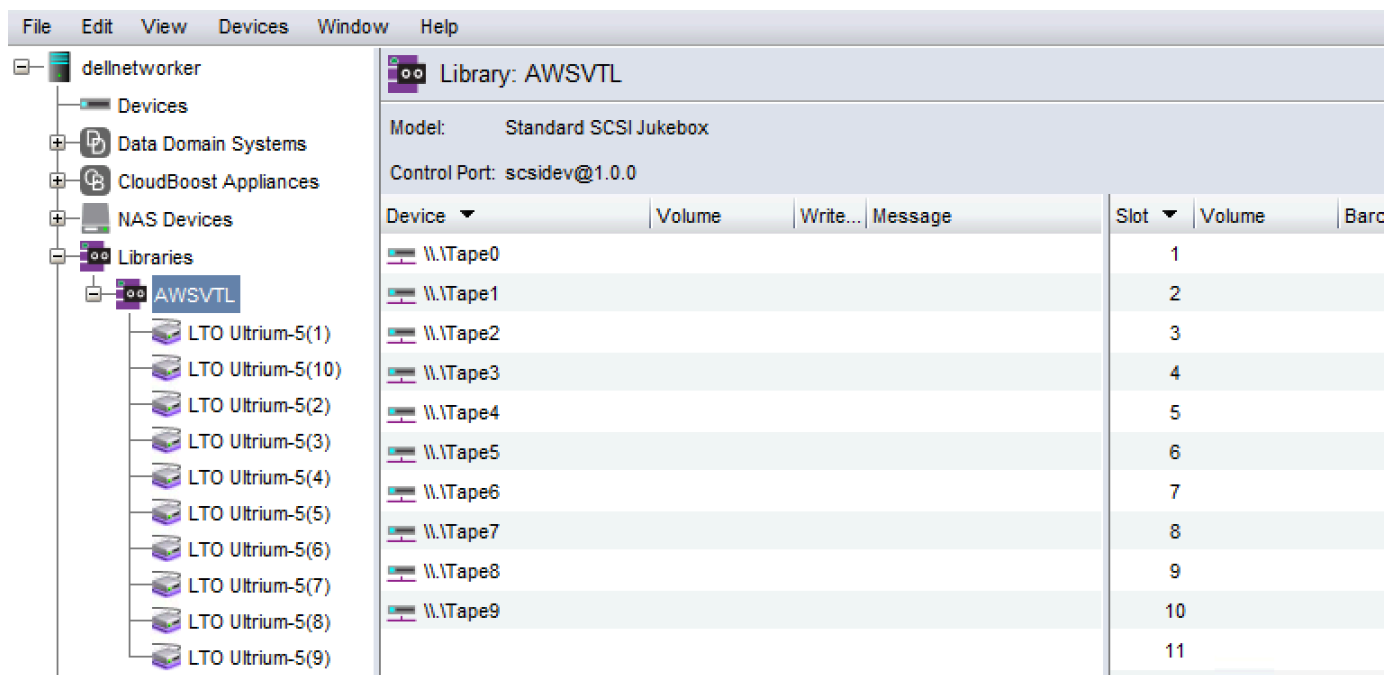
You can review and change the characteristics of the autochanger and its
associated devices using the NetWorker Management Console.

Would you like to configure another jukebox? (yes/no) [no]

C:\Users\Administrator>_

```

7. Cuando termine «jbconfig», regrese a NetWorker GUI y presione F5 para actualizar.
8. Elija la biblioteca para ver las cintas en el panel izquierdo y las correspondientes ranuras vacías en el panel derecho. En esta captura de pantalla, se selecciona la biblioteca AWSVTL "».



Device	Volume	Write...	Message	Slot	Volume	Barc
\\Tape0				1		
\\Tape1				2		
\\Tape2				3		
\\Tape3				4		
\\Tape4				5		
\\Tape5				6		
\\Tape6				7		
\\Tape7				8		
\\Tape8				9		
\\Tape9				10		
				11		

9. En la lista de volúmenes, seleccione los volúmenes que desee activar (los volúmenes seleccionados se resaltan), abra el menú contextual (clic con el botón secundario) para los volúmenes seleccionados y, a continuación, elija Depósito. Esta acción traslada la cinta de la ranura I/E a la ranura de volumen.

10. En el cuadro de diálogo que aparece, elija Yes y, a continuación, en el cuadro de diálogo Load the Cartridges into, seleccione Yes.
11. Si no tiene más cintas para depositar, elija No o Ignore. De lo contrario, elija Yes para depositar más cintas.

Permitir la importación de WORM cintas a Dell EMC NetWorker

Ahora está listo para importar cintas desde su Tape Gateway a la EMC NetWorker biblioteca de Dell.

Las cintas virtuales se escriben una vez y se leen muchas (WORM) cintas, pero Dell EMC NetWorker espera que no sean WORM cintas. Para EMC NetWorker que Dell funcione con sus cintas virtuales, debe activar la importación de las cintas a grupos no WORM multimedia.

Para permitir la importación de WORM cintas a grupos no WORM multimedia

1. En la NetWorker consola, elija Multimedia, abra el menú contextual (haga clic con el botón derecho) de localhost y, a continuación, seleccione Propiedades.
2. En la ventana Propiedades del NetWorker servidor, seleccione la pestaña Configuración.
3. En la sección Manipulación de WORM cintas helicoidales, desactive la casilla «Cintas solo en WORM grupos» y, a continuación, pulse Aceptar.

Hacer copias de seguridad de los datos en una cinta en Dell EMC NetWorker

La copia de seguridad de datos en una cinta es un proceso de dos pasos.

1. Etiquete las cintas en las que desea realizar una copia de seguridad de los datos, cree el grupo de medios de destino y agregue las cintas al grupo.

Cree un grupo de medios y escriba datos en una cinta virtual utilizando los mismos procedimientos que con las cintas físicas. Para obtener información detallada, consulte la sección sobre copias de seguridad de los datos de la [Guía de EMC NetWorker administración de Dell](#).

2. Escriba datos en la cinta. Las copias de seguridad de los datos se realizan mediante la aplicación de EMC NetWorker usuario de Dell en lugar de la consola de EMC NetWorker administración de Dell. La aplicación EMC NetWorker de usuario de Dell se instala como parte de la NetWorker instalación.

Note

Utiliza la aplicación de EMC NetWorker usuario de Dell para realizar copias de seguridad, pero puede ver el estado de las tareas de copia de seguridad y restauración en la consola EMC de administración. Para ver el estado, elija el menú Devices y vea el estado en la ventana Log.

Note

Si su Tape Gateway se reinicia por cualquier motivo durante un trabajo de respaldo en curso, el trabajo de respaldo se suspenderá y el estado de la cinta en Dell EMC NetWorker cambiará a Protección contra escritura. Puede archivar la cinta o seguir leyendo sus datos. Puede reanudar la tarea de copia de seguridad suspendida en una cinta diferente.

Archivar una cinta en Dell EMC NetWorker

Al archivar una cinta, Tape Gateway traslada la cinta de la biblioteca de EMC NetWorker cintas de Dell al almacenamiento fuera de línea. Para iniciar el archivado de cintas, extraiga un cinta de la unidad de cinta y colóquela en la ranura de almacenamiento. A continuación, extraiga la cinta de la ranura y colóquela en el archivo mediante su aplicación de respaldo, es decir, el software de Dell EMC NetWorker .

Para archivar una cinta con Dell EMC NetWorker

1. En la pestaña Dispositivos de la ventana de NetWorker administración, elija localhost o su EMC servidor y, a continuación, elija Bibliotecas.
2. Elija la biblioteca que importó desde la biblioteca de cintas virtuales.
3. Desde la lista de cintas en las que ha escrito datos, abra el menú contextual (clic con el botón secundario) de la cinta que desea archivar y, a continuación, elija Eject/Withdraw.
4. En el cuadro de diálogo que aparece, elija OK.

El proceso de archivado puede tardar algún tiempo en completarse. El estado inicial de la cinta aparece como IN TRANSIT TO VTS. Cuando se inicia el archivado, el estado cambia a ARCHIVING. Cuando se haya completado el archivado, la cinta ya no aparecerá en la lista. VTL

En el EMC NetWorker software de Dell, compruebe que la cinta ya no esté en la ranura de almacenamiento.

En el panel de navegación de la consola de Storage Gateway, elija Cintas. Compruebe que el estado de la cinta archivada sea ARCHIVED.

Restauración de datos de una cinta archivada en Dell EMC NetWorker

La restauración de datos archivados se realiza en dos fases:

1. Recupere la cinta archivada en una puerta de enlace de cinta. Para obtener instrucciones, consulte [Recuperación de cintas archivadas](#).
2. Utilice el EMC NetWorker software de Dell para restaurar los datos. Para ello, cree un archivo de carpeta de restauración, de la misma forma que cuando se restauran datos desde cintas físicas. Para obtener instrucciones, consulte la sección Uso del programa de NetWorker usuario de la [Guía de EMC NetWorker administración de Dell](#).

Paso siguiente

[Eliminación de recursos innecesarios](#)

Probar su configuración mediante IBM Spectrum Protect

Puede hacer copias de seguridad de sus datos en cintas virtuales, archivarlas y administrar sus dispositivos de biblioteca de cintas virtuales (VTL) mediante IBM Spectrum Protect with AWS Storage Gateway. (IBMSpectrum Protect se conocía anteriormente como Tivoli Storage Manager).

Este tema contiene información básica sobre cómo configurar el software de respaldo IBM Spectrum Protect, versión 8.1.10, para una puerta de enlace de cinta. También incluye información básica sobre cómo realizar operaciones de copia de seguridad y restauración con IBM Spectrum Protect. Para obtener más información sobre cómo administrar el software de respaldo IBM Spectrum Protect, consulte IBM la [descripción general de las tareas de administración de](#) IBM Spectrum Protect.

El software de respaldo IBM Spectrum Protect es compatible con AWS Storage Gateway los siguientes sistemas operativos.

- Microsoft Windows Server
- Red Hat Linux

Para obtener información sobre los dispositivos compatibles con IBM Spectrum Protect para Windows, consulte [Dispositivos compatibles con IBM Spectrum Protect \(anteriormente Tivoli Storage Manager\) para AIX HP-UX, Solaris y Windows](#).

Para obtener información sobre los dispositivos compatibles con IBM Spectrum Protect para Linux, consulte [Dispositivos compatibles con IBMSpectrum Protect \(anteriormente Tivoli Storage Manager\) para Linux](#).

Temas

- [Configuración de IBM Spectrum Protect](#)
- [Configuración de IBM Spectrum Protect para que funcione con VTL dispositivos](#)
- [Grabación de datos en una cinta en IBM Spectrum Protect](#)
- [Restauración de datos de una cinta archivada en IBM Spectrum Protect](#)

Configuración de IBM Spectrum Protect

Después de conectar VTL los dispositivos al cliente, debe configurar el software IBM Spectrum Protect, versión 8.1.10, para que los reconozca. Para obtener más información sobre la conexión de VTL dispositivos a su cliente, consulte [Conexión de sus VTL dispositivos](#)

Para configurar IBM Spectrum Protect

1. Obtenga una copia con licencia del software IBM Spectrum Protect, versión 8.1.10, en IBM
2. Instale el software IBM Spectrum Protect en su entorno local o en su instancia de Amazon EC2 en la nube. Para obtener más información, consulta IBM la documentación de [instalación y actualización](#) de IBM Spectrum Protect.

Para obtener más información sobre la configuración IBM del software Spectrum Protect, consulte [Configuración de bibliotecas de AWS cintas virtuales de Tape Gateway para un servidor IBM Spectrum Protect](#).

Configuración de IBM Spectrum Protect para que funcione con VTL dispositivos

A continuación, configure IBM Spectrum Protect para que funcione con sus VTL dispositivos. Puede configurar IBM Spectrum Protect para que funcione con VTL dispositivos de Microsoft Windows Server o Red Hat Linux.

Configuración de IBM Spectrum Protect para Windows

Para obtener instrucciones completas sobre cómo configurar IBM Spectrum Protect en Windows, consulte el [controlador de dispositivo de cinta W12 6266 para Windows 2012](#) en el sitio web de Lenovo. A continuación se muestra la documentación básica del proceso.

Para configurar IBM Spectrum Protect para Microsoft Windows

1. Obtenga el paquete de controlador correcto para el cambiador de medios. Para el controlador del dispositivo de cinta, IBM Spectrum Protect requiere la versión W12 6266 para Windows 2012. Para obtener instrucciones sobre cómo obtener los controladores, consulte la página del [controlador del dispositivo de cinta W12 6266 para Windows 2012](#) en el sitio web de Lenovo.

Note

Asegúrese de instalar el conjunto de controladores "no exclusivos".

2. En su computadora, abra Administración de computadoras, expanda Dispositivos cambiadores de medios y compruebe que el tipo de cambiador de medios aparezca como Biblioteca de cintas 3584. IBM
3. Asegúrese de que el código de barras de las cinta de la biblioteca de cintas virtuales tiene ocho caracteres o menos. Si intenta asignar un código de barras de más de ocho caracteres a la cinta, aparece este mensaje de error: "Tape barcode is too long for media changer".
4. Asegúrese de que todas las unidades de cinta y el cambiador de medios aparezcan en Spectrum Protect. IBM Para ello, utilice el siguiente comando: `\Tivoli\TSM \server>tsmdlst.exe`

Configure IBM Spectrum Protect para Linux

A continuación se incluye la documentación básica sobre cómo configurar IBM Spectrum para que funcione con VTL dispositivos en Linux.

Para configurar IBM Spectrum Protect para Linux

1. Ve a [IBMFix Central](#) en el sitio web de IBM Support y selecciona Select product.
2. En Product Group (Grupo de productos), seleccione System Storage (Almacenamiento del sistema).

3. En **Select from System Storage** (Seleccionar desde el almacenamiento del sistema), seleccione **Tape systems** (Sistemas de cinta).
4. En **Tape systems** (Sistemas de cintas), seleccione **Tape drivers and software** (Software y controladores de cintas).
5. En **Select from Tape drivers and software** (Seleccionar desde el software y los controladores de cintas), seleccione **Tape device drivers** (Controladores del dispositivo de cintas).
6. En **Platform** (Plataforma), seleccione su sistema operativo y elija **Continue** (Continuar).
7. Seleccione la versión del controlador del dispositivo que desee descargar. A continuación, siga las instrucciones de la página de descargas de Fix Central para descargar y configurar IBM Spectrum Protect.
8. Asegúrese de que el código de barras de la cinta de la biblioteca de cintas virtuales tiene ocho caracteres o menos. Si intenta asignar un código de barras de más de ocho caracteres a la cinta, aparece este mensaje de error: "Tape barcode is too long for media changer".

Grabación de datos en una cinta en IBM Spectrum Protect

Para escribir datos en una cinta virtual de puerta de enlace de cinta, utilice el mismo procedimiento y las mismas políticas de copia de seguridad que con las cintas físicas. Cree la configuración necesaria para los trabajos de copia de seguridad y restauración. Para obtener más información sobre la configuración de IBM Spectrum Protect, consulte [Descripción general de las tareas de administración de IBM Spectrum Protect](#).

Note

Si la puerta de enlace de cinta se reinicia por algún motivo durante un trabajo de copia de seguridad en curso, es posible que el trabajo de copia de seguridad se realice incorrectamente. Si el trabajo de respaldo falla, el estado de la cinta en IBM Spectrum Protect cambia a ReadOnly. Si sabe que la cinta no se ha utilizado por completo, puede volver a cambiar manualmente el estado de la cinta a y reanudar o volver a ReadWriteenviar el trabajo de respaldo con la misma cinta. IBMSpectrum Protect podría continuar con el trabajo de backup fallido en una cinta diferente si hay otras cintas en ReadWriteese estado disponibles.

Restauración de datos de una cinta archivada en IBM Spectrum Protect

La restauración de datos archivados se realiza en dos fases.

Para restaurar datos desde una cinta archivada

1. Recupere la cinta archivada desde el archivo a la puerta de enlace de cinta. Para obtener instrucciones, consulte [Recuperación de cintas archivadas](#).
2. Restaure los datos mediante el software de respaldo IBM Spectrum Protect. Para ello, cree un punto de recuperación, de la misma forma que cuando se restauran datos desde cintas físicas. Para obtener más información sobre la configuración de IBM Spectrum Protect, consulte [Descripción general de las tareas de administración de](#) IBM Spectrum Protect.

Paso siguiente

[Eliminación de recursos innecesarios](#)

Probar la configuración mediante Micro Focus Data Protector

Puede hacer copias de seguridad de sus datos en cintas virtuales, archivarlas y administrar sus dispositivos de biblioteca de cintas virtuales (VTL) mediante Micro Focus (HPE) Data Protector v9.x. En este tema encontrará documentación básica sobre cómo configurar el software Micro Focus (HPE) Data Protector para una puerta de enlace de cinta y realizar una operación de copia de seguridad y restauración. Para obtener información detallada sobre cómo utilizar el software Micro Focus (HPE) Data Protector, consulte la documentación de Hewlett Packard. Para obtener más información sobre aplicaciones de backup compatibles, consulte [Aplicaciones de copia de seguridad de terceros compatibles con una puerta de enlace de cinta](#).

Temas

- [Configuración del protector de datos Micro Focus \(HPE\) para que funcione con dispositivos VTL](#)
- [Preparación de cintas virtuales para utilizarlas con Data Protector HPE](#)
- [Carga de cintas en un grupo de medios](#)
- [Copia de seguridad de datos en una cinta](#)
- [Archivado de una cinta](#)
- [Restauración de datos desde una cinta](#)

Configuración del protector de datos Micro Focus (HPE) para que funcione con dispositivos VTL

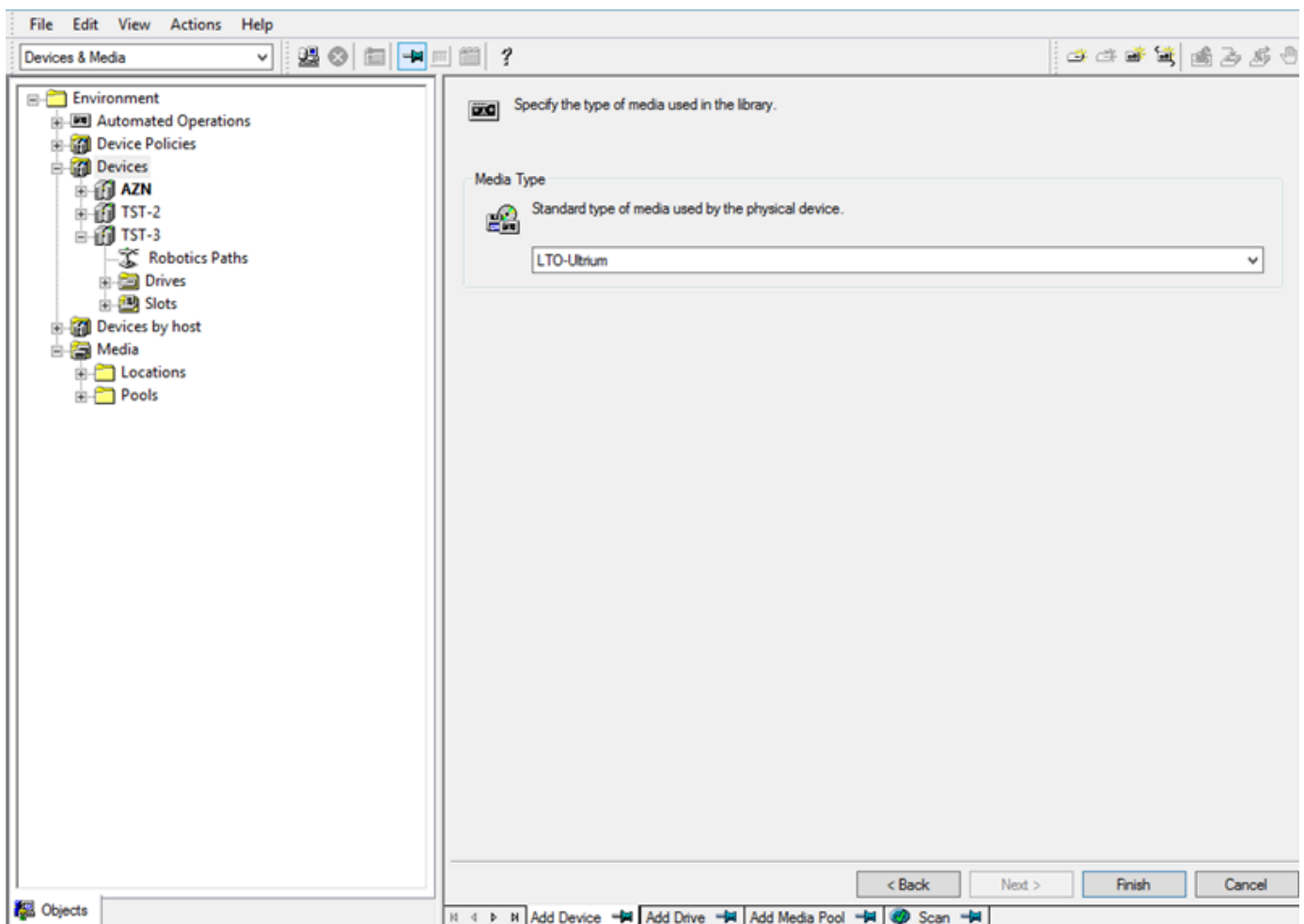
Tras conectar los dispositivos de la biblioteca de cintas virtuales (VTL) al cliente, configure Micro Focus (HPE) Data Protector para que reconozca sus dispositivos. Para obtener información sobre cómo conectar VTL los dispositivos al cliente, consulte [Conexión de sus VTL dispositivos](#).

El software Micro Focus (HPE) Data Protector no reconoce automáticamente los dispositivos Tape Gateway. Para que el software reconozca estos dispositivos, agréguelos manualmente y, a continuación, detecte los VTL dispositivos, tal y como se describe a continuación.

Para añadir los VTL dispositivos

1. En la ventana principal de Micro Focus (HPE) Data Protector, seleccione la estantería Dispositivos y multimedia en la lista situada en la parte superior izquierda.

Abra el menú contextual (clic con el botón derecho) de Device y elija Add Device.



2. En la Add Device, escriba un valor para Device Name. En Tipo de dispositivo, seleccione SCSI Biblioteca y, a continuación, Siguiente.
3. En la siguiente pantalla, haga lo siguiente:
 - a. Para SCSIver la dirección del robot de la biblioteca, selecciona tu dirección específica.
 - b. Para Select what action Data Protector should take if the drive is busy, elija "Abort" o la acción que desee.
 - c. Elija la activación de estas opciones:
 - Barcode reader support
 - Descubra automáticamente la SCSI dirección cambiada
 - SCSIReserva/Liberación (control robótico)
 - d. Deje Use barcode as medium label on initialization en blanco (sin marcar), a menos que el sistema lo requiera.
 - e. Elija Siguiente para continuar.
4. En la siguiente pantalla, especifique las ranuras que desee utilizar con HP Data Protector. Utilice un guion ("-") entre números para indicar un rango de ranuras, por ejemplo 1-6. Cuando haya especificado las ranuras que desea utilizar, seleccione Next.
5. Para el tipo de soporte estándar que utiliza el dispositivo físico, elija LTO_Ultrium y, a continuación, elija Finalizar para completar la configuración.

La biblioteca de cintas está ahora lista para utilizarse. Para cargar cintas en ella, consulte la siguiente sección.

Preparación de cintas virtuales para utilizarlas con Data Protector HPE

Antes de poder realizar una copia de seguridad de los datos de una cinta virtual, debe preparar la cinta para su uso. Para ello, debe hacer lo siguiente:

- Cargar una cinta virtual en una biblioteca de cintas
- Cargar la cinta virtual en una ranura
- Crear un grupo de medios
- Cargar la cinta virtual en un grupo de medios

En las secciones siguientes, puede encontrar pasos que le guiará a través de este proceso.

Carga de cintas virtuales en una biblioteca de cintas

Su biblioteca de cintas debe aparecer ahora en Devices. Si no aparece, pulse F5 para actualizar la pantalla. Cuando aparezca la biblioteca, puede cargar cintas virtuales en ella.

Para cargar cintas virtuales en la biblioteca de cintas

1. Elija el signo más junto a la biblioteca de cintas para mostrar los nodos de rutas de robótica, unidades y ranuras.
2. Abra el menú contextual (haga clic con el botón derecho) de Drives, elija Add Drive, escriba un nombre para la cinta y, a continuación, elija Next para continuar.
3. Elija la unidad de cinta que desee agregar como SCSI dirección de la unidad de datos, seleccione Detectar automáticamente la SCSI dirección cambiada y, a continuación, elija Siguiente.
4. En la siguiente pantalla, elija Advanced. Aparece la pantalla emergente Advanced Options.
 - a. En la pestaña Settings, debe tener en cuenta las siguientes opciones:
 - CRCCompruebe (para detectar cambios accidentales en los datos)
 - Detect dirty drive (para garantizar que la unidad está limpia antes de la copia de seguridad)
 - SCSIReserva/libere (unidad) (para evitar que la cinta se quede atascada)

Para hacer pruebas, puede dejar estas opciones desactivadas (sin marcar).
 - b. En la pestaña Sizes, establezca el valor de Block size (kB) en Default (256).
 - c. Elija OK para cerrar la pantalla de opciones avanzadas y, a continuación, elija Next para continuar.
5. En la siguiente pantalla, elija estas opciones en Device Policies:
 - Device may be used for restore
 - Device may be used as source device for object copy
6. Elija Finish para terminar de agregar la unidad de cinta a la biblioteca de cintas.

Carga de cintas virtuales en ranuras

Ahora que tiene una unidad de cinta en la biblioteca de cintas, puede cargar cintas virtuales en las ranuras.

Para cargar una cinta en una ranura

1. En el nodo del árbol de la biblioteca de cintas, abra el nodo etiquetado Slots. Cada ranura tiene un estado que se representa mediante un icono:
 - Una cinta verde significa que ya hay una cinta cargada en la ranura.
 - Una ranura gris significa que la ranura está vacía.
 - Un signo de interrogación cian significa que la cinta de esa ranura no está formateada.
2. Para una ranura vacía, abra el menú contextual (haga clic con el botón derecho) y, a continuación, elija Enter. Si dispone de cintas, elija una para cargarla en esa ranura.

Creación de un grupo de medios

Un grupo de medios es un grupo lógico que se utiliza para organizar las cintas. Para configurar un backup de cinta, cree un grupo de medios.

Para crear un grupo de medios

1. En la estantería Devices & Media, abra el nodo del árbol para Media, abra el menú contextual (haga clic con el botón derecho) del nodo Pools y, a continuación, elija Add Media Pool.
2. Para Pool name, escriba un nombre.
3. En Tipo de medio, elija LTO_Ultrium y, a continuación, elija Siguiente.
4. En la pantalla siguiente, acepte los valores predeterminados y, a continuación, elija Next.
5. Elija Finish para terminar de crear un grupo de medios.

Carga de cintas en un grupo de medios

Antes de poder realizar una copia de seguridad de los datos en las cintas, debe cargar las cintas en el grupo de medios que ha creado.

Para cargar una cinta virtual en un grupo de medios

1. En el nodo del árbol de la biblioteca de cintas, elija el nodo Slots.

2. Elija una cinta cargada, que tenga un icono verde que muestra una cinta cargada. Abra el menú contextual (haga clic con el botón derecho) y, a continuación, elija Enter.
3. Elija el grupo de medios que ha creado y, a continuación, elija Next.
4. Para Medium Description, elija Use barcode y, a continuación, elija Next.
5. Para Options, elija Force Operación y, a continuación, elija Finish.

Ahora debería ver que la ranura elegida cambia del estado sin asignar (gris) al estado de cinta insertada (verde). Aparecen una serie de mensajes para confirmar que los medios están inicializados.

En este punto, debería tener todo configurado para empezar a utilizar su biblioteca de cintas virtuales con HPE Data Protector. Para comprobar si es así, utilice el siguiente procedimiento.

Para verificar que la biblioteca de cintas está configurada para utilizarse

- Elija Drives y, a continuación, abra el menú contextual (haga clic con el botón derecho) de la unidad y elija Scan.

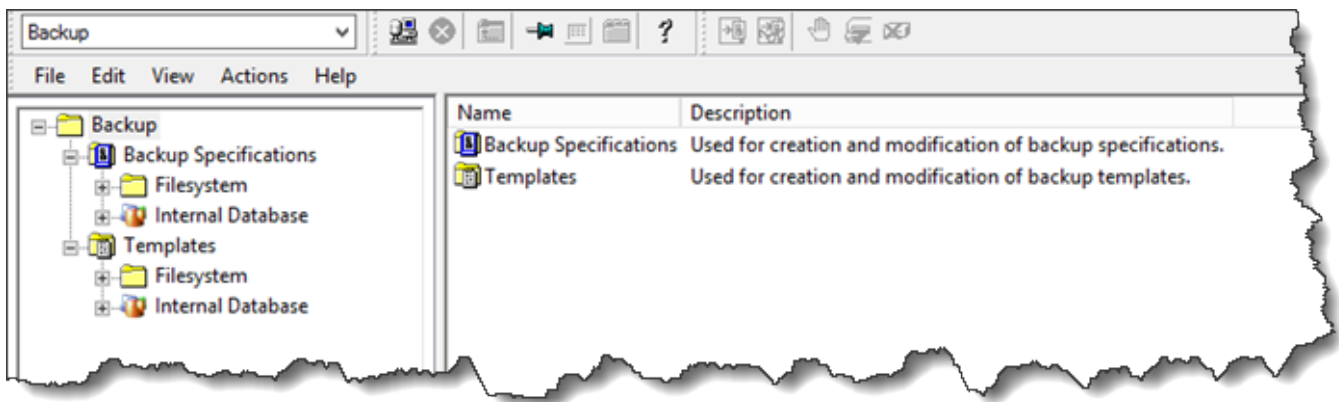
Si la configuración es correcta, un mensaje confirma que los medios se han analizado correctamente.

Copia de seguridad de datos en una cinta

Cuando las cintas se hayan cargado en un grupo de medios, puede hacer copias de seguridad de datos en ellas.

Para realizar un backup de datos en una cinta

1. Elija la estantería Backup en la parte superior izquierda de la pantalla.



2. Abra el menú contextual (haga clic con el botón derecho) de Filesystem y elija Add Backup.
3. En la pantalla Create New Backup, en Filesystem, elija Blank File System Backup y, a continuación, elija OK.
4. En el nodo de árbol que muestra el sistema del host, seleccione el sistema de archivos o los sistemas de archivos de los que desee hacer copias de seguridad y seleccione Next para continuar.
5. Abra el nodo del árbol de la biblioteca de cintas que desee utilizar, abra el menú contextual (haga clic con el botón derecho) de la unidad de cinta que desea utilizar y, a continuación, elija Properties.
6. Elija el grupo de medios, elija OK y, a continuación, elija Next.
7. Para las próximas tres pantallas, acepte la configuración predeterminada y elija Next.
8. En la pantalla Perform finishing steps in your backup/template design, elija Save as para guardar esta sesión. En la ventana emergente, dé un nombre al backup y asígnelo al grupo donde desee guardar la nueva especificación de backup.
9. Elija Start Interactive Backup.

Si el sistema del host contiene un sistema de base de datos, puede elegirlo como sistema de backup de destino. Las pantallas y selecciones son similares al backup del sistema de archivos que acabamos de describir.

Note

Si la puerta de enlace de cinta se reinicia por algún motivo durante un trabajo de copia de seguridad en curso, el trabajo de copia de seguridad se realizará incorrectamente y la unidad de cinta de Data Protector aparecerá marcada como Sucia. Data Protector también marca la calidad de la cinta como Deficiente e impide que se escriba en ella. Para seguir leyendo los datos de la cinta, debe limpiar la unidad y volver a montar la cinta. Para completar el trabajo de copia de seguridad incorrecto, debe volver a enviarlo en una cinta nueva.

Archivado de una cinta

Al archivar una cinta, la puerta de enlace de cinta traslada la cinta desde la biblioteca de cintas al almacenamiento sin conexión. Antes de expulsar y archivar una cinta, es posible que desee comprobar su contenido.

Para comprobar el contenido de una cinta antes de archivarla

1. Elija Slots y, a continuación, elija la cinta que desee comprobar.
2. Elija Objects y compruebe qué contiene la cinta.

Cuando haya elegido una cinta para archivar, utilice el siguiente procedimiento.

Para expulsar y archivar una cinta

1. Abra el menú contextual (haga clic con el botón derecho) de esa cinta y, a continuación, elija Eject.
2. En la consola Storage Gateway, elija su puerta de enlace y, a continuación, elija VTLTape Cartridges y compruebe el estado de la cinta virtual que va a archivar.

Una vez expulsada la cinta, se archivará automáticamente en el almacenamiento sin conexión (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). El proceso de archivado puede tardar algún tiempo en completarse. El estado inicial de la cinta se muestra como IN TRANSIT TO VTS. Cuando se inicia el archivado, el estado cambia a ARCHIVING. Una vez finalizado el archivado, la cinta ya no aparece en la lista, VTL sino que se archiva en S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive.

Restauración de datos desde una cinta

La restauración de datos archivados se realiza en dos fases.

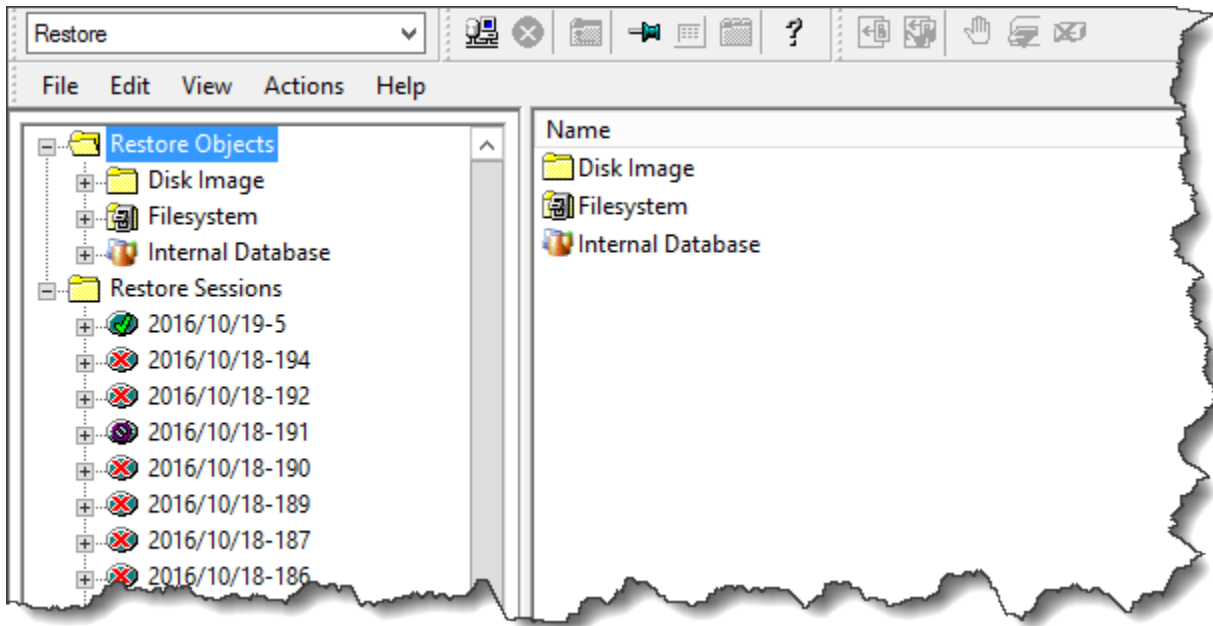
Para restaurar datos desde una cinta archivada

1. Recupere la cinta archivada en una puerta de enlace de cinta. Para obtener instrucciones, consulte [Recuperación de cintas archivadas](#).
2. Utilice HPE Data Protector para restaurar los datos. Este proceso es el mismo que la restauración de datos desde cintas físicas.

Para restaurar datos desde una cinta, utilice el siguiente procedimiento.

Para restaurar datos desde una cinta

1. Elija la estantería Restore en la parte superior izquierda de la pantalla.



2. Elija el sistema de archivos o el sistema de base de datos que desea restaurar. Asegúrese de que esté seleccionada la casilla del backup que desee restaurar. Elija Restore (Restaurar).
3. En la ventana Start Restore Session, elija Needed Media. Elija All media y deberá ver la cinta utilizada originalmente para la copia de seguridad. Elija esa cinta y, a continuación, elija Close.
4. En la ventana Start Restore Session, acepte la configuración predeterminada, elija Next y, a continuación, elija Finish.

Paso siguiente

[Eliminación de recursos innecesarios](#)

Probar la configuración mediante Microsoft System Center DPM

Puede hacer copias de seguridad de los datos en cintas virtuales, archivarlas y administrar los dispositivos de la biblioteca de cintas virtuales (VTL) mediante Microsoft System Center 2012 R2 o 2016 Data Protection Manager (DPM). En este tema, encontrará documentación básica sobre cómo configurar la aplicación de DPM copia de seguridad para una puerta de enlace de cinta y realizar una operación de copia de seguridad y restauración.

Para obtener información detallada acerca de cómo usarloDPM, consulte la [DPMdocumentación](#) en el sitio web de Microsoft System Center. Para obtener más información sobre aplicaciones de backup compatibles, consulte [Aplicaciones de copia de seguridad de terceros compatibles con una puerta de enlace de cinta](#).

Temas

- [Configuración DPM para reconocer VTL dispositivos](#)
- [Importación de una cinta a DPM](#)
- [Escribir datos en una cinta DPM](#)
- [Archivar una cinta mediante DPM](#)
- [Restauración de datos de una cinta archivada en DPM](#)

Configuración DPM para reconocer VTL dispositivos

Una vez que haya conectado los dispositivos de la biblioteca de cintas virtuales (VTL) al cliente de Windows, debe configurarlos DPM para que reconozcan sus dispositivos. Para obtener información acerca de cómo conectar VTL los dispositivos al cliente de Windows, consulte [Conexión de sus VTL dispositivos](#).

De forma predeterminada, el DPM servidor no reconoce los dispositivos Tape Gateway. Para configurar el servidor para que funcione con los dispositivos de puerta de enlace de cinta lleve a cabo las siguientes tareas:

1. Actualice los controladores de los VTL dispositivos para exponerlos al DPM servidor.
2. Asigne manualmente los VTL dispositivos a la biblioteca de DPM cintas.

Para actualizar los controladores VTL del dispositivo

- En el Administrador de dispositivos, actualice el controlador del cambiador de medios. Para obtener instrucciones, consulte [Actualización de la unidad de dispositivo para el cambiador de medios](#).

Se utiliza DPMDriveMappingTool para asignar las unidades de cinta a la biblioteca de DPM cintas.


Para asignar unidades de cinta a la biblioteca DPM de cintas del servidor

1. Cree al menos una cinta para la gateway. Para obtener información sobre cómo hacerlo en la consola, consulte [Creación de cintas](#).
2. Importe la cinta a la DPM biblioteca. Para obtener información sobre cómo hacerlo, consulte [Importación de una cinta a DPM](#).

3. Si el DPMLA servicio está en ejecución, deténgalo abriendo un terminal de comandos y escribiendo lo siguiente en la línea de comandos.

net stop DPMLA

4. Localice el siguiente archivo en el DPM servidor:%ProgramFiles%\System Center 2016 R2\DPM\DPM\Config\DPMLA.xml.

 Note

Si este archivo existe, lo DPMDriveMappingTool sobrescribe. Si desea conservar el archivo original, cree una copia de backup.

5. Abra un terminal de comando, cambie el directorio a %ProgramFiles%\System Center 2016 R2\DPM\DPM\Bin y ejecute el comando siguiente.

```
C:\Microsoft System Center 2016 R2\DPM\DPM\bin>DPMDriveMappingTool.exe
```

El resultado de este comando tendrá un aspecto similar al siguiente.

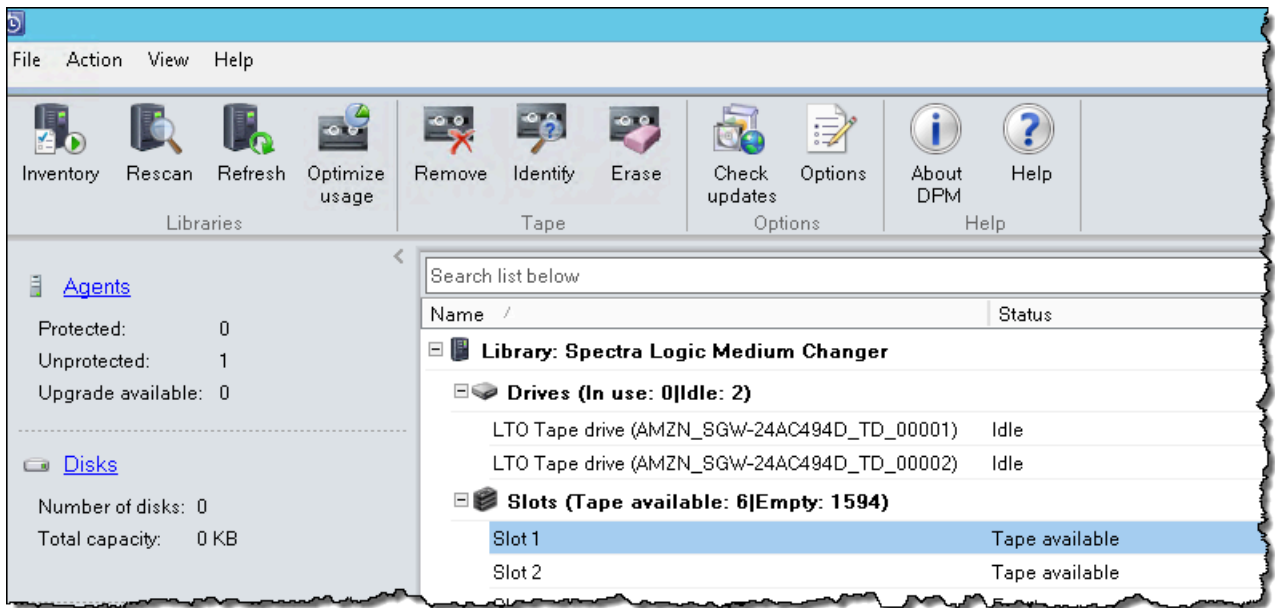
```
Performing Device Inventory ...
Mapping Drives to Library ...
Adding Standalone Drives ...
Writing the Map File ...
Drive Mapping Completed Successfully.
```

Importación de una cinta a DPM

Ahora está listo para importar cintas desde su Tape Gateway a la biblioteca DPM de aplicaciones de backup.

Para importar cintas a la biblioteca DPM de aplicaciones de respaldo

1. En el DPM servidor, abra la consola de administración, elija Volver a escanear y, a continuación, elija Actualizar. Esto muestra el cambiador de medios y las unidades de cinta.



2. Abra el menú contextual (haga clic con el botón derecho) del cambiador de medios en la sección Library y, a continuación, elija Add tape (I/E port) para agregar una cinta a la lista Slots.

Note

El proceso de adición de cintas puede tardar varios minutos en completarse.

La etiqueta de cinta aparece como Unknown y la cinta no se puede utilizar. Para que la cinta se pueda utilizar, debe identificarla.

3. Abra el menú contextual (haga clic con el botón derecho) de la cinta que desee identificar y, a continuación, elija Identify unknown tape.

Note

El proceso de identificación de cintas puede tardar unos segundos o unos minutos. Si las cintas no muestran los códigos de barras correctamente, debe cambiar el controlador del cambiador de medios a Sun/ Library. StorageTek Para obtener más

información, consulte [Visualización de códigos de barras para cintas en Microsoft System Center DPM](#).

Cuando se completa la identificación, la etiqueta de la cinta cambia a Free. Es decir, la cinta está libre para escribir datos en ella.

En la siguiente captura de pantalla, la cinta de la ranura 2 se ha identificado y está libre para autorizarla, pero la cinta de la ranura 3 no.

Name /	Status	Tape Label	Barcode
Library: Spectra Logic Medium Changer			
Drives (In use: 0 Idle: 2)			
LTO Tape drive (AMZN_SGW-...	Idle	-	None
LTO Tape drive (AMZN_SGW-...	Idle	-	None
Slots (Tape available: 7 Empty: 1593)			
Slot 1	Empty	-	None
Slot 2	Tape available	Free	AMZN9FA53A
Slot 3	Tape available	Unknown	PH27A582
Slot 4	Tape available	Free	AMZN9FA537

Escribir datos en una cinta DPM

Para escribir datos en una cinta virtual de puerta de enlace de cinta, utilice los mismos procedimientos y políticas de protección que con las cintas físicas. Cree un grupo de protección y agregue los datos que desee incluir en la copia de seguridad y, a continuación, haga una copia de seguridad de los datos mediante la creación de un punto de recuperación. Para obtener información detallada acerca de cómo usarloDPM, consulte la [DPMdocumentación](#) en el sitio web de Microsoft System Center.

De forma predeterminada, la capacidad de una cinta es de 30 GB. Cuando se hace una copia de seguridad de datos que superan la capacidad de una cinta, se produce un error de E/S en el dispositivo. Si la posición en la que se produjo el error es mayor que el tamaño de la cinta, Microsoft DPM trata el error como una indicación del final de la cinta. Si la posición en la que se produjo el error es inferior al tamaño de la cinta, el trabajo de copia de seguridad no se realiza. Para solucionar el problema, cambie el valor de TapeSize en la entrada del registro para que coincida con el tamaño de la cinta. Para obtener más información sobre cómo hacerlo, consulte [Error ID: 30101](#) en Microsoft System Center.

Note

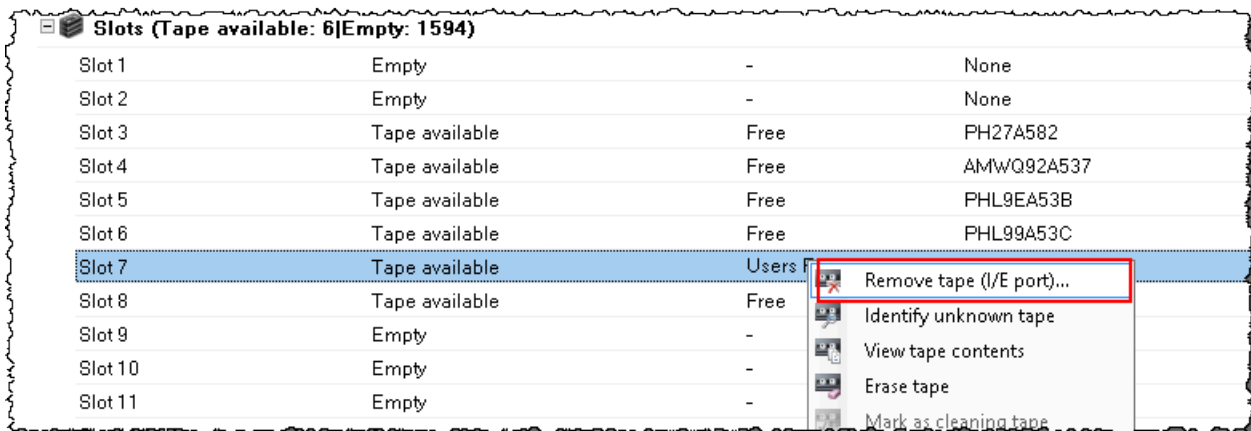
Si la puerta de enlace de cinta se reinicia por algún motivo durante un trabajo de copia de seguridad en curso, el trabajo de copia de seguridad se realizará incorrectamente. Para completar el trabajo de copia de seguridad incorrecto, debe volver a enviarlo.

Archivar una cinta mediante DPM

Al archivar una cinta, Tape Gateway la mueve de la biblioteca de DPM cintas al almacenamiento fuera de línea. Para comenzar el archivado en cinta, extraiga la cinta de la ranura con la aplicación de respaldo, es decir, DPM

Para archivar una cinta DPM

1. Abra el menú contextual (clic con el botón derecho) de la cinta que desee archivar y, a continuación, elija Remove tape (I/E port).



2. En el cuadro de diálogo que aparece, elija Yes. De esta manera, la cinta se expulsa de la ranura de almacenamiento del cambiador de medios y pasa a una de las ranuras I/E de la gateway. Cuando una cinta pasa a la ranura I/E de la gateway, se envía inmediatamente para el archivado.
3. En la consola Storage Gateway, elija su puerta de enlace y, a continuación, elija VTLTape Cartridges y compruebe el estado de la cinta virtual que va a archivar.

El proceso de archivado puede tardar algún tiempo en completarse. El estado inicial de la cinta se muestra como IN TRANSIT TO VTS. Cuando se inicia el archivado, el estado cambia a ARCHIVING. Una vez finalizado el archivado, la cinta ya no aparece en la lista. VTL

Restauración de datos de una cinta archivada en DPM

La restauración de datos archivados se realiza en dos fases.

Para restaurar datos desde una cinta archivada

1. Recupere la cinta archivada desde el archivo a la puerta de enlace de cinta. Para obtener instrucciones, consulte [Recuperación de cintas archivadas](#).
2. Utilice la aplicación DPM de copia de seguridad para restaurar los datos. Para ello, cree un punto de recuperación, de la misma forma que cuando se restauran datos desde cintas físicas. Para obtener instrucciones, consulte [Recuperación de datos del ordenador cliente](#) en el DPM sitio web.

Paso siguiente

[Eliminación de recursos innecesarios](#)

Probar la configuración mediante NovaStor DataCenter

Puede hacer copias de seguridad de sus datos en cintas virtuales, archivarlas y administrar sus dispositivos de biblioteca de cintas virtuales (VTL) mediante la versión 6.4 o 7.1 de NovaStor DataCenter /Network. En este tema, encontrará documentación básica sobre cómo configurar la aplicación de copia de seguridad NovaStor DataCenter /Network, versión 7.1, para una puerta de enlace de cinta y realizar operaciones de copia de seguridad y restauración. Para obtener información detallada sobre cómo utilizar la versión 7.1 de NovaStor DataCenter /Network, consulte la [documentación NovaStor DataCenter /Network](#).

Configuración de /Network NovaStor DataCenter

Una vez que haya conectado los dispositivos de la biblioteca de cintas virtuales (VTL) al cliente de Microsoft Windows, configure el NovaStor software para que reconozca los dispositivos. Para obtener información sobre cómo conectar VTL los dispositivos al cliente de Windows, consulte [Conexión de sus VTL dispositivos](#).

NovaStor DataCenter/La red requiere controladores de los fabricantes de los controladores. Puede utilizar los controladores de Windows, pero primero deberá desactivar otras aplicaciones de backup.

Configurar NovaStor DataCenter /Network para que funcione con dispositivos VTL

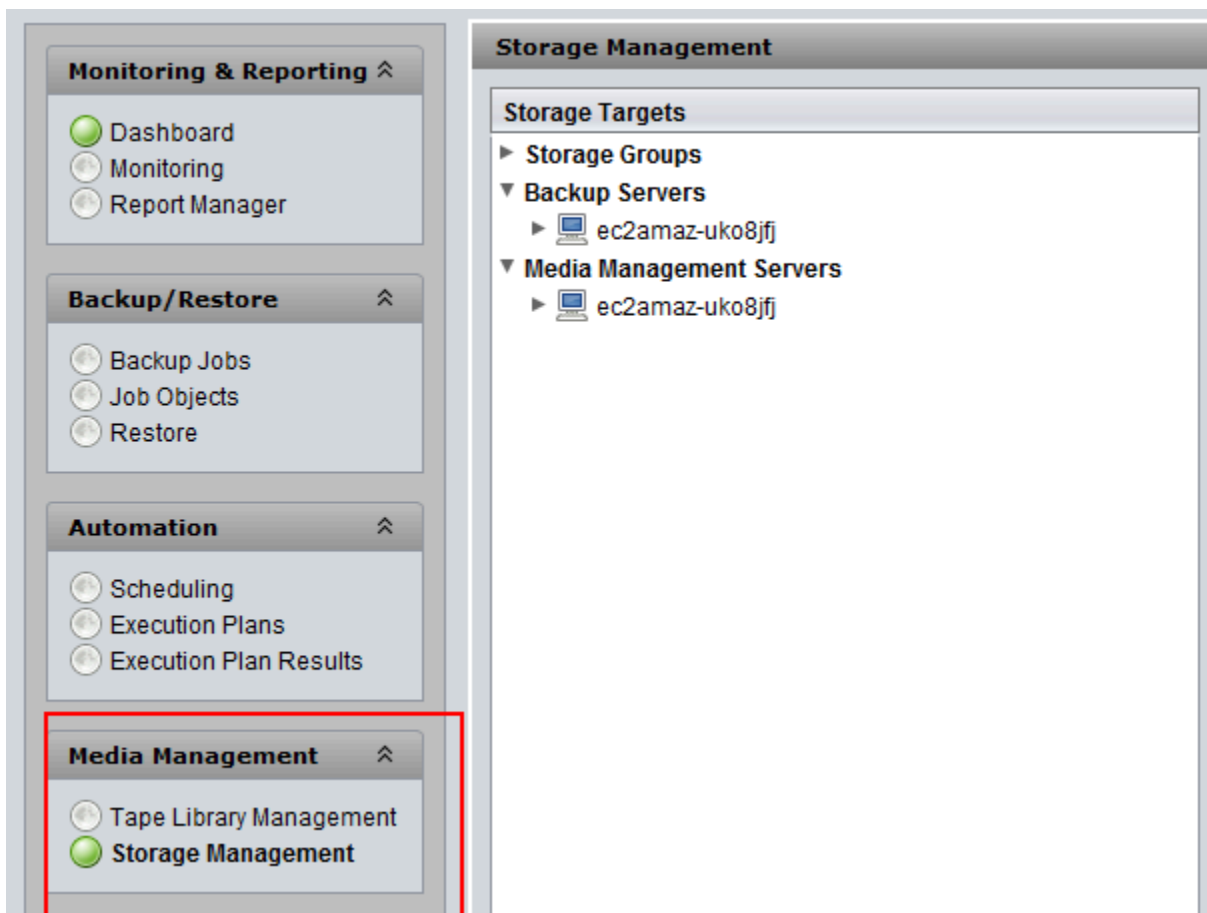
Al configurar VTL los dispositivos para que funcionen con las versiones 6.4 o 7.1 de NovaStor DataCenter /Network, es posible que aparezca un mensaje de error que diga: External Program

did not exit correctly Este problema requiere una solución provisional que se debe implementar antes de continuar.

Puede evitar este problema creando una solución alternativa antes de empezar a configurar los dispositivos VTL. Para obtener más información sobre cómo crear la solución provisional, consulte [Resolución del error "External Program Did Not Exit Correctly" \(El programa externo no ha finalizado correctamente\)](#).

Para configurar NovaStor DataCenter /Network para que funcione con dispositivos VTL

1. En la consola de administración NovaStor DataCenter de /Network, elija Administración de medios y, a continuación, Administración de almacenamiento.



2. En el menú Storage Targets, abra el menú contextual (haga clic con el botón derecho) de Media Management Servers, elija New y, a continuación, OK para crear y rellenar un nodo de almacenamiento.

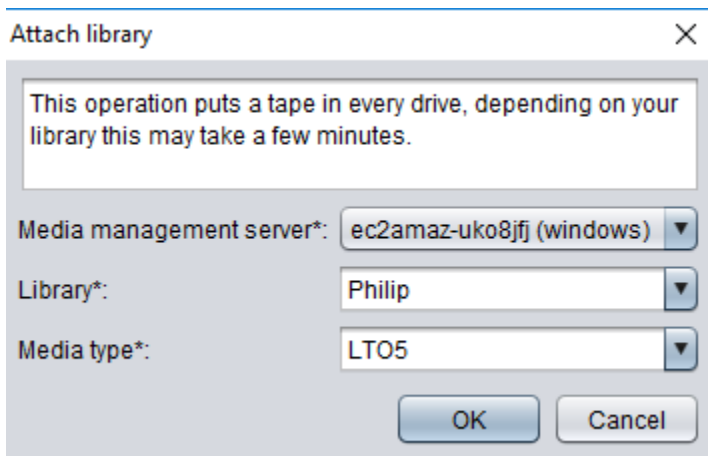
Si aparece el mensaje de error: External Program did not exit correctly, resuelva el problema antes de continuar. Este problema requiere una solución provisional. Para obtener

información acerca de cómo resolver este problema, consulte [Resolución del error "External Program Did Not Exit Correctly" \(El programa externo no ha finalizado correctamente\)](#).

⚠ Important

Este error se produce porque el rango de asignación de elementos entre AWS Storage Gateway las unidades de almacenamiento y las unidades de cinta supera el número permitido por NovaStor DataCenter /Network.

3. Abra el menú contextual (haga clic con el botón derecho) del nodo de almacenamiento que se ha creado y elija New Library.
4. Elija el servidor de bibliotecas en la lista. La lista de bibliotecas se rellena automáticamente.
5. Asigne un nombre a la biblioteca y elija OK.
6. Elija la biblioteca para mostrar todas las propiedades de la biblioteca de cintas virtuales de Storage Gateway.
7. En el menú Storage Targets, expanda Backup Servers, abra el menú contextual del servidor y elija Attach Library.
8. En el cuadro de diálogo Adjuntar biblioteca que aparece, elija el tipo de LTO5 soporte y, a continuación, elija Aceptar.



9. Expanda Servidores de copia de seguridad para ver la biblioteca de cintas virtuales de Storage Gateway y la partición de biblioteca que muestra todas las unidades de cinta montadas.

Creación de un grupo de cintas

Un grupo de cintas se crea dinámicamente en el software NovaStor DataCenter /Network y, por lo tanto, no contiene una cantidad fija de medios. El grupo de cintas que necesita una cinta la obtiene de su grupo de reserva. Un grupo de reserva es un depósito de cintas que están disponibles para que puedan utilizarlas uno o varios grupos de cintas. Un grupo de cintas devuelve al grupo de reserva todos los medios que han superado sus tiempos de retención y que ya no son necesarios.

La creación de un grupo de cintas es una tarea que consta de tres pasos:

1. Creación de un grupo de reserva.
2. Asignación de cintas al grupo de reserva.
3. Creación de un grupo de cintas.

Para crear un grupo de reserva

1. En el menú de navegación izquierdo, elija la pestaña Scratch Pools.
2. Abra el menú contextual (haga clic con el botón derecho) de Scratch Pools y elija Create Scratch Pool.
3. En el cuadro de diálogo Scratch Pools, asigne un nombre al grupo de reserva y elija el tipo de medio.
4. Elija Label Volume y cree un nivel inferior para el grupo de reserva. Cuando el grupo de reserva se vacíe hasta el nivel inferior, aparecerá una advertencia.
5. En el cuadro de diálogo de advertencia que aparece, elija OK para crear el grupo de reserva.

Para asignar cintas a un grupo de reserva

1. En el menú de navegación izquierdo, elija Tape Library Management.
2. Elija la pestaña Library para ver el inventario de la biblioteca.
3. Elija las cintas que desea asignar al grupo de reserva. Asegúrese de que las cintas se establecen en el tipo de medio correcto.
4. Abra el menú contextual (haga clic con el botón derecho) de la biblioteca y elija Add to Scratch Pool.

Ahora tiene un grupo de reserva lleno que puede utilizar para los grupos de cintas.

Para crear un grupo de cintas

1. En el menú de navegación izquierdo, elija Tape Library Management.
2. Abra el menú contextual (haga clic con el botón derecho) de la pestaña Media Pools y elija Create Media Pool.
3. Asigne un nombre al grupo de medios y elija Backup Server.
4. Elija una partición de biblioteca para el grupo de medios.
5. Elija el grupo de reserva desde el que desea que el grupo obtenga las cintas.
6. En Schedule, elija Not Scheduled.

Configuración de la importación y exportación de medios para archivar cintas

NovaStor DataCenter/Network puede utilizar ranuras de importación o exportación si forman parte del cambiador de medios.

Para realizar una exportación, NovaStor DataCenter /Network debe saber qué cintas se van a sacar físicamente de la biblioteca.

Para una importación, NovaStor DataCenter /Network reconoce los soportes de cinta que se exportan en la biblioteca de cintas y ofrece importarlos todos, ya sea desde una ranura de datos o desde una ranura de exportación. La puerta de enlace de cinta archiva las cintas en el almacenamiento sin conexión (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive).


Para configurar la importación y exportación de medios

1. Vaya a Tape Library Management, elija un servidor para Media Management Server y, a continuación, elija Library.
2. Elija la pestaña Off-site Locations.
3. Abra el menú contextual (haga clic con el botón derecho) del área blanca y elija Add para abrir un panel nuevo.
4. En el panel, escriba **S3 Glacier Flexible Retrieval** o **S3 Glacier Deep Archive** y añada una descripción opcional en el cuadro de texto.

Ejecución de backups de datos en cinta

Cree un trabajo de backup y escriba datos en una cinta virtual utilizando los mismos procedimientos que con las cintas físicas. Para obtener información detallada sobre cómo hacer copias de seguridad

de los datos mediante el NovaStor software, consulte la [documentación NovaStor DataCenter / Network](#).

 Note

Si la puerta de enlace de cinta se reinicia por algún motivo durante un trabajo de copia de seguridad en curso, el trabajo de copia de seguridad se realizará incorrectamente y la cinta no se podrá escribir. Puede archivar la cinta o seguir leyendo sus datos. Para completar el trabajo de copia de seguridad incorrecto, debe volver a enviarlo en una cinta nueva.

Archivado de una cinta

Al archivar una cinta, la puerta de enlace de cinta traslada la cinta desde la unidad de cintas a la ranura de almacenamiento. A continuación, exporta la cinta de la ranura al archivo mediante la aplicación de backup, es decir, /Network. NovaStor DataCenter

Para archivar una cinta

1. En el menú de navegación izquierdo, elija Tape Library Management.
2. Elija la pestaña Library para ver el inventario de la biblioteca.
3. Resalte las cintas que desea archivar, abra el menú contextual (haga clic con el botón derecho) de las cintas y elija la ubicación externa de archivado.

El proceso de archivado puede tardar algún tiempo en completarse. El estado inicial de la cinta aparece como IN TO. TRANSIT VTS Cuando se inicia el archivado, el estado cambia a ARCHIVING. Cuando se haya completado el archivado, la cinta ya no aparecerá en la lista. VTL

En NovaStor DataCenter /Network, compruebe que la cinta ya no esté en la ranura de almacenamiento.

En el panel de navegación de la consola de Storage Gateway, elija Cintas. Compruebe que el estado de la cinta archivada sea. ARCHIVED

Restauración de datos desde una cinta archivada y recuperada

La restauración de datos archivados se realiza en dos fases.

Para restaurar datos desde una cinta archivada

1. Recupere la cinta archivada desde el archivo a la puerta de enlace de cinta. Para obtener instrucciones, consulte [Recuperación de cintas archivadas](#).
2. Utilice el software NovaStor DataCenter /Network para restaurar los datos. Para ello, actualice la ranura de correo y mueva cada cinta que desea recuperar a una ranura vacía, de la misma forma que cuando se restauran datos desde cintas físicas. Para obtener información sobre la restauración de datos, consulte [la documentación NovaStor DataCenter /Network](#).

Escritura simultánea de varios trabajos de backup en una unidad de cinta

En el NovaStor software, puede grabar varios trabajos en una unidad de cinta al mismo tiempo mediante la función de multiplexación. Esta característica se puede utilizar si hay un multiplexor disponible para un grupo de medios. Para obtener información sobre cómo utilizar la multiplexación, consulte la [documentación NovaStor DataCenter /Red](#).

Resolución del error "External Program Did Not Exit Correctly" (El programa externo no ha finalizado correctamente)

Al configurar VTL los dispositivos para que funcionen con la versión 6.4 o 7.1 de NovaStor DataCenter /Network, es posible que aparezca un mensaje de error que diga: `External Program did not exit correctly` Este error se produce porque el rango de asignación de elementos de Storage Gateway para unidades de almacenamiento y unidades de cinta supera el número permitido por NovaStor DataCenter /Network.

Storage Gateway devuelve 3200 ranuras de almacenamiento y de importación/exportación, lo que supera el límite de 2400 que NovaStor DataCenter permite /Network. Para resolver este problema, agregue un archivo de configuración que active el NovaStor software para limitar el número de ranuras de almacenamiento y de importación/exportación y preconfigure el rango de asignación de elementos.

Para aplicar la solución provisional a un error "External program did not exit correctly" (El programa externo no ha finalizado correctamente)

1. Navegue hasta la carpeta de cintas del ordenador en la que instaló el software. NovaStor
2. En la carpeta Tape, cree un archivo de texto y asígnele el nombre `hijacc.ini`.
3. Copie el siguiente contenido, péguelo en el archivo `hijacc.ini` y guarde este.

```
port:12001
san:no
define: A3B0S0L0
*DRIVES: 10
*FIRST_DRIVE: 10000
*SLOTS: 200
*FIRST_SLOT: 20000
*HANDLERS: 1
*FIRST_HANDLER: 0
*IMP-EXPS: 30
*FIRST_IMP-EXP: 30000
```

4. Añada y asocie la biblioteca al servidor de administración de medios.
5. Mueva una cinta de la ranura de importación y exportación a la biblioteca mediante el comando que se muestra en las capturas de pantalla siguientes. En el comando, VTL sustitúyalo por el nombre de la biblioteca.

```
C:\Program Files\NovaStor\DataCenter\Hiback\tape>ophijacc.exe -c VTL-ec2amaz-uko8jffj-ec2amaz-uko8jffj.lcfg

1 Configuration
2 Status Handler
3 Status Import/Export
4 Status Drive
5 Status Slot
6 Mount Medium
7 Unmount Medium
8 Find Address by Tag

9 Reset Stacker
11 Move Element
88 Inventory
99 Exit

What ([#,#[,#]])? 1
Handlers : 1 Address: 0
Import/Export: 30 Address: 30000
Drives : 10 Address: 10000
Slots : 200 Address: 20000
```

```
1 Configuration
2 Status Handler
3 Status Import/Export
4 Status Drive
5 Status Slot
6 Mount Medium
7 Unmount Medium
8 Find Address by Tag

9 Reset Stacker
11 Move Element
88 Inventory
99 Exit

What ([,#[,#[,#[)])? 11
Source Address? 30000
Destination Address? 20000

1 Configuration
2 Status Handler
3 Status Import/Export
4 Status Drive
5 Status Slot
6 Mount Medium
7 Unmount Medium
8 Find Address by Tag
9 Reset Stacker
```

6. Asocie la biblioteca al servidor de backup.
7. En el NovaStor software, importe todas las cintas de las ranuras de importación/exportación a la biblioteca.

Probar la configuración mediante Quest NetVault Backup

Puede hacer copias de seguridad de sus datos en cintas virtuales, archivarlas y administrar sus dispositivos de biblioteca de cintas virtuales (VTL) mediante las siguientes versiones de NetVault backup de Quest (anteriormente Dell):

- Quest NetVault Backup 12.4
- Quest NetVault Backup 13.x

En este tema, encontrará documentación básica sobre cómo configurar la aplicación Quest NetVault Backup para una puerta de enlace de cinta y realizar una operación de copia de seguridad y restauración.

Para obtener información detallada sobre cómo utilizar la aplicación Quest NetVault Backup, consulte la Guía de administración NetVault de Quest Backup. Para obtener más información sobre aplicaciones de backup compatibles, consulte [Aplicaciones de copia de seguridad de terceros compatibles con una puerta de enlace de cinta](#).

Temas

- [Configuración de Quest NetVault Backup para que funcione con VTL dispositivos](#)
- [Hacer copias de seguridad de los datos en una cinta en Quest NetVault Backup](#)
- [Archivar una cinta mediante Quest Backup NetVault](#)
- [Restauración de datos de una cinta archivada en Quest Backup NetVault](#)

Configuración de Quest NetVault Backup para que funcione con VTL dispositivos

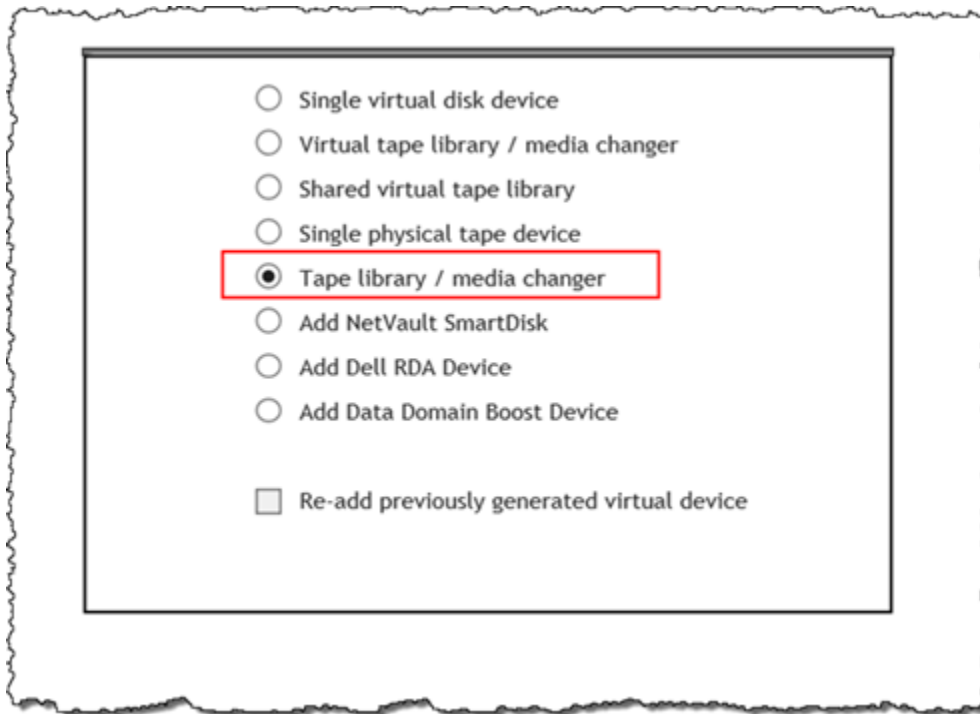
Una vez que haya conectado los dispositivos de la biblioteca de cintas virtuales (VTL) al cliente de Windows, configure Quest NetVault Backup para que reconozca sus dispositivos. Para obtener información sobre cómo conectar VTL los dispositivos al cliente de Windows, consulte [Conexión de sus VTL dispositivos](#).

La aplicación Quest NetVault Backup no reconoce automáticamente los dispositivos Tape Gateway. Debe añadir los dispositivos manualmente para exponerlos a la aplicación Quest NetVault Backup y, a continuación, VTL detectarlos.

Añadir VTL dispositivos

Para añadir los VTL dispositivos

1. En Quest NetVault Backup, seleccione Administrar dispositivos en la pestaña Configuración.
2. En la página Manage Devices, elija Add Devices.
3. En el asistente para agregar almacenamiento, seleccione Tape library/media changer y, a continuación, elija Next.



4. En la página siguiente, elija el equipo del cliente conectado físicamente a la biblioteca y elija Next para buscar dispositivos.
5. Si se encuentra algún dispositivo, se mostrará. En este caso, el cambiador de medios se muestra en el cuadro de dispositivos.
6. Seleccione el cambiador de medios y elija Next. En el asistente se muestra información detallada sobre el dispositivo.
7. En la página Agregar cintas a bahías, seleccione Scan For Devices, elija el equipo del cliente y, a continuación, elija Next.

Todas las unidades se muestran en la página. Quest NetVault Backup muestra las 10 bahías a las que puede añadir sus unidades. Los bahías se muestran de una en una.

Device	Serial Number
3-0.5.0 (IBM ULT3580-TD5)	AMZN_SGW- 54A94C3D_TD_00005
3-0.29.0 (IBM ULT3580-TD5)	AMZN_SGW- 54A94C3D_TD_00007
3-0.30.0 (IBM ULT3580-TD5)	AMZN_SGW- 54A94C3D_TD_00008
3-0.31.0 (IBM ULT3580-TD5)	AMZN_SGW- 54A94C3D_TD_00009
3-0.32.0 (IBM ULT3580-TD5)	AMZN_SGW- 54A94C3D_TD_00010

1 - 5 of 5 items

8. Elija la unidad que desea agregar a la bahía que se muestra y, a continuación, elija Next.

⚠ Important

Cuando agregue una unidad a una bahía, los números de unidad y bahía deben coincidir. Por ejemplo, si se muestra la bahía 1, debe agregar la unidad 1. Si una unidad no está conectada, deje su bahía correspondiente vacía.

9. Cuando aparezca el equipo del cliente elíjalo y, a continuación, elija Next. La máquina cliente puede aparecer varias veces.
10. Cuando se muestren las unidades, repita los pasos 7 a 9 para agregar todas las unidades a las bahías.
11. En la pestaña Configuration, elija Manage devices y, en la página Manage Devices, expanda el cambiador de medios para ver los dispositivos que ha agregado.

Hacer copias de seguridad de los datos en una cinta en Quest NetVault Backup

Cree un trabajo de backup y escriba datos en una cinta virtual utilizando los mismos procedimientos que con las cintas físicas. Para obtener información detallada sobre cómo hacer copias de seguridad de los datos, consulte la [Guía de administración NetVault de Quest Backup](#).

Note

Si la puerta de enlace de cinta se reinicia por algún motivo durante un trabajo de copia de seguridad en curso, el trabajo de copia de seguridad se realizará incorrectamente. Para completar el trabajo de copia de seguridad incorrecto, debe volver a enviarlo.

Archivar una cinta mediante Quest Backup NetVault

Al archivar una cinta, la puerta de enlace de cinta traslada la cinta desde la unidad de cintas a la ranura de almacenamiento. A continuación, exporta la cinta de la ranura al archivo mediante su aplicación de backup, es decir, Quest Backup NetVault .

Para archivar una cinta en Quest NetVault Backup

1. En la pestaña Quest NetVault Backup Configuration, selecciona y expande tu cambiador de medio para ver tus cintas.
2. En la fila Slots, elija el icono de configuración para abrir los Slots Browser para el cambiador de medios.

Manage Devices

▼ Tape Library: WIN-5E9VBD4DAQD: 3-0.0.0 (STK L700) Drives: 10 Slots: 1600 Ports: 1600 (Online) ; ⚙️

DRIVE	Model	Status	Unloaded	⚙️
DRIVE 1	3-0.1.0 (IBM ULT3580-TD5)	Online	(Idle) Unloaded	⚙️
DRIVE 2	3-0.3.0 (IBM ULT3580-TD5)	Online	(Idle) Unloaded	⚙️
DRIVE 3	3-0.5.0 (IBM ULT3580-TD5)	Online	(Idle) Unloaded	⚙️
DRIVE 4	3-0.29.0 (IBM ULT3580-TD5)	Online	(Idle) Unloaded	⚙️
DRIVE 5	3-0.31.0 (IBM ULT3580-TD5)	Online	(Idle) Unloaded	⚙️
DRIVE 6	3-0.2.0 (IBM ULT3580-TD5)	Online	(Idle) Unloaded	⚙️
DRIVE 7	3-0.4.0 (IBM ULT3580-TD5)	Online	(Idle) Unloaded	⚙️
DRIVE 8	3-0.28.0 (IBM ULT3580-TD5)	Online	(Idle) Unloaded	⚙️
DRIVE 9	3-0.30.0 (IBM ULT3580-TD5)	Online	(Idle) Unloaded	⚙️
DRIVE 10	3-0.32.0 (IBM ULT3580-TD5)	Online	(Idle) Unloaded	⚙️


Slots Total: 1600 (0 Populated, 1600 Empty), 0 Blank

Ports Total: 1600 (1600 Populated, 0 Empty)

[+ Add Device](#)

3. En las ranuras, busque la cinta que desee archivar, selecciónela y, a continuación, elija Export.

Slot ▲	Status	Barcode	Media
1	Reserved		
2	Has Blank Media	AMZND1A774	
3	Has Blank Media	AMZND6A773	
4	Empty		
5	Empty		
6	Empty		
7	Empty		
8	Empty		
9	Empty		
10	Empty		



[← Back](#)
[Ports →](#)
[Set Slot](#)
[Export](#)
[Scan 🔍](#)

El proceso de archivado puede tardar algún tiempo en completarse. El estado inicial de la cinta aparece como IN TRANSIT TO VTS. Cuando se inicia el archivado, el estado cambia a ARCHIVING. Una vez finalizado el archivado, la cinta ya no aparece en la lista. VTL

En el software Quest NetVault Backup, compruebe que la cinta ya no esté en la ranura de almacenamiento.

En el panel de navegación de la consola de Storage Gateway, elija Cintas. Compruebe que el estado de la cinta archivada sea ARCHIVED.

Restauración de datos de una cinta archivada en Quest Backup NetVault

La restauración de datos archivados se realiza en dos fases.

Para restaurar datos desde una cinta archivada

1. Recupere la cinta archivada desde el archivo a la puerta de enlace de cinta. Para obtener instrucciones, consulte [Recuperación de cintas archivadas](#).

2. Utilice la aplicación Quest NetVault Backup para restaurar los datos. Para ello, cree un archivo de carpeta de restauración, de la misma forma que cuando se restauran datos desde cintas físicas. Para obtener instrucciones sobre cómo crear un trabajo de restauración, consulte [Quest NetVault Backup: Administration Guide](#).

Paso siguiente

[Eliminación de recursos innecesarios](#)

Pruebe su configuración con Veeam Backup and Replication

Puede hacer copias de seguridad de sus datos en cintas virtuales, archivar las cintas y administrar sus dispositivos de biblioteca de cintas virtuales mediante Veeam Backup & Replication 11A. VTL En este tema, encontrará documentación básica acerca de cómo configurar el software Veeam Backup & Replication para una puerta de enlace de cinta y realizar operaciones de copia de seguridad y restauración. Para obtener información detallada sobre cómo utilizar el software Veeam, consulte la [documentación de copia de seguridad y replicación de Veeam](#) en el centro de ayuda de Veeam. Para obtener más información sobre aplicaciones de backup compatibles, consulte [Aplicaciones de copia de seguridad de terceros compatibles con una puerta de enlace de cinta](#).

Temas

- [Configuración de Veeam para que funcione con dispositivos VTL](#)
- [Importación de una cinta a Veeam](#)
- [Backup de datos en una cinta en Veeam](#)
- [Archivado de una cinta mediante Veeam](#)
- [Restablecimiento de datos desde una cinta archivada en Veeam](#)

Configuración de Veeam para que funcione con dispositivos VTL

Una vez que haya conectado sus dispositivos de biblioteca de cintas virtuales (VTL) al cliente de Windows, configure Veeam Backup & Replication para que reconozca sus dispositivos. Para obtener información sobre cómo conectar VTL los dispositivos al cliente de Windows, consulte [Conexión de sus VTL dispositivos](#).

Actualización de los controladores de VTL dispositivos

Para configurar el software para que funcione con los dispositivos Tape Gateway, debe actualizar los controladores de los VTL dispositivos para exponerlos al software de Veeam y, a continuación,

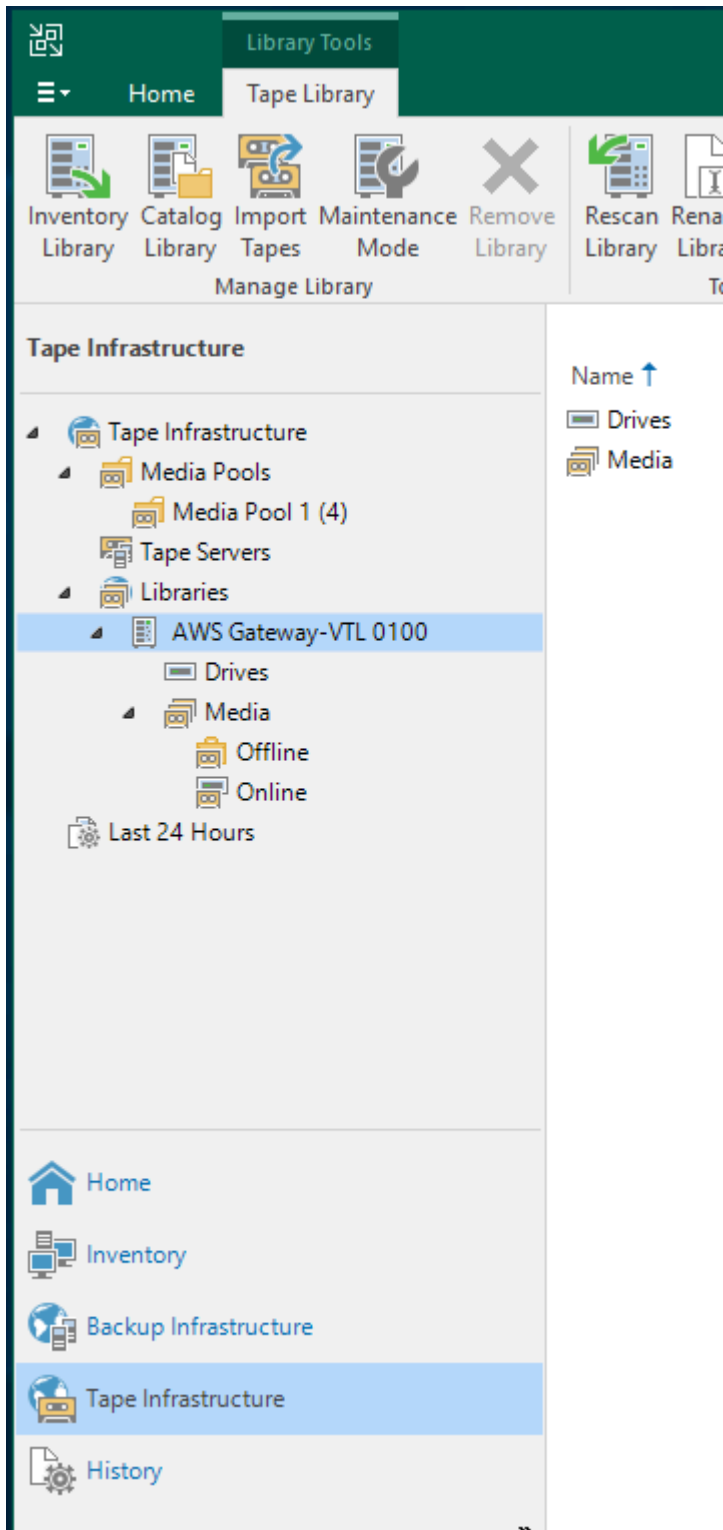
detectar los VTL dispositivos. En el Administrador de dispositivos, actualice el controlador del cambiador de medios. Para obtener instrucciones, consulte [Actualización de la unidad de dispositivo para el cambiador de medios](#).

Descubriendo VTL los dispositivos

Debe utilizar SCSI comandos nativos en lugar de un controlador de Windows para descubrir su biblioteca de cintas si desconoce el cambiador multimedia. Para obtener instrucciones detalladas, consulte [Bibliotecas de cintas](#).

Para descubrir dispositivos VTL

1. En el software Veeam, elija Infraestructura de cintas. Cuando la puerta de enlace de cinta esté conectada, las cintas virtuales se mostrarán en la pestaña Infraestructura de copia de seguridad.



2. Expanda el árbol Tape para ver las unidades de cinta y el cambiador de medios.
3. Expanda el árbol del cambiador de medios. Si las unidades de cinta están asignadas al cambiador de medios, las unidades aparecerán en Drives. De lo contrario, la biblioteca de cintas y las unidades de cinta aparecen como dispositivos independientes.

Si las unidades no se asignan automáticamente, siga las [instrucciones del sitio web Veeam](#) para asignar las unidades.

Importación de una cinta a Veeam

Ahora puede importar cintas de la puerta de enlace de cinta en la biblioteca de la aplicación de copia de seguridad Veeam.

Para importar una cinta en la biblioteca de Veeam

1. Abra el menú contextual (clic con el botón derecho) para el cambiador de medios y elija Import para importar las cintas en las ranuras I/E.
2. Abra el menú contextual (clic con el botón derecho) para el cambiador de medios y elija Inventory Library para identificar las cintas no reconocidas. Al cargar una nueva cinta virtual en una unidad de cinta por primera vez, la aplicación de backup Veeam no reconoce la cinta. Para identificar la cinta no reconocida, mantenga un inventario de cintas en la biblioteca de cintas.

Backup de datos en una cinta en Veeam

La copia de seguridad de datos en una cinta es un proceso de dos pasos:

1. Puede crear un grupo de medios y agregar la cinta al grupo de medios.
2. Escriba datos en la cinta.

Cree un grupo de medios y escriba datos en una cinta virtual utilizando los mismos procedimientos que con las cintas físicas. Para obtener información detallada acerca de cómo hacer copias de seguridad de datos, consulte [Getting Started with Tapes](#) en el centro de ayuda de Veeam.

Note

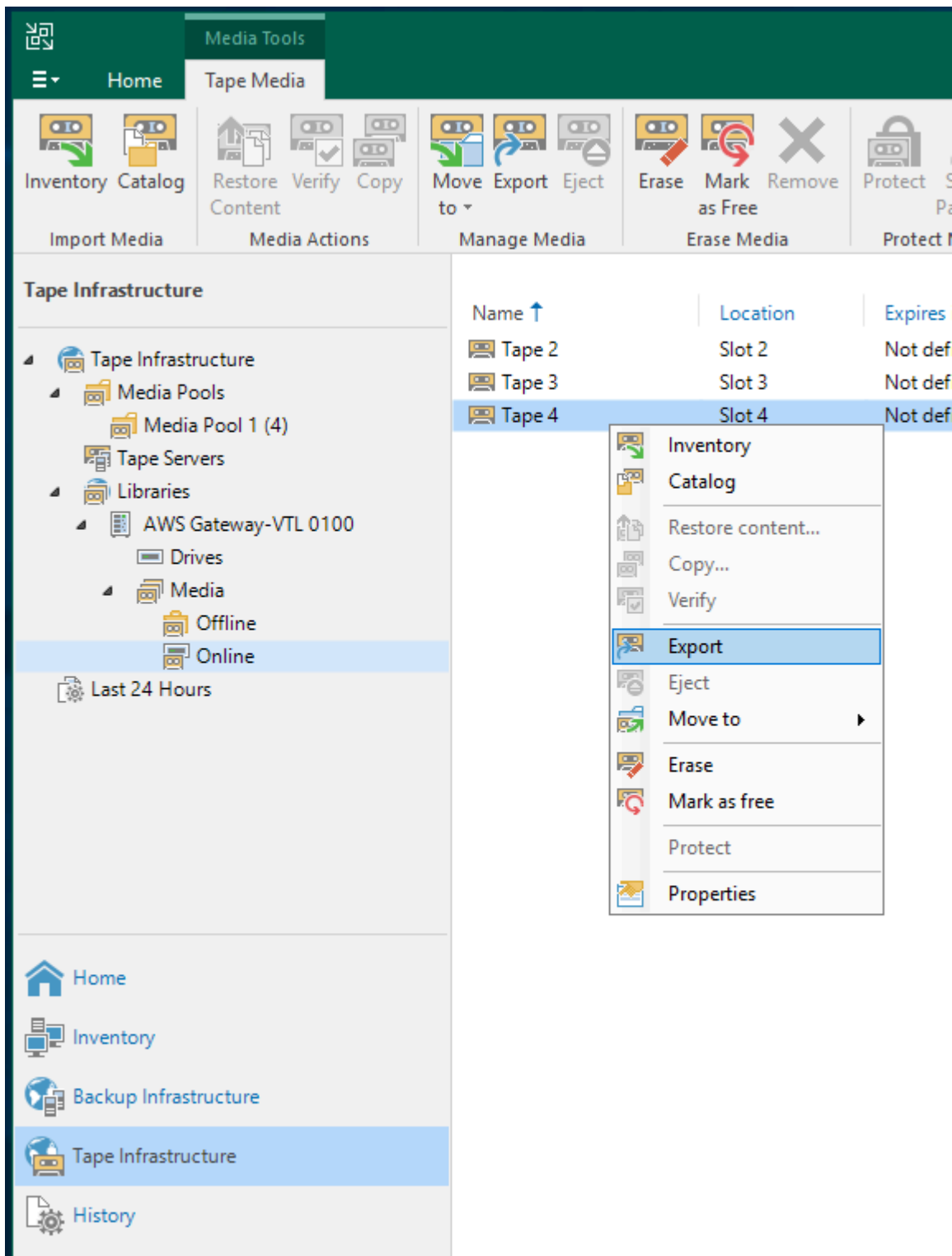
Si la puerta de enlace de cinta se reinicia por algún motivo durante un trabajo de copia de seguridad en curso, el trabajo de copia de seguridad se realizará incorrectamente. Para completar el trabajo de copia de seguridad incorrecto, debe volver a enviarlo.

Archivado de una cinta mediante Veeam

Al archivar una cinta, la puerta de enlace de cinta traslada la cinta desde la biblioteca de cintas de Veeam al almacenamiento sin conexión. Para iniciar el archivado de cintas, expulse la cinta desde la unidad de cinta a la ranura de almacenamiento y, a continuación, exporte la cinta desde la ranura hasta el archivo mediante la aplicación de copia de seguridad, es decir, el software Veeam.

Para archivar una cinta en la biblioteca de Veeam

1. Elija Infraestructura de cintas y elija el grupo de medios que contiene la cinta que desea archivar.



2. Abra el menú contextual (clic con el botón derecho) de la cinta que desee archivar y, a continuación, elija Eject Tape.
3. En el cuadro Ejecting tape, elija Close. La ubicación de la cinta cambia de una unidad de cinta a una ranura.

4. Abra otra vez el menú contextual (haga clic con el botón derecho) de la cinta y, a continuación, elija Export. El estado de la cinta cambia de Tape Drive a Offline.
5. Para Exporting tape, elija Close. La ubicación de la cinta cambia de Slot a Offline.
6. En la consola Storage Gateway, elija su puerta de enlace y, a continuación, elija VTLTape Cartridges y compruebe el estado de la cinta virtual que va a archivar.

El proceso de archivado puede tardar algún tiempo en completarse. El estado inicial de la cinta aparece como IN TRANSIT TO VTS. Cuando se inicia el archivado, el estado cambia a ARCHIVING. Una vez finalizado el archivado, la cinta ya no aparece en la lista, VTL sino que se archiva en S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive.

Restablecimiento de datos desde una cinta archivada en Veeam

La restauración de datos archivados se realiza en dos fases.

Para restaurar datos desde una cinta archivada

1. Recupere la cinta archivada desde el archivo a la puerta de enlace de cinta. Para obtener instrucciones, consulte [Recuperación de cintas archivadas](#).
2. Utilice el software Veeam para restaurar los datos. Para ello, cree un archivo de carpeta de restauración, de la misma forma que cuando se restauran datos desde cintas físicas. Para obtener instrucciones, consulte [Restoring Files from Tape](#) en el centro de ayuda de Veeam.

Paso siguiente

[Eliminación de recursos innecesarios](#)

Comprobación de la configuración mediante Veritas Backup Exec

Puede hacer copias de seguridad de sus datos en cintas virtuales, archivar las cintas y administrar sus dispositivos de biblioteca de cintas virtuales (VTL) mediante Veritas Backup Exec. En este tema, encontrará la documentación básica necesaria para realizar operaciones de backup y restauración con las siguientes versiones de Backup Exec:

- Veritas Backup Exec 2014
- Veritas Backup Exec 15
- Veritas Backup Exec 16

- Veritas Backup Exec 20.x
- Veritas Backup Exec 22.x

El procedimiento para utilizar estas versiones de Backup Exec con una puerta de enlace de cinta es el mismo. Consulte el [sitio web de soporte de Veritas](#) para obtener información detallada sobre cómo utilizar Backup Exec, incluyendo cómo crear copias de seguridad seguras con Backup Exec, listas de compatibilidad de software y hardware y guías de administrador para Backup Exec.

Para obtener más información acerca de las aplicaciones de backup compatibles, consulte [Aplicaciones de copia de seguridad de terceros compatibles con una puerta de enlace de cinta](#).

Temas

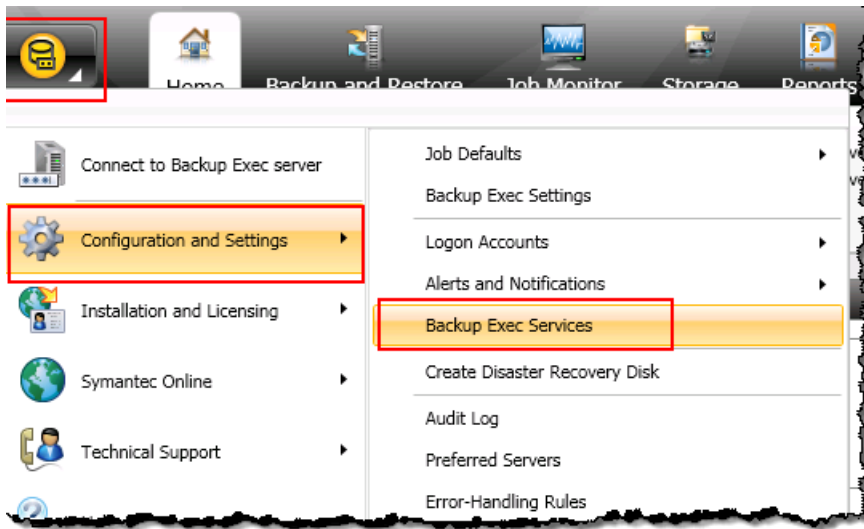
- [Configuración de almacenamiento en Backup Exec](#)
- [Importación de una cinta en Backup Exec](#)
- [Escritura de datos en una cinta en Backup Exec](#)
- [Archivado de una cinta mediante Backup Exec](#)
- [Restablecimiento de datos desde una cinta archivada en Backup Exec](#)
- [Desactivación de una unidad de cinta en Backup Exec](#)

Configuración de almacenamiento en Backup Exec

Después de conectar los dispositivos de la biblioteca de cintas virtuales (VTL) al cliente de Windows, debe configurar el almacenamiento de Backup Exec para que reconozca los dispositivos. Para obtener información sobre cómo conectar VTL los dispositivos al cliente de Windows, consulte [Conexión de sus VTL dispositivos](#).

Para configurar el almacenamiento

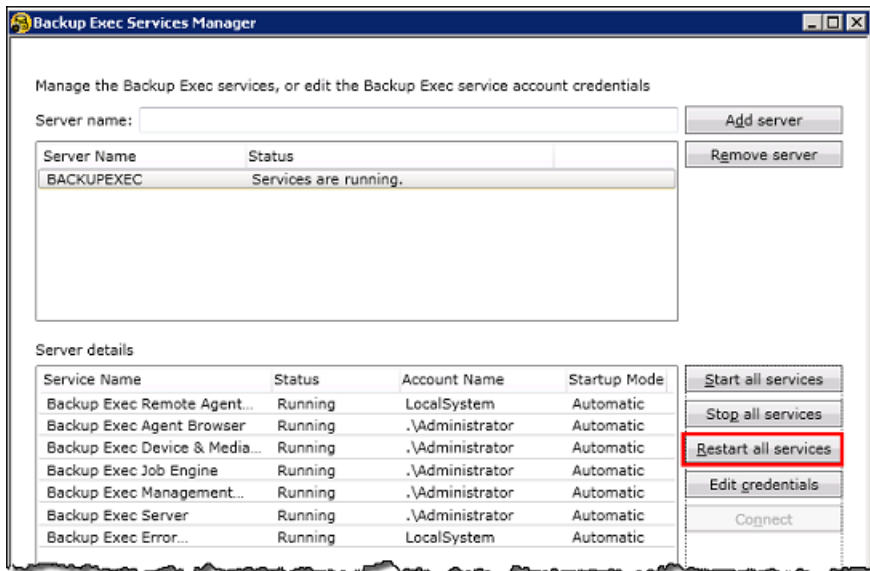
1. Inicie el software Backup Exec y, a continuación, elija el icono amarillo de la esquina superior izquierda de la barra de herramientas.
2. Elija Configuration and Settings y, a continuación, elija Backup Exec Services para abrir Backup Exec Service Manager.



3. Elija Restart All Services. A continuación, Backup Exec reconoce los VTL dispositivos (es decir, el cambiador de medio y las unidades de cinta). Este proceso de reinicio puede tardar unos minutos.

Note

La puerta de enlace de cinta proporciona 10 unidades de cinta. Sin embargo, el acuerdo de licencia de Backup Exec podría exigir que la aplicación de backup funcione con menos de 10 unidades de cinta. En ese caso, debe desactivar unidades de cinta en la biblioteca de robótica de Backup Exec para dejar únicamente el número de unidades de cinta permitidas por el acuerdo de licencia activado. Para obtener instrucciones, consulte [Desactivación de una unidad de cinta en Backup Exec](#) .



- Una vez completado el reinicio, cierre Backup Exec Service Manager.

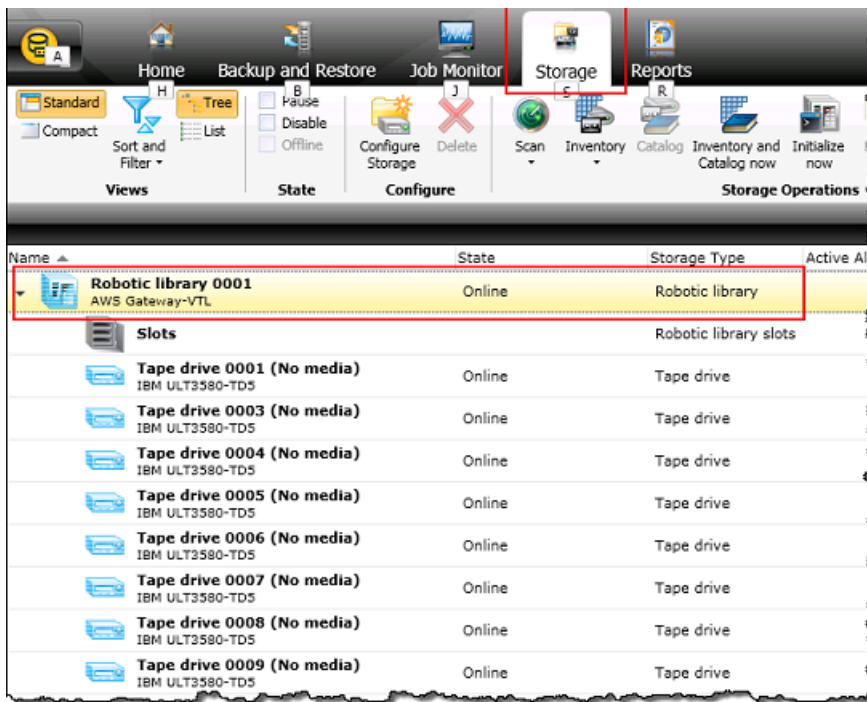
Importación de una cinta en Backup Exec

Ahora puede importar una cinta desde la gateway hasta una ranura.

- Seleccione la pestaña Almacenamiento y, a continuación, expanda el árbol de la biblioteca robótica para mostrar los VTL dispositivos.

Important

El software Veritas Backup Exec requiere el tipo de cambiador de medios de puerta de enlace de cinta. Si el tipo de cambiador de medios que aparece bajo Biblioteca de robótica no es puerta de enlace de cinta, debe cambiarlo antes de configurar el almacenamiento en la aplicación de copia de seguridad. Para obtener información sobre cómo seleccionar un tipo de cambiador de medios diferente, consulte [Selección de un cambiador de medios después de activar la gateway](#).



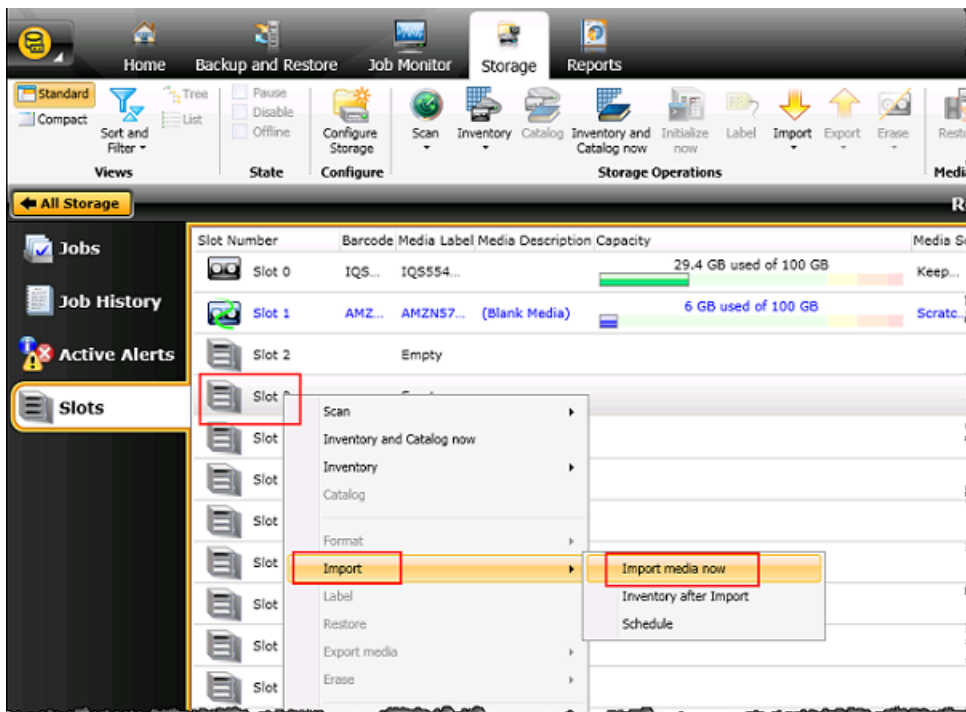
2. Elija el icono Slots para mostrar todas las ranuras.

Note

Al importar las cintas en la biblioteca de robótica, las cintas se almacenan en ranuras en lugar de unidades de cinta. Por lo tanto, las unidades de cinta podrían tener un mensaje que indica que no hay medio en las unidades (No media). Cuando inicie un trabajo de backup o restauración, las cintas se moverán a las unidades de cinta.

Debe tener cintas disponibles en la biblioteca de cintas de la gateway para importar una cinta en una ranura de almacenamiento. Para obtener instrucciones sobre cómo crear cintas, consulte [Adición de cintas virtuales](#).

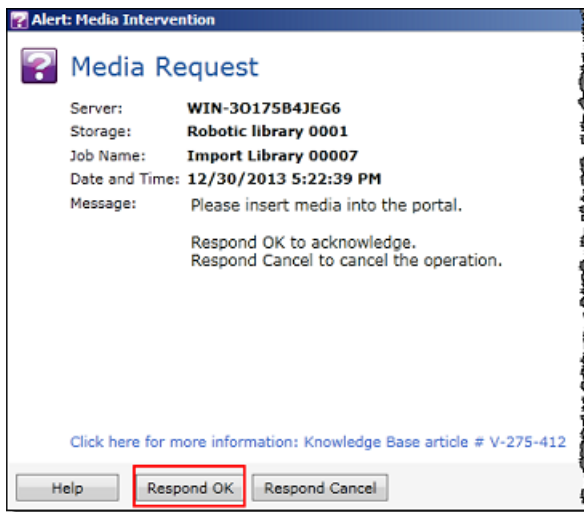
3. Abra el menú contextual (haga clic con el botón derecho) de una ranura vacía, elija Import y, a continuación, elija Import media now. En la siguiente captura de pantalla, la ranura número 3 está vacía. Puede seleccionar más de una ranura e importar varias cintas en una única operación de importación.



4. En la ventana Media Request que aparece, elija View details.



5. En la ventana Action Alert: Media Intervention, elija Respond OK para insertar el medio en la ranura.



La cinta aparece en la ranura seleccionada.

Note

Las cintas que se importan incluyen cintas vacías y cintas que se han recuperado desde el archivo hasta la gateway.

Escritura de datos en una cinta en Backup Exec

Para escribir datos en una cinta virtual de puerta de enlace de cinta, utilice el mismo procedimiento y las mismas políticas de copia de seguridad que con las cintas físicas. Para obtener información detallada, consulte Backup Exec Administrative Guide en la sección de documentación del software Backup Exec.

Note

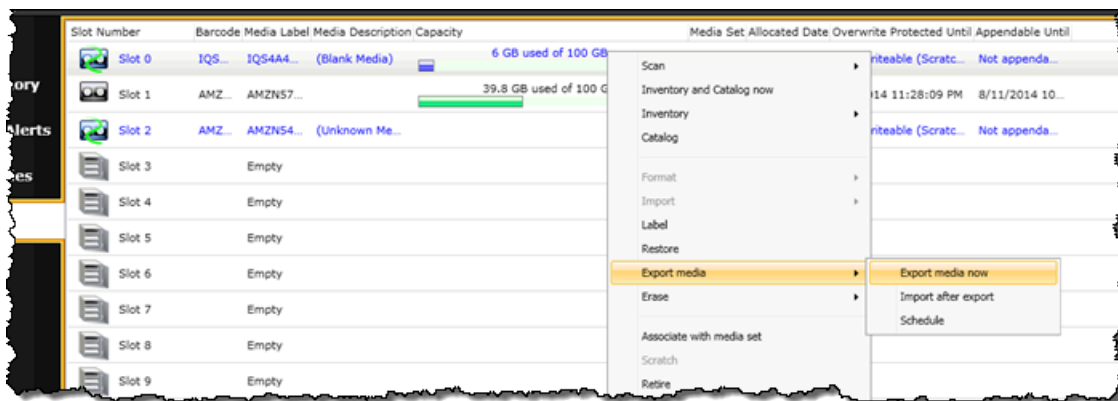
Si la puerta de enlace de cinta se reinicia por algún motivo durante un trabajo de copia de seguridad en curso, es posible que el trabajo de copia de seguridad se realice incorrectamente. Si el trabajo de copia de seguridad se realiza incorrectamente, el estado de la cinta en Veritas Backup Exec cambia a No anexable. Puede archivar la cinta o seguir leyendo sus datos. Para completar el trabajo de copia de seguridad incorrecto, debe volver a enviarlo en una cinta nueva.

Archivado de una cinta mediante Backup Exec

Al archivar una cinta, Tape Gateway la mueve de la biblioteca de cintas virtuales de la puerta de enlace (VTL) al almacenamiento fuera de línea. Para comenzar el proceso de archivado de cinta, exporte la cinta con el software Backup Exec.

Para archivar la cinta

1. Elija el menú Storage, elija Slots, abra el menú contextual (haga clic con el botón derecho) de la ranura de la que desee exportar la cinta, elija Export media y, a continuación, elija Export media now. Puede seleccionar más de una ranura y exportar varias cintas en una única operación de exportación.



2. En la ventana emergente Media Request, elija View details y, a continuación, elija Respond OK en la ventana Alert: Media Intervention.

En la consola de Storage Gateway, puede comprobar el estado de la cinta que está archivando. Puede la carga de datos en AWS tarde algún tiempo en finalizar. Durante este tiempo, la cinta exportada aparece en Tape Gateway VTL con el estado IN TRANSIT TO VTS. Cuando se complete la carga y comience el proceso de archivado, el estado cambiará a ARCHIVING. Una vez finalizado el archivado de los datos, la cinta exportada ya no aparece en la lista, VTL sino que se archiva en S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive.

3. Elija su puerta de enlace y, a continuación, elija cartuchos de VTL cinta y compruebe que la cinta virtual ya no aparezca en la lista de su puerta de enlace.
4. En el panel de navegación de la consola de Storage Gateway, elija Cintas. Compruebe que el estado de la cinta sea ARCHIVED.

Restablecimiento de datos desde una cinta archivada en Backup Exec

La restauración de datos archivados se realiza en dos fases.

Para restaurar datos desde una cinta archivada

1. Recupere la cinta archivada en una puerta de enlace de cinta. Para obtener instrucciones, consulte [Recuperación de cintas archivadas](#).
2. Utilice Backup Exec para restaurar los datos. Este proceso es el mismo que la restauración de datos desde cintas físicas. Para obtener instrucciones, consulte la Guía administrativa de Backup Exec en la sección de documentación del software de Backup Exec.

Desactivación de una unidad de cinta en Backup Exec

Una puerta de enlace de cinta proporciona 10 unidades de cinta, pero puede que decida utilizar menos unidades de cinta. En ese caso, desactive las unidades de cinta que no utilice.

1. Abra Backup Exec y elija la pestaña Storage.
2. En el árbol Biblioteca de robótica, abra el menú contextual (haga clic con el botón derecho) de la unidad de cinta que desee desactivar y, a continuación, elija Deshabilitar.

Paso siguiente

[Eliminación de recursos innecesarios](#)

Probar su configuración mediante Veritas NetBackup

Puede hacer copias de seguridad de sus datos en cintas virtuales, archivarlas y administrar sus dispositivos de biblioteca de cintas virtuales (VTL) mediante NetBackup Veritas. En este tema, encontrará documentación básica sobre cómo configurar la NetBackup aplicación para una puerta de enlace de cintas y realizar una operación de copia de seguridad y restauración. Para ello, puede utilizar las siguientes versiones de NetBackup:

- Veritas 7.x NetBackup
- Veritas 8.x NetBackup

El procedimiento para utilizar estas versiones de Backup Exec con una puerta de enlace de cinta es similar. Para obtener información detallada sobre cómo utilizarlas NetBackup, consulte las

[herramientas de preparación para las operaciones y los servicios de Veritas \(SORT\)](#) en el sitio web de Veritas. Para obtener información de soporte de Veritas sobre la compatibilidad de hardware, consulte la Lista de compatibilidad de hardware de [NetBackup 7.0 a 7.6.x](#), la [Lista de compatibilidad de hardware de NetBackup 8.0 a 8.1.x](#) o la [Lista de compatibilidad de hardware de NetBackup 8.2 a 8.x.x](#) en el [sitio web](#) de Veritas.

Para obtener más información sobre aplicaciones de backup compatibles, consulte [Aplicaciones de copia de seguridad de terceros compatibles con una puerta de enlace de cinta](#).

Temas

- [Configuración de dispositivos de almacenamiento NetBackup](#)
- [Copia de seguridad de datos en una cinta](#)
- [Archivado de la cinta](#)
- [Restauración de datos desde la cinta](#)

Configuración de dispositivos de almacenamiento NetBackup

Una vez que haya conectado los dispositivos de la biblioteca de cintas virtuales (VTL) al cliente de Windows, configure el NetBackup almacenamiento de Veritas para que reconozca sus dispositivos. Para obtener información sobre cómo conectar VTL los dispositivos al cliente de Windows, consulte [Conexión de sus VTL dispositivos](#).

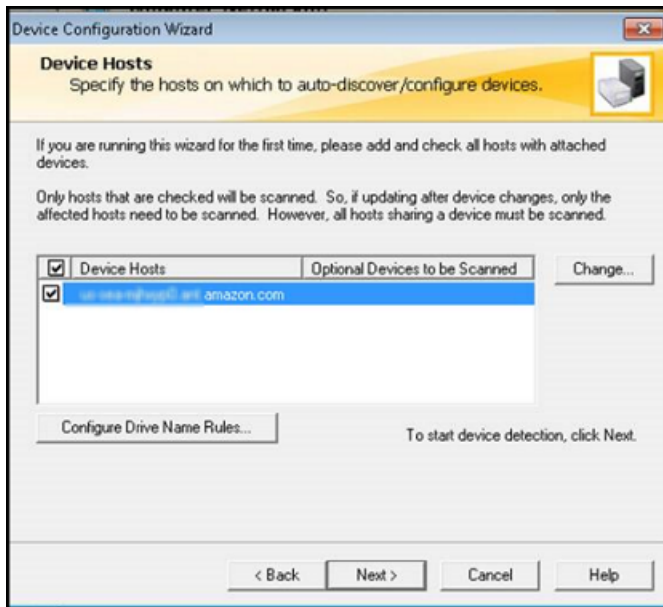
NetBackup Para configurar el uso de dispositivos de almacenamiento en su Tape Gateway

1. Abra la consola de NetBackup administración y ejecútela como administrador.

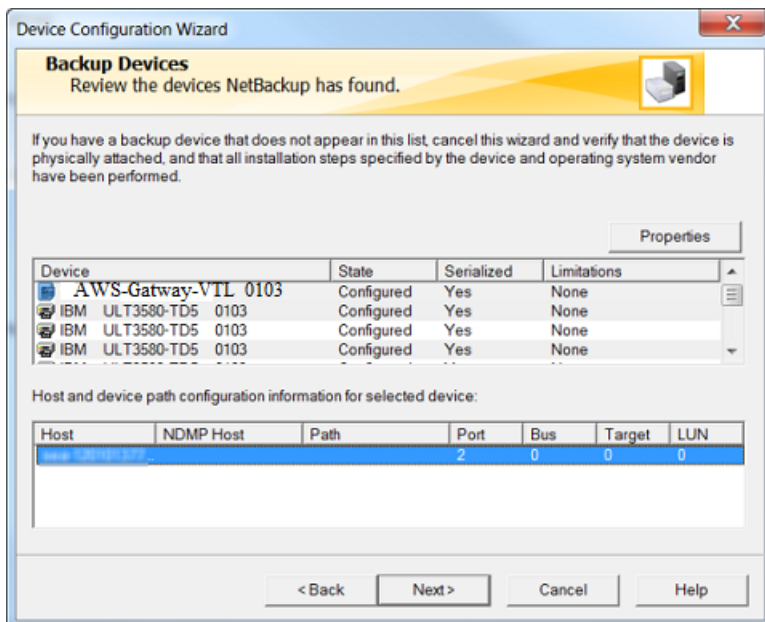


2. Elija Configure Storage Devices para abrir el asistente de configuración de dispositivos.
3. Elija Next (Siguiente). La NetBackup aplicación detecta su ordenador como anfitrión del dispositivo.

- En la columna Device Hosts, seleccione su equipo y, a continuación, elija Next. La NetBackup aplicación escanea el ordenador en busca de dispositivos y descubre todos los dispositivos.



- En la página Scanning Hosts, elija Next y, a continuación, elija Next. La NetBackup aplicación encuentra las 10 unidades de cinta y el cambiador de medio del ordenador.

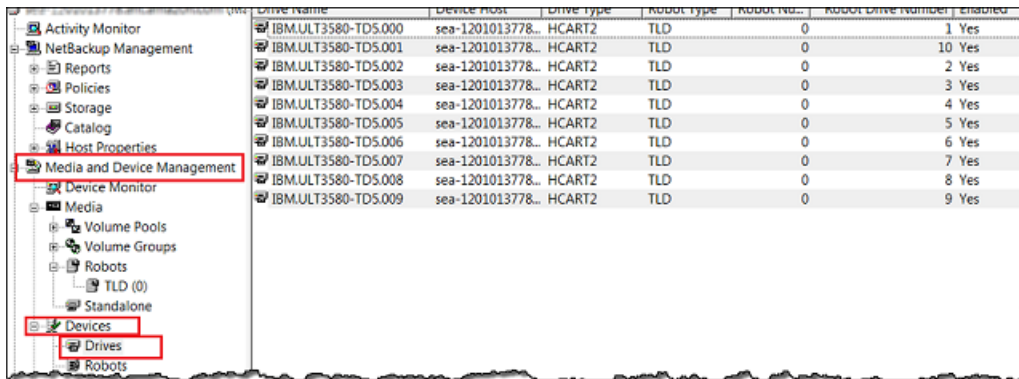


- En la ventana Backup Devices, elija Next.
- En la ventana Drag and Drop Configuration, compruebe que esté seleccionado el cambiador de medios y, a continuación, elija Next.

8. En el cuadro de diálogo que aparece, elija Yes para guardar la configuración en su equipo. La NetBackup aplicación actualiza la configuración del dispositivo.
9. Cuando se complete la actualización, seleccione Siguiente para que los dispositivos estén disponibles para la NetBackup aplicación.
10. En la ventana Finished!, elija Finish.

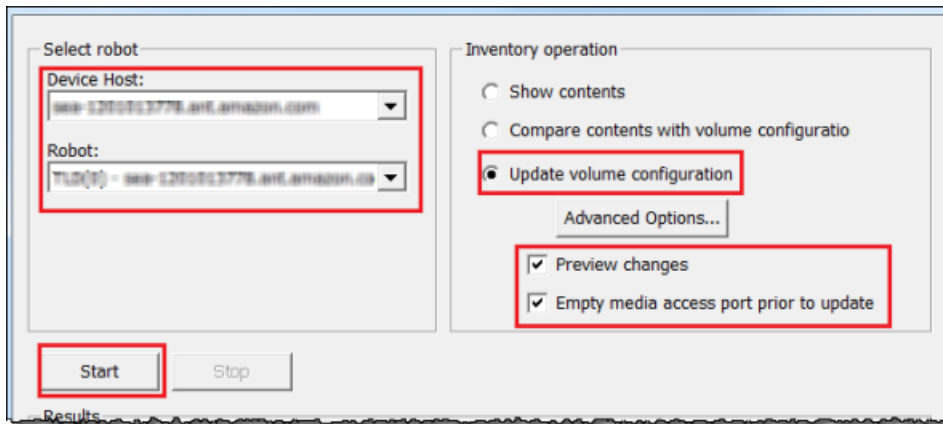
Para verificar los dispositivos en la NetBackup aplicación

1. En la consola de NetBackup administración, expanda el nodo Administración de medios y dispositivos y, a continuación, expanda el nodo Dispositivos. Elija Drives para mostrar todas las unidades de cinta.



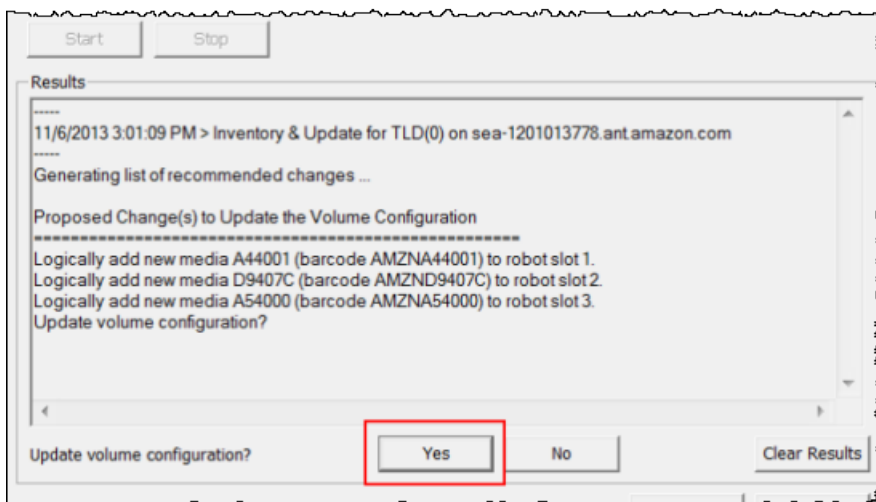
Drive Name	Device Host	Drive Type	Robot Type	Robot Num...	Robot Drive Number	Enabled
IBM.ULT3580-TD5.000	sea-1201013778...	HCART2	TLD	0	1	Yes
IBM.ULT3580-TD5.001	sea-1201013778...	HCART2	TLD	0	10	Yes
IBM.ULT3580-TD5.002	sea-1201013778...	HCART2	TLD	0	2	Yes
IBM.ULT3580-TD5.003	sea-1201013778...	HCART2	TLD	0	3	Yes
IBM.ULT3580-TD5.004	sea-1201013778...	HCART2	TLD	0	4	Yes
IBM.ULT3580-TD5.005	sea-1201013778...	HCART2	TLD	0	5	Yes
IBM.ULT3580-TD5.006	sea-1201013778...	HCART2	TLD	0	6	Yes
IBM.ULT3580-TD5.007	sea-1201013778...	HCART2	TLD	0	7	Yes
IBM.ULT3580-TD5.008	sea-1201013778...	HCART2	TLD	0	8	Yes
IBM.ULT3580-TD5.009	sea-1201013778...	HCART2	TLD	0	9	Yes

2. En el nodo Devices, elija Robots para mostrar todos los cambiadores de medios. En la NetBackup aplicación, el cambiador de medio se denomina robot.
3. En el panel Todos los robots, abra el menú contextual (haga clic con el botón derecho) de TLD(0) (es decir, su robot) y, a continuación, seleccione Inventory Robot.
4. En la ventana Robot Inventory, verifique que su host esté seleccionado en la lista Device-Host ubicada en la categoría Select robot.
5. Compruebe que el robot esté seleccionado en la lista Robot.
6. En la ventana Robot Inventory, seleccione Update volume configuration, seleccione Preview changes, seleccione Empty media access port prior to update y, a continuación, elija Start.

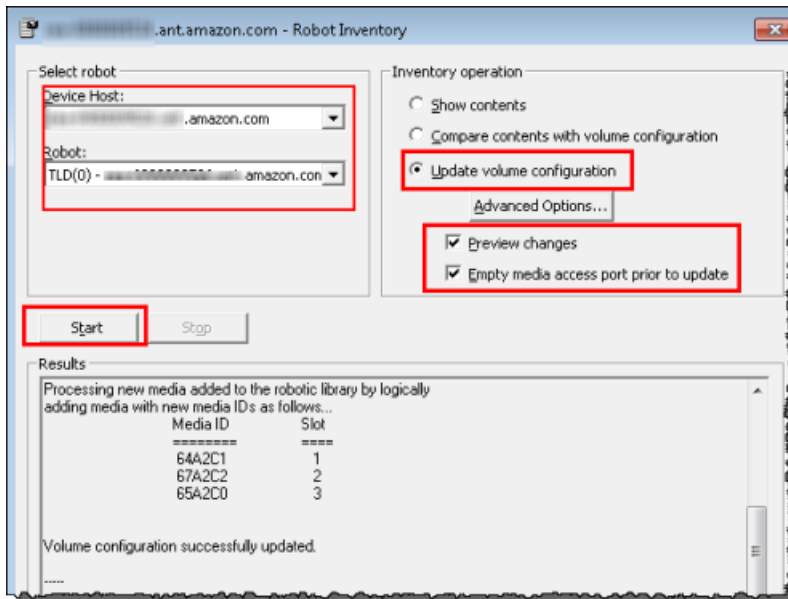


A continuación, el proceso realiza un inventario del cambiador de medios y de las cintas virtuales en la base de datos de NetBackup Enterprise Media Management (EMM). NetBackup almacena la información multimedia, la configuración del dispositivo y el estado de la cinta en EMM

7. En la ventana Robot Inventory, elija Yes una vez que se haya completado el inventario. Al elegir Yes aquí se actualiza la configuración y se transfieren las cintas virtuales que se encuentran en ranuras de importación/exportación a la biblioteca de cintas virtuales.



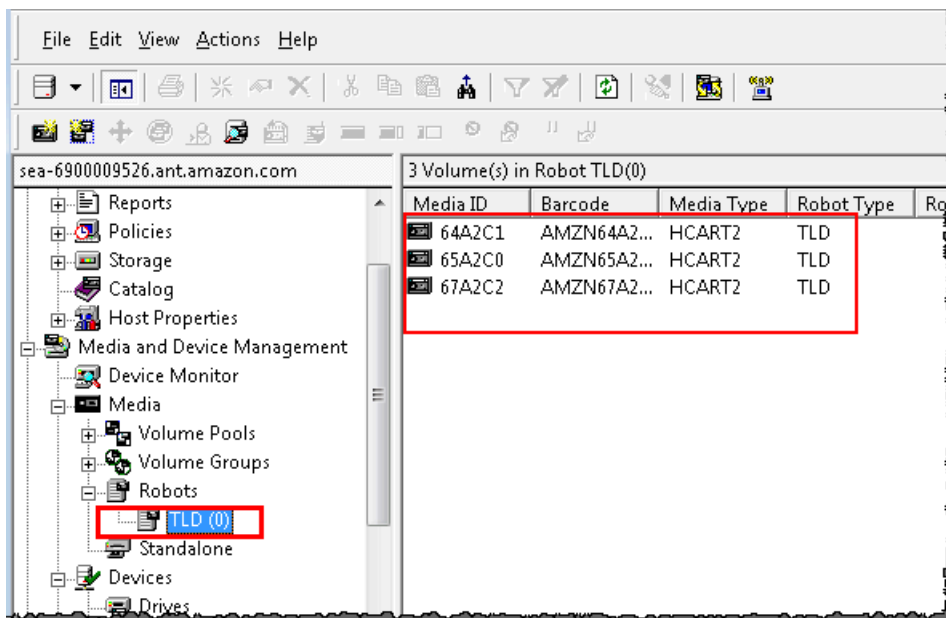
Por ejemplo, la siguiente captura de pantalla muestra tres cintas virtuales que se encuentran en las ranuras de importación y exportación.



8. Cierre la ventana Robot Inventory.
9. En el nodo Media, expanda el nodo Robots y elija TLD(0) para mostrar todas las cintas virtuales que están disponibles para su robot (cambiador de tamaño).

Note

Si ya ha conectado otros dispositivos a la NetBackup aplicación, es posible que tenga varios robots. Asegúrese de seleccionar el robot correcto.



Tras conectar los dispositivos y haberlos puesto a disposición de la aplicación de backup, puede probar la gateway. Para probar la gateway, haga copias de seguridad de los datos en las cintas virtuales que ha creado y archive las cintas.

Copia de seguridad de datos en una cinta

Puede probar la configuración de la puerta de enlace de cinta haciendo copias de seguridad de datos en las cintas virtuales.

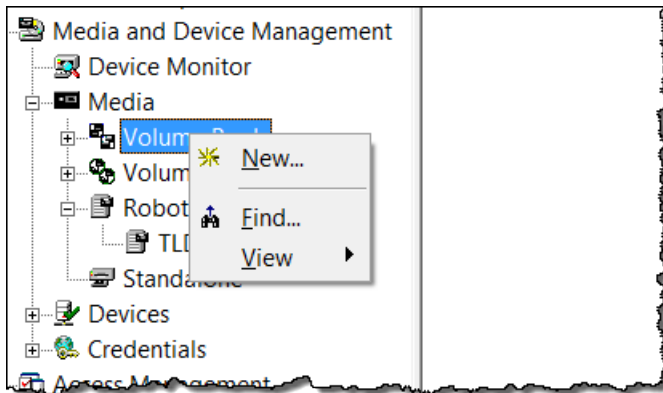
Note

- Solo debe hacer una copia de seguridad de una pequeña cantidad de datos para este ejercicio de introducción, ya que existen costos asociados con el almacenamiento, el archivado y la recuperación de datos. Para obtener información detallada sobre precios, consulte [Precios](#) en la página de detalles de Storage Gateway.
- Si la puerta de enlace de cinta se reinicia por algún motivo durante un trabajo de copia de seguridad en curso, el trabajo de copia de seguridad se suspenderá. El trabajo de copia de seguridad suspendido se reanudará automáticamente cuando la puerta de enlace termine de reiniciarse.

Para crear un grupo de volúmenes

Un grupo de volúmenes es una colección de cintas virtuales que se utilizan para una copia de seguridad.

1. Inicie la consola NetBackup de administración.
2. Expanda el nodo Media, abra el menú contextual (haga clic con el botón derecho) de Volumen Pool y, a continuación, elija New. Aparece el cuadro de diálogo New Volume Pool.



3. En Name, escriba un nombre para el grupo de volúmenes.
4. Para Description, escriba una descripción del grupo de volúmenes y, a continuación, elija OK. El grupo de volúmenes que acaba de crear se agrega a la lista de grupos de volúmenes.

La siguiente captura de pantalla muestra una lista de grupos de volúmenes.

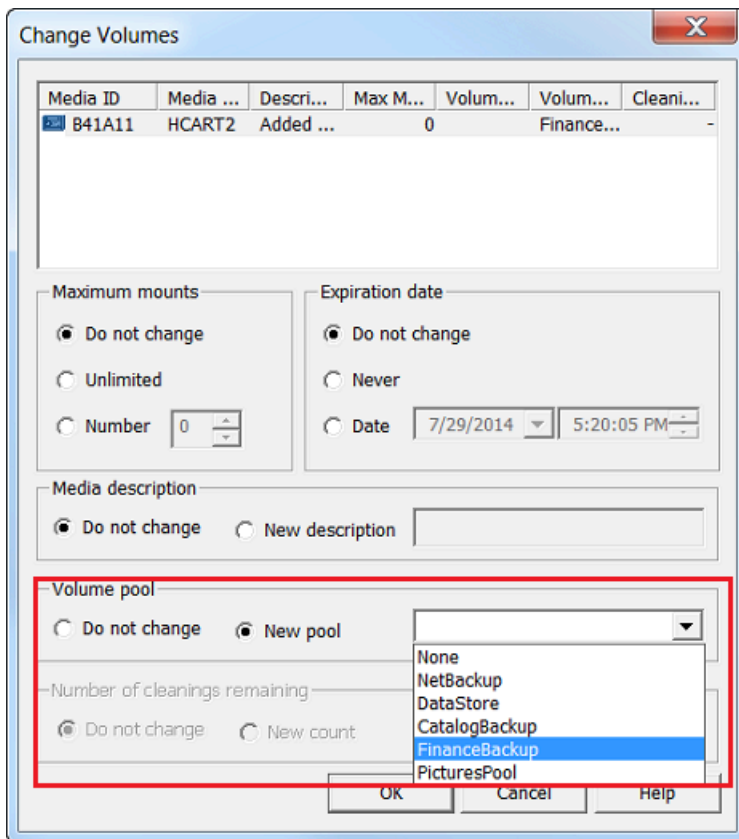
Volume Pool	Number	Max Partial...	Description	Scratch
CatalogBackup	3	0	NetBackup ...	No
DataStore	2	0	the DataSto...	No
FinanceBackup	4	0	Finance	No
NetBackup	1	0	the NetBack...	No
None	0	0	the None po...	No
PhotosPool	6	0	Backs up the...	No
PicturesPool	5	0	Pictures Only	No

Para agregar cintas virtuales a un grupo de volúmenes

1. Expanda el nodo Robots y seleccione el robot TLD(0) para mostrar las cintas virtuales que este robot conoce.

Si ha conectado un robot previamente, es posible que el robot de la puerta de enlace de cinta tenga un nombre diferente.

2. En la lista de cintas virtuales, abra el menú contextual (haga clic con el botón derecho) de la cinta que desee agregar al grupo de volúmenes y elija Cambiar para abrir el cuadro de diálogo Change Volumes. En la siguiente captura de pantalla se muestra el cuadro de diálogo Change Volumes.



3. Para Volume Pool, elija New pool.
4. Para New pool, seleccione el grupo que acaba de crear y, a continuación, elija OK.

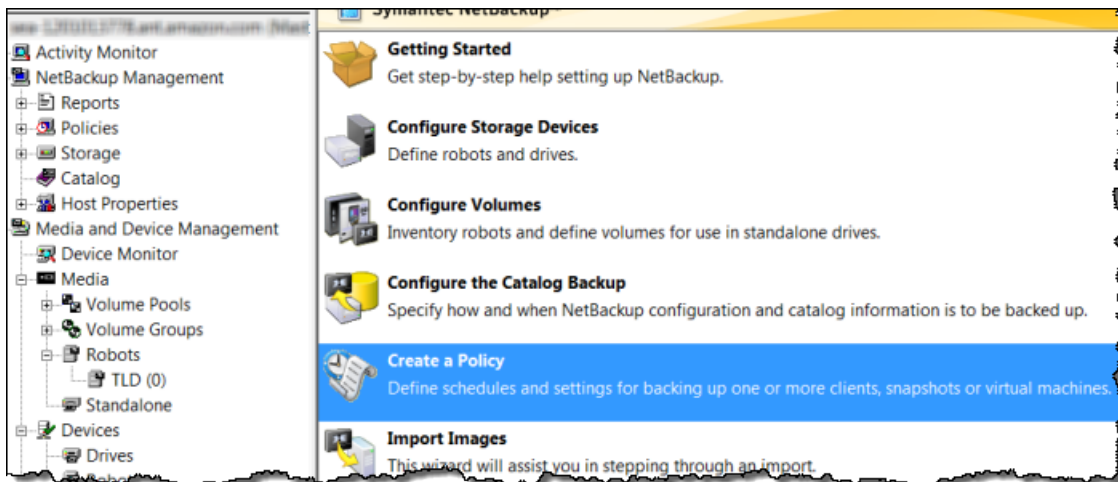
Para comprobar si el grupo de volúmenes contiene la cinta virtual que acaba de agregar, expanda el nodo Media y elija el grupo de volúmenes.

Para crear una política de backup

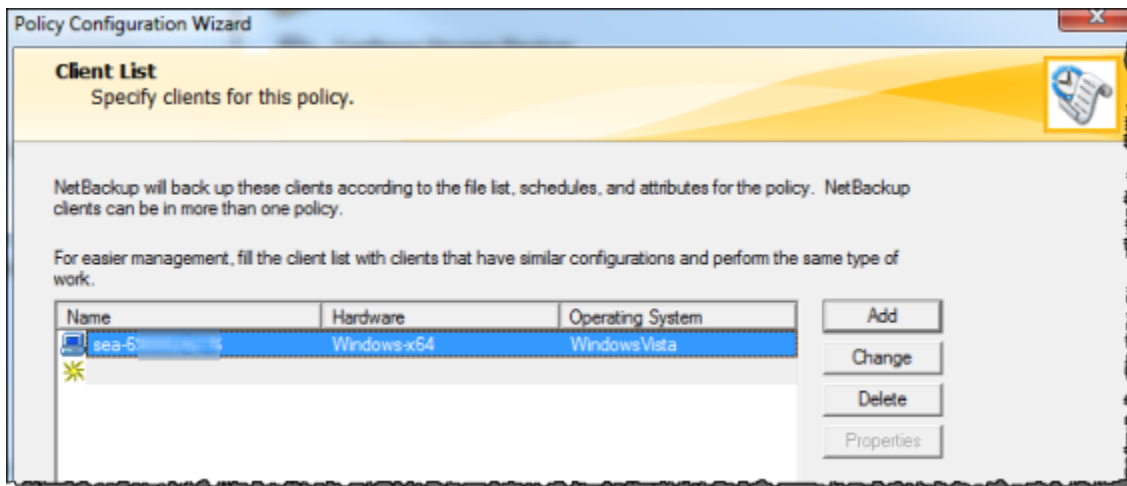
La política de backup especifica qué datos incluir en la copia de seguridad, cuándo realizarlo y qué grupo de volúmenes utilizar.

1. Elija su servidor maestro para volver a la NetBackup consola de Veritas.

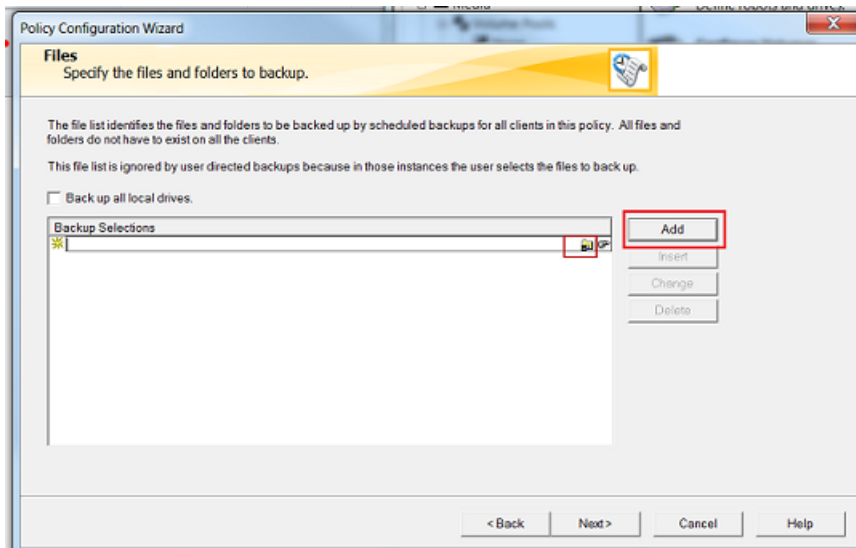
La siguiente captura de pantalla muestra la NetBackup consola con la opción Crear una política seleccionada.



2. Elija Create a Policy para abrir la ventana Policy Configuration Wizard.
3. Seleccione File systems, databases, applications y elija Next.
4. Para Policy Name, escriba un nombre para la política, compruebe que MS-Windows esté seleccionado en la lista Select the policy type y, a continuación, elija Next.
5. En la ventana Client List, elija Add, escriba el nombre de host del equipo en la columna Name y, a continuación, elija Next. Este paso aplica la política que está definiendo a localhost (el equipo cliente).



6. En la ventana Files, elija Add y, a continuación, elija el icono de la carpeta.

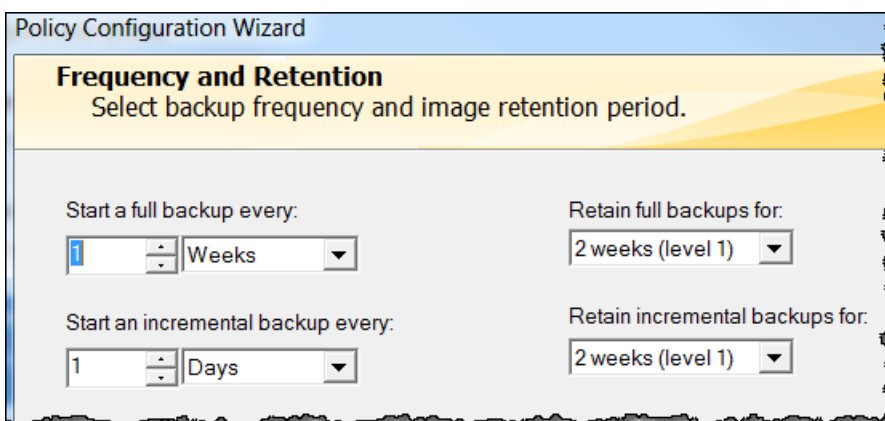


7. En la ventana Browse, navegue hasta la carpeta o hasta los archivos que desee incluir en la copia de seguridad, elija OK y, a continuación, elija Next.
8. En la Backup Types, acepte los valores predeterminados y, a continuación, elija Next.

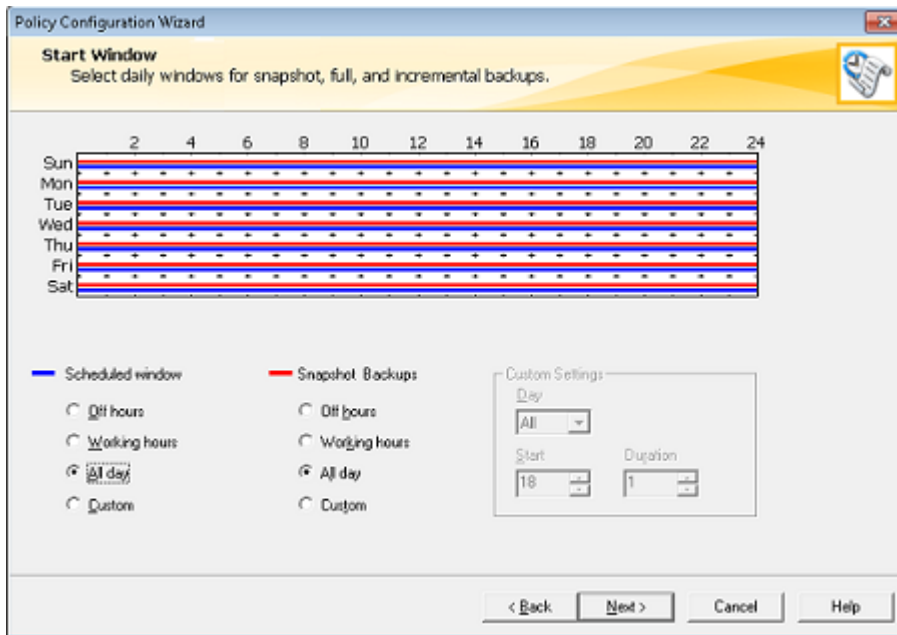
Note

Si desea iniciar la copia de seguridad usted mismo, seleccione User Backup.

9. En la ventana Frequency and Retention, seleccione la frecuencia y la política de retención que desee aplicar a la copia de seguridad. Para este ejercicio, puede aceptar todos los valores predeterminados y elegir Siguiente.



10. En la ventana Start, seleccione Off hours y, a continuación, elija Next. Esta selección específica que la copia de seguridad de la carpeta solo debe realizarse durante las horas no laborables.

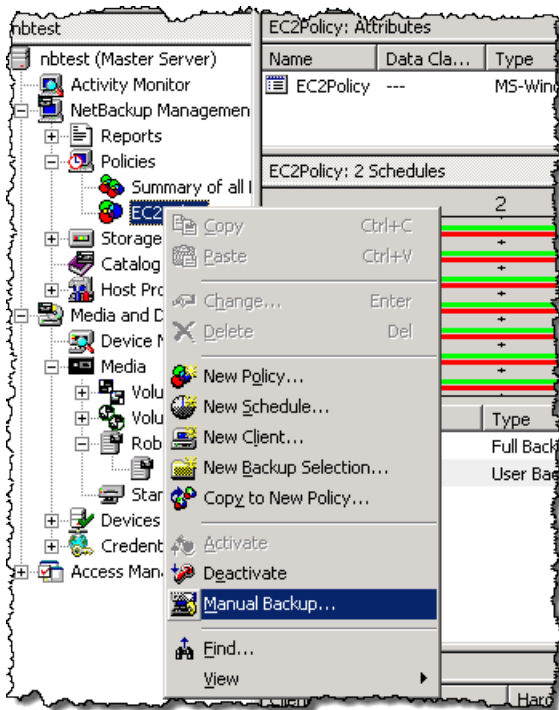


11. En el asistente Policy Configuration, elija Finish.

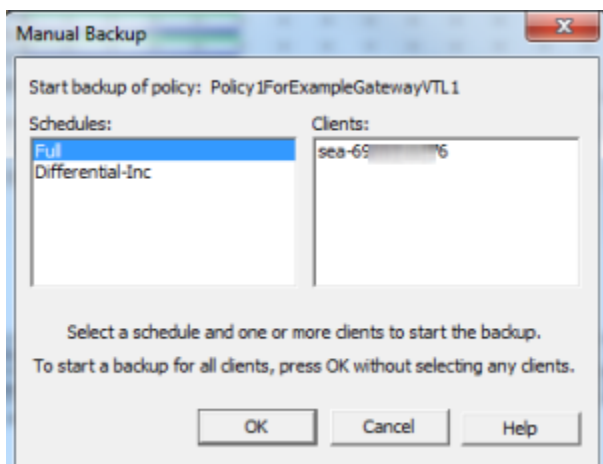
La política ejecuta los backup de acuerdo con el programa. También puede realizar un backup manual en cualquier momento, como haremos en el paso siguiente.

Para hacer un backup manual






1. En el panel de navegación de la NetBackup consola, expanda el nodo NetBackup de administración.
2. Expanda el nodo Políticas.
3. Abra el menú contextual (haga clic con el botón derecho) de la política y elija Manual Backup.



4. En la ventana Manual Backup, seleccione un programa, seleccione un cliente y, a continuación, elija OK.



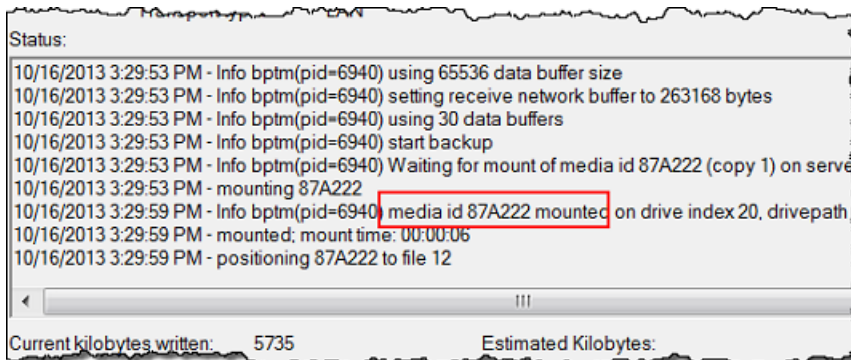
5. En el cuadro de diálogo Manual Backup Started que aparece, elija OK.
6. En el panel de navegación, elija Activity Monitor para ver el estado de la copia de seguridad en la columna Job ID.

nbtest: 11 Jobs (0 Queued 0 Active 0 Waiting for Retry 0 Suspended 0 Incomplete 11 Done)								
Job ID	Type	Job State	State Details	Status	Job Policy	Job Schedule	Client	
18	Backup	Done		0	EC2Policy	Full	localhost	
17	Backup	Done		0	EC2Policy	Full	localhost	
14	Backup	Done		0	EC2Policy	Full	localhost	
10	Image Cleanup	Done		1				
11	Image Cleanup	Done		1				

Para encontrar el código de barras de la cinta virtual en la que se NetBackup escribieron los datos del archivo durante la copia de seguridad, consulte la ventana Job Details tal y como se describe en el siguiente procedimiento. Necesitará este código de barras en el procedimiento de la siguiente sección, donde archivará la cinta.

Para buscar el código de barras de una cinta

1. En Activity Monitor, abra el menú contextual (haga clic con el botón derecho) del identificador del trabajo de la copia de seguridad en la columna Job ID y, a continuación, elija Details.
2. En la ventana Job Details, elija la pestaña Detailed Status.
3. En el cuadro Status, busque el ID de medio. Por ejemplo, en la siguiente captura de pantalla, el ID de medio es 87A222. Este ID le ayuda a determinar en qué cinta ha escrito los datos.



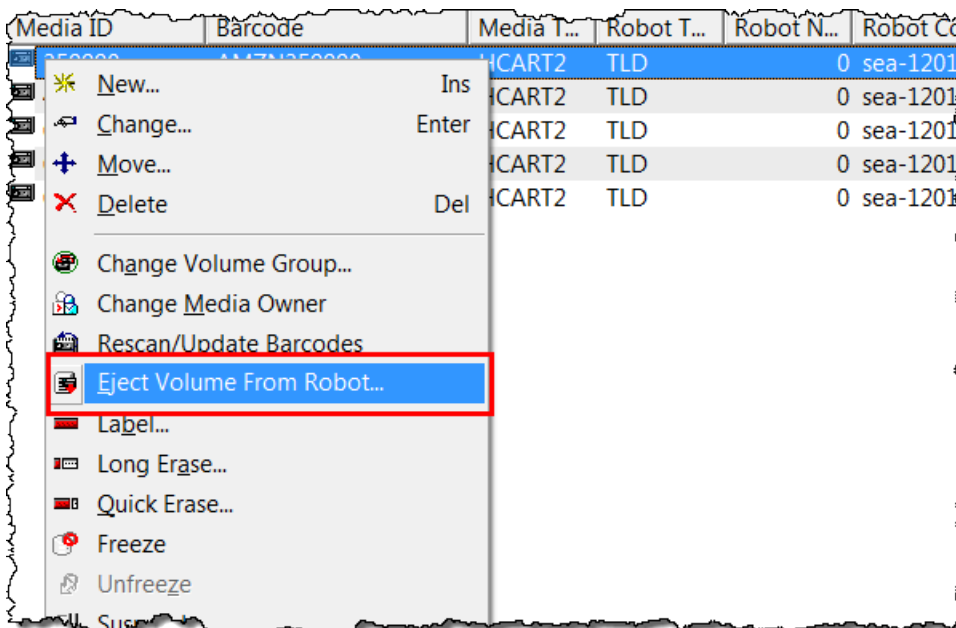
Ha implementado correctamente una puerta de enlace de cinta, ha creado cintas virtuales y ha hecho copias de seguridad de los datos. A continuación, puede archivar las cintas virtuales y recuperarlas desde el archivo.

Archivado de la cinta

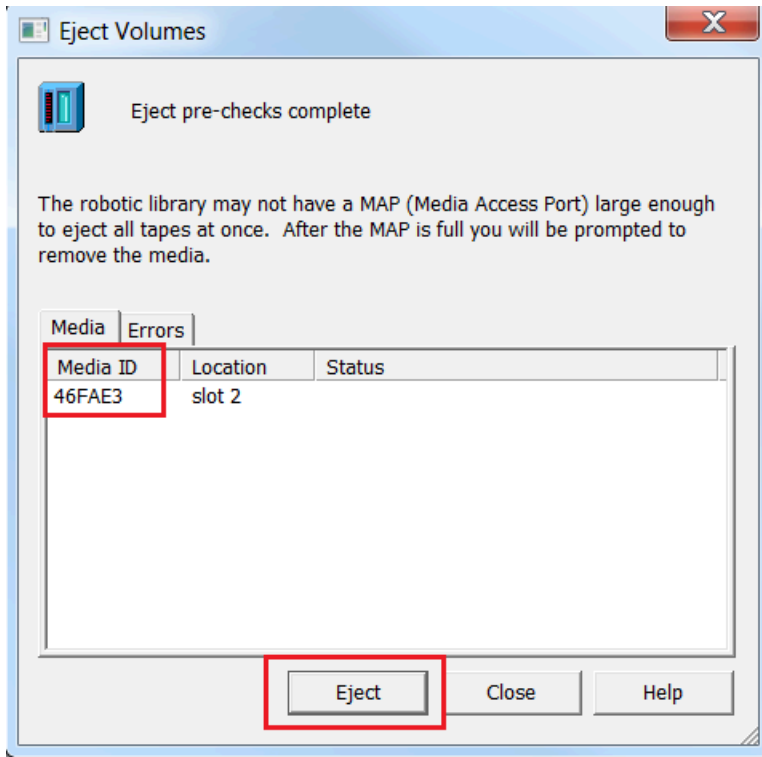
Al archivar una cinta, Tape Gateway la mueve de la biblioteca de cintas virtuales de la puerta de enlace (VTL) al archivo, lo que proporciona almacenamiento fuera de línea. Para iniciar el proceso de archivado de cinta, expulse la cinta la aplicación de backup.

Para archivar una cinta virtual

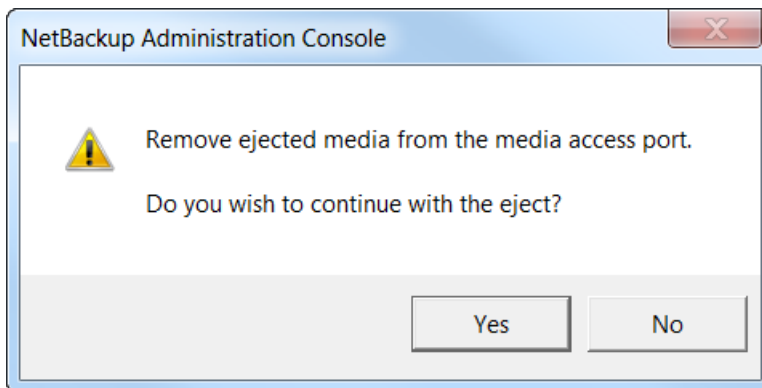
1. En la consola de NetBackup administración, expanda el nodo de administración de medios y dispositivos y expanda el nodo multimedia.
2. Expanda Robots y elija TLD(0).
3. Abra el menú contextual (haga clic con el botón derecho) de la cinta virtual que desee archivar y, a continuación, elija Eject Volume From Robot.



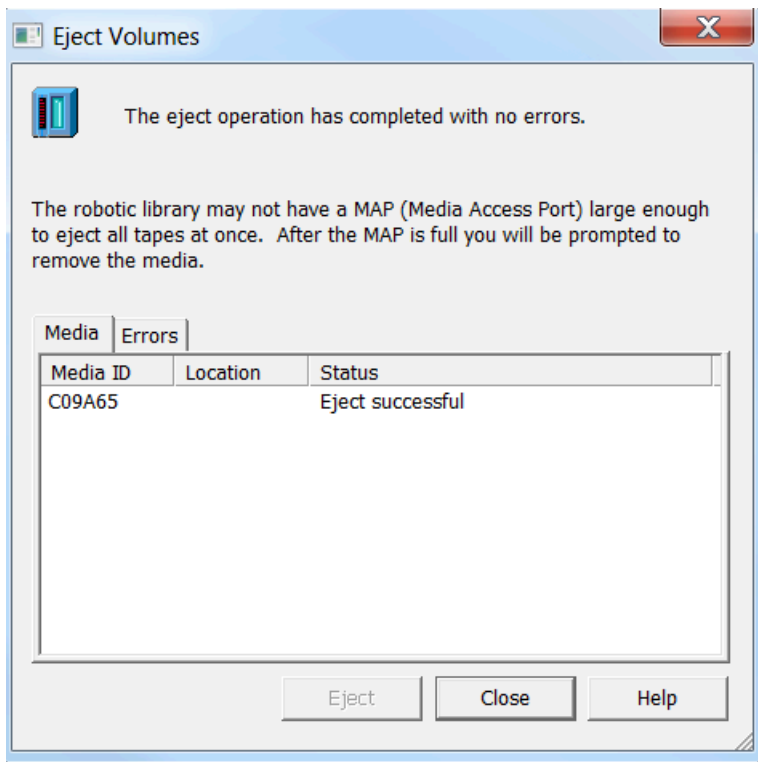
4. En la ventana Eject Volumes, asegúrese de que el valor de Media ID coincida con la cinta virtual que desea expulsar y, a continuación, elija Eject.



5. En el cuadro de diálogo, elija Yes. El cuadro de diálogo se muestra a continuación.



Cuando el proceso de expulsión se complete, el estado de la cinta en el cuadro de diálogo Eject Volumes indica que la expulsión ha sido correcta.



6. Elija Close para cerrar la ventana Eject Volumes.
7. En la consola Storage Gateway, compruebe el estado de la cinta que va a archivar en la puerta de VTL enlace. Puede que la carga de datos en AWS tarde algún tiempo en finalizar. Durante este tiempo, la cinta expulsada aparece en la lista de la puerta de enlace VTL con el estado IN TRANSIT TO. VTS Cuando se inicia el archivado, el estado es. ARCHIVING Una vez finalizada la carga de los datos, la cinta expulsada deja de figurar en la lista, VTL sino que se archiva en S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive.
8. Para comprobar que la cinta virtual ya no aparece en la lista de la puerta de enlace, elija la puerta de enlace y, a continuación, elija los cartuchos de cinta. VTL
9. En el panel de navegación de la consola de Storage Gateway, elija Cintas. Compruebe que el estado de la cinta archivada sea ARCHIVED.

Restauración de datos desde la cinta

La restauración de datos archivados se realiza en dos fases.

Para restaurar datos desde una cinta archivada

1. Recupere la cinta archivada en una puerta de enlace de cinta. Para obtener instrucciones, consulte [Recuperación de cintas archivadas](#).

2. Utilice el software Backup, Archive y Restore instalado con la NetBackup aplicación Veritas. Este proceso es el mismo que la restauración de datos desde cintas físicas. Para obtener instrucciones, consulte las [herramientas de preparación operativa y de servicios de Veritas \(SORT\)](#) en el sitio web de Veritas.

Paso siguiente

[Eliminación de recursos innecesarios](#)

¿Qué tengo que hacer ahora?

Una vez que la puerta de enlace de cinta esté en producción, puede realizar varias tareas de mantenimiento, tales como agregar y retirar cintas, supervisar y optimizar el rendimiento de la puerta de enlace y solucionar problemas. Para obtener información general sobre estas tareas de administración, consulte [Administración de la gateway](#).

Puede realizar algunas de las tareas de mantenimiento de la puerta de enlace en cinta AWS Management Console, como configurar los límites de velocidad de ancho de banda de la puerta de enlace y administrar las actualizaciones del software de la puerta de enlace. Si la puerta de enlace de cinta está implementada en las instalaciones, puede realizar algunas tareas de mantenimiento en la consola local de la puerta de enlace. Entre estas se incluyen el enrutamiento de la puerta de enlace de cinta a través de un proxy y la configuración de la puerta de enlace para que utilice una dirección IP estática. Si ejecuta su gateway como una EC2 instancia de Amazon, puede realizar tareas de mantenimiento específicas en la EC2 consola de Amazon, como añadir y eliminar EBS volúmenes de Amazon. Para obtener más información sobre el mantenimiento de LA puerta de enlace de cinta, consulte [Administración de la puerta de enlace de cinta](#).

Si planea implementar la gateway en producción, debe tener en cuenta la carga de trabajo real para determinar los tamaños de los discos. Para obtener información sobre cómo determinar los tamaños de disco en el mundo real, consulte [Administración de discos locales para Storage Gateway](#). Además, considere la posibilidad de realizar limpieza si no planea utilizar la puerta de enlace de cinta. La limpieza permite evitar incurrir en gastos. Para obtener información sobre la limpieza, consulte [Eliminación de recursos innecesarios](#).

Eliminación de 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.

Si tiene previsto seguir utilizando su puerta de enlace de cinta, consulte información adicional en [¿Qué tengo que hacer ahora?](#)

Para eliminar los recursos innecesarios

1. Elimine las cintas tanto de la biblioteca de cintas virtuales (VTL) como del archivo de la puerta de enlace. Para obtener más información, consulte [Eliminar la puerta de enlace y eliminar los recursos asociados](#).
 - a. Archive todas las cintas que tengan el RETRIEVEDestado en el de su puerta de enlaceVTL. Para obtener instrucciones, consulte [Archivado de cintas](#).
 - b. Elimine las cintas restantes de la puerta de enlaceVTL. Para obtener instrucciones, consulte [Eliminar cintas virtuales de la puerta de enlace de cintas](#).
 - c. Elimine las cintas que haya en el archivo. Para obtener instrucciones, consulte [Eliminar cintas virtuales de la puerta de enlace de cintas](#).
2. A menos que desee seguir utilizando la puerta de enlace de cinta, debe eliminarla. Para obtener instrucciones, consulte [Eliminar la puerta de enlace y eliminar los recursos asociados](#).
3. Elimine la máquina virtual de Storage Gateway desde el host en las instalaciones. Si has creado tu gateway en una EC2 instancia de Amazon, finaliza la instancia.

Activación de una puerta de enlace en una nube virtual privada

Puede crear una conexión privada entre su dispositivo de puerta de enlace en las instalaciones y una infraestructura de almacenamiento basada en la nube. Puede utilizar esta conexión para activar su puerta de enlace y permitir que transfiera datos a los servicios AWS de almacenamiento sin comunicarse a través de la Internet pública. Con el VPC servicio Amazon, puede lanzar AWS recursos, incluidos los puntos finales de la interfaz de red privada, en una nube privada virtual personalizada (VPC). A VPC le permite controlar la configuración de la red, como el rango de direcciones IP, las subredes, las tablas de enrutamiento y las puertas de enlace de red. Para obtener más informaciónVPCs, consulta [¿Qué es AmazonVPC?](#) en la Guía del VPC usuario de Amazon.

Para activar su puerta de enlace en unVPC, utilice Amazon VPC Console para crear un VPC punto de enlace para Storage Gateway y obtenga el ID del VPC punto de enlace. A continuación, especifique este ID de VPC punto de enlace al crear y activar la puerta de enlace. Para obtener más información, consulte [Connect your Tape Gateway to AWS](#) a.

Note

Debe activar la puerta de enlace en la misma región en la que creó el VPC punto final para Storage Gateway.

Temas

- [Creación de un VPC punto final para Storage Gateway](#)

Creación de un VPC punto final para Storage Gateway

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

Para crear un VPC punto final para Storage Gateway

1. Inicia sesión en la VPC consola de Amazon AWS Management Console y ábrela en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Endpoints (Puntos de enlace) y, a continuación, elija Create Endpoint (Crear punto de enlace).
3. En la página Crear punto de conexión, elija Servicios de AWS en Categoría de servicio.
4. En Service Name (Nombre de servicio), seleccione `com.amazonaws.region.storagegateway`, Por ejemplo, `com.amazonaws.us-east-2.storagegateway`.
5. Para VPC, elija su zona de disponibilidad VPC y anote sus zonas de disponibilidad y subredes.
6. Compruebe que la opción Activar DNS nombre privado no esté seleccionada.
7. En Grupo de seguridad, elija el grupo de seguridad que desee usar para su VPC. Puede aceptar el grupo de seguridad predeterminado. Compruebe que todos los TCP puertos siguientes estén permitidos en su grupo de seguridad:
 - TCP443
 - TCP1026
 - TCP1027
 - TCP1028
 - TCP1031

- TCP2222
8. Seleccione Crear punto de conexión. El estado inicial del punto de enlace es pending (pendiente). Cuando se cree el punto final, anote el ID del VPC punto final que acaba de crear.
 9. Cuando se cree el punto final, elija Puntos finales y, a continuación, elija el nuevo VPC punto final.
 10. En la pestaña Detalles del punto de enlace de almacenamiento seleccionado, en DNSNombres, utilice el primer DNS nombre que no especifique una zona de disponibilidad. Su DNS nombre tiene un aspecto similar al siguiente:
`vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

Ahora que tiene un VPC punto final, puede crear su puerta de enlace. Para obtener más información, consulte [Creación de una puerta de enlace](#).

Administración de la gateway

Administrar su gateway incluye tareas tales como configurar el almacenamiento en caché y el espacio del búfer de carga, usar volúmenes o cintas virtuales y realizar el mantenimiento general. Si no ha creado una gateway, consulte [Empezar con AWS Storage Gateway](#).

Las versiones del software de la puerta de enlace incluirán periódicamente actualizaciones del SO y parches de seguridad que se hayan validado. Estas actualizaciones se aplican como parte del proceso normal de actualización de la puerta de enlace durante los períodos de mantenimiento programados y se publican generalmente cada seis meses. Nota: Los usuarios deben tratar el dispositivo de Storage Gateway como una máquina virtual administrada y no deben intentar acceder a la instancia del dispositivo de Storage Gateway ni modificarla. El intento de instalar o actualizar cualquier paquete de software mediante métodos distintos del mecanismo de actualización habitual (p. ej., mediante herramientas de hipervisor) puede provocar la interrupción del correcto funcionamiento de la puerta de enlace. SSM

Temas

- [Administración de la puerta de enlace de cinta](#)
- [Transferir los datos a una nueva puerta de enlace](#)

Administración de la puerta de enlace de cinta

A continuación, encontrará información acerca de cómo administrar los recursos de la puerta de enlace de cinta en AWS Storage Gateway.

Temas

- [Edición de información básica de la puerta de enlace](#)
- [Adición de cintas virtuales](#)
- [Administración de la creación automática de cintas](#)
- [Archivado de cintas virtuales](#)
- [Traslado de cintas a la clase de almacenamiento S3 Glacier Deep Archive](#)
- [Recuperación de cintas archivadas](#)
- [Visualizar el uso de cintas](#)
- [Eliminar cintas virtuales de la puerta de enlace de cinta](#)

- [Eliminación de grupos de cintas personalizados](#)
- [Desactivación de la puerta de enlace de cinta](#)
- [Información sobre el estado de las cintas](#)

Edición de información básica de la puerta de enlace

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

Para editar la información básica de una puerta de enlace existente

1. Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa>.
2. Elija Puertas de enlace y, a continuación, elija la puerta de enlace para la que desee editar la información básica.
3. En el menú desplegable Acciones, seleccione Editar información de la puerta de enlace.
4. Elija la configuración que desea cambiar y, a continuación, elija Guardar cambios.

Note

Al cambiar el nombre de una puerta de enlace, se desconectarán todas CloudWatch las alarmas configuradas para monitorear la puerta de enlace. Para volver a conectar las alarmas, actualice las GatewayNamede cada alarma de la CloudWatch consola.

Adición de cintas virtuales

Puede agregar cintas a la puerta de enlace de cinta cuando las necesite. Para obtener información sobre cómo crear cintas, consulte [Creación de cintas](#).

Una vez creada la cinta, encontrará información sobre ella en la página Información general sobre la cinta. De forma predeterminada, esta lista muestra hasta 1000 cintas a la vez, pero las búsquedas que realice se aplican a todas las cintas. Puede utilizar la barra de búsqueda para buscar cintas que coincidan con un criterio específico o para reducir la lista a menos de 1000 cintas. Si la lista contiene 1000 cintas o menos, puede ordenarlas en orden ascendente o descendente según una serie de propiedades. Para obtener información acerca de las cuotas de cinta de la puerta de enlace de cinta, consulte [AWS Storage Gateway cuotas](#).

Administración de la creación automática de cintas

La puerta de enlace de cinta crea automáticamente nuevas cintas virtuales para mantener el número mínimo de cintas disponibles que configure. A continuación, hace que estas cintas estén disponibles para importación en la aplicación de copia de seguridad para que los trabajos de copia de seguridad puedan ejecutarse sin interrupción. La creación automática de cintas elimina la necesidad de crear secuencias de comandos personalizadas, además del proceso manual para crear nuevas cintas virtuales.

Para eliminar una política de creación automática de cintas

1. Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa>.
2. En el panel de navegación, elija la pestaña Gateways.
3. Elija la puerta de enlace para la que necesita administrar la creación automática de cintas.
4. En el menú Actions (Acciones), elija Configure tape auto-create (Configurar creación automática de cintas).
5. Para eliminar una política de creación automática de cintas en una puerta de enlace, elija la Eliminar a la derecha de la política que desea eliminar.

Para detener la creación automática de cintas en una puerta de enlace, elimine todas las políticas de creación automática de cintas de esa puerta de enlace.

Elija Guardar cambios para confirmar la eliminación de políticas de creación automática de cintas de la puerta de enlace de cinta seleccionada.


Note

No se puede deshacer la eliminación de una política de creación automática de cintas de una gateway.

Para cambiar las políticas de creación automática de cintas de una puerta de enlace de cinta

1. Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa>.
2. En el panel de navegación, elija la pestaña Gateways.
3. Elija la puerta de enlace para la que necesita administrar la creación automática de cintas.

4. En el menú Acciones, elija Configurar la creación automática de cintas y cambie los ajustes en la página que aparece.
5. En Cantidad mínima de cintas, escriba la cantidad mínima de cintas virtuales que deben estar disponibles en la puerta de enlace de cinta en todo momento. El intervalo válido para este valor es 1 como mínimo y 10 como máximo.
6. En Capacity (Capacidad), escriba el tamaño, en bytes de la capacidad de la cinta virtual. El intervalo válido para este valor es 100 GiB como mínimo y 5 TiB como máximo.
7. En Barcode prefix (Prefijo de código de barras), escriba el prefijo que desee anteponer al código de barras de las cintas virtuales.

 Note

Las cintas virtuales se identifican de forma única mediante un código de barras y puede agregar un prefijo al código de barras. El prefijo es opcional, pero puede utilizarlo para ayudar a identificar las cintas virtuales. El prefijo debe constar de letras mayúsculas (A - Z) y tener entre uno y cuatro caracteres.

8. En Pool (Grupo), elija Glacier Pool (Grupo de Glacier) o Deep Archive Pool (Grupo de Deep Archive). Este grupo representa la clase de almacenamiento en la que se almacenarán las cintas cuando el software de copia de seguridad las expulse.
 - Elija Grupo de Glacier si desea archivar las cintas en la clase de almacenamiento S3 Glacier Flexible Retrieval. Cuando el software de copia de seguridad expulsa la cinta, se archivan automáticamente en S3 Glacier Flexible Retrieval. S3 Glacier Flexible Retrieval se utiliza para archivos más activos en los que se pueden recuperar la cinta en un plazo que suele ser de entre 3 y 5 horas. Para obtener información detallada, consulte [Clases de almacenamiento para el archivado de objetos](#) en la Guía del usuario de Amazon Simple Storage Service.
 - Elija Grupo de Deep Archive si desea archivar las cintas en S3 Glacier Deep Archive. Cuando el software de copia de seguridad expulsa la cinta, esta se archiva automáticamente en S3 Glacier Deep Archive. S3 Glacier Deep Archive se utiliza para la retención de datos y la conservación digital a largo plazo en las que se tiene acceso a los datos una o dos veces al año. Por lo general, puede recuperar una cinta archivada en S3 Glacier Deep Archive en un plazo de 12 horas. Para obtener información detallada, consulte [Clases de almacenamiento para el archivado de objetos](#) en la Guía del usuario de Amazon Simple Storage Service.

Si archiva las cintas en S3 Glacier Flexible Retrieval, puede trasladarlas a S3 Glacier Deep Archive más adelante. Para obtener más información, consulte [Traslado de cintas a la clase de almacenamiento S3 Glacier Deep Archive](#).

9. Encontrará información sobre las cintas en la página Información general sobre la cinta. De forma predeterminada, esta lista muestra hasta 1000 cintas a la vez, pero las búsquedas que realice se aplican a todas las cintas. Puede utilizar la barra de búsqueda para buscar cintas que coincidan con un criterio específico o para reducir la lista a menos de 1000 cintas. Si la lista contiene 1000 cintas o menos, puede ordenarlas en orden ascendente o descendente según una serie de propiedades.

El estado de las cintas virtuales disponibles se establece inicialmente en el CREATING momento en que se crean las cintas. Una vez creadas las cintas, su estado cambia a AVAILABLE. Para obtener más información, consulte [Administración de la puerta de enlace de cinta](#).

Para obtener más información sobre cómo habilitar la creación automática de cintas, consulte [Creación automática de cintas](#).

Archivado de cintas virtuales

Puede archivar las cintas en S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. Al crear una cinta, puede elegir el grupo de archivado que desea utilizar para archivar la cinta.

Elija Grupo de Glacier si desea archivar la cinta en S3 Glacier Flexible Retrieval. Cuando el software de copia de seguridad expulsa la cinta, se archiva automáticamente en S3 Glacier Flexible Retrieval. S3 Glacier Flexible Retrieval se utiliza para entornos de archivado más activos en los que los datos se recuperan periódicamente y se necesitan en cuestión de minutos. Para obtener información detallada, consulte [Clases de almacenamiento para el archivado de objetos](#).

Elija Grupo de Deep Archive si desea archivar la cinta en S3 Glacier Deep Archive. Cuando el software de copia de seguridad expulsa la cinta, esta se archiva automáticamente en S3 Glacier Deep Archive. Puede utilizar S3 Glacier Deep Archive para la retención de datos y la conservación digital a largo plazo a un precio muy económico. Los datos de S3 Glacier Deep Archive se recuperan con poca frecuencia o se recuperan en raras ocasiones. Para obtener información detallada, consulte [Clases de almacenamiento para el archivado de objetos](#).

Note

Todas las cintas creadas antes del 27 de marzo de 2019 se archivan directamente en S3 Glacier Deep Archive cuando el software de copia de seguridad las expulsa.

Cuando el software de copia de seguridad expulsa una cinta, se archiva automáticamente en el grupo elegido al crear la cinta. El proceso para expulsar una cinta depende del software de copia de seguridad. Algunos software de copia de seguridad requieren que se exporten las cintas después de expulsarlas para que pueda comenzar el archivado. Para obtener más información sobre el software de copia de seguridad compatible, consulte [Uso del software de copia de seguridad para comprobar la configuración de la puerta de enlace](#).

Traslado de cintas a la clase de almacenamiento S3 Glacier Deep Archive

Puede trasladar cintas de S3 Glacier Flexible Retrieval a S3 Glacier Deep Archive Storage Class para la retención de datos a largo plazo y la conservación digital a un precio muy económico. S3 Glacier Deep Archive se utiliza para la retención de datos y la conservación digital a largo plazo en las que se tiene acceso a los datos una o dos veces al año. Para obtener información detallada, consulte [Clases de almacenamiento para el archivado de objetos](#).

Para trasladar una cinta desde S3 Glacier Flexible Retrieval a S3 Glacier Deep Archive

1. En el panel de navegación, elija Biblioteca de cintas > Cintas para ver las cintas. De forma predeterminada, esta lista muestra hasta 1000 cintas a la vez, pero las búsquedas que realice se aplican a todas las cintas. Puede utilizar la barra de búsqueda para buscar cintas que coincidan con un criterio específico o para reducir la lista a menos de 1000 cintas. Si la lista contiene 1000 cintas o menos, puede ordenarlas en orden ascendente o descendente según una serie de propiedades.
2. Seleccione las casillas de verificación de las cintas que desee trasladar a S3 Glacier Deep Archive. Puede ver el grupo al que está asociado cada cinta en la columna Grupo.
3. Elija Asignar a grupo.
4. En el cuadro de diálogo Asignar cinta al grupo, compruebe el ID de la cinta que va a trasladar y elija Asignar.

Note

Si la aplicación de copia de seguridad ha expulsado una cinta y la ha archivado en S3 Glacier Deep Archive, no es posible volver a trasladarla a S3 Glacier Flexible Retrieval. Se cobra un cargo por trasladar sus cintas virtuales de S3 Glacier Flexible Retrieval a S3 Glacier Deep Archive. Además, si traslada cintas de S3 Glacier Flexible Retrieval a S3 Glacier Deep Archive antes de 90 días, se cobra una tarifa por eliminación anticipada de S3 Glacier Flexible Retrieval.

- Una vez trasladada la cinta, podrá ver el estado actualizado en la columna Grupo de la página Información general sobre la cinta.

Recuperación de cintas archivadas

Para obtener acceso a los datos almacenados en una cinta virtual archivada, antes debe recuperarla de la puerta de enlace de cinta. Su puerta de enlace de cintas proporciona una biblioteca de cintas virtuales (VTL) para cada puerta de enlace.

Si tiene más de una puerta de enlace de cinta en una Región de AWS, solo puede recuperar una cinta en una puerta de enlace.

La cinta recuperada está protegida contra escritura; los datos que contiene únicamente se pueden leer.

Important

Si archiva una cinta en S3 Glacier Flexible Retrieval, normalmente puede recuperarla en un plazo de entre 3 y 5 horas. Si archiva una cinta en S3 Glacier Deep Archive, normalmente puede recuperarla en un plazo de 12 horas.

Note

La recuperación de cintas del archivo devenga un cargo. Para obtener información detallada sobre precios, consulte [Precios de Storage Gateway](#).

Para recuperar en la gateway una cinta archivada

1. Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa>.
2. En el panel de navegación, elija Biblioteca de cintas > Cintas para ver las cintas. De forma predeterminada, esta lista muestra hasta 1000 cintas a la vez, pero las búsquedas que realice se aplican a todas las cintas. Puede utilizar la barra de búsqueda para buscar cintas que coincidan con un criterio específico o para reducir la lista a menos de 1000 cintas. Si la lista contiene 1000 cintas o menos, puede ordenarlas en orden ascendente o descendente según una serie de propiedades.
3. Elija la cinta virtual que desea recuperar en la pestaña Estantería de cintas virtuales y seleccione Recuperar cinta.

Note

El estado de la cinta virtual que desea recuperar debe ser el siguiente ARCHIVED.

4. En el cuadro de diálogo Retrieve tape (Recuperar cinta), fíjese en Barcode (Código de barras) y compruebe que el código de barras identifique la cinta virtual que desea recuperar.
5. En Gateway, elija la gateway en la que desea recuperar la cinta archivada. A continuación, elija Retrieve tape (Recuperar cinta).

El estado de la cinta cambia de ARCHIVED a RETRIEVING. En este punto, los datos se están trasladando de la estantería de cintas virtuales (basada en S3 Glacier Flexible Retrieval o en S3 Glacier Deep Archive) a la biblioteca de cintas virtuales (basada en Amazon S3). Una vez movidos todos los datos, el estado de la cinta virtual en el archivo cambia a RETRIEVED.

Note


Las cintas virtuales recuperadas son de solo lectura.

Visualizar el uso de cintas

Al escribir datos en una cinta, puede ver la cantidad de datos almacenados en dicha cinta desde la consola de Storage Gateway. La pestaña Details (Detalles) de cada cinta muestra información de su uso.

Para ver la cantidad de datos almacenados en una cinta


1. Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa>.
2. En el panel de navegación, elija Biblioteca de cintas > Cintas para ver las cintas. De forma predeterminada, esta lista muestra hasta 1000 cintas a la vez, pero las búsquedas que realice se aplican a todas las cintas. Puede utilizar la barra de búsqueda para buscar cintas que coincidan con un criterio específico o para reducir la lista a menos de 1000 cintas. Si la lista contiene 1000 cintas o menos, puede ordenarlas en orden ascendente o descendente según una serie de propiedades.
3. Elija la cinta que le interese.
4. La página que aparece proporciona varios detalles e información sobre la cinta, que incluyen lo siguiente:
 - Size (Tamaño): capacidad total de la cinta seleccionada.
 - Used (En uso): tamaño de los datos grabados en la cinta por la aplicación de copia de seguridad.

 Note

Este valor no está disponible para las cintas creadas antes del 13 de mayo de 2015.

Eliminar cintas virtuales de la puerta de enlace de cintas

Puede eliminar cintas virtuales de la puerta de enlace de cinta desde la consola de Storage Gateway.

 Note

Si la cinta que desea eliminar de la puerta de enlace de cintas tiene un estado de RETRIEVED, primero debe expulsar la cinta con la aplicación de respaldo antes de eliminarla. Para obtener instrucciones sobre cómo expulsar una cinta con el NetBackup software de Symantec, consulte [Archivar](#) la cinta. Una vez expulsada la cinta, el estado de la cinta vuelve a ser ARCHIVED. En este punto, puede eliminar la cinta.

Realice copias de los datos antes de eliminar cintas. Una vez eliminada una cinta, no podrá recuperarla.

Para eliminar una cinta virtual

Warning

Este procedimiento elimina de forma permanente la cinta virtual seleccionada.

1. Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa>.
2. En el panel de navegación, elija Biblioteca de cintas > Cintas para ver las cintas. De forma predeterminada, esta lista muestra hasta 1000 cintas a la vez, pero las búsquedas que realice se aplican a todas las cintas. Puede utilizar la barra de búsqueda para buscar cintas que coincidan con un criterio específico o para reducir la lista a menos de 1000 cintas. Si la lista contiene 1000 cintas o menos, puede ordenarlas en orden ascendente o descendente según una serie de propiedades.
3. Seleccione una o varias cintas para eliminarlas.
4. En Acciones, elija Eliminar cinta. Aparece el cuadro de diálogo de confirmación.
5. Compruebe que desea eliminar las cintas especificadas, escriba la palabra eliminar en el cuadro de confirmación y seleccione Eliminar.

Una vez que la cinta se ha eliminado, desaparece de la puerta de enlace de cinta.

Eliminación de grupos de cintas personalizados

Solo puede eliminar un grupo de cintas personalizado si no hay cintas archivadas en el grupo y no hay políticas de creación automática de cintas asociadas al grupo.


Para eliminar el grupo de cintas personalizado

1. Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa>.
2. En el panel de navegación, elija Grupos para ver los grupos disponibles.
3. Seleccione uno o varios grupos de cintas para eliminarlos.

Si el Recuento de cintas de los grupos de cintas que desea eliminar es 0 y si no hay políticas de creación automática de cintas que hagan referencia al grupo de cintas personalizado, puede eliminar los grupos.

4. Elija Eliminar. Aparece el cuadro de diálogo de confirmación.

5. Compruebe que desea eliminar los grupos de cintas especificados y, a continuación, escriba la palabra eliminar en el cuadro de confirmación y elija Eliminar.

 Warning

Este procedimiento elimina de forma permanente los grupos de cintas seleccionados y no se puede deshacer.

Una vez eliminados los grupos de cintas, desaparecen de la biblioteca de cintas.

Desactivación de la puerta de enlace de cinta

Debe desactivar una puerta de enlace de cinta si ha producido un error y desea recuperar las cintas en otra puerta de enlace.

Para recuperar las cintas, primero debe desactivar la puerta de enlace en la que se ha producido el error. La desactivación de una puerta de enlace de cinta bloquea las cintas virtuales de esa puerta de enlace. Es decir, los datos que escriba en estas cintas después de la desactivación de la puerta de enlace no se envían a AWS. Solo puede desactivar una puerta de enlace en la consola de Storage Gateway si la puerta de enlace ya no está conectada a AWS. Si la puerta de enlace está conectada a AWS, no se puede desactivar la puerta de enlace de cinta.

Puede desactivar una puerta de enlace de cinta como parte de la recuperación de datos. Para obtener más información sobre la recuperación de cintas, consulte [Necesita recuperar una cinta virtual desde una puerta de enlace de cinta que no funciona correctamente](#).

Para desactivar la puerta de enlace

1. Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa>.
2. En el panel de navegación, elija Puertas de enlace y, a continuación, elija la puerta de enlace donde se produjo el error.
3. Elija la pestaña Detalles de la puerta de enlace para mostrar el mensaje de desactivación de la puerta de enlace.
4. Elija Create recovery tapes (Crear cintas de recuperación).
5. Elija Disable gateway (Deshabilitar gateway).

Información sobre el estado de las cintas

Cada cinta 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 la cinta funciona normalmente y que no se requiere ninguna intervención por parte del usuario. En ocasiones, el estado indica algún problema con la cinta; en este caso, podría ser preciso que intervenga. A continuación encontrará información que le ayudará a decidir cuándo debe intervenir.


Temas

- [Descripción de la información sobre el estado de la cinta en un VTL](#)
- [Determinación del estado de las cintas en el archivo](#)

Descripción de la información sobre el estado de la cinta en un VTL

El estado de una cinta debe ser AVAILABLE el mismo que para poder leer o escribir en ella. En la siguiente tabla se muestran y describen los posibles valores de estado.

Estado	Descripción	Cinta en la que se han almacenado los datos
CREATING	La cinta virtual se está creando. La cinta no se puede cargar en una unidad de cinta, ya que se está creando.	—
AVAILABLE	La cinta virtual se ha creado y está lista para cargarla en una unidad de cinta.	Amazon S3
TRANSITING	La cinta virtual se ha expulsado y se está cargando para archivarla. En este punto, su Tape Gateway está cargando datos a AWS. Si la cantidad de datos cargados es reducida, es posible que este estado no aparezca. Cuando se complete la carga, el estado cambiará a ARCHIVING.	Amazon S3
ARCHIVING	La cinta virtual se traslada a la puerta de enlace de cinta, que está respaldada por S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. Este proceso	Los datos se transfieren de Amazon S3 a S3 Glacier Flexible Retrieval

Estado	Descripción	Cinta en la que se han almacenado los datos
	se produce una vez finalizada la carga de los datos a AWS .	o S3 Glacier Deep Archive.
DELETING	La cinta virtual se está eliminando.	Los datos se eliminarán de Amazon S3
DELETED	La cinta virtual se ha eliminado correctamente.	—
RETRIEVING	<p>La cinta virtual se recupera del archivo a la puerta de enlace de cinta.</p> <div data-bbox="354 758 386 793" style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; display: inline-block;">  </div> Note La cinta virtual puede recuperarse únicamente en una puerta de enlace de cinta.	Los datos se transfieren de S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive a Amazon S3
RETRIEVED	La cinta virtual se ha recuperado del archivo. La cinta recuperada está protegida contra escritura.	Amazon S3
RECOVERABLE	<p>La cinta virtual se ha recuperado y es de solo lectura.</p> <p>Cuando la puerta de enlace de cinta no es accesible por algún motivo, puede recuperar las cintas virtuales asociadas con esa puerta de enlace de cinta en otra puerta de enlace de cinta. Para recuperar las cintas virtuales, primero debe desactivar la puerta de enlace de cinta inaccesible.</p>	Amazon S3
IRRECOVERABLE	La cinta virtual no se puede leer ni escribir. Este estado indica un error en la puerta de enlace de cinta.	Amazon S3

Determinación del estado de las cintas en el archivo


Puede seguir el siguiente procedimiento para determinar el estado de una cinta virtual en un archivo.

Para determinar el estado de una cinta virtual

1. Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa>.
2. En el panel de navegación, elija Tapes (Cintas).
3. En la columna Status (Estado) de la cuadrícula de la biblioteca de cintas, consulte el estado de la cinta.

El estado de la cinta también aparece en la pestaña Details (Detalles) de cada cinta virtual.

A continuación, encontrará una descripción de los posibles valores de estados.

Estado	Descripción
ARCHIVED	La cinta virtual se ha expulsado y se está cargando en el archivo.
RETRIEVING	<p>La cinta virtual se está recuperando del archivo.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>La cinta virtual puede recuperarse únicamente en una puerta de enlace de cinta.</p> </div>
RETRIEVED	La cinta virtual se ha recuperado del archivo. La cinta recuperada es de solo lectura.

Para obtener información adicional sobre cómo trabajar con cintas y VTL dispositivos, consulte [Trabajo con cintas](#).


Transferir los datos a una nueva puerta de enlace

Puede mover datos entre puertas de enlace a medida que aumenten sus necesidades de datos y rendimiento, o si recibe una AWS notificación para migrar su puerta de enlace. A continuación se muestran algunos de los motivos para hacerlo:

- Mueva sus datos a mejores plataformas de alojamiento o a EC2 instancias de Amazon más nuevas.

- Actualizar el hardware subyacente para el servidor.

Los pasos que debe seguir para mover los datos a una nueva puerta de enlace dependen del tipo de puerta de enlace que tenga.

 Note

Los datos solo se pueden mover entre los mismos tipos de puerta de enlace.

Trasladar cintas virtuales a una nueva puerta de enlace de cinta

Para trasladar la cinta virtual a una nueva puerta de enlace de cinta

1. Use su aplicación de copia de seguridad para hacer copias de seguridad de todos sus datos en una cinta virtual. Espere a que la copia de seguridad finalice correctamente.
2. Utilice la aplicación de copia de seguridad para expulsar la cinta. La cinta se almacenará en una de las clases de almacenamiento de Amazon S3. Las cintas expulsadas se archivan en S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive y son de solo lectura.

Antes de continuar, confirme que las cintas expulsadas se hayan archivado:

- a. Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa>.
- b. En el panel de navegación, elija Biblioteca de cintas > Cintas para ver las cintas. De forma predeterminada, esta lista muestra hasta 1000 cintas a la vez, pero las búsquedas que realice se aplican a todas las cintas. Puede utilizar la barra de búsqueda para buscar cintas que coincidan con un criterio específico o para reducir la lista a menos de 1000 cintas. Si la lista contiene 1000 cintas o menos, puede ordenarlas en orden ascendente o descendente según una serie de propiedades.
- c. En la columna Estado de la lista, consulte el estado de la cinta.

El estado de la cinta también aparece en la pestaña Details (Detalles) de cada cinta virtual.

Para obtener más información sobre la determinación del estado de la cinta en un archivo, consulte [Determinación del estado de las cintas en el archivo](#).

3. Con la aplicación de copia de seguridad, compruebe que no haya ningún trabajo de copia de seguridad activo en la puerta de enlace de cinta existente antes de detenerlo. Si hay algún trabajo de copia de seguridad activo, espere a que termine y extraiga las cintas (consulte el paso anterior) antes de detener la puerta de enlace.
4. Siga estos pasos para detener la puerta de enlace de cinta existente:
 - a. En el panel de navegación, elija Puertas de enlace y, a continuación, elija la puerta de enlace de cinta anterior que desea que se detenga. El estado de la gateway es Running (En ejecución).
 - b. En Acciones, elija Detener puerta de enlace. Verifique el ID de la puerta de enlace del cuadro de diálogo y, a continuación, elija Detener puerta de enlace.


Aunque la puerta de enlace de cinta se esté deteniendo, puede que aparezca un mensaje que indica el estado de la puerta de enlace. Cuando la puerta de enlace se apague, aparecerán un mensaje y el botón Iniciar puerta de enlace en la pestaña Detalles.

Para obtener más información acerca de detener una puerta de enlace, consulte [Inicio y detención de una puerta de enlace de cinta](#).

5. Creación de una nueva puerta de enlace de cinta. Para obtener instrucciones detalladas, consulte [Creación de una puerta de enlace](#).
6. Siga los siguientes pasos para crear nuevas cintas:
 - a. En el panel de navegación, elija la pestaña Gateways.
 - b. Elija Crear cinta para abrir el cuadro de diálogo Crear cinta.
 - c. En Gateway, elija una gateway. Se crea la cinta para esta gateway.
 - d. En Number of tapes (Número de cintas), elija el número de cintas que desee crear. Para obtener más información sobre los límites de las cintas, consulte [AWS Storage Gateway cuotas](#).

También puede configurar la creación automática de cintas en este punto. Para obtener más información, consulte [Creación automática de cintas](#).

- e. En Capacity (Capacidad), escriba el tamaño de la cinta virtual que desea crear. Las cintas deben tener más de 100 GiB. Para obtener información sobre los límites de capacidad, consulte [AWS Storage Gateway cuotas](#).
- f. En Barcode prefix (Prefijo de código de barras), escriba el prefijo que desee anteponer al código de barras de las cintas virtuales.

 Note


Las cintas virtuales se identifican de forma exclusiva mediante un código de barras. Puede agregar un prefijo al el código de barras. El prefijo es opcional, pero puede utilizarlo para ayudar a identificar las cintas virtuales. El prefijo debe constar de letras mayúsculas (A - Z) y tener entre uno y cuatro caracteres.

- g. En Pool (Grupo), elija Glacier Pool (Grupo de Glacier) o Deep Archive Pool (Grupo de Deep Archive). Este grupo representa la clase de almacenamiento en la que se almacenará la cinta cuando el software de copia de seguridad la expulse.

Elija Grupo de Glacier si desea archivar la cinta en S3 Glacier Flexible Retrieval. Cuando el software de copia de seguridad expulsa la cinta, se archiva automáticamente en S3 Glacier Flexible Retrieval. S3 Glacier Flexible Retrieval se utiliza para archivos más activos en los que se pueden recuperar la cinta en un plazo que suele ser de entre 3 y 5 horas. Para más información sobre las clases de almacenamiento, consulte [Clases de almacenamiento para el archivado de objetos](#) en la Guía del usuario de Amazon Simple Storage Service.


Elija Grupo de Deep Archive si desea archivar la cinta en S3 Glacier Deep Archive. Cuando el software de copia de seguridad expulsa la cinta, esta se archiva automáticamente en S3 Glacier Deep Archive. S3 Glacier Deep Archive se utiliza para la retención de datos y la conservación digital a largo plazo en las que se tiene acceso a los datos una o dos veces al año. Por lo general, puede recuperar una cinta archivada en S3 Glacier Deep Archive en un plazo de 12 horas. Para más información sobre las clases de almacenamiento, consulte [Clases de almacenamiento para el archivado de objetos](#) en la Guía del usuario de Amazon Simple Storage Service.

Si archiva una cinta en S3 Glacier Flexible Retrieval, puede trasladarla a S3 Glacier Deep Archive más adelante. Para obtener más información, consulte [Traslado de cintas a la clase de almacenamiento S3 Glacier Deep Archive](#).

 Note


Las cintas creadas antes del 27 de marzo de 2019 se archivan directamente en S3 Glacier Deep Archive cuando el software de copia de seguridad las expulsa.

- h. (Opcional) En Tags (Etiquetas), introduzca una clave y un valor para añadir una etiqueta a la cinta. Una etiqueta es un par clave-valor que distingue entre mayúsculas y minúsculas, y que le ayuda a administrar, filtrar y buscar cintas.
 - i. Elija Create tapes (Crear cintas).
- 7. Use su aplicación de copia de seguridad para iniciar un trabajo de copia de seguridad y haga una copia de seguridad de sus datos en la nueva cinta.
- 8. (Opcional) Si la cinta está archivada y necesita restaurar los datos de ella, recupérela en la nueva puerta de enlace de cinta. La cinta estará en modo de solo lectura. Para obtener más información acerca de la recuperación de cintas archivadas, consulte [Recuperación de cintas archivadas](#).

 Note

Se pueden aplicar cargos de datos salientes.


- a. En el panel de navegación, elija Biblioteca de cintas > Cintas para ver las cintas. De forma predeterminada, esta lista muestra hasta 1000 cintas a la vez, pero las búsquedas que realice se aplican a todas las cintas. Puede utilizar la barra de búsqueda para buscar cintas que coincidan con un criterio específico o para reducir la lista a menos de 1000 cintas. Si la lista contiene 1000 cintas o menos, puede ordenarlas en orden ascendente o descendente según una serie de propiedades.
- b. Elija la cinta virtual que desee recuperar. En Acciones, seleccione Recuperar cinta.

 Note

El estado de la cinta virtual que desea recuperar debe ser ARCHIVED.


- c. En el cuadro de diálogo Retrieve tape (Recuperar cinta), fíjese en Barcode (Código de barras) y compruebe que el código de barras identifique la cinta virtual que desea recuperar.
 - d. En Puerta de enlace, elija la nueva puerta de enlace de cinta en la que desea recuperar la cinta archivada. A continuación, elija Recuperar cinta.

Cuando haya confirmado que la nueva puerta de enlace de cinta funciona correctamente, puede eliminar la antigua puerta de enlace de cinta.

 Important

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

9. Siga estos pasos para eliminar la antigua puerta de enlace de cinta:

 Warning

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

- a. En el panel de navegación, elija Puertas de enlace y, a continuación, seleccione la puerta de enlace que desea eliminar.
- b. En Actions (Acciones), elija Delete gateway (Eliminar la gateway).

En el cuadro de diálogo de confirmación que aparece, asegúrese de que el ID de la puerta de enlace que aparece especifica la antigua puerta de enlace de cinta que desea eliminar, introduzca **delete** el campo de confirmación y, a continuación, elija Eliminar.

- c. Elimine la VM. Para obtener más información sobre la eliminación de una VM, consulte la documentación del hipervisor.

Supervisión de Storage Gateway

En esta sección se describe cómo monitorizar una puerta de enlace, incluida la supervisión de los recursos asociados a la puerta de enlace, mediante Amazon CloudWatch. Puede monitorizar el búfer de carga y el almacenamiento en caché de la gateway. Utilice la consola de Storage Gateway para ver las métricas y alarmas de la puerta de enlace. Por ejemplo, puede ver el número de bytes utilizados en las operaciones de lectura y escritura, el tiempo empleado en las operaciones de lectura y escritura y el tiempo necesario para recuperar datos desde Amazon Web Services Cloud. Con las métricas, puede realizar un seguimiento de la salud de la gateway y configurar alarmas que le avisen cuando una o varias métricas superen un umbral definido.

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

Temas


- [Información acerca de las métricas de gateway](#)
- [Dimensiones de las métricas de Storage Gateway](#)
- [Supervisión del búfer de carga](#)
- [Supervisión del almacenamiento en caché](#)
- [Entender CloudWatch las alarmas](#)
- [Crear CloudWatch las alarmas recomendadas para su puerta de enlace](#)
- [Crear una CloudWatch alarma personalizada para su puerta de enlace](#)
- [Supervisión de la puerta de enlace de cinta](#)

Información acerca de las métricas de gateway

Para las explicaciones de este tema, definiremos las métricas de puerta de enlace como métricas en el ámbito de la puerta de enlace, es decir, que midan algo relativo a la puerta de enlace. Dado que una gateway contiene uno o varios volúmenes, una métrica específica de gateway es representativa de todos los volúmenes de la gateway. Por ejemplo, la métrica `CloudBytesUploaded` es el número

total de bytes que la gateway ha enviado a la nube durante el periodo de notificación. Esta métrica incluye la actividad de todos los volúmenes de la gateway.

Cuando trabaje con datos de métricas de gateway, debe especificar la identificación única de la gateway cuyas métricas le interese ver. Para ello, debe especificar los valores de GatewayId y GatewayName. Cuando desee trabajar con las métricas de una gateway, debe especificar la dimensión de la gateway en el espacio de nombres de métricas, que distingue una métrica específica de la gateway de una métrica específica del volumen. Para obtener más información, consulte [Uso de Amazon CloudWatch Metrics](#).

 Note

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

Métrica	Descripción
AvailabilityNotifications	<p>Número de notificaciones de estado relacionadas con la disponibilidad que ha generado la gateway.</p> <p>Utilice esta métrica con la estadística Sum para comprobar si se está produciendo algún evento relacionado con la disponibilidad en la gateway. Para obtener más información sobre los eventos, consulte el grupo de CloudWatch registros configurado.</p> <p>Unidad: número</p>
CacheHitPercent	Porcentaje de lecturas de aplicación servidas desde la

Métrica	Descripción	
	caché. La muestra se obtiene al final del período de notificación. Unidad: porcentaje	
CacheUsed	El número total de bytes que se utilizan en el almacenamiento en caché de la gateway. La muestra se obtiene al final del período de notificación. Unidades: bytes	
IoWaitPercent	Porcentaje de tiempo que la gateway está esperando una respuesta del disco local. Unidad: porcentaje	
MemTotalBytes	Cantidad RAM provisionada a la máquina virtual de puerta de enlace, en bytes. Unidades: bytes	
MemUsedBytes	Cantidad de material RAM actualmente en uso por la máquina virtual de puerta de enlace, en bytes. Unidades: bytes	

Métrica	Descripción	
QueuedWrites	<p>El número de bytes en espera de escribirse AWS, muestreado al final del período del informe para todos los volúmenes de la puerta de enlace. Estos bytes se conservan en el almacenamiento de trabajo de la gateway.</p> <p>Unidades: bytes</p>	
TotalCacheSize	<p>El tamaño total de la caché en bytes. La muestra se obtiene al final del período de notificación.</p> <p>Unidades: bytes</p>	
UploadBufferPercentUsed	<p>Porcentaje de uso del búfer de carga de la gateway. La muestra se obtiene al final del período de notificación.</p> <p>Unidad: porcentaje</p>	
UploadBufferUsed	<p>El número total de bytes que se utilizan en el búfer de carga de la gateway. La muestra se obtiene al final del período de notificación.</p> <p>Unidades: bytes</p>	

Métrica	Descripción
UserCpuPercent	<p>Porcentaje de CPU tiempo dedicado al procesamiento de la puerta de enlace, promediado en todos los núcleos.</p> <p>Unidad: porcentaje</p>

Dimensiones de las métricas de Storage Gateway

El espacio de CloudWatch nombres del servicio Storage Gateway es. `AWS/StorageGateway` Los datos se encuentran disponibles automáticamente en periodos de 5 minutos sin costo alguno.

Dimensión	Descripción
GatewayId , GatewayName	<p>Estas dimensiones filtran los datos que solicita a las métricas específicas de la gateway. Puede identificar una gateway para trabajar mediante el valor de GatewayId o GatewayName . Si el nombre de la gateway era diferente al intervalo de tiempo para el que desea consultar las métricas, utilice el GatewayId .</p> <p>Los datos de velocidad y latencia de una gateway se basan en todos los volúmenes de esa gateway. Para obtener información sobre cómo trabajar con las métricas de las puertas de enlace, consulte Cómo medir el rendimiento entre su puerta de enlace y AWS</p>

Supervisión del búfer de carga

A continuación puede encontrar información sobre cómo monitorizar el búfer de carga de una gateway y cómo crear una alarma para recibir una notificación cuando el búfer supere un umbral especificado. Al adoptar este enfoque, puede añadir almacenamiento de búfer a una gateway antes de que se llene completamente y la aplicación deje de hacer copias de seguridad en AWS.

La supervisión del búfer de carga se hace de la misma forma en las arquitecturas de puerta de enlace de cinta y volúmenes en caché. Para obtener más información, consulte [Funcionamiento de puerta de enlace de cinta \(arquitectura\)](#).

Note

Las métricas `WorkingStoragePercentUsed`, `WorkingStorageUsed` y `WorkingStorageFree` representan el búfer de carga para los volúmenes almacenados antes del lanzamiento de la característica de volumen en caché en Storage Gateway. Ahora utilice las métrica de búfer de carga equivalentes `UploadBufferPercentUsed`, `UploadBufferUsed` y `UploadBufferFree`. Estas métricas se aplican a ambas arquitecturas de gateway.

Elemento de Interés	Cómo medirlo
Uso del búfer de carga	Utilice las métricas <code>UploadBufferPercentUsed</code> , <code>UploadBufferUsed</code> y <code>UploadBufferFree</code> con la estadística <code>Average</code> . Por ejemplo, utilice <code>UploadBufferUsed</code> con la estadística <code>Average</code> para analizar el uso del almacenamiento durante un periodo de tiempo.

Para medir el porcentaje del búfer de carga que se utiliza

1. Abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.
2. Elija la dimensión `StorageGateway: Gateway Metrics` y busque la puerta de enlace con la que desee trabajar.
3. Elija la métrica `UploadBufferPercentUsed`.
4. Para `Time Range` (Intervalo de tiempo), elija un valor.
5. Elija la estadística `Average`.
6. Para `Period` (Periodo), elija un valor de 5 minutos para que coincida con el tiempo de informe predeterminado.

El conjunto resultante de puntos de datos ordenado temporalmente contiene el porcentaje utilizado del búfer de carga.

Mediante el siguiente procedimiento, puede crear una alarma mediante la CloudWatch consola.

Para obtener más información sobre las alarmas y los umbrales, consulte [Creación de CloudWatch alarmas](#) en la Guía del CloudWatch usuario de Amazon.

Para establecer una alarma de umbral superior para el búfer de carga de una gateway

1. Abra la CloudWatch consola en. <https://console.aws.amazon.com/cloudwatch/>
2. Seleccione Create Alarm (Crear alarma) para iniciar el asistente Crear alarma.
3. Especifique una métrica para la alarma:
 - a. En la página de selección de métricas del asistente de creación de alarmas, elija la GatewayName dimensión AWS/StorageGateway: GatewayId y, a continuación, busque la puerta de enlace con la que desee trabajar.
 - b. Elija la métrica UploadBufferPercentUsed. Utilice la estadística Average y un periodo de 5 minutos.
 - c. Elija Continuar.
4. Defina el nombre de alarma, la descripción y el umbral:
 - a. En la página Define Alarm (Definir alarma) del asistente Crear alarma, identifique la alarma mediante la asignación de un nombre y una descripción en los cuadros Name (Nombre) y Description (Descripción).
 - b. Defina el umbral de la alarma.
 - c. Elija Continuar.
5. Configure una acción de correo electrónico para la alarma:
 - a. En la página Configure Actions (Configurar acciones) del asistente Crear alarma, seleccione Alarm (Alarma) en Alarm State (Estado de alarma).
 - b. Elija Choose or create email topic (Elegir o crear un tema de correo electrónico) para Topic (Tema).

Crear un tema de correo electrónico significa configurar un SNS tema de Amazon. Para obtener más información sobre AmazonSNS, consulta [Configurar Amazon SNS](#) en la Guía del CloudWatch usuario de Amazon.
 - c. En Topic (Tema), introduzca un nombre descriptivo para el tema.
 - d. Elija Añadir acción.

- e. Elija Continuar.
6. Revise la configuración de la alarma y, a continuación, cree la alarma:
 - a. En la página Review (Revisar) del asistente Crear alarma, revise la definición, la métrica y las acciones asociadas de la alarma (por ejemplo, enviar una notificación de correo electrónico).
 - b. Tras revisar el resumen de la alarma, elija Save Alarm (Guardar alarma).
 7. Confirme la suscripción al tema de alarma:
 - a. Abra el SNS correo electrónico de Amazon que se envió a la dirección de correo electrónico que especificaste al crear el tema.

En la siguiente imagen se muestra una notificación de correo electrónico habitual.



- b. Confirme la suscripción haciendo clic en el enlace del correo electrónico.

Aparece una confirmación de suscripción.

Supervisión del almacenamiento en caché

A continuación, puede encontrar información sobre cómo monitorizar el almacenamiento en caché de una gateway y cómo crear una alarma para recibir una notificación cuando los parámetros de la memoria caché superen los umbrales especificados. Con esta alarma, puede saber cuándo añadir almacenamiento en caché a una gateway.

Monitoree el almacenamiento en caché solamente en la arquitectura de volúmenes almacenados en caché. Para obtener más información, consulte [Funcionamiento de puerta de enlace de cinta \(arquitectura\)](#).

Elemento de Interés	Cómo medirlo
Uso total de caché	<p>Utilice las métricas <code>CachePercentUsed</code> y <code>TotalCacheSize</code> con la estadística <code>Average</code>. Por ejemplo, utilice <code>CachePercentUsed</code> con la estadística <code>Average</code> para analizar el uso de la memoria caché durante un periodo de tiempo.</p> <p>La métrica <code>TotalCacheSize</code> solo cambia cuando se agrega caché a la gateway.</p>
Porcentaje de solicitudes de lectura que se sirven desde la caché	<p>Utilice la métrica <code>CacheHitPercent</code> con la estadística <code>Average</code>.</p> <p>Normalmente, es deseable que el valor <code>CacheHitPercent</code> se mantenga alto.</p>
Porcentaje de la caché que está sucia, es decir, contiene contenido que no se ha cargado en AWS	<p>Utilice la métrica <code>CachePercentDirty</code> con la estadística <code>Average</code>.</p> <p>Normalmente, es deseable que el valor <code>CachePercentDirty</code> se mantenga bajo.</p>

Para medir el porcentaje de caché sucia de una gateway y todos sus volúmenes

1. Abra la consola en CloudWatch . <https://console.aws.amazon.com/cloudwatch/>
2. Elija la dimensión `StorageGateway: Gateway Metrics` y busque la puerta de enlace con la que desee trabajar.
3. Elija la métrica `CachePercentDirty`.
4. Para `Time Range` (Intervalo de tiempo), elija un valor.
5. Elija la estadística `Average`.
6. Para `Period` (Periodo), elija un valor de 5 minutos para que coincida con el tiempo de informe predeterminado.

El conjunto resultante de puntos de datos ordenados temporalmente contiene el porcentaje de caché sucia durante 5 minutos.

Para medir el porcentaje de caché sucia de un volumen

1. Abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.
2. Elija la dimensión StorageGateway: Volume Metrics y busque el volumen con el que desee trabajar.
3. Elija la métrica CachePercentDirty.
4. Para Time Range (Intervalo de tiempo), elija un valor.
5. Elija la estadística Average.
6. Para Period (Periodo), elija un valor de 5 minutos para que coincida con el tiempo de informe predeterminado.

El conjunto resultante de puntos de datos ordenados temporalmente contiene el porcentaje de caché sucia durante 5 minutos.

Entender CloudWatch las alarmas

CloudWatch las alarmas supervisan la información sobre su puerta de enlace en función de métricas y expresiones. Puede añadir CloudWatch alarmas a la puerta de enlace y ver sus estados en la consola de Storage Gateway. Para obtener más información sobre las métricas que se utilizan para supervisar la puerta de enlace de cinta, consulte [Información acerca de las métricas de puerta de enlace](#) y [Descripción de las métricas de cintas virtuales](#). Para cada alarma, especifique las condiciones que iniciarán su ALARM estado. Los indicadores de estado de alarma de la consola Storage Gateway se vuelven rojos cuando están en ese ALARM estado, lo que facilita la supervisión del estado de forma proactiva. Puede configurar las alarmas para que invoquen acciones automáticamente en función de los cambios sostenidos de estado. Para obtener más información sobre CloudWatch las alarmas, consulta [Uso de CloudWatch alarmas de Amazon](#) en la Guía del CloudWatch usuario de Amazon.


Note

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

Para cada puerta de enlace activada, le recomendamos que cree las siguientes CloudWatch alarmas:

- Espera de E/S de alto desempeño: `IoWaitpercent >= 20` para 3 puntos de datos en 15 minutos

- Porcentaje de caché sucia: `CachePercentDirty` > 80 para 4 puntos de datos en 20 minutos
- Notificaciones de estado: `HealthNotifications` >= 1 para 1 punto de datos en 5 minutos. Al configurar esta alarma, defina Tratamiento de datos faltantes en `notBreaching`.

 Note

Puede configurar una alarma de notificación de estado solo si la puerta de enlace tenía una notificación de estado anterior CloudWatch.

Para las puertas de enlace en plataformas VMware host con el modo HA activado, también recomendamos esta CloudWatch alarma adicional:

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

En la siguiente tabla se describe el estado de una alarma.

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

Estado	Descripción
	información de error en la pestaña Monitoring (Monitorización) .

Crear CloudWatch las alarmas recomendadas para su puerta de enlace

Al crear una nueva puerta de enlace mediante la consola Storage Gateway, puede optar por crear automáticamente todas CloudWatch las alarmas recomendadas como parte del proceso de configuración inicial. Para obtener más información, consulte [Configuración de la puerta de enlace de cinta](#). Si desea agregar o actualizar CloudWatch las alarmas recomendadas para una puerta de enlace existente, utilice el siguiente procedimiento.

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

Note

Esta función requiere permisos CloudWatch de política, que no se otorgan automáticamente como parte de la política de acceso total preconfigurada de Storage Gateway. Asegúrese de que su política de seguridad conceda los siguientes permisos antes de intentar crear CloudWatch las alarmas recomendadas:

- `cloudwatch:PutMetricAlarm`: crear alarmas
- `cloudwatch:DisableAlarmActions`: desactivar acciones de alarma
- `cloudwatch:EnableAlarmActions`: activar acciones de alarma
- `cloudwatch>DeleteAlarms`: eliminar alarmas

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

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

Crear una CloudWatch alarma personalizada para su puerta de enlace

CloudWatch utiliza Amazon Simple Notification Service (AmazonSNS) para enviar notificaciones de alarma cuando una alarma cambia de estado. Una alarma vigila una única métrica durante el periodo que especifique y realiza una o varias acciones en función del valor de la métrica relativo a un determinado umbral durante una serie de periodos de tiempo. La acción es una notificación que se envía a un SNS tema de Amazon. Puedes crear un SNS tema de Amazon al crear una CloudWatch alarma. Para obtener más información sobre AmazonSNS, consulta [¿Qué es AmazonSNS?](#) en la guía para desarrolladores de Amazon Simple Notification Service.

Para crear una CloudWatch alarma en la consola Storage Gateway

1. Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa/>.
2. En el panel de navegación, elija Puertas de enlace y, a continuación, elija la puerta de enlace para la que desea crear la alarma.
3. En la página de detalles de la puerta de enlace, elija la pestaña Supervisión.
4. En Alarmas, seleccione Crear alarma para abrir la CloudWatch consola.
5. Usa la CloudWatch consola para crear el tipo de alarma que desees. Puede crear los siguientes tipos de alarma:
 - Alarma de umbral estático: alarma basada en un umbral establecido para una métrica elegida. La alarma entra en ALARM estado cuando la métrica supera el umbral durante un número específico de periodos de evaluación.

Para crear una alarma de umbral estático, consulta [Cómo crear una CloudWatch alarma basada en un umbral estático](#) en la Guía del CloudWatch usuario de Amazon.

- Alarma de detección de anomalías: la detección de anomalías extrae datos métricos pasados y crea un modelo de valores esperados. Establece un valor para el umbral de detección de anomalías y lo CloudWatch utiliza con el modelo para determinar el rango «normal» de valores de la métrica. Un valor mayor del umbral produce un intervalo mayor de valores

“normales”. Puede elegir activar la alarma solo cuando el valor de la métrica esté por encima de la banda de valores esperados, solo cuando esté por debajo de la banda o cuando esté por encima o por debajo de la banda.

Para crear una alarma de detección de anomalías, consulta [Cómo crear una CloudWatch alarma basada en la detección de anomalías](#) en la Guía CloudWatch del usuario de Amazon.

- Alarma de expresión matemática métrica: alarma basada en una o más métricas utilizadas en una expresión matemática. A continuación, especifique la expresión, el umbral y los periodos de evaluación.

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

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

Para crear una alarma compuesta, consulta [Cómo crear una alarma compuesta](#) en la Guía del CloudWatch usuario de Amazon.

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

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

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

- En el panel de navegación, elija Puertas de enlace y, a continuación, elija el estado de alarma de la puerta de enlace para el que desea ver las alarmas.

Para obtener información sobre cómo editar o eliminar una alarma, consulte [Edición o eliminación de una CloudWatch alarma](#).

Note

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

Supervisión de la puerta de enlace de cinta

En esta sección se describe cómo supervisar la puerta de enlace de cinta, las cintas virtuales asociadas a la puerta de enlace de cinta, el almacenamiento en caché y el búfer de carga. Se utiliza AWS Management Console para ver las métricas de su Tape Gateway. Con las métricas, puede realizar un seguimiento del estado de la puerta de enlace de cinta y configurar alarmas que le avisen cuando una o varias métricas superen un umbral definido.

Storage Gateway proporciona CloudWatch métricas sin costo adicional. Las métricas de Storage Gateway se registran durante un periodo de dos semanas. Puede utilizar estas métricas para tener acceso a información histórica y obtener una mejor perspectiva del rendimiento de la puerta de enlace de cinta y las cintas virtuales. Para obtener información detallada al respecto CloudWatch, consulta la [Guía del CloudWatch usuario de Amazon](#).

Temas

- [Obtener registros de salud de Tape Gateway con CloudWatch grupos de registros](#)
- [Uso de Amazon CloudWatch Metrics](#)
- [Descripción de las métricas de cintas virtuales](#)
- [Medición del rendimiento entre su puerta de enlace de cinta y AWS](#)

Obtener registros de salud de Tape Gateway con CloudWatch grupos de registros

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

Por ejemplo, supongamos que su puerta de enlace está desplegada en un clúster activado con VMware alta disponibilidad y necesita conocer cualquier error. Puede configurar un grupo de CloudWatch registros para supervisar la puerta de enlace y recibir una notificación cuando la puerta de enlace detecte un error. Puede configurar el grupo cuando active la gateway o cuando ya esté activada y en funcionamiento. Para obtener información sobre cómo configurar un grupo de CloudWatch registros al activar una puerta de enlace, [consulte Configurar una puerta de enlace de cinta](#). Para obtener información general sobre los grupos de CloudWatch registros, consulte [Trabajar con grupos de registros y transmisiones de registros](#) en la Guía del CloudWatch usuario de Amazon.

Para obtener información acerca de cómo solucionar este tipo de errores, consulte [Solución de problemas con cintas virtuales](#).

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

Para configurar un grupo de CloudWatch registros para que funcione con su puerta de enlace de archivos

1. Inicie sesión en la consola Storage Gateway de su <https://console.aws.amazon.com/storagegateway/casa> AWS Management Console y ábrala.
2. En el panel de navegación, elija Gateways y, a continuación, elija la puerta de enlace para la que desea configurar el grupo de CloudWatch registros.
3. En Acciones, elija Editar información de la puerta de enlace o, en la pestaña Detalles, en Registros de salud y No activado, elija Configurar grupo de registros para abrir el cuadro de CustomerGatewayNamediálogo Editar.
4. En Grupo de registros de estado de Gateway, elija una de las siguientes opciones:
 - Desactive el registro si no desea supervisar la puerta de enlace mediante grupos de CloudWatch registros.
 - Cree un nuevo grupo de registros para crear un nuevo grupo de CloudWatch registros.
 - Use un grupo de registros existente para usar un grupo de CloudWatch registros que ya existe.

Elija un grupo de registro de la Lista de grupos de registros existentes.
5. Elija Guardar cambios.
6. Para consultar los registros del estado de la puerta de enlace, haga lo siguiente:

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

A continuación se muestra un ejemplo de un mensaje de evento de Tape Gateway que se envía a CloudWatch. En este ejemplo se muestra un mensaje TapeStatusTransition.

```
{
  "severity": "INFO",
  "source": "FZTT16FCF5",
  "type": "TapeStatusTransition",
  "gateway": "sgw-C51DFEAC",
  "timestamp": "1581553463831",
  "newStatus": "RETRIEVED"
}
```

Uso de Amazon CloudWatch Metrics

Puede obtener los datos de supervisión de su Tape Gateway utilizando el AWS Management Console o el CloudWatch API. La consola muestra una serie de gráficos basados en los datos sin procesar del CloudWatch API. También se CloudWatch API pueden utilizar a través de uno de los [kits de desarrollo de AWS software de Amazon \(SDKs\)](#) o las CloudWatch API herramientas de [Amazon](#). Según sus necesidades, es posible que prefiera utilizar los gráficos que se muestran en la consola o los extraídos de la API.

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

- La dimensión de las métricas con las que va a trabajar. Una dimensión es un par de nombre-valor que le ayuda a identificar una métrica de forma inequívoca. Las dimensiones de Storage Gateway son GatewayId y GatewayName. En la CloudWatch consola, puede utilizar la Gateway Metrics vista para seleccionar fácilmente las dimensiones específicas de la pasarela y de la cinta. Para obtener más información sobre las dimensiones, consulta [Dimensiones](#) en la Guía del CloudWatch usuario de Amazon.

- El nombre de la métrica, como ReadBytes.

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

Espacio de CloudWatch nombres Amazon	Dimensión	Descripción
AWS/StorageGateway	GatewayId , GatewayName	<p>Estas dimensiones filtran datos de métricas que describen aspectos de la puerta de enlace de cinta. Puede identificar una puerta de enlace de cinta con la que trabajar especificando las dimensiones GatewayId y GatewayName .</p> <p>Los datos de velocidad y latencia de una puerta de enlace de cinta se basan en todas las cintas virtuales de la puerta de enlace de cinta.</p> <p>Los datos se encuentran disponibles automáticamente en periodos de 5 minutos sin costo alguno.</p>


Trabajar con métricas de gateway y de cinta es similar a trabajar con otras métricas de servicio. Puede encontrar un análisis de algunas de las tareas de métricas más comunes en la siguiente CloudWatch documentación:

- [Visualización de métricas disponibles](#)
- [Obtención de estadísticas de una métrica](#)
- [Creación de CloudWatch alarmas](#)

Descripción de las métricas de cintas virtuales

A continuación puede encontrar información acerca de las métricas de Storage Gateway que abarcan las cintas virtuales. Cada cinta tiene un conjunto de métricas asociado.

Algunas de las métricas específicas de las cintas pueden tener el mismo nombre que determinadas métricas específicas de gateways. Estas métricas representan los mismos tipos de medidas, pero se asignan a una cinta en lugar de a una gateway. Antes de comenzar a trabajar, especifique si desea trabajar con una métrica de gateway o una métrica de cinta. Cuando trabaje con métricas de cinta, especifique el ID de la cinta para la que desea ver las métricas. Para obtener más información, consulte [Uso de Amazon CloudWatch Metrics](#).

 Note

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

En la siguiente tabla se describen las métricas de Storage Gateway que puede utilizar para obtener información acerca de las cintas.

Métrica	Descripción
CachePercentDirty	<p>La contribución de la cinta al porcentaje total de memoria caché de la gateway que no se ha almacenado de forma persistente en AWS. La muestra se obtiene al final del período de notificación.</p> <p>Utilice la métrica CachePercentDirty de la gateway para ver el porcentaje total de memoria caché de la gateway que no se ha almacenado de forma persistente en AWS. Para obtener más información, consulte Información acerca de las métricas de gateway.</p> <p>Unidades: porcentaje</p>
CloudTraffic	<p>La cantidad de bytes cargados y descargados desde la nube a la cinta.</p> <p>Unidades: bytes</p>

Métrica	Descripción
IoWaitPercent	<p>El porcentaje de IoWait unidades asignadas que utiliza actualmente la cinta.</p> <p>Unidades: porcentaje</p>
HealthNotification	<p>Número de notificaciones de estado que ha enviado la cinta.</p> <p>Unidades: recuento</p>
MemUsedBytes	<p>Porcentaje de memoria asignada que utiliza actualmente la cinta.</p> <p>Unidades: bytes</p>
MemTotalBytes	<p>Porcentaje de memoria total que utiliza actualmente la cinta.</p> <p>Unidades: bytes</p>
ReadBytes	<p>El número total de bytes leídos desde las aplicaciones en las instalaciones en el período de notificación para un recurso compartido de archivos.</p> <p>Utilice esta métrica con la Sum estadística para medir el rendimiento y con la Samples estadística para medir. IOPS</p> <p>Unidades: bytes</p>
UserCpuPercent	<p>El porcentaje de unidades de CPU cómputo asignadas al usuario que utiliza actualmente la cinta.</p> <p>Unidades: porcentaje</p>

Métrica	Descripción
WriteBytes	<p>El número total de bytes escritos en las aplicaciones on-premises en el período de notificación.</p> <p>Utilice esta métrica con la Sum estadística para medir el rendimiento y con la Samples estadística para medirlo. IOPS</p> <p>Unidades: bytes</p>

Medición del rendimiento entre su puerta de enlace de cinta y AWS

El rendimiento de datos, la latencia de datos y las operaciones por segundo son medidas que puede utilizar para conocer el rendimiento del almacenamiento de aplicación que está utilizando la puerta de enlace de cinta. Cuando utilice la estadística de agregación correcta, estos valores pueden medirse utilizando las métricas de Storage Gateway que se le proporcionan.

Una estadística es una agregación de una métrica a lo largo de un periodo de tiempo especificado. Al ver los valores de una métrica en CloudWatch, utilice la Average estadística para la latencia de los datos (milisegundos) y utilice la Samples estadística para las operaciones de entrada/salida por segundo (IOPS). Para obtener más información, consulta [Estadísticas](#) en la Guía del CloudWatch usuario de Amazon.

En la siguiente tabla se resumen las métricas y las estadísticas correspondientes que puede utilizar para medir el rendimiento, la latencia y IOPS entre su Tape Gateway y AWS.

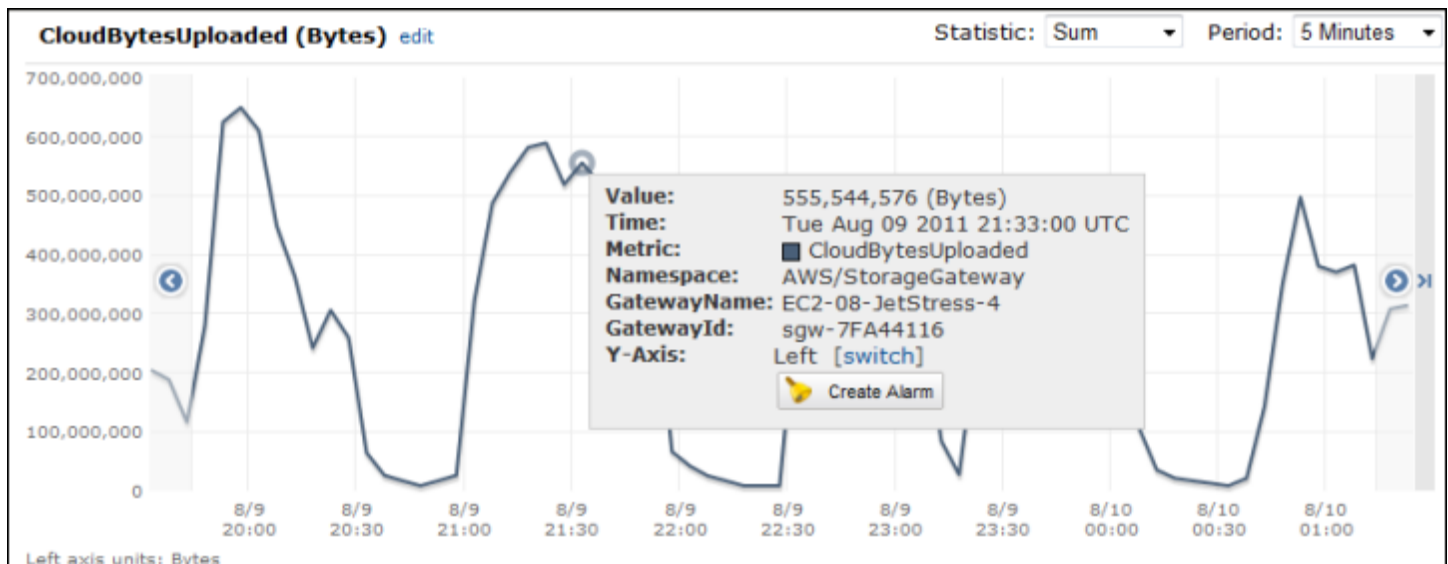
Elemento de Interés	Cómo medirlo
Latencia	Utilice las WriteTime métricas ReadTime y con la estadística. Average CloudWatch. Por ejemplo, el valor Average de la métrica ReadTime proporciona la latencia por operación a lo largo del periodo de tiempo de muestra.
Rendimiento para AWS	Utilice las CloudBytesUploaded métricas CloudBytesDownloaded y con la Sum CloudWatch estadística. Por ejemplo, el Sum valor de la CloudBytesDownloaded métrica durante un período de muestra de 5

Elemento de Interés	Cómo medirlo
	minutos dividido entre 300 segundos indica el rendimiento desde AWS la puerta de enlace de cinta expresado en bytes por segundo.
Latencia de los datos hasta AWS	Utilice la métrica <code>CloudDownloadLatency</code> con la estadística <code>Average</code> . Por ejemplo, la estadística <code>Average</code> de la métrica <code>CloudDownloadLatency</code> proporciona la latencia por operación.

Para medir el rendimiento de los datos de carga desde una puerta de enlace de cinta a AWS

1. Abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>
2. Elija la pestaña Metrics (Métricas).
3. Elija la dimensión StorageGateway: Gateway Metrics y busque la puerta de enlace de cinta con la que desee trabajar.
4. Elija la métrica `CloudBytesUploaded`.
5. Para Time Range (Intervalo de tiempo), elija un valor.
6. Elija la estadística `Sum`.
7. Para Period (Periodo), elija un valor de 5 minutos o mayor.
8. En el conjunto resultante de puntos de datos ordenados temporalmente, divida cada punto de datos por el periodo (en segundos) para obtener el rendimiento en ese periodo de muestra.

La imagen siguiente muestra la métrica `CloudBytesUploaded` para una cinta de gateway con la estadística `Sum`. En la imagen, al colocar el cursor sobre un punto de datos se muestra información sobre el punto de datos, incluidos su valor y el número de bytes cargados. Divida este valor de bytes entre el valor de Period (Periodo) (5 minutos) para obtener el rendimiento en ese punto de muestra. Para el punto destacado, el rendimiento de la puerta de enlace de cinta AWS es de 555.544.576 bytes divididos entre 300 segundos, lo que equivale a 1,7 megabytes por segundo.



Para medir la latencia de los datos desde una puerta de enlace de cinta a AWS

1. Abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.
2. Elija la pestaña Metrics (Métricas).
3. Elija la GatewayMetrics dimensión StorageGateway: y busque la puerta de enlace de cinta con la que desee trabajar.
4. Elija la métrica CloudDownloadLatency.
5. Para Time Range (Intervalo de tiempo), elija un valor.
6. Elija la estadística Average.
7. Para Period (Periodo), elija un valor de 5 minutos para que coincida con el tiempo de informe predeterminado.

El conjunto resultante de datos ordenados temporalmente contiene la latencia en milisegundos.

Para configurar una alarma de umbral superior para el rendimiento de una puerta de enlace de cinta en AWS

1. Abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>
2. Seleccione Create Alarm (Crear alarma) para iniciar el asistente Crear alarma.
3. Elija la dimensión StorageGateway: Gateway Metrics y busque la puerta de enlace de cinta con la que desee trabajar.
4. Elija la métrica CloudBytesUploaded.

5. Para definir la alarma, defina el estado de alarma cuando la métrica `CloudBytesUploaded` sea mayor o igual a un valor especificado durante un periodo de tiempo determinado. Por ejemplo, puede definir un estado de alarma cuando la métrica `CloudBytesUploaded` sea superior a 10 megabytes durante 60 minutos.
6. Configure las acciones que se llevarán a cabo para el estado de alarma. Por ejemplo, puede hacer que se le envíe una notificación por correo electrónico.
7. Seleccione Crear alarma.

Para configurar una alarma de umbral superior para leer los datos de AWS

1. Abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.
2. Seleccione Create Alarm (Crear alarma) para iniciar el asistente Crear alarma.
3. Elija la dimensión `StorageGateway: Gateway Metrics` y busque la puerta de enlace de cinta con la que desee trabajar.
4. Elija la métrica `CloudDownloadLatency`.
5. Para definir la alarma, defina el estado de alarma cuando la métrica `CloudDownloadLatency` sea mayor o igual a un valor especificado durante un periodo de tiempo determinado. Por ejemplo, puede definir un estado de alarma cuando `CloudDownloadLatency` sea superior a 60 000 milisegundos durante más de 2 horas.
6. Configure las acciones que se llevarán a cabo para el estado de alarma. Por ejemplo, puede hacer que se le envíe una notificación por correo electrónico.
7. Seleccione Crear alarma.

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. Si no ha creado una gateway, consulte [Creación de la puerta de enlace](#).

Temas

- [Como apagar la MV de la gateway](#)
- [Administración de discos locales para Storage Gateway](#)
- [Administración del ancho de banda de la puerta de enlace de cinta](#)
- [Administrar las actualizaciones de la pasarela](#)
- [Realizar tareas de mantenimiento mediante la consola local](#)
- [Eliminar la puerta de enlace y eliminar los recursos asociados](#)

Como apagar 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 puerta de enlace de archivo, apague la VM. Si bien esta sección se centra en iniciar y detener la puerta de enlace mediante la consola de administración de Storage Gateway, también puede detener la puerta de enlace mediante la consola local de la máquina virtual o Storage GatewayAPI. Cuando encienda la MV, recuerde reiniciar su gateway.

Important

Si detiene e inicia una EC2 puerta de enlace de Amazon que utiliza almacenamiento efímero, la puerta de enlace quedará desconectada permanentemente. Esto sucede porque se ha reemplazado el disco de almacenamiento físico. No hay una solución para este problema. La única solución es eliminar la puerta de enlace y activar una nueva en una instancia nuevaEC2.

Note

Si detiene la gateway mientras que el software de copia de seguridad está escribiendo o leyendo en una cinta, es posible que la tarea de escritura o lectura no se lleve a cabo correctamente. Antes de detener la gateway, debe consultar el software de copia de seguridad y la programación de copia de seguridad para comprobar que no haya tareas en curso.

- Consola local de la VM de la puerta de enlace: consulte [Inicio de sesión en la consola local con las credenciales predeterminadas](#).
- Storage GatewayAPI: consulte [ShutdownGateway](#)

En el caso de una puerta de enlace de archivo, apague la VM. No detenga la gateway.

Inicio y detención de una puerta de enlace de cinta

Para detener una puerta de enlace de cinta

1. Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa>.
2. En el panel de navegación, elija Gateways y, a continuación, seleccione la gateway que desee detener. El estado de la gateway es Running (En ejecución).
3. En Actions (Acciones), elija Stop gateway (Parar gateway) y verifique el ID de la gateway del cuadro de diálogo y, a continuación, elija Stop gateway (Parar gateway).

Aunque el gateway se esté deteniendo, puede que aparezca un mensaje que indica el estado de la gateway. Cuando la gateway se apague, aparecerán un mensaje y el botón Start gateway (Iniciar gateway) en la pestaña Details (Detalles).

Cuando detenga la gateway, los recursos de almacenamiento no estarán accesibles hasta que inicie el almacenamiento. Si la gateway estaba cargando datos en el momento de detenerla, la carga se reanudará cuando inicie la gateway.

Para iniciar una puerta de enlace de cinta

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

2. En el panel de navegación, elija Gateways y, a continuación, seleccione la gateway que desee iniciar. El estado de la gateway es Shutdown (Apagada).
3. Elija Details (Detalles) y, a continuación, Start gateway (Iniciar gateway).

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 puertas de enlace creadas en EC2 instancias de Amazon utilizan EBS los volúmenes de Amazon como discos locales.

Temas

- [Cálculo de la cantidad de almacenamiento en disco local](#)
- [Optimización del rendimiento de la gateway](#)
- [Determinación del tamaño que se va a asignar al búfer de carga](#)
- [Determinación del tamaño que se va a asignar al almacenamiento en caché](#)
- [Configuración adicional de búfer de carga o almacenamiento en caché](#)

Cálculo de la cantidad de almacenamiento en disco local


Puede elegir el número y el tamaño de los discos que va a asignar a la gateway. Según la solución de almacenamiento que vaya a implementar (consulte [Planee la implementación de Storage Gateway](#)), la gateway requiere el siguiente almacenamiento adicional:

- Las puertas de enlace de cinta requieren al menos dos discos. Uno para utilizarlo como caché y otro para utilizarlo como búfer de carga.

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	Descripción
Búfer de carga	El búfer de carga proporciona un espacio provisional para los datos antes de que la puerta

Almacenamiento local	Descripción	
	de enlace los cargue a Amazon S3. Su puerta de enlace carga estos datos del búfer a través de una conexión cifrada de Secure Sockets Layer (SSL) a. AWS	
Almacenamiento en caché	El almacenamiento en caché funciona como un almacén en las instalaciones permanente para los datos que están pendientes de carga desde el búfer de carga en Amazon S3. Cuando la aplicación efectúa entradas y salidas en un volumen o cinta, la gateway guarda los datos en el almacenamiento en caché para permitir el acceso a ellos con baja latencia. Cuando la aplicación solicita datos de un volumen o una cinta, la gateway los busca primero en el almacenamiento en caché antes de descargarlos desde AWS.	

 Note

Cuando aprovisiona discos, recomendamos encarecidamente que no aprovisiona discos locales que utilicen el mismo recurso físico (el mismo disco) para el búfer de carga y el almacenamiento en caché. Los recursos de almacenamiento físico subyacentes se representan como un almacén de datos en VMware. Al implementar la máquina virtual de gateway, debe elegir el almacén de datos en el que se almacenarán los archivos de la máquina virtual. Al aprovisionar un disco local (por ejemplo, para utilizarlo como almacenamiento en caché o búfer de carga), tiene la opción de almacenar el disco virtual en el mismo almacén de datos que la máquina virtual o en otro distinto.

Si hay más de un almacén de datos, recomendamos encarecidamente elegir un almacén de datos para el almacenamiento en caché y otro para el búfer de carga. Un almacén de datos respaldado por un único disco físico subyacente puede hacer que disminuya el rendimiento en algunas situaciones si se utiliza simultáneamente para el almacenamiento en caché y del búfer de carga. Esto también es cierto si la copia de seguridad es una RAID configuración de menor rendimiento, por ejemplo. RAID1

Tras la configuración e implementación iniciales de la gateway, puede ajustar el almacenamiento local añadiendo o eliminando discos para un búfer de carga. También puede añadir discos para el almacenamiento en caché.

Optimización del rendimiento de la gateway

Para lograr un rendimiento óptimo, utilice SSD discos de alto rendimiento tanto para la memoria caché como para el búfer de carga

- Utilice discos diferentes para la memoria caché y el búfer de carga. Si los utiliza RAID, asegúrese de que los discos de caché y búfer de carga utilicen RAID controladores independientes a nivel de hardware.
- Agregue al menos 2 discos de búfer de carga diferentes.
- Utilice una configuración RAID con franjas de RAID 0 para los dispositivos de caché y búfer de carga a fin de mejorar el rendimiento. Esto es especialmente importante para el disco de la memoria caché.

Determinación del tamaño que se va a asignar al búfer de carga

Puede determinar el tamaño que se va a asignar al búfer de carga mediante una fórmula específica. Recomendamos encarecidamente asignar al menos 150 GiB para el búfer de carga. Si la fórmula devuelve un valor inferior a 150 GiB, asigne 150 GiB al búfer de carga. Puede configurar hasta 2 TiB de capacidad para el búfer de carga de cada gateway.

Note

En las puertas de enlace de cinta, cuando el búfer de carga alcanza su capacidad, las aplicaciones pueden continuar leyendo y escribiendo datos en los volúmenes de almacenamiento. Sin embargo, Tape Gateway no escribe ninguno de los datos del volumen

en su búfer de carga ni carga ninguno de estos datos AWS hasta que Storage Gateway sincronice los datos almacenados localmente con la copia de los datos almacenados en AWS. Esta sincronización se produce cuando los volúmenes están en BOOTSTRAPPING estado.

Para calcular la cantidad que se va a asignar al búfer de carga, puede determinar las velocidades de datos entrantes y salientes previstas y utilizarlas en la fórmula siguiente.

Velocidad de datos entrantes

Esta velocidad se refiere al rendimiento de la aplicación, la velocidad a la que las aplicaciones on-premise escriben datos en la gateway en un periodo de tiempo determinado.

Velocidad de datos salientes

Esta velocidad se refiere al rendimiento de la red, la velocidad a la que la gateway carga datos en AWS. Esta velocidad depende de la velocidad de la red, del grado de utilización de esta y de si se ha activado la limitación de ancho de banda. Esta velocidad debe ajustarse para la compresión. Al cargar datos a AWS, la puerta de enlace aplica la compresión de datos siempre que es posible. Por ejemplo, si los datos de la aplicación son de solo texto, puede obtener una relación de compresión efectiva de 2:1. Sin embargo, cuando se escriben vídeos, puede que la gateway no consiga aplicar ningún tipo de compresión y, por consiguiente, que requiera más capacidad del búfer de carga.

Recomendamos encarecidamente que asigne al menos 150 GiB de espacio en búfer de carga si se cumple alguna de las siguientes condiciones:

- Su tasa de entrada es más alta que la tasa de salida.
- La fórmula devuelve un valor inferior a 150 GiB.

$$\left(\text{Application Throughput (MB/s)} - \text{Network Throughput to AWS (MB/s)} \times \text{Compression Factor} \right) \times \text{Duration of writes (s)} = \text{Upload Buffer (MB)}$$

Por ejemplo, supongamos que sus aplicaciones empresariales escriben texto en la gateway a una velocidad de 40 MB por segundo durante 12 horas al día y que el rendimiento de la red es de 12 MB

por segundo. Suponiendo un factor de compresión de 2:1 para los datos de texto, debe asignar aproximadamente 690 GiB de espacio al búfer de carga.

Example

```
((40 MB/sec) - (12 MB/sec * 2)) * (12 hours * 3600 seconds/hour) = 691200 megabytes
```

Puede utilizar esta aproximación inicialmente para determinar el tamaño del disco que desea asignar a la gateway como espacio de búfer de carga. Puede agregar más espacio de búfer de carga cuando lo necesite desde la consola de Storage Gateway. Además, puedes usar las métricas CloudWatch operativas de Amazon para monitorear el uso del búfer de carga y determinar los requisitos de almacenamiento adicionales. Para obtener información sobre las métricas y cómo configurar las alarmas, consulte [Supervisión del búfer de carga](#).

Determinación del tamaño que se va a asignar al almacenamiento en caché

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 en las instalaciones permanente para los datos que están pendientes de carga desde el búfer de carga en Amazon S3. En términos generales, el tamaño del almacenamiento de caché debe ser 1,1 veces el tamaño del búfer de carga. Para obtener más información sobre cómo calcular el tamaño del almacenamiento en caché, consulte [Determinación del tamaño que se va a asignar al búfer de carga](#).

Inicialmente se puede utilizar esta aproximación para aprovisionar los discos para el almacenamiento en caché. A continuación, puede utilizar las métricas CloudWatch operativas de Amazon para supervisar el uso del almacenamiento en caché y aprovisionar más almacenamiento según sea necesario mediante la consola. Para obtener información sobre cómo usar las métricas y configurar las alarmas, consulte [Supervisión del almacenamiento en caché](#).

Configuración adicional de búfer de carga o almacenamiento en caché

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

⚠ Important

Al añadir caché o búfer de carga a una puerta de enlace existente, debe crear nuevos discos en el hipervisor del host de la puerta de enlace o en la EC2 instancia de Amazon. No elimine ni cambie el tamaño de los discos existentes que ya se hayan asignado como memoria caché o búfer de carga.

Para configurar búfer de carga o el almacenamiento en caché adicional a la puerta de enlace

1. Aprovechone uno o más discos nuevos en el hipervisor del host de la puerta de enlace o en la EC2 instancia de Amazon. Para obtener información sobre cómo aprovisionar un disco en un hipervisor, consulte el manual de usuario del hipervisor. Para obtener información sobre el aprovisionamiento de EBS volúmenes de Amazon para una EC2 instancia de Amazon, consulte [Amazon EBS volumes](#) en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux. En los siguientes pasos, configurará este disco como búfer de carga o almacenamiento en caché.
2. Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa>.
3. En el panel de navegación, seleccione Puertas de enlace.
4. Busque la puerta de enlace y selecciónela de la lista.
5. En el menú Acciones, seleccione Configurar almacenamiento.
6. En la sección Configurar almacenamiento, identifique los discos que aprovisionó. Si no ve los discos, seleccione el icono de actualización para actualizar la lista. Para cada disco, elija una opción UPLOADBUFFER o CACHESTORAGE una opción en el menú desplegable Asignado a.
7. Elija Guardar cambios para guardar los ajustes de configuración.

Administración del ancho de banda de la puerta de enlace de cinta

Puede limitar (o limitar) el rendimiento de carga desde la puerta de enlace AWS o el rendimiento de descarga desde AWS su puerta de enlace. El uso de la limitación controlada del ancho de banda permite controlar la cantidad de ancho de banda de red que utiliza la gateway. De forma predeterminada, una gateway activada no tiene límites de carga o descarga.

Puede especificar el límite de velocidad mediante el AWS Management Console Storage Gateway API (consulte [UpdateBandwidthRateLimit](#)) o un kit de desarrollo de AWS software () mediante

programación. SDK Si limita el ancho de banda mediante programación, puede cambiar los límites automáticamente a lo largo del día, por ejemplo, programando tareas que cambien el ancho de banda.

También puede definir una limitación del ancho de banda basada en la programación para la puerta de enlace. Para programar la limitación del ancho de banda, defina uno o más intervalos. `bandwidth-rate-limit` Para obtener más información, consulte [Limitación del ancho de banda basada en la programación mediante la consola de Storage Gateway](#).

Configurar una configuración única para la limitación del ancho de banda es el equivalente funcional de definir una programación con un único `bandwidth-rate-limit` intervalo establecido para todos los días, con una hora de inicio `00:00` y una hora de finalización de `23:59`

Note

La información de esta sección es específica para las puertas de enlace de cinta y de volumen. Para administrar el ancho de banda de una puerta de enlace de archivo de Amazon S3, consulte [Managing Bandwidth for Your Amazon S3 File Gateway](#). Los límites de velocidad de ancho de banda no son compatibles actualmente con Amazon FSx File Gateway.

Temas

- [Cambio de la limitación controlada del ancho de banda mediante la consola de Storage Gateway](#)
- [Limitación del ancho de banda basada en la programación mediante la consola de Storage Gateway](#)
- [Actualización de los límites de ancho de banda de la pasarela mediante AWS SDK for Java](#)
- [Actualización de los límites de ancho de banda de Gateway mediante AWS SDK for .NET](#)
- [Actualización de los límites de ancho de banda de Gateway mediante AWS Tools for Windows PowerShell](#)

Cambio de la limitación controlada del ancho de banda mediante la consola de Storage Gateway

En el procedimiento siguiente, se muestra cómo cambiar la limitación controlada del ancho de banda de la puerta de enlace con la consola de Storage Gateway.

Para cambiar la limitación controlada de ancho de banda de una gateway mediante la consola

1. Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa>.
2. En el panel de navegación izquierdo, elija Puertas de enlace y, a continuación, elija la puerta de enlace que desee administrar.
3. En Acciones, elija Editar el límite de velocidad del ancho de banda.
4. En el cuadro de diálogo Editar límites de velocidad, escriba nuevos valores para los límites y, a continuación, elija Guardar. Los cambios aparecen en la pestaña Details (Detalles) de la gateway.

Limitación del ancho de banda basada en la programación mediante la consola de Storage Gateway


En el procedimiento siguiente se muestra cómo programar cambios en la limitación del ancho de banda de una puerta de enlace utilizando la consola de Storage Gateway.

Para agregar o modificar una programación para la limitación del ancho de banda de la puerta de enlace

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


La bandwidth-rate-limit programación de la puerta de enlace se muestra en el cuadro de diálogo Editar la programación del límite de velocidad de ancho de banda. De forma predeterminada, la nueva bandwidth-rate-limit programación de la puerta de enlace está vacía.

4. En el cuadro de diálogo Editar el programa de límite de velocidad de ancho de banda, elija Agregar nuevo elemento para agregar un nuevo bandwidth-rate-limit intervalo. Introduzca la siguiente información para cada bandwidth-rate-limit intervalo:
 - Días de la semana: puede crear el bandwidth-rate-limit intervalo para los días de la semana (de lunes a viernes), los fines de semana (sábado y domingo), para todos los días de la semana o para uno o más días específicos de la semana.
 - Hora de inicio: introduzca la hora de inicio del intervalo de ancho de banda en la zona horaria local de la puerta de enlace con el formato HH:MM.

 Note

El bandwidth-rate-limit intervalo comienza al principio del minuto que especifique aquí.

- Hora de finalización: introduzca la hora de finalización del bandwidth-rate-limit intervalo en la zona horaria local de la puerta de enlace con el formato HH:MM.

 Important

El bandwidth-rate-limit intervalo finaliza al final del minuto especificado aquí. Para programar un intervalo que finalice al final de una hora, introduzca **59**.

Para programar intervalos continuos consecutivos, con transferencia al principio de la hora, sin interrupción entre los intervalos, introduzca **59** para el minuto final del primer intervalo. Introduzca **00** para el minuto de inicio del siguiente intervalo.

- Velocidad de descarga: introduzca el límite de velocidad de descarga en kilobits por segundo (Kbps), o seleccione Sin límite para desactivar la limitación del ancho de banda para la descarga. El valor mínimo de la velocidad de descarga es 100 Kbps.
- Velocidad de carga: introduzca el límite de velocidad de carga en Kbps o seleccione Sin límite para desactivar la limitación del ancho de banda para la carga. El valor mínimo de la velocidad de carga es 50 Kbps.

Para modificar los bandwidth-rate-limit intervalos, puede introducir valores revisados para los parámetros del intervalo.

Para eliminar bandwidth-rate-limit los intervalos, puede seleccionar Eliminar a la derecha del intervalo que desee eliminar.

Cuando haya completado los cambios, elija Guardar.

5. Para seguir añadiendo bandwidth-rate-limit intervalos, selecciona Añadir nuevo elemento e introduce el día, las horas de inicio y finalización y los límites de velocidad de descarga y carga.

⚠ Important

bandwidth-rate-limit Los intervalos B no se pueden superponer. La hora de inicio de un intervalo debe producirse después de la hora de finalización del intervalo anterior y antes de la hora de inicio del intervalo siguiente.

6. Tras introducir todos los bandwidth-rate-limit intervalos, selecciona Guardar cambios para guardar la bandwidth-rate-limit programación.

Cuando la bandwidth-rate-limit programación se haya actualizado correctamente, podrás ver los límites actuales de velocidad de descarga y carga en el panel de detalles de la pasarela.

Actualización de los límites de ancho de banda de la pasarela mediante AWS SDK for Java

Si actualiza los límites de velocidad del ancho de banda mediante programación, puede ajustar los 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 velocidad del ancho de banda de una puerta de enlace mediante AWS 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 puerta de enlace mediante el AWS SDK for Java

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

```
import java.io.IOException;

import com.amazonaws.AmazonClientException;
import com.amazonaws.auth.PropertiesCredentials;
import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitRequest;
```

```
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitResult;

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 = 51200; // Bits per second, minimum 51200
    static long downloadRate = 102400; // Bits per second, minimum 102400

    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, downloadRate);

    }

    private static void UpdateBandwidth(String gatewayARN2, long uploadRate2,
        long downloadRate2) {
        try
        {
            UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
                new UpdateBandwidthRateLimitRequest()
                    .withGatewayARN(gatewayARN)
                    .withAverageDownloadRateLimitInBitsPerSec(downloadRate)
                    .withAverageUploadRateLimitInBitsPerSec(uploadRate);

            UpdateBandwidthRateLimitResult updateBandwidthRateLimitResult =
sgClient.updateBandwidthRateLimit(updateBandwidthRateLimitRequest);
            String returnGatewayARN = updateBandwidthRateLimitResult.getGatewayARN();
            System.out.println("Updated the bandwidth rate limits of " +
returnGatewayARN);
        }
    }
}
```

```
        System.out.println("Upload bandwidth limit = " + uploadRate + " bits per
second");
        System.out.println("Download bandwidth limit = " + downloadRate + " bits
per second");
    }
    catch (AmazonClientException ex)
    {
        System.err.println("Error updating gateway bandwidth.\n" + ex.toString());
    }
}
```

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

Si actualiza los límites de velocidad del ancho de banda mediante programación, puede ajustar los 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 velocidad del ancho de banda de una puerta de enlace mediante el AWS SDK for .NET. Para usar el código de ejemplo, debe estar familiarizado con la ejecución de un .NET aplicación de consola. 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 Gateway mediante el AWS SDK for .NET

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

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

namespace AWSStorageGateway
{
```

```
class UpdateBandwidthExample
{
    static AmazonStorageGatewayClient sgClient;
    static AmazonStorageGatewayConfig sgConfig;

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

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

    // Rates
    static long uploadRate = 51200; // Bits per second, minimum 51200
    static long downloadRate = 102400; // Bits per second, minimum 102400

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

        UpdateBandwidth(gatewayARN, uploadRate, downloadRate);

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

    public static void UpdateBandwidth(string gatewayARN, long uploadRate, long
downloadRate)
    {
        try
        {
            UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
                new UpdateBandwidthRateLimitRequest()
                    .WithGatewayARN(gatewayARN)
                    .WithAverageDownloadRateLimitInBitsPerSec(downloadRate)
                    .WithAverageUploadRateLimitInBitsPerSec(uploadRate);

            UpdateBandwidthRateLimitResponse updateBandwidthRateLimitResponse =
sgClient.UpdateBandwidthRateLimit(updateBandwidthRateLimitRequest);
            String returnGatewayARN =
updateBandwidthRateLimitResponse.UpdateBandwidthRateLimitResult.GatewayARN;
```

```
        Console.WriteLine("Updated the bandwidth rate limits of " +
returnGatewayARN);
        Console.WriteLine("Upload bandwidth limit = " + uploadRate + " bits per
second");
        Console.WriteLine("Download bandwidth limit = " + downloadRate + " bits
per second");
    }
    catch (AmazonStorageGatewayException ex)
    {
        Console.WriteLine("Error updating gateway bandwidth.\n" +
ex.ToString());
    }
}
}
```

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

Si actualiza los límites de velocidad del ancho de banda mediante programación, puede ajustar los 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 velocidad del ancho de banda de una puerta de enlace mediante AWS Tools for Windows PowerShell. Para usar el código de ejemplo, debe estar familiarizado con la ejecución de un PowerShell script. 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 Gateway mediante el AWS Tools for Windows PowerShell

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

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

.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 = 51200
$DownloadBandwidthRate = 102400
$gatewayARN = "*** provide gateway ARN ***"

#Update Bandwidth Rate Limits
Update-SGBandwidthRateLimit -GatewayARN $gatewayARN `
                             -AverageUploadRateLimitInBitsPerSec $UploadBandwidthRate `
                             -AverageDownloadRateLimitInBitsPerSec
                             $DownloadBandwidthRate

$limits = Get-SGBandwidthRateLimit -GatewayARN $gatewayARN

Write-Output("`nGateway: " + $gatewayARN);
Write-Output("`nNew Upload Rate: " + $limits.AverageUploadRateLimitInBitsPerSec)
Write-Output("`nNew Download Rate: " + $limits.AverageDownloadRateLimitInBitsPerSec)
```

Administrar las actualizaciones de la pasarela

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

Important

Debe tratar el dispositivo de Storage Gateway como una máquina virtual administrada y no debe intentar acceder a su instalación ni modificarla de forma alguna. Si intenta instalar o actualizar cualquier paquete de software mediante métodos distintos al mecanismo de actualización habitual de la AWS puerta de enlace (por ejemplo, SSM o las herramientas del hipervisor), es posible que la puerta de enlace no funcione correctamente.

Frecuencia de actualización y comportamiento esperado

AWS actualiza el componente de servicios en la nube según sea necesario sin interrumpir las pasarelas implementadas. Los dispositivos de puerta de enlace implementados reciben actualizaciones de mantenimiento mensuales. Las actualizaciones de mantenimiento mensuales pueden incluir actualizaciones del sistema operativo y del software, correcciones para mejorar la estabilidad, el rendimiento y la seguridad, y el acceso a nuevas funciones. Todas las actualizaciones son acumulativas y actualizan las pasarelas a la versión actual cuando se aplican. Para obtener información sobre los cambios específicos incluidos en cada actualización, consulte las [notas de la versión del software Tape Gateway Appliance](#) y las [notas de la versión del software](#).

Las actualizaciones de mantenimiento mensuales pueden provocar una breve interrupción del servicio. El host de máquinas virtuales de la puerta de enlace no necesita reiniciarse durante las actualizaciones, pero la puerta de enlace no estará disponible durante un breve período de tiempo mientras el dispositivo de puerta de enlace se actualiza y se reinicia. Puede minimizar la posibilidad de que se produzcan interrupciones en sus aplicaciones debido al reinicio de la puerta de enlace aumentando los tiempos de espera de su SCSI iniciador i. Para obtener más información sobre cómo aumentar los tiempos de espera SCSI del iniciador i en Windows y Linux, consulte y. [Personalización de la configuración de Windows i SCSI](#) [Personalización de la configuración de Linux i SCSI](#)

Al implementar y activar la puerta de enlace, se establece un programa de mantenimiento semanal predeterminado. Puede modificar la programación de los períodos de mantenimiento en cualquier momento. También puede desactivar las actualizaciones de mantenimiento mensuales, pero le recomendamos que las deje activadas.

Note

A veces, las actualizaciones urgentes se aplican de acuerdo con el calendario de mantenimiento, incluso si las actualizaciones de mantenimiento periódicas están desactivadas.

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

Cuando hay actualizaciones disponibles, la pestaña Detalles de la puerta de enlace muestra un mensaje de mantenimiento. También puede ver la fecha y la hora en que se aplicó correctamente la última actualización en la pestaña Detalles.

Activa o desactiva las actualizaciones de mantenimiento

Cuando se activan las actualizaciones de mantenimiento, la puerta de enlace las aplica automáticamente según el cronograma de ventanas de mantenimiento configurado. Para obtener más información, consulte [enlace](#).

Si las actualizaciones de mantenimiento están desactivadas, la puerta de enlace no las aplicará automáticamente, pero siempre puede aplicarlas manualmente mediante la consola de Storage Gateway API, o CLI. En ocasiones, las actualizaciones urgentes se aplicarán durante el período de mantenimiento configurado, independientemente de esta configuración.

Note

El siguiente procedimiento describe cómo activar o desactivar las actualizaciones de gateway mediante la consola Storage Gateway. Para cambiar esta configuración mediante programación mediante el API, consulte [UpdateMaintenanceStartTime](#) la referencia de Storage Gateway API.

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

1. Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa>.
2. En el panel de navegación, elija Gateways y, a continuación, elija la puerta de enlace para la que desee configurar las actualizaciones de mantenimiento.
3. Elija Acciones y, a continuación, elija Editar la configuración de mantenimiento.
4. Para las actualizaciones de mantenimiento, selecciona Activar o Desactivar.
5. Selecciona Guardar cambios cuando hayas terminado.

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

Modifique la programación del período de mantenimiento de la puerta de enlace

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

Note

El siguiente procedimiento describe cómo modificar la programación del período de mantenimiento mediante la consola Storage Gateway. Para cambiar esta configuración mediante programación mediante el API, consulte [UpdateMaintenanceStartTime](#) la referencia de Storage Gateway API.

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

1. Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa>.
2. En el panel de navegación, elija Gateways y, a continuación, elija la puerta de enlace para la que desee configurar las actualizaciones de mantenimiento.
3. Elija Acciones y, a continuación, elija Editar la configuración de mantenimiento.
4. En Hora de inicio de la ventana Mantenimiento, haga lo siguiente:
 - a. En Programar, seleccione Semanal o Mensual para establecer la cadencia del período de mantenimiento.
 - b. Si elige Semanalmente, modifique los valores del día de la semana y la hora para establecer el punto específico de cada semana en el que comenzará el período de mantenimiento.

Si elige Mensual, modifique los valores del día del mes y la hora para establecer el punto específico de cada mes en el que comenzará el período de mantenimiento.

Note

El valor máximo que se puede establecer para el día del mes es 28. No es posible configurar el programa de mantenimiento para que comience los días 29 a 31.

Si recibes un error al configurar esta configuración, es posible que el software de la puerta de enlace esté desactualizado. Considere actualizar primero la puerta de enlace manualmente y, a continuación, intentar configurar de nuevo el programa de ventanas de mantenimiento.

5. Seleccione Guardar cambios cuando haya terminado.

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

Realizar tareas de mantenimiento mediante la consola local

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

Realización de tareas en la consola local de la MV de

Para una gateway implementada on-premises, puede realizar las siguientes tareas de mantenimiento utilizando la consola local del host de la MV. Estas tareas son comunes a los hosts VMware de máquinas virtuales () basadas en el núcleo de Hyper-V y Linux. KVM

Temas

- [Inicio de sesión en la consola local con las credenciales predeterminadas](#)
- [Ajuste de la contraseña de la consola local desde la consola de Storage Gateway](#)
- [Ruteo de la gateway local a través de un proxy](#)
- [Configuración de red de la gateway](#)
- [Prueba de conexión de la gateway a Internet](#)
- [Sincronización de la hora de la MV de la gateway](#)
- [Ejecución de comandos de Storage Gateway en la consola local](#)
- [Visualización del estado de los recursos de sistema de la gateway](#)
- [Configuración de adaptadores de red para la gateway](#)

Inicio de sesión en la consola local con las credenciales predeterminadas

Cuando la MV está lista para el inicio de sesión, se muestra la pantalla de inicio de sesión. Si es la primera vez que inicia sesión en la consola local, utilice las credenciales predeterminadas para iniciar sesión. Estas credenciales de inicio de sesión predeterminadas proporcionan acceso a menús donde puede configurar los ajustes de red de la puerta de enlace y cambiar la contraseña de la consola local. Storage Gateway le permite establecer su propia contraseña desde la AWS Storage Gateway consola en lugar de cambiarla desde la consola local. No es necesario que conozca la contraseña predeterminada para establecer una nueva contraseña. Para obtener más información, consulte [Ajuste de la contraseña de la consola local desde la consola de Storage Gateway](#).

Para iniciar sesión en la consola local de la gateway

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

De lo contrario, utilice las credenciales para iniciar sesión.

Note

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

Important

Para las versiones anteriores de puerta de enlace de cinta o volumen, el nombre de usuario es `sguser` y la contraseña es `sgpassword`. Si restablece la contraseña y la gateway se actualiza a una versión más reciente, el nombre de usuario cambiará a `admin`, pero se conservará la contraseña.

- Tras iniciar sesión, verá el menú principal Configuración de AWS Storage Gateway, desde el que puede realizar diversas tareas.

Para obtener información sobre esta tarea	Consulte este tema
Configure un SOCKS proxy para su puerta de enlace	Ruteo de la gateway local a través de un proxy.
Configurar la red	Configuración de red de la gateway.
Probar la conectividad de red	Prueba de conexión de la gateway a Internet.
Administrar el tiempo de la MV	Sincronización de la hora de la MV de la gateway.
Ejecute los comandos de la consola de Storage Gateway	Ejecución de comandos de Storage Gateway en la consola local.
Ver una comprobación de recursos del sistema	Visualización del estado de los recursos de sistema de la gateway.

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

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


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

Cuando inicie sesión en la consola local por primera vez, inicie sesión en la VM con las credenciales predeterminadas: 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

- Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa>.
- En el panel de navegación, elija Gateways y, a continuación, elija la gateway para la que desea establecer una contraseña nueva.


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), escriba una contraseña nueva, confirme la contraseña 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 VM.

 Note

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

Ruteo de la gateway local a través de un proxy

Las pasarelas de volumen y las pasarelas de cinta admiten la configuración de un proxy Socket Secure versión 5 (SOCKS5) entre su puerta de enlace local y AWS.

 Note

La única configuración de proxy admitida es SOCKS5.

Si su puerta de enlace debe usar un servidor proxy para comunicarse con Internet, debe configurar los ajustes del SOCKS proxy de su puerta de enlace. 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 enruta todo el tráfico a través del servidor proxy. Para obtener más información sobre los requisitos de red para la gateway, consulte [Requisitos de red y firewall](#).

El siguiente procedimiento muestra cómo configurar el SOCKS proxy para Volume Gateway y Tape Gateway.

Para configurar un SOCKS5 proxy para pasarelas de volumen y cinta

1. Inicie sesión en la consola local de la gateway.
 - VMware ESXi— para obtener más información, consulte [Acceder a la consola local de Gateway con VMware ESXi](#).

- Microsoft Hyper-V: para obtener más información, consulte [Acceso a la consola local de la gateway con Microsoft Hyper-V](#).
 - KVM— para obtener más información, consulte [Acceso a la consola local de Gateway con Linux KVM](#).
2. En el menú principal AWS Storage Gateway: Configuration, introduzca el número correspondiente para seleccionar SOCKSProxy Configuration.
 3. En el menú de configuración del SOCKS proxy de AWS Storage Gateway, introduzca el número correspondiente para realizar una de las siguientes tareas:

Para llevar a cabo esta tarea	Haga lo siguiente
Configure un proxy SOCKS	<p>Introduzca el número correspondiente para seleccionar Configurar SOCKS proxy.</p> <p>Deberá proporcionar un nombre de host y un puerto para completar la configuración.</p>
Vea la configuración de SOCKS proxy actual	<p>Introduzca el número correspondiente para seleccionar Ver la configuración de SOCKS proxy actual.</p> <p>Si el SOCKS proxy no está configurado, SOCKS Proxy not configured se muestra el mensaje. Si hay un SOCKS proxy configurado, se muestran el nombre del host y el puerto del proxy.</p>
Eliminar una configuración de SOCKS proxy	<p>Introduzca el número correspondiente para seleccionar Eliminar configuración de SOCKS proxy.</p> <p>Se muestra el mensaje SOCKS Proxy Configuration Removed .</p>

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

Configuración de red de la gateway

La configuración de red predeterminada para la puerta de enlace es el Protocolo de configuración dinámica de host (DHCP). Con DHCP, a su puerta de enlace 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.
 - VMware ESXi— para obtener más información, consulte [Acceder a la consola local de Gateway con VMware ESXi](#).
 - Microsoft Hyper-V: para obtener más información, consulte [Acceso a la consola local de la gateway con Microsoft Hyper-V](#).
 - KVM— para obtener más información, consulte [Acceso a la consola local de Gateway con Linux KVM](#).
2. En el menú principal AWS Storage Gateway - Configuración, introduzca el número correspondiente para seleccionar Configuración de red.
3. En el menú Configuración de red de AWS Storage Gateway, realice una de las siguientes tareas:


Para llevar a cabo esta tarea	Haga lo siguiente
Describir el adaptador de red	<p>Introduzca el número correspondiente para seleccionar Describir el adaptador.</p> <p>Aparecerá una lista de nombres de adaptador y se le pedirá que escriba el nombre de un adaptador por ejemplo, eth0. Si el adaptador que especifique está en uso, se mostrará la siguiente información acerca del adaptador:</p> <ul style="list-style-type: none"> • Dirección de control de acceso al medio (MAC) •

Para llevar a cabo esta tarea	Haga lo siguiente
	<p data-bbox="862 212 1036 243">Dirección IP</p> <ul data-bbox="829 275 1240 512" style="list-style-type: none"><li data-bbox="829 302 1084 333">• Máscara de red<li data-bbox="829 390 1240 422">• Dirección IP de la gateway<li data-bbox="829 478 1175 510">• DHCP estado activado <p data-bbox="829 621 1507 800">Al configurar una dirección IP estática o al configurar el adaptador predeterminado de la puerta de enlace, se utilizan los nombres de los adaptadores que aparecen aquí.</p>
Configurar DHCP	<p data-bbox="829 911 1442 989">Introduzca el número correspondiente para seleccionar Configurar DHCP.</p> <p data-bbox="829 1037 1487 1115">Se le solicitará que configure la interfaz de red que va a utilizar DHCP.</p>

Para llevar a cabo esta tarea	Haga lo siguiente
Configurar una dirección IP estática para la gateway	<p data-bbox="829 260 1442 342">Introduzca el número correspondiente para seleccionar Configurar IP estática.</p> <p data-bbox="829 388 1484 470">Se le pedirá que escriba la siguiente información para configurar una IP estática:</p> <ul data-bbox="829 520 1507 1071" style="list-style-type: none"><li data-bbox="829 520 1279 579">• Nombre del adaptador de red<li data-bbox="829 611 1032 669">• Dirección IP<li data-bbox="829 701 1084 760">• Máscara de red<li data-bbox="829 791 1433 850">• Dirección de la gateway predeterminada<li data-bbox="829 882 1507 984">• Dirección del servicio de nombres de dominio principal (DNS)<li data-bbox="829 1016 1227 1075">• DNS Dirección secundaria <div data-bbox="829 1209 1507 1619" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p data-bbox="857 1249 1047 1283">⚠ Important</p><p data-bbox="906 1306 1474 1581">Si la puerta de enlace ya se ha activado, debe cerrarla y reiniciarla desde la consola de Storage Gateway para que la configuración surta efecto. Para obtener más información, consulte Como apagar la MV de la gateway.</p></div> <p data-bbox="829 1724 1414 1803">Si su puerta de enlace utiliza más de una interfaz de red, debe configurar todas las</p>

Para llevar a cabo esta tarea	Haga lo siguiente
	<p>interfaces activadas para que utilicen direcciones IP DHCP estáticas.</p> <p>Por ejemplo, supongamos que la máquina virtual de la puerta de enlace utiliza dos interfaces configuradas como DHCP. Si más tarde establece una interfaz en una IP estática, la otra interfaz se desactivará. Para activar la interfaz en este caso, debe establecerla en una IP estática.</p> <p>Si ambas interfaces están configuradas inicialmente para usar direcciones IP estáticas y, a continuación, configuras la puerta de enlace para que se usen DHCP, se utilizarán ambas interfaces DHCP.</p>

Para llevar a cabo esta tarea	Haga lo siguiente
Configuración de un nombre de host para la puerta de enlace	<p data-bbox="829 226 1442 310">Introduzca el número correspondiente para seleccionar Configurar nombre de host.</p> <p data-bbox="829 352 1479 531">Se le solicitará que elija si la puerta de enlace utilizará un nombre de host estático que especifique o adquirirá uno automáticamente mediante rDCHP. DNS</p> <p data-bbox="829 573 1495 758">Si selecciona Estático, se le solicitará que proporcione un nombre de host estático, como <code>testgateway.example.com</code>. Introduzca y para aplicar la configuración.</p> <div data-bbox="829 800 1507 1304" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p data-bbox="857 835 976 869"> Note</p><p data-bbox="906 890 1474 1262">Si configura un nombre de host estático para la puerta de enlace, asegúrese de que el nombre de host proporcionado esté en el dominio al que está unida la puerta de enlace. También debe crear un registro A en su DNS sistema que apunte la dirección IP de la puerta de enlace a su nombre de host estático.</p></div>

Para llevar a cabo esta tarea	Haga lo siguiente
<p>Restablezca toda la configuración de red de la puerta de enlace a DHCP</p>	<p>Introduzca el número correspondiente para seleccionar Restablecer todo a DHCP.</p> <p>Todas las interfaces de red están configuradas para usarse DHCP.</p> <div data-bbox="829 541 1507 951" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Important</p><p>Si la puerta de enlace ya se ha activado, debe cerrarla y reiniciarla desde la consola de Storage Gateway para que la configuración surta efecto. Para obtener más información, consulte Como apagar la MV de la gateway.</p></div>
<p>Establecer el adaptador de ruta predeterminada del gateway</p>	<p>Introduzca el número correspondiente para seleccionar Establecer adaptador predeterminado.</p> <p>Se mostrarán los adaptadores disponibles para la puerta de enlace y se le pedirá que seleccione uno de los adaptadores, por ejemplo, eth0.</p>
<p>Vea la DNS configuración de su puerta de enlace</p>	<p>Introduzca el número correspondiente para seleccionar Ver DNS configuración.</p> <p>Se muestran las direcciones IP de los servidores de DNS nombres principal y secundario.</p>

Para llevar a cabo esta tarea	Haga lo siguiente
Ver tablas de ruteo	<p>Introduzca el número correspondiente para seleccionar Ver rutas.</p> <p>Se muestra la ruta predeterminada de la gateway.</p>

Prueba de conexión de la gateway a Internet

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

Para probar la conexión de la gateway a Internet

1. Inicie sesión en la consola local de la gateway.
 - VMwareESXi— para obtener más información, consulte [Acceder a la consola local de Gateway con VMware ESXi](#).
 - Microsoft Hyper-V: para obtener más información, consulte [Acceso a la consola local de la gateway con Microsoft Hyper-V](#).
 - KVM— para obtener más información, consulte [Acceso a la consola local de Gateway con Linux KVM](#).
2. En el menú principal AWS Storage Gateway - Configuración, introduzca el número correspondiente para seleccionar Probar conexión de red.

Si la puerta de enlace ya se ha activado, la prueba de conexión comienza inmediatamente. En el caso de las puertas de enlace que aún no se han activado, debe especificar el tipo de punto final y tal Región de AWS como se describe en los pasos siguientes.

3. Si la puerta de enlace aún no está activada, introduzca el número correspondiente para seleccionar el tipo de punto de conexión de la puerta de enlace.
4. Si ha seleccionado el tipo de punto final público, introduzca el número correspondiente para seleccionar el Región de AWS que desee probar. Para ver los puntos de enlace de AWS servicio compatibles Regiones de AWS y una lista de los que puede usar con Storage Gateway, consulte los [AWS Storage Gateway puntos de enlace y las cuotas](#) en Referencia general de AWS

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

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

Sincronización de la hora de la MV de la gateway

Una vez que la gateway esté implementada y en funcionamiento, es posible que en algunos casos la hora de la MV se desvíe. Por ejemplo, si hay una interrupción prolongada de la red y el host del hipervisor y la gateway no reciben actualizaciones de hora, la hora de la MV del 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.

En el caso de una puerta de enlace implementada en VMwareESXi, basta con configurar la hora del host del hipervisor y sincronizar la hora de la máquina virtual con el host para evitar desviaciones horarias. Para obtener más información, consulte [Sincronización de la hora de la máquina virtual y el host](#).

En el caso de gateways implementadas en Microsoft Hyper-V, debe comprobar periódicamente la hora de la MV. Para obtener más información, consulte [Sincronización de la hora de la MV de la gateway](#).

Ejecución de comandos de Storage Gateway en la consola local


La consola local de la máquina virtual de Storage Gateway contribuye a proporcionar un entorno seguro para la configuración y el diagnóstico de problemas de la puerta de enlace. Con los comandos de la consola local, puede realizar tareas de mantenimiento, como guardar tablas de enrutamiento, conectarse a AWS 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 cómo iniciar sesión en la consola VMware ESXi local, consulte [Acceder a la consola local de Gateway con VMware ESXi](#).
 - Para obtener más información sobre el inicio de sesión en la consola local de Microsoft Hyper-V, consulte [Acceso a la consola local de la gateway con Microsoft Hyper-V](#).
 - Para obtener más información sobre cómo iniciar sesión en la consola KVM local, consulte [Acceso a la consola local de Gateway con Linux KVM](#).
2. En el menú principal Activación de dispositivo de AWS - Configuración, introduzca el número correspondiente para seleccionar Consola de puerta de enlace.
 3. En la línea de comandos de la consola de la puerta de enlace, introduzca **h**.

La consola muestra el AVAILABLECOMMANDSmenú, que muestra los comandos disponibles:

Comando	Función
dig	Recopile los resultados de la excavación para DNS solucionar problemas.
exit	Volver al menú de configuración.
h	Mostrar la lista de comandos disponibles.
ifconfig	Visualizar o configurar las interfaces de red. <div data-bbox="836 1228 1510 1690" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Recomendamos configurar los ajustes de red o IP mediante la consola de Storage Gateway o la opción de menú de la consola local dedicada. Para obtener instrucciones, consulte Configuración de red de la puerta de enlace.</p> </div>
ip	Mostrar/manipular el enrutamiento, los dispositivos y los túneles.

Comando	Función
	<p> Note</p> <p>Recomendamos configurar los ajustes de red o IP mediante la consola de Storage Gateway o la opción de menú de la consola local dedicada. Para obtener instrucciones, consulte Configuración de red de la puerta de enlace.</p>
iptables	Herramienta de administración para el filtrado de IPv4 paquetes y NAT.
ncport	Prueba la conectividad a un TCP puerto específico de una red.
nping	Recopilar los resultados de nping para la solución de problemas de red.
open-support-channel	Connect to AWS Support.
passwd	Actualizar tokens de autenticación.
save-iptables	Mantener tablas de IP.
save-routing-table	Guardar una entrada de la tabla de enrutamiento recién agregada.

Comando	Función
sslcheck	Devuelve el resultado con el emisor del certificado
	<div data-bbox="834 352 1510 953" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p> Note</p> <p>Storage Gateway utiliza la verificación del emisor del certificado y no admite la inspección de SSL. Si este comando devuelve un emisor distinto de <code>aws-appliance@amazon.com</code>, es probable que se trate de una aplicación que esté realizando una inspección de SSL. En ese caso, se recomienda omitir la inspección SSL del dispositivo Storage Gateway.</p> </div>
tcptraceroute	Recopile la salida de traceroute sobre el TCP tráfico que se dirige a un destino.

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

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

Visualización del estado de los recursos de sistema de la gateway

Cuando se inicia la puerta de enlace, comprueba sus CPU núcleos virtuales, el tamaño del volumen raíz y 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

- Inicie sesión en la consola local de la gateway:

- Para obtener más información sobre cómo iniciar sesión en la VMware ESXi consola, consulte [Acceder a la consola local de Gateway con VMware ESXi](#).
 - Para obtener más información sobre el inicio de sesión en la consola local de Microsoft Hyper-V, consulte [Acceso a la consola local de la gateway con Microsoft Hyper-V](#).
 - Para obtener más información sobre cómo iniciar sesión en la consola KVM local, consulte [Acceso a la consola local de Gateway con Linux KVM](#).
2. En el menú principal Activación de dispositivo de AWS - Configuración, introduzca el número correspondiente para seleccionar Ver comprobación de recursos del sistema.

Cada recurso muestra [OK], [WARNING] o [FAIL], lo que indica el estado del recurso de la siguiente manera:

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

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

Configuración de adaptadores de red para la gateway

De forma predeterminada, Storage Gateway está configurado para usar el tipo de adaptador de red E1000, pero puede volver a configurar su puerta de enlace para usar 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 puerta de enlace para usar el adaptador de red VMXNET3](#)
- [Configuración de su puerta de enlace para varios NICs](#)

Configuración de la puerta de enlace para usar el adaptador de red VMXNET3

Storage Gateway admite el tipo de adaptador de red E1000 tanto en los hosts del VMware ESXi hipervisor Hyper-V de Microsoft. Sin embargo, el tipo de adaptador de red VMXNET3 (10 GbE) solo se admite en el VMware ESXi hipervisor. Si la puerta de enlace está alojada en un VMware ESXi hipervisor, puede volver a configurarla para que utilice el tipo de adaptador VMXNET3 (10 GbE). Para obtener más información sobre estos adaptadores, consulte [Elegir un adaptador de red para su máquina virtual en el sitio web](#) de Broadcom (VMware).

Important

Para seleccionarlo VMXNET3, el tipo de sistema operativo invitado debe ser Other Linux64.

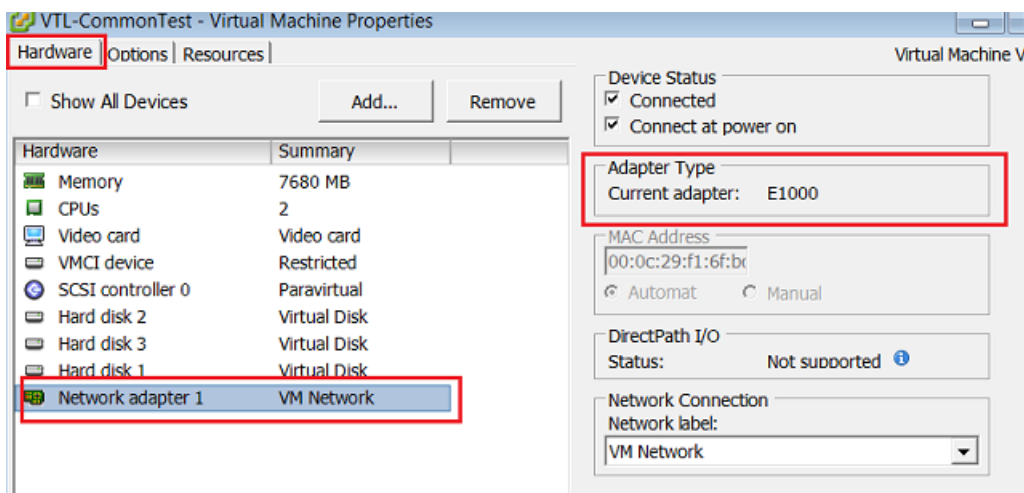
A continuación, se indican los pasos que debe seguir para configurar la puerta de enlace para que utilice el VMXNET3 adaptador:

1. Elimine el adaptador E1000 predeterminado.
2. Añada el VMXNET3 adaptador.
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 puerta de enlace para que utilice el VMXNET3 adaptador

1. EnVMware, abra el menú contextual (haga clic con el botón derecho) de su puerta de enlace y seleccione 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). Sustituirá este adaptador por el VMXNET3 adaptador.



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 el E1000 y los adaptadores de VMXNET3 red en la puerta de enlace 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 (Siguiete).
7. En el asistente de tipo de red, seleccione **VMXNET3** para Adapter Type (Tipo de adaptador) y, a continuación, elija Next (Siguiete).
8. En el asistente de propiedades de la máquina virtual, compruebe en la sección Tipo de adaptador que el adaptador actual esté configurado y VMXNET3, a continuación, pulse Aceptar.

9. En el VMware vSphere cliente, cierre la puerta de enlace.
10. En el VMware vSphere cliente, reinicie la puerta de enlace.

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 vSphere cliente, seleccione la pestaña 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 con las credenciales predeterminadas](#).
2. Cuando se le solicite, introduzca el número correspondiente para seleccionar Configuración de red.
3. Cuando se le solicite, escriba el número correspondiente para seleccionar Restablecer todo a yDHCP, a continuación, escriba **y** (sí) en el mensaje para configurar todos los adaptadores para que utilicen el Protocolo de configuración dinámica de host (DHCP). Todos los adaptadores disponibles están configurados para usarse DHCP.

Si la puerta de enlace 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 información sobre cómo probar la conexión de red, consulte [Prueba de conexión de la puerta de enlace a Internet](#).

Configuración de su puerta de enlace para varios NICs

Si configura la puerta de enlace para que utilice varios adaptadores de red (NICs), podrá acceder a ella desde más de una dirección IP. Es posible que desee hacerlo en las siguientes situaciones:

- Maximización del rendimiento: quizá desee maximizar el rendimiento para una gateway cuando los adaptadores de red sean un cuello de botella.
- Separación de aplicaciones: quizá necesite separar la manera en que las aplicaciones escriben en los volúmenes de una puerta de enlace. Por ejemplo, quizá desee que una aplicación de almacenamiento crítica utilice exclusivamente un adaptador determinado definido para la gateway.

- **Restricciones de la red:** el entorno de su aplicación puede requerir que mantenga SCSI los destinos i y los iniciadores que se conectan a ellos en una red aislada distinta de la red con AWS la que se comunica la puerta de enlace.

En un caso de uso típico de varios adaptadores, un adaptador está configurado como la ruta por la que se comunica la puerta de enlace AWS (es decir, como la puerta de enlace predeterminada). A excepción de este adaptador, los iniciadores deben estar en la misma subred que el adaptador que contiene los SCSI destinos i a los que se conectan. De lo contrario, puede que la comunicación con los objetivos reales no sea posible. Si un destino está configurado en el mismo adaptador con el que se utiliza para la comunicación AWS, el SCSI tráfico de ese destino y el AWS tráfico fluirán a través del mismo adaptador.

Cuando configure un adaptador para conectarse a la consola de Storage Gateway y, a continuación, agregue un segundo adaptador, Storage Gateway configurará automáticamente la tabla de enrutamiento para que utilice el segundo adaptador como ruta preferida. Para obtener instrucciones sobre cómo configurar varios adaptadores, consulte las secciones siguientes.

- [Configuración de su puerta de enlace para varios NICs en un VMware ESXi host](#)
- [Configuración de su puerta de enlace para varios NICs servidores en Microsoft Hyper-V](#)

Realización de tareas en la consola EC2 local de Amazon

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

Temas

- [Inicio de sesión en la consola local de Amazon EC2 Gateway](#)
- [Enrutar la puerta de enlace implementada EC2 a través de un HTTP proxy](#)
- [Probar la conexión de red de la puerta de enlace](#)
- [Visualización del estado de los recursos de sistema de la puerta de enlace](#)
- [Ejecución de comandos de Storage Gateway en la consola local](#)

Inicio de sesión en la consola local de Amazon EC2 Gateway

Puedes conectarte a tu EC2 instancia de Amazon mediante un cliente Secure Shell (SSH). Para obtener información detallada, consulte [Connect to Your Instance](#) en la Guía del EC2 usuario de Amazon. Para conectarte de esta manera, necesitarás el SSH key pair que especificaste al lanzar la instancia. Para obtener información sobre los pares de EC2 claves de Amazon, consulte [Amazon EC2 Key Pairs](#) en la Guía del EC2 usuario de Amazon.

Para iniciar sesión en la consola local de la gateway

1. Inicie sesión en la consola local. Si te conectas a la EC2 instancia desde un ordenador con Windows, inicia sesión como administrador.
2. Tras iniciar sesión, verá el menú principal AWS Storage Gateway - Configuración, desde el que puede realizar diversas tareas.

Para obtener información sobre esta tarea	Consulte este tema
Configura un SOCKS proxy para tu puerta de enlace	Enrutar la puerta de enlace implementada EC2 a través de un HTTP proxy
Probar la conectividad de red	Probar la conexión de red de la puerta de enlace
Ejecute los comandos de la consola de Storage Gateway	Ejecución de comandos de Storage Gateway en la consola local
Ver una comprobación de recursos del sistema	Visualización del estado de los recursos de sistema de la puerta de enlace.

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

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

Enrutar la puerta de enlace implementada EC2 a través de un HTTP proxy

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

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

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

1. Inicie sesión en la consola local de la gateway. Para obtener instrucciones, consulte [Inicio de sesión en la consola local de Amazon EC2 Gateway](#).
2. En el menú principal Activación y configuración del AWS dispositivo, introduzca el número correspondiente para seleccionar Configurar HTTP proxy.
3. En el menú de configuración del HTTP proxy de activación del AWS dispositivo, introduzca el número correspondiente a la tarea que desee realizar:
 - Configurar el HTTP proxy: deberá proporcionar un nombre de host y un puerto para completar la configuración.
 - Ver la configuración de HTTP proxy actual: si no hay ningún HTTP proxy configurado, HTTP Proxy not configured se muestra el mensaje. Si hay un HTTP proxy configurado, se muestran el nombre de host y el puerto del proxy.
 - Eliminar una configuración de HTTP proxy: HTTP Proxy Configuration Removed se muestra el mensaje.

Probar la conexión de red de la puerta de enlace

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

Para probar la conexión de red de la puerta de enlace

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

Si la puerta de enlace ya se ha activado, la prueba de conexión comienza inmediatamente. En el caso de las puertas de enlace que aún no se han activado, debe especificar el tipo de punto final y tal Región de AWS como se describe en los pasos siguientes.

3. Si la puerta de enlace aún no está activada, introduzca el número correspondiente para seleccionar el tipo de punto de conexión de la puerta de enlace.
4. Si ha seleccionado el tipo de punto final público, introduzca el número correspondiente para seleccionar el Región de AWS que desee probar. Para ver los puntos de enlace de AWS servicio compatibles Regiones de AWS y una lista de los que puede usar con Storage Gateway, consulte los [AWS Storage Gateway puntos de enlace y las cuotas](#) en. Referencia general de AWS

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

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

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

Cuando se inicia la puerta de enlace, comprueba sus CPU núcleos virtuales, el tamaño del volumen raíz y 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 Amazon EC2 Gateway](#).
2. En el menú principal Activación de dispositivo de AWS - Configuración, introduzca el número correspondiente para seleccionar Ver comprobación de recursos del sistema.

Cada recurso muestra [OK], [WARNING] o [FAIL], lo que indica el estado del recurso de la siguiente manera:

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

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



Ejecución de comandos de Storage Gateway en la consola local

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

Para ejecutar un comando de configuración o diagnóstico

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

La consola muestra el AVAILABLECOMMANDSmenú, que muestra los comandos disponibles:

Comando	Función
dig	Recopile los resultados de la excavación para DNS solucionar problemas.
exit	Volver al menú de configuración.
h	Mostrar la lista de comandos disponibles.
ifconfig	Visualizar o configurar las interfaces de red. <div data-bbox="834 621 1507 932"><p> Note Recomendamos configurar los ajustes de red o IP mediante la consola de Storage Gateway o la opción de menú de la consola local dedicada.</p></div>
ip	Mostrar/manipular el enrutamiento, los dispositivos y los túneles. <div data-bbox="834 1098 1507 1409"><p> Note Recomendamos configurar los ajustes de red o IP mediante la consola de Storage Gateway o la opción de menú de la consola local dedicada.</p></div>
iptables	Herramienta de administración para el filtrado de IPv4 paquetes y NAT.
ncport	Pruebe la conectividad a un TCP puerto específico de una red.
nping	Recopilar los resultados de nping para la solución de problemas de red.

Comando	Función
open-support-channel	Connect to AWS Support.
save-iptables	Mantener tablas de IP.
save-routing-table	Guardar una entrada de la tabla de enrutamiento recién agregada.
sslcheck	Compruebe SSL la validez para solucionar problemas de red.
tcptraceroute	Recopile la salida del traceroute sobre el TCP tráfico hacia un destino.

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

Para obtener información sobre un comando, introduzca el nombre del comando seguido de la opción `-h` (por ejemplo, `sslcheck -h`).

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

Temas

- [Acceso a la consola local de Gateway con Linux KVM](#)
- [Acceder a la consola local de Gateway con VMware ESXi](#)
- [Acceso a la consola local de la gateway con Microsoft Hyper-V](#)

Acceso a la consola local de Gateway con Linux KVM

Existen diferentes formas de configurar las máquinas virtuales en las que se estén ejecutando KVM, según la distribución de Linux que se utilice. A continuación se indican las instrucciones para acceder

a las opciones de KVM configuración desde la línea de comandos. Las instrucciones pueden variar en función de KVM la implementación.

Para acceder a la consola local de su puerta de enlace con KVM

1. Utilice el siguiente comando para enumerar las VMs que están disponibles actualmente enKVM.

```
# virsh list
```

Puede elegir entre disponibles VMs medianteId.

```
[root@localhost vms]# virsh list
 Id   Name          State
-----
 7    SGW_KVM       running

[root@localhost vms]# virsh console 7
```

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

```
# virsh console VM_Id
```

```
[root@localhost vms]# virsh console 7
Connected to domain SGW_KVM
Escape character is ^]

AWS Appliance

Login to change your network configuration and other settings.
localhost login: _
```

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


```
AWS Appliance Activation - Configuration

#####
## Currently connected network adapters:
##
## eth0: 10.0.3.32
#####

1: HTTP/SOCKS Proxy Configuration
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: System Time Management
6: License Information
7: Command Prompt

0: Get activation key

Press "x" to exit session

Enter command: _
```

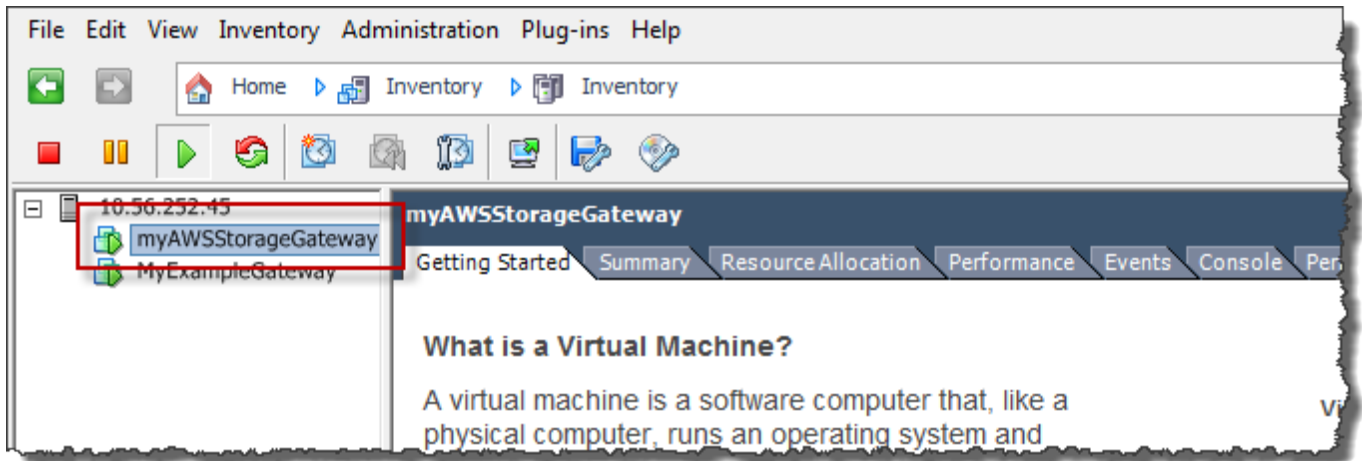
Acceder a la consola local de Gateway con VMware ESXi

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

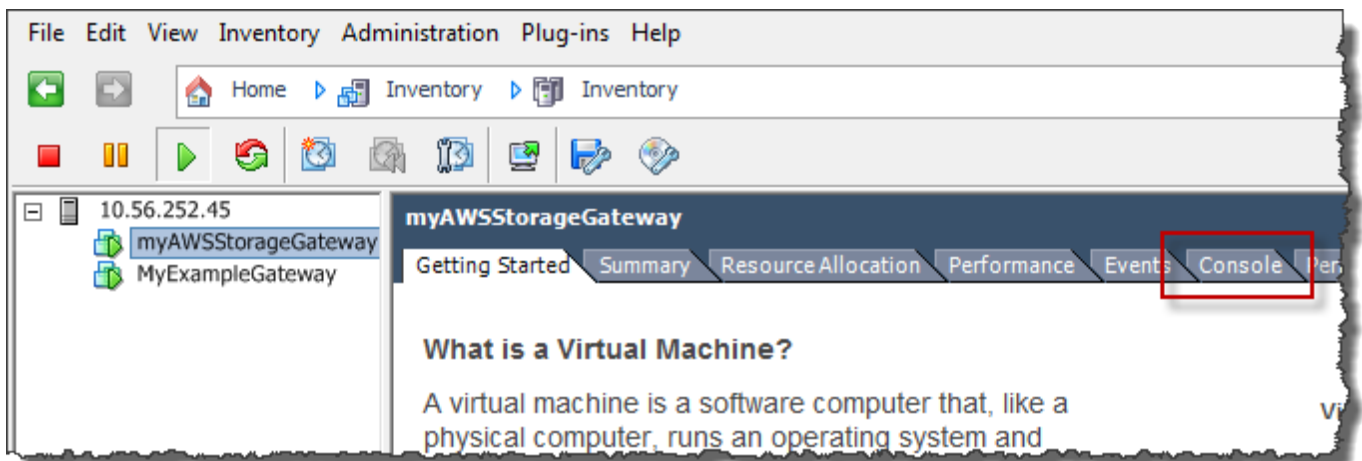
1. En el VMware vSphere cliente, seleccione la máquina virtual de su puerta de enlace.
2. Asegúrese de que la puerta de enlace esté encendida.

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.

```
AWS Storage Gateway

Login to change your network configuration and other gateway settings.

For more information, please see:
https://docs.aws.amazon.com/console/storagegateway/LocalConsole

localhost login: _
```

4. Para iniciar sesión con las credenciales predeterminadas, siga el procedimiento [Inicio de sesión en la consola local con las credenciales predeterminadas](#).

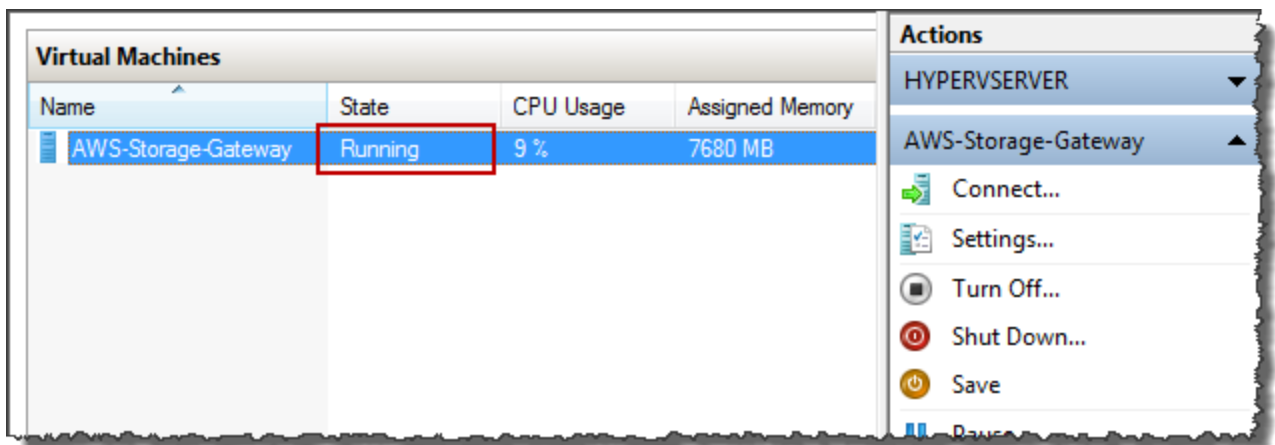
Acceso a la consola local de la gateway con Microsoft Hyper-V

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 puerta de enlace esté encendida.

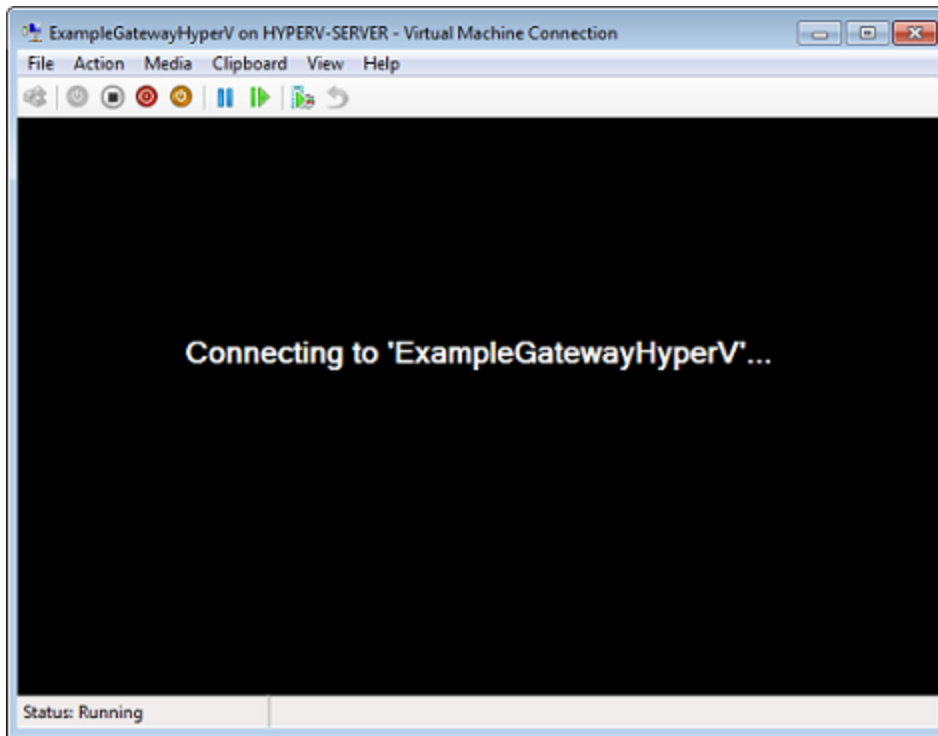
Note

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 las credenciales proporcionados por el administrador del hipervisor.



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

```
AWS Storage Gateway

Login to change your network configuration and other gateway settings.

For more information, please see:
https://docs.aws.amazon.com/console/storagegateway/LocalConsole

localhost login: _
```

4. Para iniciar sesión con las credenciales predeterminadas, siga el procedimiento [Inicio de sesión en la consola local con las credenciales predeterminadas](#).

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 su puerta de enlace para varios NICs en un VMware ESXi host](#)
- [Configuración de su puerta de enlace para varios NICs servidores en Microsoft Hyper-V](#)

Configuración de su puerta de enlace para varios NICs en un VMware ESXi host

En el siguiente procedimiento se supone que la máquina virtual de puerta de enlace ya tiene definido un adaptador de red y se describe cómo añadir un adaptador VMware ESXi.

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

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


La MV puede mantenerse activada para este procedimiento.

3. En el cliente, abra el menú contextual (haga clic con el botón derecho) de la MV de la gateway y elija Edit Settings (Editar configuración).
4. En la pestaña Hardware del cuadro de diálogo Virtual Machine Properties (Propiedades de la MV), elija Add (Agregar) para agregar un dispositivo.
5. Siga el asistente para agregar hardware para agregar un adaptador de red.
 - a. En el panel Device Type (Tipo de dispositivo), elija Ethernet Adapter (Adaptador de Ethernet) para agregar un adaptador y, a continuación, elija Next (Siguiente).
 - b. En el panel Network Type (Tipo de red), asegúrese de que se haya seleccionado Connect at power on (Conectar al inicio) para Type (Tipo) y, a continuación, elija Next (Siguiente).

Se recomienda utilizar el adaptador de VMXNET3 red con Storage Gateway. Para obtener más información sobre los tipos de adaptadores que pueden aparecer en la lista de adaptadores, consulte los tipos de adaptadores de red en la [ESXi documentación vCenter del servidor](#).

- c. En el panel Ready to Complete (Listo para completar), revise la información y, a continuación, elija Finish (Finalizar).
6. Elija la pestaña Resumen de la VM y elija Ver todo junto al cuadro Dirección IP. En la ventana Direcciones IP de máquina virtual se muestran todas las direcciones IP que se pueden utilizar

para obtener acceso a la puerta de enlace. Confirme que aparece una segunda dirección IP para la gateway.

 Note

Pueden pasar unos momentos hasta que los cambios del adaptador surtan efecto y el resumen de información de la MV se actualice.

7. En la consola de Storage Gateway, active la puerta de enlace.
8. En el panel Navegación de la consola de Storage Gateway, elija Puertas de enlace y elija la puerta de enlace a la que ha agregado el adaptador. Confirme que la segunda dirección IP aparece en la pestaña Details.

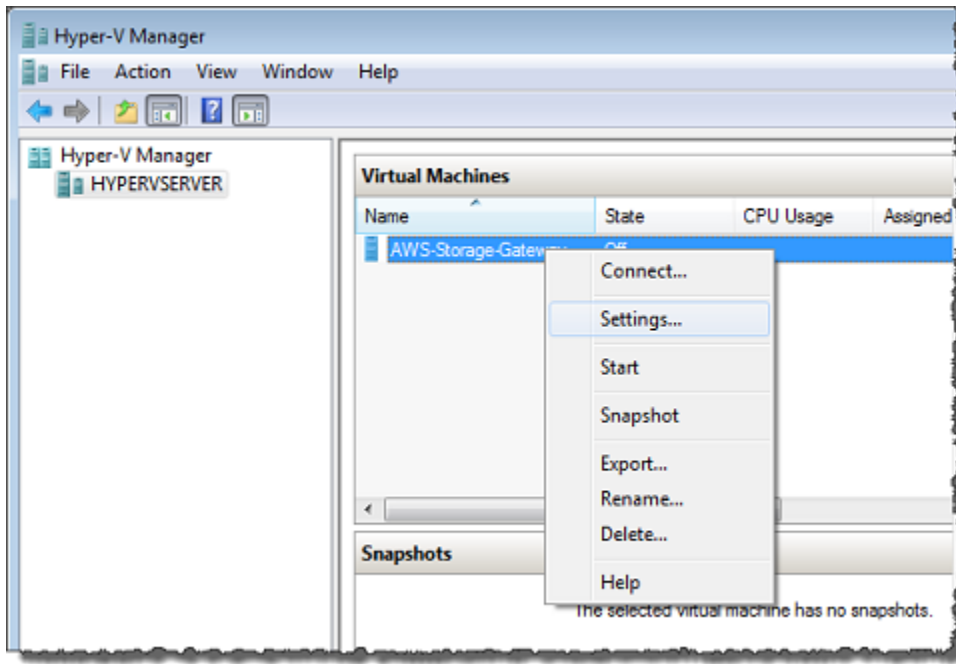
Para obtener información sobre las tareas de la consola local comunes a VMware Hyper-V y a los KVM hosts, consulte [Realización de tareas en la consola local de la MV de](#)

Configuración de su puerta de enlace para varios NICs servidores en Microsoft Hyper-V

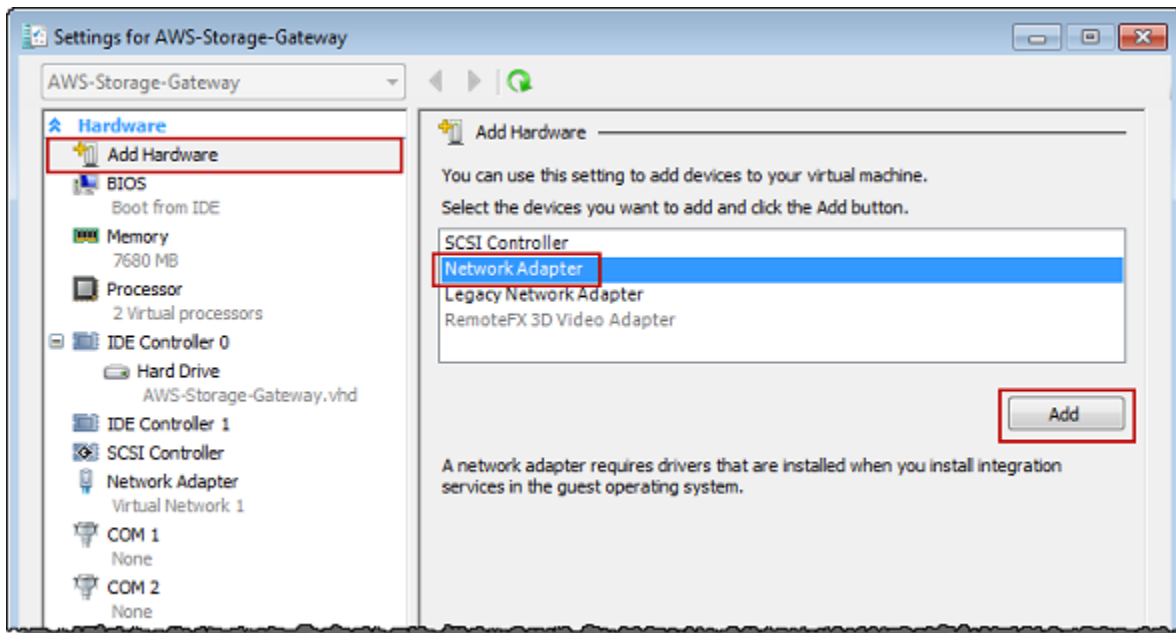
En el siguiente procedimiento se supone que la MV de la gateway ya tiene un adaptador de red definido y que está agregando un segundo adaptador. Este procedimiento muestra cómo añadir un adaptador para el host Microsoft Hyper-V.

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

1. En la consola de Storage Gateway, desactive la puerta de enlace. Para obtener instrucciones, consulte [Para detener una puerta de enlace de cinta](#).
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.

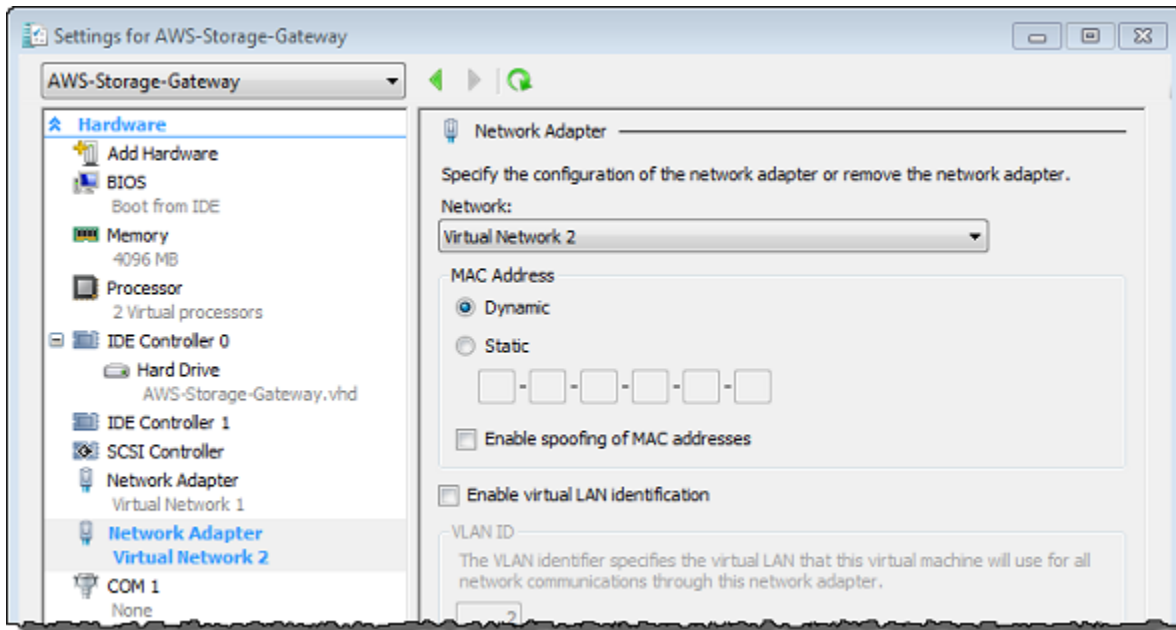


5. En el cuadro de diálogo Settings de la MV, para Hardware, elija Add Hardware.
6. En el panel Add Hardware, elija Network Adapter y, a continuación, elija Add para agregar un dispositivo.



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 puerta de enlace. Para obtener instrucciones, consulte [Para iniciar una puerta de enlace de cinta](#).
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.

Note

Los ejemplos de comandos de montaje que se proporcionan en la página de información de un recurso compartido de archivos en la consola de Storage Gateway siempre incluirán la dirección IP del adaptador de red que se agregó más recientemente a la puerta de enlace asociada al recurso compartido de archivos.

Para obtener información sobre las tareas de la consola local que son comunes a VMware Hyper-V y a los hosts, consulte KVM [Realización de tareas en la consola local de la MV de](#)

Eliminar la puerta de enlace y eliminar 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 planea continuar utilizando y ayuda a reducir la factura mensual.

Al eliminar una puerta de enlace, deja de aparecer en la consola AWS Storage Gateway de administración y su SCSI conexión con el 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.

Note

Al eliminar una puerta de enlace de cintas, también se eliminan todas las cintas que se encuentren actualmente en ese AVAILABLE estado y se pierden todos los datos de esas cintas. Si desea conservar los datos de las cintas utilizadas por una puerta de enlace que desee eliminar, debe archivar las cintas antes de eliminar la puerta de enlace. Para obtener más información, consulte [Archivado de cintas virtuales](#).

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

Temas

- [Eliminación de la puerta de enlace mediante la consola de Storage Gateway](#)
- [Eliminación de recursos de una gateway implementada on-premises](#)
- [Eliminar recursos de una puerta de enlace implementada en una EC2 instancia de Amazon](#)

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

El procedimiento para eliminar una gateway es el mismo para todos los tipos de gateway. Sin embargo, según el tipo de gateway que desee eliminar y el host en el que se haya implementado la

gateway, es posible que tenga que realizar tareas adicionales para eliminar los recursos asociados a la gateway. La eliminación de estos recursos le ayudará a evitar pagar por recursos que no planea utilizar.

Note

En el caso de las puertas de enlace implementadas en una EC2 instancia de Amazon, la instancia seguirá existiendo hasta que la elimine.

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

Para eliminar una gateway

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

Warning

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

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

⚠ Important

Ya no paga cargos de software después de eliminar una puerta de enlace, pero recursos como las cintas virtuales, las instantáneas de Amazon Elastic Block Store (AmazonEBS) y las EC2 instancias de Amazon persisten. Estos recursos se le seguirán facturando. Puedes optar por eliminar las EC2 instancias de Amazon y las EBS instantáneas de Amazon cancelando tu suscripción a AmazonEC2. Si quieres conservar tu EC2 suscripción a Amazon, puedes eliminar tus EBS instantáneas de Amazon desde la EC2 consola de Amazon.

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 puerta de enlace de cinta implementada en una VM

Al eliminar una puerta de enlace (biblioteca de cintas virtualesVTL), se realizan pasos de limpieza adicionales antes y después de eliminar la puerta de enlace. Estos pasos adicionales le ayudan a eliminar los recursos que no necesite para que no tenga que continuar pagando por ellos.

Si la puerta de enlace de cinta que desea eliminar está implementada en una máquina virtual (VM), le sugerimos que realice las acciones siguientes para limpiar los recursos.

⚠ Important

Antes de eliminar una puerta de enlace de cinta, debe cancelar todas las operaciones de recuperación de cintas y extraer todas las cintas recuperadas.

Una vez eliminada la puerta de enlace de cinta, debe eliminar cualquier recurso asociado a ella que no necesite, para evitar pagar por ellos.

Al eliminar una puerta de enlace de cinta, se encontrará en una de dos posibles situaciones.

- La puerta de enlace de cinta está conectada a AWS: si la puerta de enlace de cinta está conectada a AWS y usted la elimina, los SCSI destinos i asociados a la puerta de enlace (es decir, las unidades de cinta virtuales y el cambiador de medios) dejarán de estar disponibles.

- La puerta de enlace de cinta no está conectada a AWS: si la puerta de enlace de cinta no está conectada a AWS, por ejemplo, si la máquina virtual subyacente está apagada o la red no funciona, no podrá eliminar la puerta de enlace. Si intenta hacerlo, una vez que el entorno vuelva a funcionar, es posible que tenga una puerta de enlace de cinta ejecutándose localmente con SCSI destinos i disponibles. Sin embargo, no se cargarán ni descargarán datos de Tape Gateway. AWS

Si la puerta de enlace de cinta que desea eliminar no funciona, primero debe desactivarla como se describe a continuación:

- Para eliminar las cintas que tienen ese RETRIEVED estado de la biblioteca, extraiga la cinta con el software de respaldo. Para obtener instrucciones, consulte [Archivado de la cinta](#).

Tras desactivar la puerta de enlace de cinta y eliminar las cintas, puede eliminar la puerta de enlace de cinta. Para obtener instrucciones sobre cómo eliminar una gateway, consulte [Eliminación de la puerta de enlace mediante la consola de Storage Gateway](#).

Si tiene cintas archivadas, estas cintas se mantendrán y continuará pagando por el almacenamiento hasta que las elimine. Para obtener instrucciones sobre cómo eliminar cintas de un archivo, consulte [Eliminar cintas virtuales de la puerta de enlace de cintas](#).

Important

Se le cobrará un mínimo de 90 días de almacenamiento por las cintas virtuales que se encuentren en un archivo. Si recupera una cinta virtual que haya estado almacenada en el archivo durante menos de 90 días, se le seguirá cobrando por 90 días de almacenamiento.

Eliminar recursos de una puerta de enlace implementada en una EC2 instancia de Amazon

Si desea eliminar una puerta de enlace que implementó en una EC2 instancia de Amazon, le recomendamos que limpie AWS los recursos que se usaron con la puerta de enlace, específicamente la EC2 instancia de Amazon, cualquier EBS volumen de Amazon y también las cintas si implementó una puerta de enlace de cinta. Así contribuirá a evitar cargos por uso no deseados.

Eliminar recursos de su puerta de enlace de cinta implementada en Amazon EC2

Si ha implementado una puerta de enlace de cinta, le sugerimos que haga lo siguiente para eliminar la puerta de enlace y limpiar los recursos:

1. Elimine todas las cintas virtuales que haya recuperado en la puerta de enlace de cinta. Para obtener más información, consulte [Eliminar cintas virtuales de la puerta de enlace de cintas](#).
2. Elimine todas las cintas virtuales de la biblioteca de cintas. Para obtener más información, consulte [Eliminar cintas virtuales de la puerta de enlace de cintas](#).
3. Elimine la puerta de enlace de cinta. Para obtener más información, consulte [Eliminación de la puerta de enlace mediante la consola de Storage Gateway](#).
4. Termina todas las EC2 instancias de Amazon y elimina todos los EBS volúmenes de Amazon. Para obtener más información, consulta [Limpiar tu instancia y volumen](#) en la Guía del EC2 usuario de Amazon.
5. Elimine todas las cintas virtuales archivadas. Para obtener más información, consulte [Eliminar cintas virtuales de la puerta de enlace de cintas](#).

Important

Se le cobrará un mínimo de 90 días de almacenamiento por las cintas virtuales que se encuentren en el archivo. Si recupera una cinta virtual que haya estado almacenada en el archivo durante menos de 90 días, se le seguirá cobrando por 90 días de almacenamiento.

Rendimiento y optimización para Tape Gateway

En esta sección se describe el rendimiento de Storage Gateway.

Temas

- [Directrices de rendimiento para las puertas de enlace de cinta](#)
- [Optimización del rendimiento de la gateway](#)
- [Uso de la VMware vSphere alta disponibilidad con Storage Gateway](#)

Directrices de rendimiento para las puertas de enlace de cinta

En esta sección, encontrará directrices de configuración para aprovisionar hardware para su máquina virtual de puerta de enlace de cinta. Los tamaños y tipos de EC2 instancias de Amazon que se muestran en la tabla son ejemplos y se proporcionan como referencia.

Configuración	Rendimiento de escritura en Gbps	Rendimiento de lectura de caché en Gbps	Lea desde Gbps de rendimiento de Amazon Web Services Cloud
Plataforma de alojamiento: EC2 instancia de Amazon: c5.4xlarge CPU: 16 v CPU RAM: 32 GB Disco raíz: 80 GB, io1SSD, 4.000 IOPS Disco caché: rayado RAID (2 x 500 GB, io1, 25000) EBS SSD IOPs Disco de búfer de carga: 450 GB, io1, 2000 SSD IOPs Ancho de banda de red para la nube: 10 Gbps	2.3	4.0	2.2

Configuración	Rendimiento de escritura en Gbps	Rendimiento de lectura de caché en Gbps	Lea desde Gbps de rendimiento de Amazon Web Services Cloud
Plataforma de host: dispositivo de hardware de Storage Gateway Disco en caché: 2,5 TB Disco de búfer de carga: 2 TB Ancho de banda de red para la nube: 10 Gbps	2.3	8.8	3.8
Plataforma de alojamiento: Amazon EC2instance — c5d.9xlarge CPU: 36 v 72 GB CPU RAM Disco raíz: 80 GB, io1SSD, 4.000 IOPS Disco caché: disco de 900 GB NVMe Disco de búfer de carga: NVMe disco de 900 GB Ancho de banda de red para la nube: 10 Gbps	5.2	11.6	5.2

Configuración	Rendimiento de escritura en Gbps	Rendimiento de lectura de caché en Gbps	Lea desde Gbps de rendimiento de Amazon Web Services Cloud
Plataforma de alojamiento: Amazon EC2instance — c5d.metal CPU: 96 V CPU RAM: 192 GB Disco raíz: 80 GB, io1SSD, 4.000 IOPS Disco caché: rayado RAID (2 discos de 900 GBNVMe) Disco de búfer de carga: disco de 900 GB NVMe Ancho de banda de red para la nube: 10 Gbps	5.2	11.6	7.2

Note

Este rendimiento se ha logrado utilizando un tamaño de bloque de 1 MB y diez unidades de cinta al mismo tiempo.

Las EC2 configuraciones de la tabla anterior solo pretenden ser representativas del rendimiento que podría alcanzar en sus propios servidores físicos con recursos similares. Por ejemplo, las EC2 configuraciones con bandas RAID se realizaron mediante un mecanismo especial que, por lo general, no es compatible con nuestra puerta de enlaceEC2. Para lograr un rendimiento similar, debería utilizar en su lugar un RAID controlador de hardware conectado al servidor local en el que se ejecuta la puerta de enlace.

El rendimiento puede variar en función de la configuración de la plataforma de host y el ancho de banda de la red.

Para mejorar el rendimiento de escritura y lectura de la puerta de enlace de cinta, consulte [Optimiza la configuración de TI SCSI](#), [Utilice un tamaño de bloques mayor para las unidades de cinta](#) y [Optimice el rendimiento de las unidades de cinta virtuales en el software de copia de seguridad](#).

Optimización del rendimiento de la gateway

Configuración recomendada del servidor de la puerta de enlace

Para obtener el mejor rendimiento de la puerta de enlace, Storage Gateway recomienda la siguiente configuración de puerta de enlace para el servidor host de la puerta de enlace:

- Al menos 64 núcleos físicos CPU dedicados
- En el caso de Tape Gateway , su hardware debe dedicar las siguientes cantidades de RAM:
 - Al menos 16 GiB reservados RAM para pasarelas con un tamaño de caché de hasta 16 TiB
 - Al menos 32 GiB reservados RAM para pasarelas con un tamaño de caché de 16 TiB a 32 TiB
 - Al menos 48 GiB reservados RAM para pasarelas con un tamaño de caché de 32 TiB a 64 TiB

Note

Para un rendimiento óptimo de la puerta de enlace, debe aprovisionar al menos 32 GiB de RAM

- Disco 1, que se utilizará como caché de puerta de enlace de la siguiente manera:
 - Rayado RAID (conjunto redundante de discos independientes) compuesto por. NVMe SSDs
- Disco 2, que se utilizará como búfer de carga de la puerta de enlace de la siguiente manera:
 - A rayas RAID compuesto por. NVMe SSDs
- Disco 3, que se utilizará como búfer de carga de la puerta de enlace de la siguiente manera:
 - A rayas RAID compuesto por. NVMe SSDs
- Adaptador de red 1 configurado en red de MV 1:
 - Utilice la red VM 1 y añada VMXnet3 (10 Gbps) para utilizarla en la ingestión.
- Adaptador de red 2 configurado en red de MV 2:
 - Utilice la red VM 2 y añada una VMXnet3 (10 Gbps) para conectarla. AWS

Añada recursos a la gateway

Los siguientes obstáculos pueden reducir el rendimiento de su Tape Gateway por debajo del rendimiento máximo sostenido teórico (su ancho de banda a la nube): AWS

- CPU Recuento de núcleos
- Rendimiento del disco de búfer de carga/caché
- RAM Importe total
- Ancho de banda de red para AWS
- Ancho de banda de la red desde el iniciador hasta la puerta de enlace

Esta sección contiene los pasos que puede seguir para optimizar el rendimiento de su puerta de enlace. Esta orientación se basa en la adición de recursos a la puerta de enlace o al servidor de aplicaciones.

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

Rendimiento del disco de búfer de carga y caché puede limitar el rendimiento de carga y descarga de la puerta de enlace. Si la puerta de enlace presenta un rendimiento muy inferior al esperado, considere la posibilidad de mejorar el rendimiento del disco de búfer de carga y caché de la siguiente manera:

- Usar una banda RAID como RAID 10 para mejorar el rendimiento del disco, idealmente con un controlador de hardware RAID.


Note

RAID (matriz redundante de discos independientes) o, específicamente, RAID configuraciones divididas en discos, como RAID 10, es el proceso de dividir un conjunto de datos en bloques y distribuirlos entre varios dispositivos de almacenamiento. El RAID nivel que utilice afectará a la velocidad exacta y a la tolerancia a errores que podrá alcanzar. Al dividir las cargas de trabajo de E/S en varios discos, el rendimiento general del RAID dispositivo es mucho mayor que el de cualquier disco de un solo miembro.

- Uso de discos de alto rendimiento conectados directamente

Para optimizar el rendimiento de la puerta de enlace, puede añadir discos de alto rendimiento, como unidades de estado sólido (SSDs) y una controladora NVMe. También puede conectar discos virtuales a su máquina virtual directamente desde una red de área de almacenamiento (SAN) en lugar de Microsoft Hyper-VNTFS. La mejora del rendimiento del disco generalmente se traduce en un mejor rendimiento y en más operaciones de entrada/salida por segundo (IOPS).

Para medir el rendimiento, usa las métricas `WriteBytes` y `ReadBytes` con la estadística `CloudWatch Samples` de Amazon. Por ejemplo, la estadística `ReadBytes` sobre un período de muestra de 5 minutos dividido entre 300 segundos da como resultado la IOPS. Como regla general, cuando revise estas métricas para una puerta de enlace, busque un rendimiento bajo y tendencias bajas para indicar los cuellos de botella relacionados con los discos. Para obtener más información sobre métricas de puerta de enlace, consulte [Medición del rendimiento entre su puerta de enlace de cinta y AWS](#).

 Note

CloudWatch las métricas no están disponibles para todas las pasarelas. Para obtener información sobre métricas de puertas de enlace, consulte [Supervisión de Storage Gateway](#).

Adición de más discos del búfer de carga

Para lograr un mayor rendimiento de escritura, añade al menos dos discos del búfer de carga. Cuando los datos se escriben en la puerta de enlace, se escriben y almacenan localmente en los discos del búfer de carga. Posteriormente, los datos locales almacenados se leen de forma asíncrona desde los discos que se van a procesar y cargar en AWS. Añadir más discos del búfer de carga puede reducir la cantidad de operaciones de E/S simultáneas que se realizan en cada disco individual. Esto puede provocar un aumento del rendimiento de escritura en la puerta de enlace.

Respalde los discos virtuales de la gateway con discos físicos independientes

Cuando aprovisiones discos para una puerta de enlace, le recomendamos encarecidamente que no aprovisiones discos locales para el búfer de carga y el almacenamiento en caché que utilicen el mismo disco de almacenamiento físico subyacente. Por ejemplo, para VMware ESXi, los recursos de almacenamiento físico subyacentes se representan como un almacén de datos.

Al implementar la máquina virtual de gateway, debe elegir el almacén de datos en el que se almacenarán los archivos de la máquina virtual. Cuando aprovisiona 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 RAID configuración de menor rendimiento, como RAID 1 o RAID 6, puede provocar un rendimiento deficiente.

Añada CPU recursos al host de su puerta de enlace

El requisito mínimo para un servidor de alojamiento de gateway son cuatro procesadores virtuales. Para optimizar el rendimiento de la puerta de enlace, confirme que cada procesador virtual asignado a la máquina virtual de puerta de enlace esté respaldado por un CPU núcleo dedicado. Además, confirme que no está sobresuscribiendo la CPUs del servidor host.

Cuando agrega más CPUs al servidor host de la puerta de enlace, aumenta la capacidad de procesamiento de la puerta de enlace. De este modo, la puerta de enlace es capaz de realizar en paralelo el almacenamiento de datos de la aplicación en el almacenamiento local y la carga de dichos datos en Amazon S3. Además, CPUs también ayudan a garantizar que su puerta de enlace reciba suficientes CPU recursos cuando el host se comparte con otros VMs. Proporcionar CPU recursos suficientes tiene el efecto general de mejorar el rendimiento.

Aumente el ancho de banda entre la puerta de enlace y la nube de AWS

Al aumentar el ancho de banda hacia y desde la nube, AWS aumentará la velocidad máxima de entrada de datos a su puerta de enlace y salida a la nube. Esto puede mejorar el rendimiento de la puerta de enlace si la velocidad de la red es el factor limitante de la configuración de la puerta de enlace, en lugar de otros factores, como la lentitud de los discos o el bajo ancho de banda de conexión del iniciador de la puerta de enlace.

El ancho de banda de la red de ida y AWS vuelta define el rendimiento medio máximo teórico de su Tape Gateway durante cargas de trabajo sostenidas.

- La velocidad media a la que puede escribir datos en la puerta de enlace de cinta durante intervalos prolongados no superará el ancho de banda de carga a AWS.

- La velocidad media a la que puede leer los datos de su Tape Gateway durante intervalos prolongados no superará el ancho de banda de descarga. AWS

Note

Es probable que el rendimiento observado de la puerta de enlace sea inferior al ancho de banda de la red debido a otros factores limitantes que se enumeran aquí, como el rendimiento del disco con búfer de carga y caché, el número de CPU núcleos, la RAM cantidad total o el ancho de banda entre el iniciador y la puerta de enlace. Además, el funcionamiento normal de la puerta de enlace implica la adopción de muchas medidas para proteger los datos, lo que puede provocar que el rendimiento observado sea inferior al ancho de banda de la red.

Optimiza la configuración de TI SCSI

Puede optimizar la SCSI configuración i de su SCSI iniciador i para lograr un mayor rendimiento de E/S. Recomendamos elegir 256 KiB para `MaxReceiveDataSegmentLength` y `FirstBurstLength`, y 1 MiB para `MaxBurstLength`. Para obtener más información sobre la configuración de los SCSI ajustes i, consulte. [Personalización de los ajustes SCSI](#)

Note

Estos ajustes recomendados pueden facilitar un mejor rendimiento general. Sin embargo, los SCSI ajustes i específicos necesarios para optimizar el rendimiento varían en función del software de copia de seguridad que utilice. Para obtener más información, consulte la documentación del software de copia de seguridad.

Utilice un tamaño de bloques mayor para las unidades de cinta

Para una puerta de enlace de cinta, el tamaño de bloque predeterminado para una unidad de cinta es de 64 KB. Sin embargo, puede aumentar el tamaño de bloque hasta 1 MB a mejorar el rendimiento de E/S.

El tamaño de bloque que elija dependerá del tamaño de bloque máximo que admita el software de copia de seguridad. Le recomendamos que establezca el máximo tamaño de bloque posible para

las unidades de cinta en el software de copia de seguridad. Sin embargo, este tamaño de bloque no debe ser mayor que el tamaño máximo de 1 MB que admite la gateway.

Las puertas de enlace de cinta negocian el tamaño de bloque de las unidades de cinta virtuales para que coincida automáticamente con el que está definido en el software de copia de seguridad. Cuando aumente el tamaño de bloque en el software de copia de seguridad, le recomendamos que también compruebe la configuración para asegurarse de que el iniciador de host admite el nuevo tamaño de bloque. Para obtener más información, consulte la documentación del software de copia de seguridad. Para obtener más información sobre orientación específica para el rendimiento del gateway, consulte [Rendimiento y optimización para Tape Gateway](#).

Optimice el rendimiento de las unidades de cinta virtuales en el software de copia de seguridad

El software de copia de seguridad puede hacer copias de seguridad de los datos en un máximo de 10 unidades de cinta virtuales de una puerta de enlace de cinta al mismo tiempo. Le recomendamos que configure tareas de copia de seguridad en el software de copia de seguridad para utilizar al menos 4 unidades de cinta virtuales simultáneamente en la puerta de enlace de cinta. Puede lograr un mejor rendimiento de escritura cuando el software de copia de seguridad realiza copias de seguridad de datos en más de una cinta virtual al mismo tiempo.

Como regla general, puede lograr un rendimiento máximo superior si utiliza (leer o escribir) más cintas virtuales al mismo tiempo. Al utilizar más unidades de cinta, permite que la puerta de enlace atienda más solicitudes de forma simultánea, lo que podría mejorar el rendimiento.

Añada recursos al entorno de aplicaciones

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

La conexión entre el SCSI iniciador *i* y la puerta de enlace puede limitar el rendimiento de carga y descarga. Si su gateway presenta un rendimiento considerablemente inferior al esperado y ya ha mejorado el número de CPU núcleos y el rendimiento del disco, considere lo siguiente:

- Actualizar los cables de red para que tengan un mayor ancho de banda entre el iniciador y la puerta de enlace.
- Utilizar tantas unidades de cinta al mismo tiempo como sea posible. *i* SCSI no permite poner en cola varias solicitudes para el mismo destino, lo que significa que cuantas más unidades de cinta utilice, más solicitudes podrá atender su gateway de forma simultánea. Esto le permitirá

utilizar mejor el ancho de banda entre la puerta de enlace y el iniciador, lo que aumentará el rendimiento aparente de la puerta de enlace.

Para optimizar el rendimiento de la puerta de enlace, asegúrese de que el ancho de banda de la red entre la aplicación y la puerta de enlace puede sostener las necesidades de la aplicación. Puede utilizar las métricas `ReadBytes` y `WriteBytes` de la puerta de enlace para medir el rendimiento de datos total. Para obtener más información acerca de estas métricas, consulte [Medición del rendimiento entre su puerta de enlace de cinta y AWS](#).

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.

Agregue recursos a su entorno de aplicaciones CPU

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

Uso de la VMware vSphere alta disponibilidad con Storage Gateway

Storage Gateway proporciona alta disponibilidad VMware mediante un conjunto de comprobaciones de estado a nivel de aplicación integradas con VMware vSphere High Availability (VMwareHA). 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.

vSphere La alta disponibilidad funciona agrupando las máquinas virtuales y los hosts en los que residen en un clúster para garantizar la redundancia. Los hosts del clúster se supervisan y, en caso de error, las máquinas virtuales de un host defectuoso se reinician en hosts alternativos. Por lo general, esta recuperación se produce rápidamente y sin pérdida de datos. Para obtener más información acerca de vSphere la alta disponibilidad, consulte [Cómo vSphere funciona la alta disponibilidad](#) en la VMware documentación.

Note

El tiempo necesario para reiniciar una máquina virtual averiada y restablecer la SCSI conexión i en un nuevo host depende de muchos factores, como el sistema operativo del

host y la carga de recursos, la velocidad del disco, la conexión de red y la infraestructura de SAN /storage. [Para minimizar el tiempo de inactividad de la conmutación por error, implemente las recomendaciones descritas en de enlace.](#)

Para usar VMware HA con Storage Gateway, siga los pasos que se indican a continuación.

Temas

- [Configure su clúster vSphere VMware de alta disponibilidad](#)
- [Descarga de la imagen .ova de la consola de Storage Gateway](#)
- [Implementar la gateway](#)
- [\(Opcional\) Agregue opciones de anulación para otras opciones VMs del clúster](#)
- [Activar la gateway](#)
- [Pruebe su configuración VMware de alta disponibilidad](#)

Configure su clúster vSphere VMware de alta disponibilidad

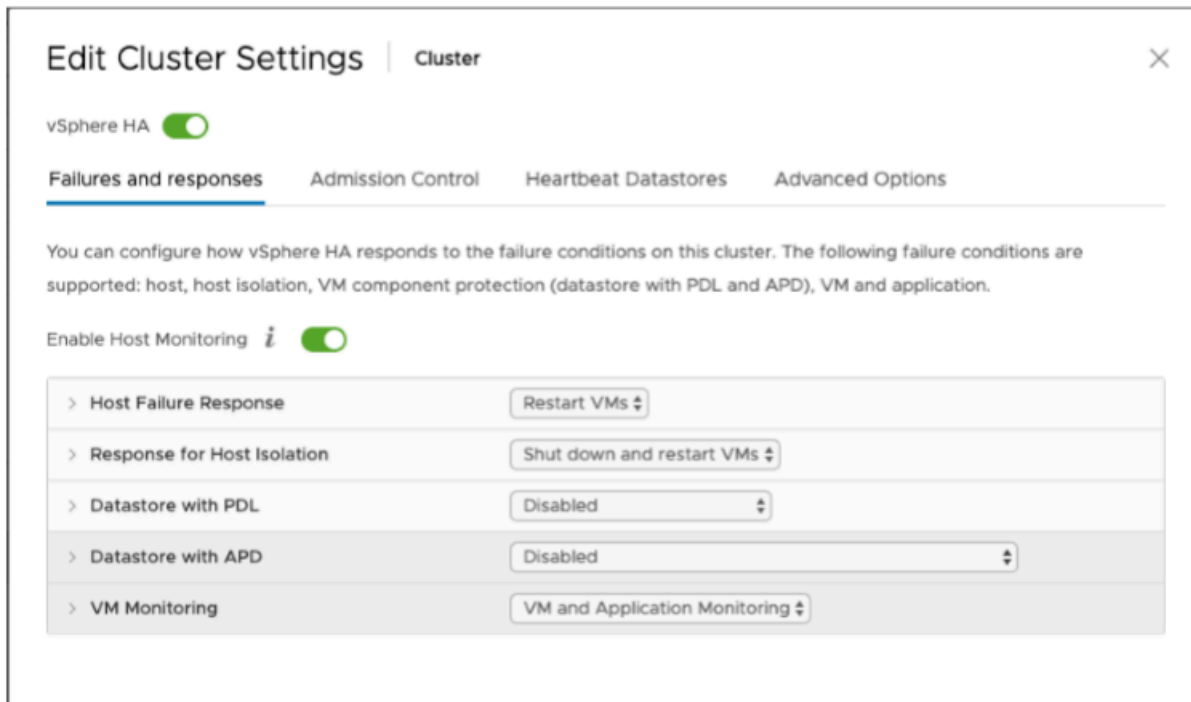
En primer lugar, si aún no ha creado un VMware clúster, cree uno. Para obtener información sobre cómo crear un VMware clúster, consulte [Crear un clúster vSphere de alta disponibilidad](#) en la VMware documentación.

A continuación, configure el VMware clúster para que funcione con Storage Gateway.

Para configurar el VMware clúster

1. En la página Editar la configuración del clúster de VMwarevSphere, asegúrese de que la supervisión de máquinas virtuales esté configurada para la supervisión de máquinas virtuales y aplicaciones. Para ello, configure las siguientes opciones como se indica a continuación:
 - Respuesta a un error del host: reinicie VMs
 - Respuesta al aislamiento del host: apague y reinicie VMs
 - Almacén de datos con PDL: desactivado
 - Almacén de datos con: Desactivado APD
 - VM Monitoring (Monitorización de MV): VM and Application Monitoring (Monitorización de aplicaciones y MV)

Para ver un ejemplo, consulte las siguientes capturas de pantalla.



2. Ajuste la sensibilidad del clúster mediante la configuración de los siguientes valores:

- Failure interval: después de este intervalo, la máquina virtual se reinicia si no se recibe un latido de la máquina virtual.
- Minimum uptime: el clúster espera este tiempo después de que una máquina virtual comience a supervisar los latidos de las herramientas de la máquina virtual.
- Maximum per-VM resets: el clúster reinicia la máquina virtual un máximo de estas veces dentro del intervalo de tiempo máximo de reinicios.
- Maximum resets time window: el intervalo de tiempo en el que se cuentan los reinicios máximos por máquina virtual.

Si no está seguro de los valores que tiene que establecer, utilice esta configuración de ejemplo:

- Failure interval (Intervalo de error): **30** segundos
- Minimum uptime (Tiempo de actividad mínimo): **120** segundos
- Maximum per-VM resets (Reinicios máximos por MV): **3**
- Maximum resets time window (Periodo de tiempo de reinicio máximo): **1** hora

Si tiene otros en VMs ejecución en el clúster, puede que desee establecer estos valores específicamente para su máquina virtual. No puede hacerlo hasta que implemente la MV desde la imagen .ova. Para obtener más información acerca de la configuración de estos valores, consulte [\(Opcional\) Agregue opciones de anulación para otras opciones VMs del clúster](#).

Descarga de la imagen .ova de la consola de Storage Gateway

Para descargar la imagen .ova de la puerta de enlace

- En la página Configurar puerta de enlace de la consola de Storage Gateway, seleccione el tipo de puerta de enlace y la plataforma host y, a continuación, utilice el enlace que se proporciona en la consola para descargar el archivo .ova, tal como se describe en [Configuración de una puerta de enlace de cinta](#).

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. Al implementar el archivo.ova de Storage Gateway en un entorno local VMware o local, los discos se describen como discos paravirtualizados. SCSI La paravirtualización es un modo en que la máquina virtual de la gateway funciona con el sistema operativo host de tal forma que la consola pueda identificar los discos virtuales que se añaden a la máquina virtual.

Para configurar la máquina virtual de forma que use controladores paravirtualizados

1. En el VMware vSphere cliente, abra el menú contextual (haga clic con el botón derecho) de la máquina virtual de la puerta de enlace y, a continuación, seleccione Editar configuración.
2. En el cuadro de diálogo Propiedades de la máquina virtual, seleccione la pestaña Hardware, seleccione el SCSI controlador 0 y, a continuación, elija Cambiar tipo.
3. En el cuadro de diálogo Cambiar tipo de SCSI controlador, seleccione el tipo de SCSI controlador VMwareparavirtual y, a continuación, elija Aceptar.

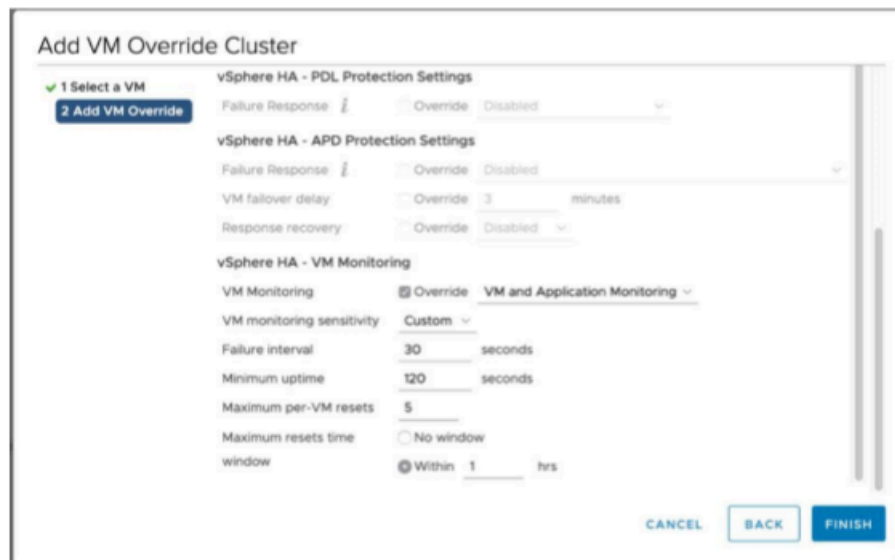
(Opcional) Agregue opciones de anulación para otras opciones VMs del clúster

Si tiene otros en VMs ejecución en su clúster, es posible que desee establecer los valores del clúster específicamente para cada máquina virtual.

Para añadir opciones de anulación para otras VMs del clúster

1. En la página de resumen VMwarevSphere, selecciona tu clúster para abrir la página del clúster y, a continuación, selecciona Configurar.
2. Seleccione la pestaña Configuration (Configuración) y, a continuación, seleccione VM Overrides (Anulaciones de MV).
3. Adición de una nueva opción de anulación de VM para cambiar cada valor.

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

- Siga los procedimientos que se describen en los siguientes temas:

- a. [Conecte su Tape Gateway a AWS](#)
- b. [Revisión de la configuración y activación de la puerta de enlace de cinta](#)
- c. [Configuración de la puerta de enlace de cinta](#)

Pruebe su configuración VMware de alta disponibilidad

Después de activar la gateway, pruebe la configuración.

Para probar su configuración de VMware alta disponibilidad

1. Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa>.
2. En el panel de navegación, elija Gateways y, a continuación, elija la puerta de enlace en la que desee probar su alta disponibilidadVMware.
3. En Acciones, elija Verificar alta disponibilidadVMware.
4. En el cuadro Verificar la configuración de VMware alta disponibilidad que aparece, selecciona Aceptar.

Note

Al probar la configuración de VMware alta disponibilidad, se reinicia la máquina virtual de la puerta de enlace e interrumpe la conectividad con la puerta de enlace. La prueba puede tardar unos minutos en completarse.

Si la prueba se realiza correctamente, el estado de Verified (Verificado) aparece en la pestaña de detalles de la gateway en la consola.

5. Seleccione Exit (Salir).

Puede encontrar información sobre los eventos de VMware alta disponibilidad en los grupos de CloudWatch registros de Amazon. Para obtener más información, consulte [Cómo obtener los registros de estado de Tape Gateway con CloudWatch grupos de registros](#) [Cómo obtener los](#) .

Seguridad en AWS Storage Gateway

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El [modelo de responsabilidad compartida](#) la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la nube de Amazon Web Services. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los [AWS programas](#) de de . Para obtener información sobre los programas de cumplimiento que se aplican a AWS Storage Gateway, consulte [AWS Servicios dentro del alcance por programa de cumplimiento AWS](#) .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted 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 puede aplicar el modelo de responsabilidad compartida cuando se utiliza Storage Gateway. En los siguientes temas, se le mostrará cómo configurar Storage Gateway para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a usar otros AWS servicios que le ayudan a monitorear y proteger los recursos de Storage Gateway.

Temas

- [Protección de datos en AWS Storage Gateway](#)
- [Identity and Access Management para AWS Storage Gateway](#)
- [Inicio de sesión y supervisión AWS Storage Gateway](#)
- [Validación de conformidad para AWS Storage Gateway](#)
- [Resiliencia en AWS Storage Gateway](#)
- [Seguridad de la infraestructura en AWS Storage Gateway](#)
- [AWS Mejores prácticas de seguridad](#)

Protección de datos en AWS Storage Gateway

El [modelo de](#) se aplica a protección de datos en AWS Storage Gateway. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte la sección [Privacidad de datos FAQ](#). Para obtener información sobre la protección de datos en Europa, consulte el [modelo de responsabilidad AWS compartida](#) y la entrada del GDPR blog sobre AWS seguridad.

Para proteger los datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactorial (MFA) con cada cuenta.
- Use SSL/TLS para comunicarse con AWS los recursos. Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Configure API y registre la actividad del usuario con AWS CloudTrail.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita entre FIPS 140 y 3 módulos criptográficos validados para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un FIPS terminal. Para obtener más información sobre los FIPS puntos finales disponibles, consulte la [Norma federal de procesamiento de información \(\) FIPS 140-3](#).

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con Storage Gateway u otro servicios de AWS dispositivo mediante la consola API, AWS CLI, o AWS SDKs. Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, le recomendamos

encarecidamente que no incluya información sobre las credenciales URL para validar la solicitud a ese servidor.

Cifrado de datos mediante AWS KMS

Storage Gateway utiliza SSL/TLS (Secure Socket Layers/Transport Layer Security) para cifrar los datos que se transfieren entre el dispositivo de puerta de enlace y el almacenamiento. De forma predeterminada, Storage Gateway usa claves de cifrado administradas por Amazon SSE S3 (-S3) para cifrar en el servidor todos los datos que almacena en Amazon S3. Tiene la opción de usar Storage Gateway API para configurar su puerta de enlace para cifrar los datos almacenados en la nube mediante el cifrado del lado del servidor con claves AWS Key Management Service (SSE-KMS).

Important

Cuando utilice una AWS KMS clave para el cifrado del lado del servidor, debe elegir una clave simétrica. Storage Gateway no es compatible con claves asimétricas. Para obtener más información, consulte [Uso de claves simétricas y asimétricas](#) en la guía para desarrolladores de AWS Key Management Service .

Cifrado de un recurso compartido de archivos

En el caso de compartir archivos, puede configurar su puerta de enlace para cifrar sus objetos con claves AWS KMS administradas mediante SSE KMS. Para obtener información sobre el uso de Storage Gateway API para cifrar los datos escritos en un recurso compartido de archivos, consulte [CreateNFSFile Share](#) en la AWS Storage Gateway API referencia.

Cifrado de un volumen

Para los volúmenes almacenados y en caché, puede configurar su puerta de enlace para cifrar los datos de volumen almacenados en la nube con claves AWS KMS administradas mediante Storage Gateway API. Puede especificar una de las claves administradas como clave. KMS No se puede cambiar la clave que se utiliza para cifrar el volumen después de crearlo. Para obtener información sobre el uso de Storage Gateway API para cifrar datos escritos en un volumen almacenado o en caché, consulte [CreateCachediSCSIVolume](#) o [CreateStorediSCSIVolume](#) en la AWS Storage Gateway API Referencia.

Cifrado de una cinta

En el caso de una cinta virtual, puede configurar su puerta de enlace para cifrar los datos de la cinta almacenados en la nube con AWS KMS claves administradas mediante Storage Gateway. API Puede especificar una de las claves administradas como clave. KMS No se puede cambiar la clave que se utiliza para cifrar los datos de la cinta después de crearla. Para obtener información sobre el uso de Storage Gateway API para cifrar datos escritos [CreateTapes](#) en una cinta virtual, consulte la [AWS Storage Gateway API Referencia](#).

Cuando AWS KMS lo utilice para cifrar sus datos, tenga en cuenta lo siguiente:

- Los datos se cifran en reposo en la nube. Es decir, los datos se cifran en Amazon S3.
- IAM los usuarios deben tener los permisos necesarios para realizar llamadas a las AWS KMS API operaciones. Para obtener más información, consulte [Uso de IAM políticas AWS KMS](#) en la Guía para AWS Key Management Service desarrolladores.
- Si eliminas o desactivas tu AWS KMS clave o revocas el token de concesión, no podrás acceder a los datos del volumen o la cinta. Para obtener más información, consulta [Eliminar KMS claves](#) en la Guía para AWS Key Management Service desarrolladores.
- Si crea una instantánea a partir de un volumen que está KMS cifrado, la instantánea estará cifrada. La instantánea hereda la clave del KMS volumen.
- Si crea un volumen nuevo a partir de una instantánea KMS cifrada, el volumen estará cifrado. Puede especificar una KMS clave diferente para el nuevo volumen.

Note

Storage Gateway no admite la creación de un volumen sin cifrar desde un punto de recuperación de un volumen KMS cifrado o una KMS instantánea cifrada.

[Para obtener más información al respecto AWS KMS, consulte ¿Qué es? AWS Key Management Service](#)

Identity and Access Management para AWS Storage Gateway

AWS Identity and Access Management (IAM) es un servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. IAM los administradores controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar AWS SGW los recursos. IAM es un servicio de AWS que puede utilizar sin coste adicional.

Temas

- [Público](#)
- [Autenticación con identidades](#)
- [Administración de acceso mediante políticas](#)
- [Cómo funciona AWS Storage Gateway con IAM](#)
- [Ejemplos de políticas basadas en identidad para AWS Storage Gateway](#)
- [Solución de problemas AWS de identidad y acceso a Storage Gateway](#)

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo en el que se realice AWS SGW.

Usuario del servicio: si utiliza el AWS SGW servicio para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más AWS SGW funciones para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una función en AWS SGW, consulte [Solución de problemas AWS de identidad y acceso a Storage Gateway](#).

Administrador de servicios: si está a cargo de AWS SGW los recursos de su empresa, probablemente tenga acceso total a ellos AWS SGW. Su trabajo consiste en determinar a qué AWS SGW funciones y recursos deben acceder los usuarios del servicio. A continuación, debe enviar solicitudes a su IAM administrador para cambiar los permisos de los usuarios del servicio. Revise la información de esta página para comprender los conceptos básicos del IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con AWS SGW, consulte [Cómo funciona AWS Storage Gateway con IAM](#).

IAM administrador: si es IAM administrador, puede que desee obtener más información sobre cómo puede redactar políticas para administrar el acceso a ellas AWS SGW. Para ver ejemplos de políticas AWS SGW basadas en la identidad que puede utilizar IAM, consulte. [Ejemplos de políticas basadas en identidad para AWS Storage Gateway](#)

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como IAM usuario o asumiendo un IAM rol.

Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (IAM Identity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, el administrador configuró previamente la federación de identidades mediante roles. IAM Cuando accede AWS mediante la federación, asume indirectamente un rol.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte [Cómo iniciar sesión Cuenta de AWS en su](#) Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS incluye un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte [Firmar AWS API las solicitudes](#) en la Guía del IAM usuario.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactorial (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte [Autenticación multifactorial](#) en la Guía del AWS IAM Identity Center usuario y [Uso de la autenticación multifactorial \(MFA\) AWS en](#) la Guía del IAM usuario.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de tareas que requieren que inicie sesión como usuario root, consulte [Tareas que requieren credenciales de usuario root](#) en la Guía del IAM usuario.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en IAM Identity Center, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus aplicaciones Cuentas de AWS. Para obtener información sobre IAM Identity Center, consulte [¿Qué es IAM Identity Center?](#) en la Guía AWS IAM Identity Center del usuario.

Usuarios y grupos de IAM

Un [IAMusuario](#) es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos utilizar credenciales temporales en lugar de crear IAM usuarios con credenciales de larga duración, como contraseñas y claves de acceso. Sin embargo, si tiene casos de uso específicos que requieren credenciales a largo plazo con IAM los usuarios, le recomendamos que rote las claves de acceso. Para obtener más información, consulte [Rotar las claves de acceso con regularidad para los casos de uso que requieran credenciales de larga duración](#) en la Guía del IAM usuario.

Un [IAMgrupo](#) es una identidad que especifica un conjunto de IAM usuarios. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar IAM los recursos.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte [Cuándo crear un IAM usuario \(en lugar de un rol\)](#) en la Guía del IAM usuario.

IAMroles

Un [IAMrol](#) es una identidad dentro de tu Cuenta de AWS que tiene permisos específicos. Es similar a un IAM usuario, pero no está asociado a una persona específica. Puede asumir temporalmente un IAM rol en el AWS Management Console [cambiando de rol](#). Puede asumir un rol llamando a una AWS API operación AWS CLI o utilizando una operación personalizadaURL. Para obtener más información sobre los métodos de uso de roles, consulte [Uso de IAM roles](#) en la Guía del IAM usuario.

IAMlos roles con credenciales temporales son útiles en las siguientes situaciones:

- **Acceso de usuario federado:** para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información sobre los roles para la federación, consulte [Creación de un rol para un proveedor de identidad externo](#) en la Guía del IAM usuario. Si usa IAM Identity Center, configura un conjunto de permisos. Para controlar a qué pueden acceder sus identidades después de autenticarse, IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM. Para obtener información acerca de los conjuntos de permisos, consulte [Conjuntos de permisos](#) en la Guía del usuario de AWS IAM Identity Center .
- **Permisos IAM de usuario temporales:** un IAM usuario o rol puede asumir un IAM rol para asumir temporalmente diferentes permisos para una tarea específica.
- **Acceso multicuenta:** puedes usar un IAM rol para permitir que alguien (un responsable de confianza) de una cuenta diferente acceda a los recursos de tu cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunos servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para conocer la diferencia entre las funciones y las políticas basadas en recursos para el acceso multicuenta, consulta el tema sobre el acceso a los [recursos entre cuentas IAM en](#) la Guía del IAM usuario.
- **Acceso entre servicios:** algunos servicios de AWS utilizan funciones en otros servicios de AWS. Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
- **Sesiones de acceso directo (FAS):** cuando utilizas un IAM usuario o un rol para realizar acciones en AWS ellas, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FASutiliza los permisos del principal que llama a un servicio de AWS, junto con los que solicitan, servicio de AWS para realizar solicitudes a los servicios descendentes. FASlas solicitudes solo se realizan

cuando un servicio recibe una solicitud que requiere interacciones con otros servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener detalles sobre la política a la hora de realizar FAS solicitudes, consulte [Reenviar sesiones de acceso](#).

- **Función de servicio:** una función de servicio es una [IAMfunción](#) que un servicio asume para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentro IAM. Para obtener más información, consulte [Crear un rol para delegar permisos servicio de AWS en un rol](#) en el IAMManual del usuario.
- **Función vinculada a un servicio:** una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un IAM administrador puede ver los permisos de los roles vinculados al servicio, pero no editarlos.
- **Aplicaciones que se ejecutan en Amazon EC2:** puedes usar un IAM rol para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y que realizan AWS CLI o AWS API solicitan. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte [Uso de un IAM rol para conceder permisos a aplicaciones que se ejecutan en EC2 instancias de Amazon](#) en la Guía del IAM usuario.

Para saber si se deben usar IAM roles o IAM usuarios, consulte [Cuándo crear un IAM rol \(en lugar de un usuario\)](#) en la Guía del IAM usuario.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como JSON documentos. Para obtener más información sobre la estructura y el contenido de los documentos de JSON políticas, consulte [Descripción general de JSON las políticas](#) en la Guía del IAM usuario.

Los administradores pueden usar AWS JSON las políticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder a los usuarios permiso para realizar acciones en los recursos que necesitan, un IAM administrador puede crear IAM políticas. A continuación, el administrador puede añadir las IAM políticas a las funciones y los usuarios pueden asumir las funciones.

IAM las políticas definen los permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de AWS Management Console AWS CLI, el o el AWS API.

Políticas basadas en identidad

Las políticas basadas en la identidad son documentos de política de JSON permisos que se pueden adjuntar a una identidad, como un IAM usuario, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener información sobre cómo crear una política basada en la identidad, consulte [Creación de IAM políticas](#) en la Guía del usuario. IAM

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y funciones de su empresa. Cuenta de AWS Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para saber cómo elegir entre una política gestionada o una política integrada, consulte [Elegir entre políticas gestionadas y políticas integradas en la Guía del IAM](#) usuario.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de JSON política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe [especificar una entidad principal](#) en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puede usar políticas AWS administradas desde una política IAM basada en recursos.

Listas de control de acceso (ACLs)

Las listas de control de acceso (ACLs) controlan qué responsables (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de JSON de políticas.

Amazon S3, AWS WAF y Amazon VPC son ejemplos de servicios compatibles con ACLs. Para obtener más información sobre ACLs, consulte la [descripción general de la lista de control de acceso \(ACL\)](#) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- **Límites de permisos:** un límite de permisos es una función avanzada en la que se establecen los permisos máximos que una política basada en la identidad puede conceder a una IAM entidad (IAM usuario o rol). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte los [límites de los permisos para IAM las entidades](#) en la Guía del IAM usuario.
- **Políticas de control de servicios (SCPs):** SCPs son JSON políticas que especifican los permisos máximos para una organización o unidad organizativa (OU) AWS Organizations. AWS Organizations es un servicio para agrupar y administrar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una Usuario raíz de la cuenta de AWS. Para obtener más información sobre Organizations SCPs, consulte las [políticas de control de servicios](#) en la Guía del AWS Organizations usuario.
- **Políticas de sesión:** las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información, consulte [las políticas de sesión](#) en la Guía del IAM usuario.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la [lógica de evaluación de políticas](#) en la Guía del IAM usuario.

Cómo funciona AWS Storage Gateway con IAM

Antes de utilizar IAM para administrar el acceso AWS SGW, infórmese sobre las IAM funciones disponibles para su uso AWS SGW.

IAM funciones que puede usar con AWS Storage Gateway

IAM característica	AWS SGW apoyo
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
ACLs	No
ABAC(etiquetas en las políticas)	Parcial
Credenciales temporales	Sí
Sesiones de acceso directo (FAS)	Sí
Roles de servicio	Sí
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo AWS SGW funcionan otros AWS servicios con la mayoría de las IAM funciones, consulte [AWS los servicios con los que funcionan IAM](#) en la Guía del IAM usuario.

Políticas basadas en la identidad para AWS SGW

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en la identidad son documentos de política de JSON permisos que se pueden adjuntar a una identidad, como un IAM usuario, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener información sobre cómo crear una política basada en la identidad, consulte [Creación de IAM políticas](#) en la Guía del usuario. IAM

Con las políticas IAM basadas en la identidad, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para obtener más información sobre todos los elementos que puede utilizar en una JSON política, consulte la [referencia sobre los elementos de la IAM JSON política](#) en la Guía del IAM usuario.

Ejemplos de políticas basadas en la identidad para AWS SGW

Para ver ejemplos de políticas AWS SGW basadas en la identidad, consulte. [Ejemplos de políticas basadas en identidad para AWS Storage Gateway](#)

Políticas basadas en recursos incluidas AWS SGW

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de JSON política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe [especificar una entidad principal](#) en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar una cuenta completa o IAM entidades de otra cuenta como principales en una política basada en recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el IAM administrador de la cuenta de confianza también debe conceder permiso a la entidad principal (usuario o rol) para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte [Acceso a recursos entre cuentas IAM en](#) la Guía del IAM usuario.

Acciones políticas para AWS SGW

Compatibilidad con las acciones de política: sí

Los administradores pueden usar AWS JSON políticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El `Action` elemento de una JSON política describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de política suelen tener el mismo nombre que la AWS API operación asociada. Hay algunas excepciones, como las acciones que solo permiten permisos y que no tienen una operación coincidente. API También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de AWS SGW acciones, consulte [Acciones definidas por AWS Storage Gateway](#) en la Referencia de autorización de servicios.

Las acciones políticas utilizadas AWS SGW utilizan el siguiente prefijo antes de la acción:

```
sgw
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [  
  "sgw:action1",  
  "sgw:action2"
```

```
] ]
```

Para ver ejemplos de políticas AWS SGW basadas en la identidad, consulte. [Ejemplos de políticas basadas en identidad para AWS Storage Gateway](#)

Recursos de políticas para AWS SGW

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar AWS JSON políticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` JSON de política especifica el objeto o los objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso mediante su [nombre de recurso de Amazon \(ARN\)](#). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*" ]
```

Para ver una lista de los tipos de AWS SGW recursos y sus respectivos tiposARNs, consulte [Recursos definidos por AWS Storage Gateway](#) en la Referencia de autorización de servicios. Para saber con qué acciones puede especificar cada recurso, consulte [Actions Defined by AWS Storage Gateway](#). ARN

Para ver ejemplos de políticas AWS SGW basadas en la identidad, consulte. [Ejemplos de políticas basadas en identidad para AWS Storage Gateway](#)

Claves de condición de la política para AWS SGW

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar AWS JSON políticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen [operadores de condición](#), tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación AND lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una OR operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder a un IAM usuario permiso para acceder a un recurso solo si está etiquetado con su nombre de IAM usuario. Para obtener más información, consulte [los elementos de IAM política: variables y etiquetas](#) en la Guía del IAM usuario.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de [contexto de condición AWS globales](#) en la Guía del IAM usuario.

Para ver una lista de claves de AWS SGW condición, consulte Claves de [condición de AWS Storage Gateway](#) en la Referencia de autorización de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte [Actions Defined by AWS Storage Gateway](#).

Para ver ejemplos de políticas AWS SGW basadas en la identidad, consulte. [Ejemplos de políticas basadas en identidad para AWS Storage Gateway](#)

ACLs en AWS SGW

Soportes ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de JSON políticas.

ABAC con AWS SGW

Soportes ABAC (etiquetas en las políticas): parciales

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define los permisos en función de los atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a IAM entidades (usuarios o roles) y a muchos AWS recursos. Etiquetar entidades y recursos es el primer paso de ABAC. Luego, diseñe ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso al que está intentando acceder.

ABAC es útil en entornos de rápido crecimiento y ayuda en situaciones en las que la administración de políticas se vuelve engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el [elemento de condición](#) de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información al respecto ABAC, consulte [¿Qué es? ABAC](#) en la Guía IAM del usuario. Para ver un tutorial con los pasos de configuración ABAC, consulte [Usar el control de acceso basado en atributos \(ABAC\)](#) en la Guía del IAM usuario.

Uso de credenciales temporales con AWS SGW

Compatibilidad con credenciales temporales: sí

Algunos servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. [Para obtener información adicional, incluida la información sobre cuáles servicios de AWS funcionan con credenciales temporales, consulte servicios de AWS IAM la guía del IAM usuario.](#)

Está utilizando credenciales temporales si inicia sesión AWS Management Console con cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes a AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de rol, consulte [Cambiar a un rol \(consola\)](#) en la Guía del IAM usuario.

Puede crear credenciales temporales manualmente con la tecla AWS CLI o AWS API. A continuación, puede utilizar esas credenciales temporales para acceder a AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte [Credenciales de seguridad temporales en IAM](#).

Sesiones de acceso directo para AWS SGW

Admite sesiones de acceso directo (FAS): Sí

Cuando utilizas un IAM usuario o un rol para realizar acciones en AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama a un servicio de AWS y los solicita servicio de AWS para realizar solicitudes a los servicios descendentes. FAS las solicitudes solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener detalles sobre la política a la hora de realizar FAS solicitudes, consulte [Reenviar sesiones de acceso](#).

Roles de servicio para AWS SGW

Compatibilidad con roles de servicio: sí

Una función de servicio es una [IAM función](#) que un servicio asume para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentro IAM. Para obtener más información, consulte [Crear un rol para delegar permisos servicio de AWS en un rol](#) en el IAM Manual del usuario.

Warning

Cambiar los permisos de un rol de servicio podría interrumpir AWS SGW la funcionalidad. Edite las funciones de servicio solo cuando se AWS SGW proporcionen instrucciones para hacerlo.

Funciones vinculadas al servicio para AWS SGW

Admite roles vinculados al servicio: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un servicio de AWS. El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en su Cuenta de AWS y son propiedad del servicio. Un IAM administrador puede ver los permisos de los roles vinculados al servicio, pero no editarlos.

Para obtener más información sobre la creación o la administración de funciones vinculadas a un servicio, consulte los [AWS servicios](#) que funcionan con IAM. Busque un servicio en la tabla

que incluya Yes en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en identidad para AWS Storage Gateway

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar AWS SGW recursos. Tampoco pueden realizar tareas con AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS API. Para conceder a los usuarios permiso para realizar acciones en los recursos que necesitan, un IAM administrador puede crear IAM políticas. A continuación, el administrador puede añadir las IAM políticas a las funciones y los usuarios pueden asumir las funciones.

Para obtener información sobre cómo crear una política IAM basada en la identidad mediante estos documentos de JSON política de ejemplo, consulte [Creación de IAM políticas](#) en la Guía del IAM usuario.

Para obtener más información sobre las acciones y los tipos de recursos definidos por AWS SGW, incluido el ARNs formato de cada uno de los tipos de recursos, consulte [Acciones, recursos y claves de condición de AWS Storage Gateway](#) en la Referencia de autorización de servicio.

Temas

- [Prácticas recomendadas sobre las políticas](#)
- [Uso de la AWS SGW consola](#)
- [Cómo permitir a los usuarios consultar sus propios permisos](#)

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear AWS SGW recursos de su cuenta, acceder a ellos o eliminarlos. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de

uso. Para obtener más información, consulte [las políticas AWS gestionadas](#) o [las políticas AWS gestionadas para las funciones laborales](#) en la Guía del IAM usuario.

- Aplique permisos con privilegios mínimos: cuando establezca permisos con IAM políticas, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Para obtener más información sobre cómo IAM aplicar permisos, consulte [Políticas y permisos IAM en](#) la IAM Guía del usuario.
- Utilice las condiciones en IAM las políticas para restringir aún más el acceso: puede añadir una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de política para especificar que todas las solicitudes deben enviarse medianteSSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte [los elementos IAM JSON de la política: Condición](#) en la Guía del IAM usuario.
- Utilice IAM Access Analyzer para validar sus IAM políticas y garantizar permisos seguros y funcionales: IAM Access Analyzer valida las políticas nuevas y existentes para que se ajusten al lenguaje de las políticas (JSON) y IAM a las IAM mejores prácticas. IAMAccess Analyzer proporciona más de 100 comprobaciones de políticas y recomendaciones prácticas para ayudarlo a crear políticas seguras y funcionales. Para obtener más información, consulte la [validación de políticas de IAM Access Analyzer](#) en la Guía del IAM usuario.
- Requerir autenticación multifactorial (MFA): si se encuentra en una situación en la que se requieren IAM usuarios o un usuario raíz Cuenta de AWS, actívela MFA para aumentar la seguridad. Para solicitarlo MFA cuando se convoque a API las operaciones, añada MFA condiciones a sus políticas. Para obtener más información, consulte [Configuración del API acceso MFA protegido](#) en la Guía del IAM usuario.

Para obtener más información sobre las prácticas recomendadasIAM, consulte las [prácticas recomendadas de seguridad IAM en](#) la Guía del IAM usuario.

Uso de la AWS SGW consola

Para acceder a la consola AWS Storage Gateway, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los AWS SGW recursos de su cuenta Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que realicen llamadas únicamente al AWS CLI o al AWS API. En su lugar, permita el acceso únicamente a las acciones que coincidan con la API operación que están intentando realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la AWS SGW consola, asocie también la AWS SGW *ConsoleAccess* política *ReadOnly* AWS gestionada a las entidades. Para obtener más información, consulte [Añadir permisos a un usuario](#) en la Guía del IAM usuario.

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo se muestra cómo se puede crear una política que permita a IAM los usuarios ver las políticas integradas y administradas asociadas a su identidad de usuario. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la tecla o. AWS CLI AWS API

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ]
    }
  ]
}
```

```
    ],  
    "Resource": "*"    
  }  
]  
}
```

Solución de problemas AWS de identidad y acceso a Storage Gateway

Utilice la siguiente información para ayudarle a diagnosticar y solucionar los problemas más comunes que pueden surgir al trabajar con AWS SGW y IAM.

Temas

- [No estoy autorizado a realizar ninguna acción en AWS SGW](#)
- [No estoy autorizado a realizar tareas como: PassRole](#)
- [Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis AWS SGW recursos](#)

No estoy autorizado a realizar ninguna acción en AWS SGW

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

El siguiente ejemplo de error se produce cuando el usuario IAM mateojackson intenta usar la consola para ver los detalles de un *my-example-widget* recurso ficticio, pero no tiene los `sgw:GetWidget` permisos ficticios.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:  
sgw:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario mateojackson debe actualizarse para permitir el acceso al recurso *my-example-widget* mediante la acción `sgw:GetWidget`.

Si necesita ayuda, póngase en contacto con AWS el administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibes un mensaje de error que indica que no estás autorizado a realizar la `iam:PassRole` acción, debes actualizar tus políticas para que puedas transferirle AWS SGW una función.

Algunos servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

El siguiente ejemplo de error se produce cuando un IAM usuario denominado `marymajor` intenta utilizar la consola para realizar una acción en ella. AWS SGW Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con AWS el administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis AWS SGW recursos

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que respaldan las políticas basadas en recursos o las listas de control de acceso (ACLs), puedes usar esas políticas para permitir que las personas accedan a tus recursos.

Para más información, consulte lo siguiente:

- Para saber si AWS SGW es compatible con estas funciones, consulte. [Cómo funciona AWS Storage Gateway con IAM](#)
- Para obtener información sobre cómo proporcionar acceso a los recursos de su propiedad, consulte [Proporcionar acceso a un IAM usuario en otro Cuenta de AWS de su propiedad](#) en la Guía del IAM usuario. Cuentas de AWS
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta [Cómo permitir el acceso a recursos que Cuentas de AWS son propiedad de terceros](#) en la Guía del IAM usuario.

- Para obtener información sobre cómo proporcionar acceso mediante la federación de identidades, consulte [Proporcionar acceso a usuarios autenticados externamente \(federación de identidades\)](#) en la Guía del IAM usuario.
- Para saber la diferencia entre el uso de roles y políticas basadas en recursos para el acceso entre cuentas, consulte el acceso a [recursos entre cuentas IAM en la Guía](#) del usuario. IAM

Inicio de sesión y supervisión AWS Storage Gateway

Storage Gateway está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Storage Gateway. CloudTrail captura todas las API llamadas de Storage Gateway como eventos. Las llamadas capturadas incluyen llamadas desde la consola de Storage Gateway y llamadas en código a las API operaciones de Storage Gateway. Si crea una ruta, puede activar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Storage Gateway. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a Storage Gateway, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la [Guía AWS CloudTrail del usuario](#).

Información sobre Storage Gateway en CloudTrail

CloudTrail se activa en su cuenta de Amazon Web Services al crear la cuenta. Cuando se produce una actividad en Storage Gateway, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los últimos eventos de la cuenta de Amazon Web Services. Para obtener más información, consulte [Visualización de eventos con el historial de CloudTrail eventos](#).

Para mantener un registro continuo de eventos en la cuenta de Amazon Web Services, incluidos los eventos de Storage Gateway, cree un registro de seguimiento. Un rastro permite CloudTrail entregar los archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando crea una ruta en la consola, la ruta se aplica a todas AWS las regiones. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- [Introducción a la creación de registros de seguimiento](#)
- [CloudTrail Integraciones y servicios compatibles](#)
- [Configuración de Amazon SNS Notifications para CloudTrail](#)
- [Recibir archivos de CloudTrail registro de varias regiones](#) y [recibir archivos de CloudTrail registro de varias cuentas](#)

Todas las acciones de Storage Gateway están registradas y documentadas en el tema [Acciones](#). Por ejemplo, las llamadas a las `ActivateGateway` `ShutdownGateway` acciones y las llamadas `ListGateways` generan entradas en los archivos de CloudTrail registro.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el [CloudTrail userIdentityElemento](#).

Descripción de las entradas de archivos de registro de Storage Gateway

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las API llamadas públicas, por lo que no aparecen en ningún orden específico.

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la acción.

```
{ "Records": [{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAI15AUEPBH2M7JTNVC",
        "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": "cloudtrailgatewayv1",
    "gatewayRegion": "us-east-2",
    "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
    "gatewayType": "VTL"
  },
  "responseElements": {
    "gatewayARN":
"arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayv1"
  },
  "requestID":
"54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
  "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
  "eventType": "AwsApiCall",
  "apiVersion": "20130630",
  "recipientAccountId": "444455556666"
  ]
}

```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la ListGateways acción.

```

{
  "Records": [{
    "eventVersion": "1.02",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "AIDAI5AUPEPBH2M7JTNCV",
      "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 ":"
6U2N42CU37KA08BG6V1I23FRSJ1Q8GLLE1QEUI3KPGG6F0KSTAUU0 ",
" eventID ":" f76e5919 - 9362 - 48ff - a7c4 -
d203a189ec8d ",
" eventType ":" AwsApiCall ",
" apiVersion ":" 20130630 ",
" recipientAccountId ":" 444455556666"
    ]}
}

```

Validación de conformidad para AWS Storage Gateway

Los auditores externos evalúan la seguridad y el cumplimiento de AWS Storage Gateway como parte de varios programas de AWS cumplimiento. Estos incluyen SOC, PCIISO, FedRAMP, HIPAA, MTSC, C5, K- ISMSOSPAR, ENS High y HITRUSTCSF.

Para obtener una lista de AWS los servicios incluidos en el ámbito de los programas de cumplimiento específicos, consulte los [AWS servicios incluidos en el ámbito de aplicación por programa de cumplimiento y AWS los servicios incluidos](#) . Para obtener información general, consulte Programas de [AWS cumplimiento > Programas AWS](#) .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte [Descarga de informes en AWS Artifact](#) .

Su responsabilidad en el ámbito de la conformidad al usar Storage Gateway viene determinada por la confidencialidad de los datos, los objetivos de conformidad de la empresa y las leyes y

regulaciones aplicables. AWS proporciona los siguientes recursos para ayudarlo con los requisitos de conformidad:

- [Guías de inicio rápido](#) sobre : estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en la seguridad y el cumplimiento. AWS
- Documento técnico sobre [la arquitectura basada en HIPAA la seguridad y el cumplimiento: en este documento técnico](#) se describe cómo pueden utilizar las empresas para crear aplicaciones que cumplan con las normas. AWS HIPAA
- [AWS Recursos de cumplimiento Recursos AWS](#) : esta colección de libros de trabajo y guías puede aplicarse a su sector y ubicación.
- [Evaluación de los recursos con las reglas](#) de la Guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- [AWS Security Hub](#)— Este AWS servicio proporciona una visión integral del estado de su seguridad AWS que le ayuda a comprobar su conformidad con los estándares y las mejores prácticas del sector de la seguridad.

Resiliencia en AWS Storage Gateway

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. AWS Las regiones proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

[Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte Infraestructura global.AWS](#)

Además de la infraestructura AWS global, Storage Gateway ofrece varias funciones que ayudan a respaldar sus necesidades de respaldo y resiliencia de datos:

- Utilice la VMware vSphere alta disponibilidad (VMwareHA) para proteger las cargas de trabajo de almacenamiento contra los fallos de hardware, hipervisor o red. Para obtener más información, consulte [Uso de la VMware vSphere alta disponibilidad con Storage Gateway](#).

- Archive cintas virtuales en S3 Glacier Flexible Retrieval. Para obtener más información, consulte [Archivado de cintas virtuales](#).

Seguridad de la infraestructura en AWS Storage Gateway

Como servicio gestionado, AWS Storage Gateway está protegido por los procedimientos de seguridad de red AWS global que se describen en el documento técnico [Amazon Web Services: Overview of Security Processes](#).

APIs llamadas AWS publicadas se utilizan para acceder a Storage Gateway a través de la red. Los clientes deben ser compatibles con Transport Layer Security (TLS) 1.2. Los clientes también deben admitir conjuntos de cifrado con total confidencialidad (PFS), como Ephemeral Diffie-Hellman () o Elliptic Curve Ephemeral Diffie-Hellman (DHE). ECDHE La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben firmarse con un identificador de clave de acceso y una clave de acceso secreta que esté asociada a un director. IAM También puede utilizar [AWS Security Token Service](#) (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Note

Debe tratar el dispositivo AWS Storage Gateway como una máquina virtual administrada y no debe intentar acceder a su instalación ni modificarla de ninguna manera. Si intenta instalar el software de escaneo o actualizar cualquier paquete de software utilizando métodos distintos al mecanismo de actualización de la puerta de enlace normal, puede provocar un mal funcionamiento de la puerta de enlace y afectar a nuestra capacidad de soporte o reparación de la puerta de enlace.

AWS revisa, analiza y CVEs corrige periódicamente. Incorporamos correcciones para estos problemas en Storage Gateway como parte de nuestro ciclo normal de lanzamiento de software. Por lo general, estas correcciones se aplican como parte del proceso normal de actualización de la puerta de enlace durante los períodos de mantenimiento programados. Para obtener más información sobre las actualizaciones de las puertas de enlace, consulte .

AWS Mejores prácticas de seguridad

AWS proporciona una serie de características de seguridad que debe tener en cuenta a la hora de desarrollar e implementar sus propias políticas de seguridad. Estas prácticas recomendadas

son directrices generales y no suponen una solución de seguridad completa. Puesto que es posible que estas prácticas no sean adecuadas o suficientes para el entorno, considérelas como consideraciones útiles en lugar de como normas. Para obtener más información, consulte [AWS Prácticas recomendadas de seguridad de](#) .

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 puertas de enlace locales abarca las puertas de enlace implementadas tanto en los clientes Hyper-V como en los de VMware ESXi Microsoft Hyper-V. La información de solución de problemas para recursos compartidos de archivos también se aplica al tipo de puerta de enlace de archivo. La información de solución de problemas para volúmenes se aplica al tipo de puerta de enlace de volumen. La información de solución de problemas para cintas se aplica al tipo de puerta de enlace de cinta. La información de solución de problemas relacionados con las puertas de enlace se refiere al uso de métricas. CloudWatch La información de solución de problemas de alta disponibilidad abarca las puertas de enlace que se ejecutan en VMware vSphere una plataforma de alta disponibilidad (HA).

Temas

- [Solución de problemas: gateway offline en la consola Storage Gateway](#)
- [Solución de problemas: error interno durante la activación de la puerta de enlace](#)
- [Solución de problemas de puerta de enlace en las instalaciones](#)
- [Solución de problemas de configuración de Microsoft Hyper-V](#)
- [Solución de problemas de Amazon EC2 Gateway](#)
- [Solución de problemas del dispositivo de hardware](#)
- [Solución de problemas con cintas virtuales](#)
- [Solución de problemas de alta disponibilidad](#)
- [Prácticas recomendadas para la recuperación de datos](#)

Solución de problemas: gateway offline en la consola Storage Gateway

Utilice la siguiente información de solución de problemas para determinar qué hacer si la AWS Storage Gateway consola muestra que la puerta de enlace está desconectada.

Es posible que la puerta de enlace aparezca como desconectada por uno o varios de los siguientes motivos:

- La puerta de enlace no puede llegar a los puntos finales del servicio Storage Gateway.
- La puerta de enlace se cerró inesperadamente.
- Se desconectó o modificó un disco caché asociado a la puerta de enlace, o se produjo un error.

Para volver a conectar la puerta de enlace, identifique y resuelva el problema que provocó que la puerta de enlace se desconectara.

Compruebe el firewall o el proxy asociados

Si configuró la puerta de enlace para usar un proxy o la colocó detrás de un firewall, revise las reglas de acceso del proxy o el firewall. El proxy o el firewall deben permitir el tráfico hacia y desde los puertos de red y los puntos finales de servicio requeridos por Storage Gateway. Para obtener más información, consulte [Requisitos de red y firewall Requisitos](#).

Compruebe si hay una inspección continua SSL o exhaustiva del tráfico de su puerta de enlace

Si actualmente se está realizando una SSL inspección exhaustiva de los paquetes del tráfico de red entre la puerta de enlace y la puerta de enlace AWS, es posible que la puerta de enlace no pueda comunicarse con los puntos finales de servicio necesarios. Para que su puerta de enlace vuelva a estar en línea, debe deshabilitar la inspección.

Compruebe si hay un corte de energía o un fallo de hardware en el host del hipervisor

Un corte de energía o un fallo de hardware en el host del hipervisor de la puerta de enlace pueden provocar que la puerta de enlace se cierre inesperadamente y no se pueda acceder a ella. Tras restablecer la alimentación y la conectividad de red, se volverá a poder acceder a la puerta de enlace.


Cuando la puerta de enlace vuelva a estar en línea, asegúrate de tomar las medidas necesarias para recuperar los datos. Para obtener más información, consulte [Prácticas recomendadas para recuperar datos](#).

Compruebe si hay problemas con un disco caché asociado

La puerta de enlace se puede desconectar si al menos uno de los discos de caché asociados a la puerta de enlace se ha eliminado, modificado o redimensionado, o si está dañado.

Si se ha eliminado un disco de caché en funcionamiento del host del hipervisor:

1. Apague la gateway.
2. Vuelva a añadir el disco.

 Note

Asegúrese de añadir el disco al mismo nodo de disco.

3. Reinicie la gateway.

Si un disco de caché está dañado, se reemplazó o se cambió su tamaño:

1. Apague la gateway.
2. Reinicie el disco caché.
3. Vuelva a configurar el disco para el almacenamiento en caché.
4. Reinicie la gateway.

Para obtener más información sobre la solución de problemas de un disco caché dañado para una puerta de enlace de cinta, consulte [Necesita recuperar una cinta virtual de un disco de caché que no funciona correctamente](#).

Solución de problemas: error interno durante la activación de la puerta de enlace

Las solicitudes de activación de Storage Gateway atraviesan dos rutas de red. Las solicitudes de activación entrantes enviadas por un cliente se conectan a la máquina virtual (VM) de la puerta de enlace o a la instancia de Amazon Elastic Compute Cloud (AmazonEC2) a través del puerto 80. Si la puerta de enlace recibe correctamente la solicitud de activación, la puerta de enlace se comunica con los puntos finales de Storage Gateway para recibir una clave de activación. Si la puerta de enlace no puede llegar a los puntos finales de Storage Gateway, la puerta de enlace responde al cliente con un mensaje de error interno.

Utilice la siguiente información de solución de problemas para determinar qué hacer si recibe un mensaje de error interno al intentar activar su AWS Storage Gateway.

Note

- Asegúrese de implementar nuevas puertas de enlace con el archivo de imagen de máquina virtual o la versión más reciente de Amazon Machine Image (AMI). Recibirá un error interno si intenta activar una puerta de enlace que utilice una puerta de enlace obsoletaAMI.
- Asegúrese de seleccionar el tipo de puerta de enlace correcto que desea implementar antes de descargarlaAMI. Los archivos.ova y AMIs para cada tipo de puerta de enlace son diferentes y no son intercambiables.

Resuelva los errores al activar su puerta de enlace mediante un punto final público

Para resolver los errores de activación al activar la puerta de enlace mediante un punto final público, realice las siguientes comprobaciones y configuraciones.


Compruebe los puertos necesarios

En el caso de las puertas de enlace implementadas localmente, compruebe que los puertos estén abiertos en el firewall local. En el caso de las puertas de enlace implementadas en una EC2 instancia de Amazon, comprueba que los puertos estén abiertos en el grupo de seguridad de la instancia. Para confirmar que los puertos están abiertos, ejecuta un comando telnet en el punto final público desde un servidor. Este servidor debe estar en la misma subred que la puerta de enlace. Por ejemplo, los siguientes comandos de telnet prueban la conexión al puerto 443:

```
telnet d4kdq0yaxexbo.cloudfront.net 443
telnet storagegateway.region.amazonaws.com 443
telnet dp-1.storagegateway.region.amazonaws.com 443
telnet proxy-app.storagegateway.region.amazonaws.com 443
telnet client-cp.storagegateway.region.amazonaws.com 443
telnet anon-cp.storagegateway.region.amazonaws.com 443
```

Para confirmar que la propia puerta de enlace puede llegar al punto final, acceda a la consola de máquina virtual local de la puerta de enlace (para las puertas de enlace implementadas localmente). O bien, puede ir SSH a la instancia de la puerta de enlace (para las puertas de enlace implementadas en AmazonEC2). A continuación, ejecute una prueba de conectividad de red.

Confirme que la prueba se ha realizado correctamente [PASSED]. Para obtener más información, enlace [Probar la conexión de la puerta de enlace a Internet](#).


 Note

El nombre de usuario de inicio de sesión predeterminado para la consola de puerta de enlace es `admin` y la contraseña predeterminada es `password`.

Asegúrese de que la seguridad del firewall no modifique los paquetes enviados desde la puerta de enlace a los puntos finales públicos

SSL las inspecciones, las inspecciones exhaustivas de paquetes u otras formas de seguridad mediante firewall pueden interferir con los paquetes enviados desde la puerta de enlace. El SSL protocolo de enlace falla si el SSL certificado se modifica con respecto a lo esperado por el punto final de activación. Para confirmar que no hay ninguna SSL inspección en curso, ejecute un SSL comando Open en el punto final de activación principal (`anon-cp.storagegateway.region.amazonaws.com`) del puerto 443. Debe ejecutar este comando desde una máquina que esté en la misma subred que la puerta de enlace:

```
$ openssl s_client -connect anon-cp.storagegateway.region.amazonaws.com:443 -  
servername anon-cp.storagegateway.region.amazonaws.com
```

 Note

Reemplazar *region* con tu. Región de AWS

Si no hay ninguna SSL inspección en curso, el comando devuelve una respuesta similar a la siguiente:

```
$ openssl s_client -connect anon-cp.storagegateway.us-east-2.amazonaws.com:443 -  
servername anon-cp.storagegateway.us-east-2.amazonaws.com  
CONNECTED(00000003)  
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1  
verify return:1  
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon  
verify return:1
```

```
depth=0 CN = anon-cp.storagegateway.us-east-2.amazonaws.com
verify return:1
---
Certificate chain
 0 s:/CN=anon-cp.storagegateway.us-east-2.amazonaws.com
  i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
 1 s:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
  i:/C=US/O=Amazon/CN=Amazon Root CA 1
 2 s:/C=US/O=Amazon/CN=Amazon Root CA 1
  i:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
  Root Certificate Authority - G2
 3 s:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
  Root Certificate Authority - G2
  i:/C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification Authority
---
```

Si hay una SSL inspección en curso, la respuesta muestra una cadena de certificados alterada, similar a la siguiente:

```
$ openssl s_client -connect anon-cp.storagegateway.ap-southeast-1.amazonaws.com:443 -
servername anon-cp.storagegateway.ap-southeast-1.amazonaws.com
CONNECTED(00000003)
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.ap-southeast-1.amazonaws.com
  i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

El punto final de activación solo acepta SSL apretones de manos si reconoce el SSL certificado. Esto significa que el tráfico saliente de la puerta de enlace hacia los puntos finales debe estar exento de las inspecciones realizadas por los firewalls de la red. Estas inspecciones pueden ser una SSL inspección o una inspección profunda de paquetes.

Compruebe la sincronización horaria de la puerta de enlace

Los sesgos temporales excesivos pueden provocar errores en el SSL apretón de manos. En el caso de las puertas de enlace locales, puede utilizar la consola de máquina virtual local de la puerta de enlace para comprobar la sincronización horaria de la puerta de enlace. El intervalo de tiempo no debe ser superior a 60 segundos.

La opción de administración del tiempo del sistema no está disponible en las pasarelas alojadas en EC2 instancias de Amazon. Para asegurarte de que EC2 las pasarelas de Amazon pueden sincronizar la hora correctamente, confirma que la EC2 instancia de Amazon se puede conectar a la siguiente lista de grupos de NTP servidores a través de los puertos 1 UDP y TCP 123:

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

Resuelva los errores al activar su puerta de enlace mediante un VPC punto de conexión de Amazon

Para resolver los errores de activación al activar la puerta de enlace mediante un punto de conexión de Amazon Virtual Private Cloud (AmazonVPC), lleve a cabo las siguientes comprobaciones y configuraciones.

Compruebe los puertos necesarios


Asegúrese de que los puertos necesarios del firewall local (para las puertas de enlace implementadas en las instalaciones) o del grupo de seguridad (para las puertas de enlace implementadas en AmazonEC2) estén abiertos. Los puertos necesarios para conectar una puerta de enlace a un VPC punto final de Storage Gateway son diferentes de los necesarios para conectar una puerta de enlace a puntos finales públicos. Se requieren los siguientes puertos para conectarse a un VPC punto final de Storage Gateway:

- TCP443
- TCP1026
- TCP1027
- TCP1028

- TCP1031
- TCP2222

Para obtener más información, consulte [Creación de un VPC punto final para Storage Gateway](#).

Además, compruebe el grupo de seguridad que está conectado a su VPC endpoint Storage Gateway. Es posible que el grupo de seguridad predeterminado adjunto al punto final no permita los puertos necesarios. Cree un nuevo grupo de seguridad que permita el tráfico desde el rango de direcciones IP de la puerta de enlace a través de los puertos necesarios. A continuación, asocie ese grupo de seguridad al VPC punto final.

 Note

Usa la [VPCconsola de Amazon](#) para verificar el grupo de seguridad que está conectado al VPC punto final. Vea su VPC terminal Storage Gateway desde la consola y, a continuación, seleccione la pestaña Grupos de seguridad.

Para confirmar que los puertos necesarios están abiertos, puede ejecutar comandos de telnet en el Storage Gateway VPC Endpoint. Debe ejecutar estos comandos desde un servidor que esté en la misma subred que la puerta de enlace. Puede ejecutar las pruebas con el DNS nombre de pila que no especifique una zona de disponibilidad. Por ejemplo, los siguientes comandos de telnet prueban las conexiones de puerto necesarias con el DNS nombre `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`:

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 443
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1026
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1027
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1028
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1031
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 2222
```

Asegúrese de que la seguridad del firewall no modifique los paquetes enviados desde la puerta de enlace a su VPC punto de conexión Storage Gateway Amazon

SSL las inspecciones, las inspecciones exhaustivas de paquetes u otras formas de seguridad mediante firewall pueden interferir con los paquetes enviados desde la puerta de enlace. El SSL protocolo de enlace falla si el SSL certificado se modifica con respecto a lo esperado por el punto

final de activación. Para confirmar que no hay ninguna SSL inspección en curso, ejecute un SSL comando Open en el VPC endpoint de Storage Gateway. Debe ejecutar este comando desde una máquina que esté en la misma subred que la puerta de enlace. Ejecute el comando para cada puerto requerido:

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:443 -servername vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:1026 -servername vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:1027 -servername vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:1028 -servername vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:1031 -servername vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:2222 -servername vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

Si no hay ninguna SSL inspección en curso, el comando devuelve una respuesta similar a la siguiente:

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:1027 -servername vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-1.amazonaws.com
verify return:1
```

```

---
Certificate chain
 0 s:CN = anon-cp.storagegateway.us-east-1.amazonaws.com
   i:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
 1 s:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
   i:C = US, O = Amazon, CN = Amazon Root CA 1
 2 s:C = US, O = Amazon, CN = Amazon Root CA 1
   i:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
Starfield Services Root Certificate Authority - G2
 3 s:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
Starfield Services Root Certificate Authority - G2
   i:C = US, O = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification
Authority
---

```

Si hay una SSL inspección en curso, la respuesta muestra una cadena de certificados alterada, similar a la siguiente:

```

openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.us-
east-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.us-east-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---

```

El punto final de activación solo acepta SSL apretones de manos si reconoce el SSL certificado. Esto significa que el tráfico saliente de la puerta de enlace hacia su VPC punto final a través de los puertos requeridos está exento de las inspecciones que realizan los firewalls de la red. Estas inspecciones pueden ser inspecciones o SSL inspecciones exhaustivas de paquetes.

Compruebe la sincronización horaria de la puerta de enlace

Los sesgos temporales excesivos pueden provocar errores en el SSL apretón de manos. En el caso de las puertas de enlace locales, puede utilizar la consola de máquina virtual local de la puerta de enlace para comprobar la sincronización horaria de la puerta de enlace. El intervalo de tiempo no debe ser superior a 60 segundos.

La opción de administración del tiempo del sistema no está disponible en las pasarelas alojadas en EC2 instancias de Amazon. Para asegurarte de que EC2 las pasarelas de Amazon pueden sincronizar la hora correctamente, confirma que la EC2 instancia de Amazon se puede conectar a la siguiente lista de grupos de NTP servidores a través de los puertos 1 UDP y TCP 123:

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

Comprueba si hay un HTTP proxy y confirma la configuración del grupo de seguridad asociado

Antes de la activación, compruebe si tiene un HTTP proxy en Amazon EC2 configurado en la máquina virtual de puerta de enlace local como un proxy de Squid en el puerto 3128. En este caso, confirme lo siguiente:

- El grupo de seguridad adjunto al HTTP proxy de Amazon EC2 debe tener una regla de entrada. Esta regla de entrada debe permitir el tráfico de proxy de Squid en el puerto 3128 desde la dirección IP de la máquina virtual de la puerta de enlace.
- El grupo de seguridad adjunto al EC2 VPC punto de conexión de Amazon debe tener reglas de entrada. Estas reglas de entrada deben permitir el tráfico en los puertos 1026-1028, 1031, 2222 y 443 desde la dirección IP del proxy de Amazon. HTTP EC2

Resuelva los errores al activar su puerta de enlace mediante un punto final público y haya un VPC punto final de Storage Gateway en el mismo VPC

Para resolver los errores al activar su puerta de enlace mediante un punto de enlace público cuando hay un punto de enlace de Amazon Virtual Private Cloud (AmazonVPC) en el mismoVPC, lleve a cabo las siguientes comprobaciones y configuraciones.

Confirme que la configuración Habilitar DNS nombre privado no esté habilitada en el VPC punto final de Storage Gateway

Si la opción Activar DNS nombre privado está habilitada, no podrá activar ninguna puerta de enlace desde esa ubicación VPC hasta el punto final público.

Para deshabilitar la opción de DNS nombre privado:

1. Abra la [VPCconsola de Amazon](#).
2. En el panel de navegación, elija Puntos de conexión.
3. Elija su VPC terminal Storage Gateway.
4. Elija Actions.
5. Elija Administrar DNS nombres privados.
6. En Habilitar el DNS nombre privado, desactive Habilitar para este punto final.
7. Seleccione Modificar DNS nombres privados para guardar la configuración.

Solución de problemas de puerta de enlace en las instalaciones

A continuación, encontrará información sobre los problemas habituales que se pueden producir al trabajar con las puertas de enlace locales y sobre cómo activarlos para ayudar AWS Support a solucionar los problemas de las puertas de enlace.

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.

Problema	Acción que ejecutar
	<ul style="list-style-type: none">• Por ejemplo VMwareESXi, la dirección IP de la máquina virtual se encuentra en el vSphere cliente, en la pestaña Resumen.• Para Microsoft Hyper-V, la dirección IP de la MV puede encontrarse al iniciar sesión en la consola local. <p>Si continúa teniendo problemas para encontrar la dirección IP de la gateway:</p> <ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• Asigne permisos a los puertos adecuados para la gateway.• SSLLa validación/inspección de los certificados no debe estar activada. Storage Gateway utiliza una TLS autenticación mutua que fallaría si una aplicación de terceros intentara interceptar o firmar alguno de los certificados.• Si utiliza un firewall o un router para filtrar o limitar el tráfico de red, debe configurar el firewall y el router para dar permiso a los puntos de conexión de servicio para mantener comunicaciones de salida con AWS. Para obtener más información sobre los requisitos de red y firewall, consulte Requisitos de red y firewall.

Problema	Acción que ejecutar
<p>La activación de la puerta de enlace produce un error al hacer clic en el botón Proceder a la activación de la consola de administración de Storage Gateway.</p>	<ul style="list-style-type: none">• 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, tendrá que configurar un proxy. SOCKS Para obtener más información sobre cómo hacerlo, consulte Ruteo de la gateway local a través de un proxy.• Compruebe que el host tenga la hora correcta, que esté configurado para sincronizar su hora automáticamente con un servidor de protocolo de tiempo de red (Network Time ProtocolNTP) y que la máquina virtual de puerta de enlace tenga la hora correcta. Para obtener información sobre la sincronización de la hora de los hosts del hipervisor yVMs, consulte. Sincronización de la hora de la MV de la gateway• Tras realizar estos pasos, puede reintentar la implementación de la puerta de enlace mediante la consola de Storage Gateway y el asistente Configurar y activar puerta de enlace.• SSLLa validación/inspección de los certificados no debe activarse. Storage Gateway utiliza una TLS autenticación mutua que fallaría si una aplicación de terceros intentara interceptar o firmar alguno de los certificados.• Compruebe que su máquina virtual tenga al menos 7,5 GB de RAM La asignación de la puerta de enlace falla si hay menos de 7,5 GB deRAM. Para obtener más información, consulte Requisitos para configurar Tape Gateway.

Problema	Acción que ejecutar
<p>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.</p>	<p>Para obtener instrucciones sobre cómo eliminar un disco asignado como espacio de búfer de carga, consulte Retirada de discos de la gateway.</p>
<p>Debe mejorar el ancho de banda entre la puerta de enlace y AWS.</p>	<p>Puede mejorar el ancho de banda de la puerta de enlace AWS configurando la conexión a Internet AWS en un adaptador de red (NIC) independiente del que conecta las aplicaciones y la máquina virtual de la puerta de enlace. Este enfoque resulta útil si tiene una conexión con un ancho de banda elevado AWS y quiere evitar la contención del ancho de banda, especialmente durante una restauración instantánea. Para necesidades de carga de trabajo de alto rendimiento, puede usar AWS Direct Connect para establecer una conexión de red dedicada entre la puerta de enlace en las instalaciones y AWS. Para medir el ancho de banda de la conexión desde la puerta de enlace AWS, utilice las CloudByte sUploaded métricas CloudBytesDownloaded y de la puerta de enlace. Para obtener más información sobre este tema, consulte Medición del rendimiento entre su puerta de enlace de cinta y AWS. Mejorar la conectividad a Internet ayuda a garantizar que el búfer de carga no se llene.</p>

Problema	Acción que ejecutar
El rendimiento hacia o desde la gateway disminuye a cero.	<ul style="list-style-type: none">• En la pestaña Gateway de la consola Storage Gateway, compruebe que las direcciones IP de la máquina virtual de puerta de enlace son las mismas que las que ve al utilizar el software cliente del hipervisor (es decir, el VMware vSphere cliente o Microsoft Hyper-V Manager). Si encuentra una discrepancia, reinicie la puerta de enlace desde la consola de Storage Gateway, como se muestra en Como apagar la MV de la gateway. Tras el reinicio, las direcciones de la lista Direcciónes IP de la pestaña Puerta de enlace de la consola de Storage Gateway deberían coincidir con las direcciones IP de la puerta de enlace, las cuales determina desde el cliente del hipervisor.• VMwareESXiEn efecto, la dirección IP de la máquina virtual se encuentra en el vSphere cliente, en la pestaña Resumen.• Para Microsoft Hyper-V, la dirección IP de la MV puede encontrarse al iniciar sesión en la consola local.• Compruebe la conectividad de la puerta de enlace tal y AWS como se describe en Prueba de conexión de la gateway a Internet.• Compruebe la configuración del adaptador de red de la puerta de enlace y asegúrese de que todas las interfaces que desee activar para la puerta de enlace estén activadas. Para ver la configuración del adaptador de red para la gateway, siga las instrucciones de Configuración de red de la gateway y seleccione la opción para ver la configuración de red de la gateway. <p>Puedes ver el rendimiento desde y hacia tu puerta de enlace desde la CloudWatch consola de Amazon. Para obtener más información sobre cómo medir el rendimiento desde y hacia tu puerta de enlace AWS, consulta. Medición del rendimiento entre su puerta de enlace de cinta y AWS</p>

Problema	Acción que ejecutar
Tiene problemas para importar (implementar) Storage Gateway en Microsoft Hyper-V.	Consulte Solución de problemas de configuración de Microsoft Hyper-V , donde se explican algunos de los problemas comunes de implementar una gateway en Microsoft Hyper-V.
Recibirá un mensaje que indica: “Los datos que se han escrito en el volumen en la puerta de enlace no se almacenan de forma segura en AWS”.	Recibirá este mensaje si la máquina virtual de la gateway se creó a partir de un clon o de una instantánea de otra máquina virtual de gateway. Si este no es el caso, póngase en contacto con AWS Support.


Permiten ayudar AWS Support a solucionar los problemas de su puerta de enlace alojada en las instalaciones

Storage Gateway proporciona una consola local que puede usar para realizar varias tareas de mantenimiento, incluida la activación AWS Support para acceder a su puerta de enlace para ayudarlo a solucionar problemas de la puerta de enlace. De forma predeterminada, el AWS Support acceso a la puerta de enlace está desactivado. Proporcione este acceso mediante la consola local del host. Para AWS Support acceder a su puerta de enlace, primero debe iniciar sesión en la consola local del host, ir a la consola de Storage Gateway y, a continuación, conectarse al servidor de soporte.

Para permitir el AWS Support acceso a su puerta de enlace

- Inicie sesión en la consola local del host.
 - VMwareESXi— para obtener más información, consulte [Acceder a la consola local de Gateway con VMware ESXi](#).
 - Microsoft Hyper-V: para obtener más información, consulte [Acceso a la consola local de la gateway con Microsoft Hyper-V](#).
- Cuando se le solicite, introduzca el número correspondiente para seleccionar Consola de puerta de enlace.
- Introduzca **h** para abrir la lista de comandos disponibles.
- Realice una de las siguientes acciones siguientes:

- Si su puerta de enlace utiliza un punto final público, en la AVAILABLECOMMANDSventana, introduzca **open-support-channel** para conectarse al servicio de atención al cliente de Storage Gateway. Habilite el TCP puerto 22 para poder abrir un canal de soporte AWS. Cuando conecte con el servicio de atención al cliente, Storage Gateway le asignará un número de soporte. Apunte el número de soporte.
- Si su puerta de enlace utiliza un VPC punto final, introduzca en la AVAILABLECOMMANDSventana **open-support-channel**. Si la puerta de enlace no está activada, proporcione el VPC punto final o la dirección IP para conectarse al servicio de atención al cliente de Storage Gateway. Habilite el TCP puerto 22 para poder abrir un canal de soporte AWS. Cuando conecte con el servicio de atención al cliente, Storage Gateway le asignará un número de soporte. Apunte el número de soporte.

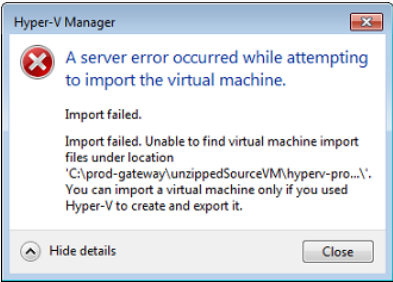
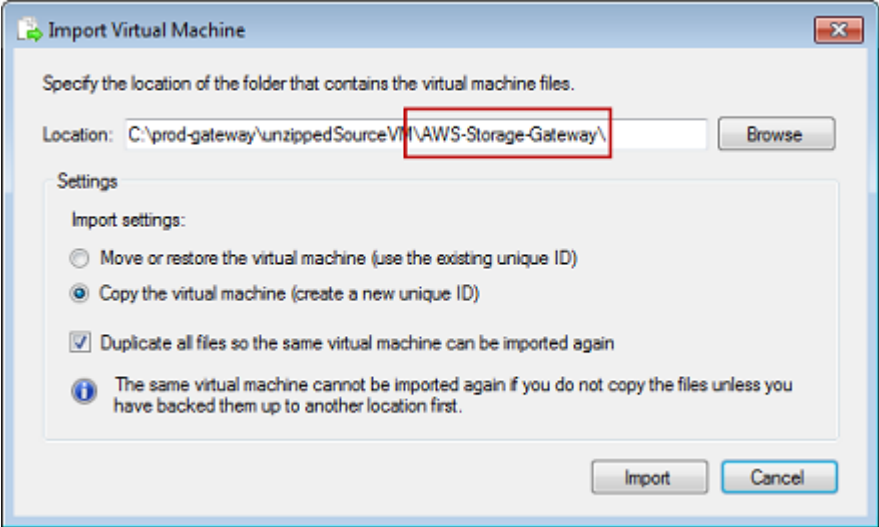
 Note

El número de canal no es un número de puerto del Protocolo de control de transmisión/ Protocolo de datagramas de usuario (TCP/UDP). En su lugar, la puerta de enlace establece una conexión Secure Shell (SSH) (TCP22) con los servidores Storage Gateway y proporciona el canal de soporte para la conexión.

5. Una vez establecido el canal de soporte, proporcione su número de servicio de soporte para AWS Support que AWS Support pueda ayudarlo a solucionar problemas.
6. Cuando se complete la sesión de soporte, introduzca **q** para finalizarla. No cierre la sesión hasta que el servicio de soporte de Amazon Web Services le notifique que la sesión de soporte se ha completado.
7. Introduzca **exit** para cerrar sesión en la consola de la puerta de enlace.
8. Siga las instrucciones para salir de la consola local.

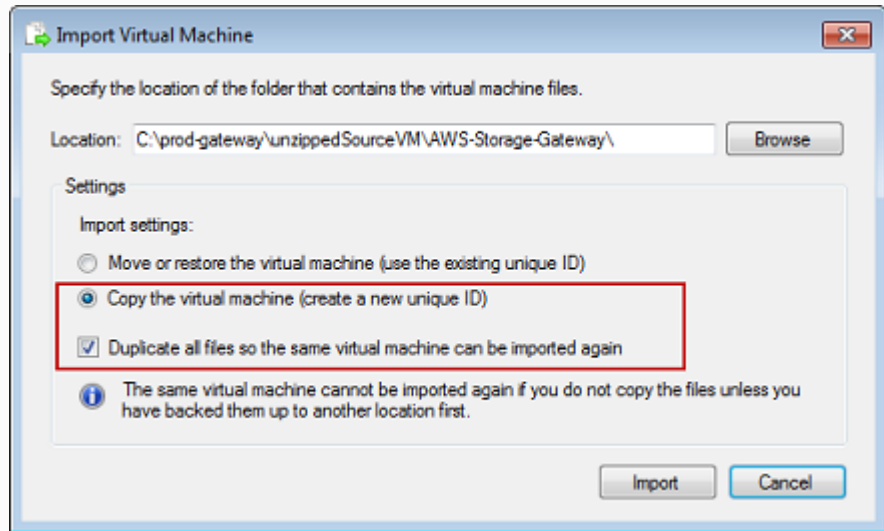
Solución de problemas de configuración de Microsoft Hyper-V

En la siguiente tabla se muestran los problemas habituales que podrían surgir al implementar Storage Gateway en la plataforma de Microsoft Hyper-V.

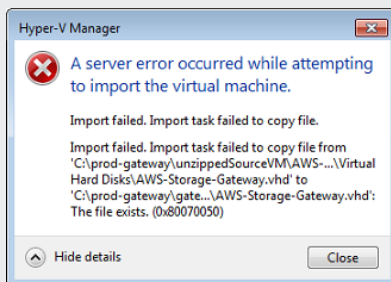
Problema	Acción que ejecutar
<p>Intenta importar una gateway y recibe el mensaje de error: "Import failed. Unable to find virtual machine import file under location ...".</p>  <p>The screenshot shows an error dialog box from Hyper-V Manager. The title is 'Hyper-V Manager'. The main text reads: 'A server error occurred while attempting to import the virtual machine.' Below this, it says 'Import failed.' and 'Import failed. Unable to find virtual machine import files under location 'C:\prod-gateway\unzippedSourceVM\hyperv-pro...\'.' It also includes a note: 'You can import a virtual machine only if you used Hyper-V to create and export it.' There are 'Hide details' and 'Close' buttons at the bottom.</p>	<p>Este error puede producirse por las razones siguientes:</p> <ul style="list-style-type: none">• 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 <code>AWS-Storage-Gateway\</code>, como se muestra en el siguiente ejemplo:  <p>The screenshot shows the 'Import Virtual Machine' dialog box. The title is 'Import Virtual Machine'. The main text reads: 'Specify the location of the folder that contains the virtual machine files.' Below this, there is a 'Location:' field with the text 'C:\prod-gateway\unzippedSourceVM\AWS-Storage-Gateway\' and a 'Browse' button. The 'Settings' section has the following options: 'Import settings:' with three radio buttons: 'Move or restore the virtual machine (use the existing unique ID)', 'Copy the virtual machine (create a new unique ID)' (which is selected), and 'Duplicate all files so the same virtual machine can be imported again' (which is checked). There is also an information icon and a note: 'The same virtual machine cannot be imported again if you do not copy the files unless you have backed them up to another location first.' There are 'Import' and 'Cancel' buttons at the bottom.</p> <ul style="list-style-type: none">• 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

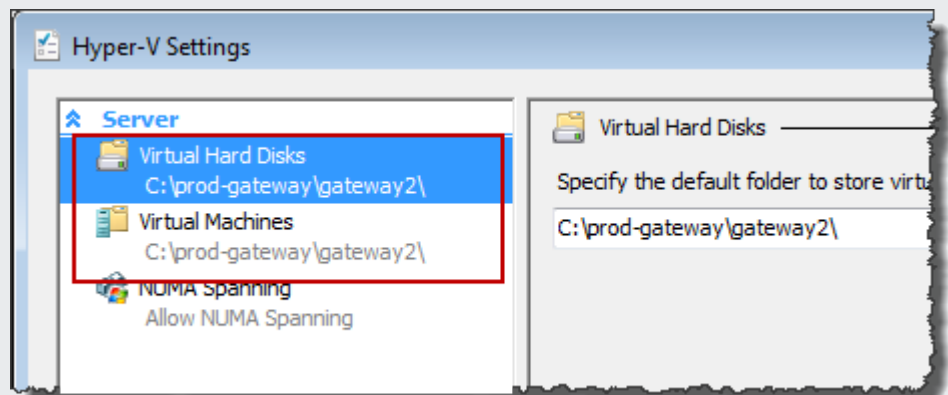
Acción que ejecutar



Intenta importar una gateway y recibe el mensaje de error: "Import failed. Import task failed to copy file."

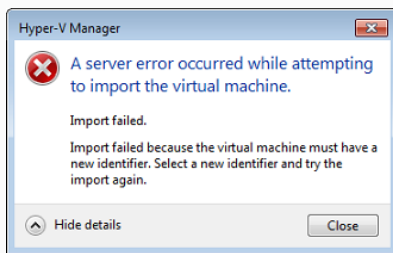


Si ya ha implementado una gateway e intenta reutilizar las carpetas predeterminadas donde se almacenan los archivos del disco duro virtual y los archivos de configuración de máquinas virtuales, se producirá este error. Para solucionar este problema, especifique nuevas ubicaciones en el cuadro de diálogo Hyper-V Settings (Configuración de Hyper-V).

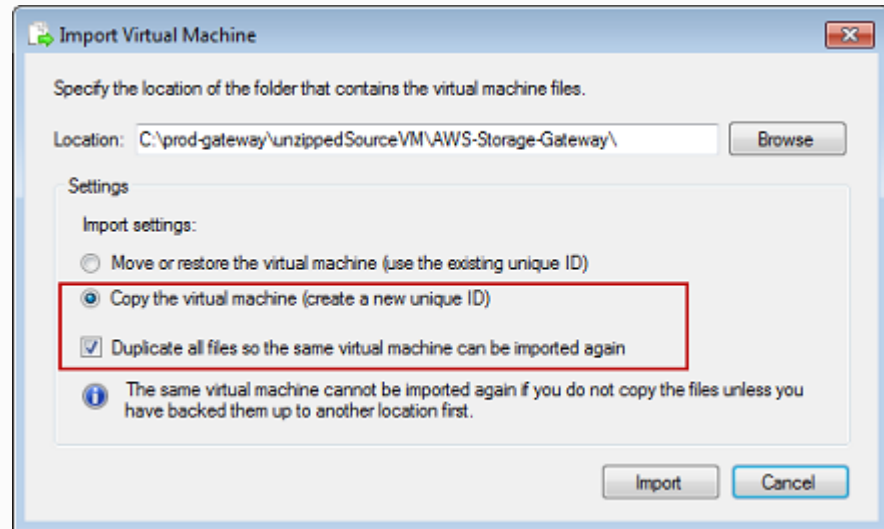


Problema	Acción que ejecutar
----------	---------------------

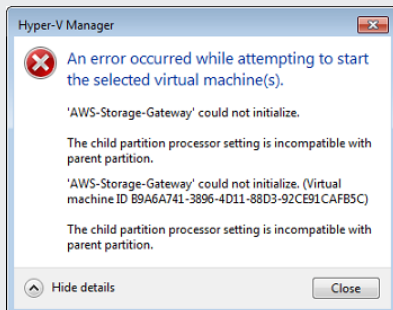
Intenta importar una gateway y recibe un mensaje de error: "Import failed. Import failed because the virtual machine must have a new identifier. Select a new identifier and try the import again."



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.



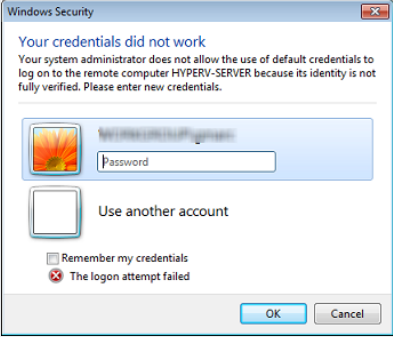
Intenta iniciar una MV de gateway y recibe un mensaje de error "The child partition processor setting is incompatible with parent partition."



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 compatible con el hipervisor subyacente.

Para obtener más información sobre los requisitos de Storage Gateway, consulte [Requisitos para configurar Tape Gateway](#).

Problema	Acción que ejecutar
<p>Intenta iniciar una MV de la gateway y recibe un mensaje de error "Failed to create partition: Insufficient resources exist to complete the requested service."</p> 	<p>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.</p> <p>Para obtener más información sobre los requisitos de Storage Gateway, consulte Requisitos para configurar Tape Gateway.</p>
<p>Las actualizaciones del software de la gateway y de las instantáneas se producen a horas ligeramente diferentes de lo esperado.</p>	<p>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 Sincronización de la hora de la MV de la gateway.</p>
<p>Debe colocar los archivos de Microsoft Hyper-V Storage Gateway sin comprimir en el sistema de archivos del host.</p>	<p>Acceda al host como lo hace en un servidor de Microsoft Windows típico. Por ejemplo, si el host del hipervisor se llama <code>hyperv-server</code>, puede utilizar la siguiente ruta UNC <code>\\hyperv-server\c\$</code>, en la que se asume que el nombre <code>hyperv-server</code> se puede resolver o está definido en el archivo del host local.</p>

Problema	Acción que ejecutar
<p>Se le solicitan credenciales al conectarse al hipervisor.</p> 	<p>Agregue sus credenciales de usuario como administrador local para el host del hipervisor a través de la herramienta Sconfig.cmd.</p>
<p>Es posible que observe un rendimiento de red deficiente si activa la cola de máquinas virtuales (VMQ) en un host Hyper-V que utilice un adaptador de red Broadcom.</p>	<p>Para obtener información sobre una solución alternativa, vea la documentación de Microsoft y consulte Poor network performance on virtual machines on a Windows Server 2012 Hyper-V host if VMQ is activated.</p>

Solución de problemas de Amazon EC2 Gateway

En las siguientes secciones, puede encontrar los problemas típicos que puede encontrar al trabajar con su puerta de enlace implementada en AmazonEC2. Para obtener más información sobre la diferencia entre una puerta de enlace local y una puerta de enlace implementada en AmazonEC2, consulte [Implementación de una EC2 instancia de Amazon para alojar su Tape Gateway.](#)

Temas

- [La puerta de enlace no se ha activado poco tiempo después](#)
- [No encuentra su instancia de EC2 gateway en la lista de instancias](#)
- [Creaste un EBS volumen de Amazon pero no puedes adjuntarlo a tu instancia de EC2 gateway](#)
- [Obtiene un mensaje que indica que no tiene discos disponibles al tratar de agregar volúmenes de almacenamiento](#)
- [Necesita eliminar un disco asignado como espacio del búfer de carga para reducir la cantidad de espacio del búfer de carga](#)

- [El rendimiento hacia o desde su EC2 puerta de enlace se reduce a cero](#)
- [¿Desea ayudar AWS Support a solucionar los problemas de su puerta de enlace EC2](#)
- [Quieres conectarte a tu instancia de gateway mediante la consola EC2 serie de Amazon](#)

La puerta de enlace no se ha activado poco tiempo después

Comprueba lo siguiente en la EC2 consola de Amazon:

- El puerto 80 está activado en el grupo de seguridad que ha asociado a la instancia. Para obtener más información sobre cómo añadir una regla de grupo de seguridad, consulte [Añadir una regla de grupo de seguridad](#) en la Guía del EC2 usuario de Amazon.
- La instancia de la gateway está marcada como en ejecución. En la EC2 consola de Amazon, el valor de estado de la instancia debe ser RUNNING.
- Asegúrese de que el tipo de EC2 instancia de Amazon cumpla los requisitos mínimos, tal y como se describe en [Requisitos de almacenamiento](#).

Después de corregir el problema, intente activar la gateway de nuevo. Para ello, abra la consola de Storage Gateway, elija Deploy a new Gateway on Amazon EC2 y vuelva a introducir la dirección IP de la instancia.

No encuentra su instancia de EC2 gateway en la lista de instancias

Si no asignó a la instancia una etiqueta de recurso y tiene muchas instancias en funcionamiento, puede ser difícil saber qué instancia lanzó. En este caso, puede realizar las siguientes acciones para encontrar la instancia de la gateway:

- Comprueba el nombre de Amazon Machine Image (AMI) en la pestaña Descripción de la instancia. Una instancia basada en Storage Gateway AMI debe empezar por el texto **aws-storage-gateway-ami**.
- Si tiene varias instancias basadas en Storage Gateway AMI, compruebe la hora de lanzamiento de la instancia para encontrar la instancia correcta.

Creaste un EBS volumen de Amazon pero no puedes adjuntarlo a tu instancia de EC2 gateway

Compruebe que el EBS volumen de Amazon en cuestión esté en la misma zona de disponibilidad que la instancia de puerta de enlace. Si hay una discrepancia en las zonas de disponibilidad, crea un nuevo EBS volumen de Amazon en la misma zona de disponibilidad que tu instancia.

Obtiene un mensaje que indica que no tiene discos disponibles al tratar de agregar volúmenes de almacenamiento

Para una gateway recién activada, no hay almacenamiento de volumen definido. Antes de definir el almacenamiento de volumen, debe asignar discos locales a la gateway para utilizarlos como búfer de carga y almacenamiento en caché. En el caso de una puerta de enlace implementada en AmazonEC2, los discos locales son EBS volúmenes de Amazon conectados a la instancia. Es probable que este mensaje de error se deba a que no hay ningún EBS volumen de Amazon definido para la instancia.

Consulte los dispositivos de bloques definidos para la instancia que está ejecutando la gateway. Si solo hay dos dispositivos en bloque (los dispositivos predeterminados que vienen con AMI ellos), debes añadir almacenamiento. Para obtener más información sobre cómo hacerlo, consulte [Implementación de una EC2 instancia de Amazon para alojar su Tape Gateway](#). Tras adjuntar dos o más EBS volúmenes de Amazon, intenta crear un volumen de almacenamiento en la puerta de enlace.

Necesita eliminar un disco asignado como espacio del búfer de carga para reducir la cantidad de espacio del búfer de carga

Siga los pasos de [Determinación del tamaño que se va a asignar al búfer de carga](#).

El rendimiento hacia o desde su EC2 puerta de enlace se reduce a cero

Compruebe que la instancia de la gateway esté en funcionamiento. Si la instancia se está iniciando debido a un reinicio, por ejemplo, espere a que la instancia se reinicie.

Compruebe también que la IP de la gateway no haya cambiado. Si la instancia se ha detenido y, a continuación, se ha reiniciado, es posible que la dirección IP de la instancia haya cambiado. En este caso, debe activar una nueva gateway.

Puedes ver el rendimiento desde y hacia tu puerta de enlace desde la CloudWatch consola de Amazon. Para obtener más información sobre cómo medir el rendimiento desde y hacia tu pasarela AWS, consulta [Medición del rendimiento entre su puerta de enlace de cinta y AWS](#)

¿Desea ayudar AWS Support a solucionar los problemas de su puerta de enlace EC2

Storage Gateway proporciona una consola local que puede usar para realizar varias tareas de mantenimiento, incluida la activación AWS Support para acceder a su puerta de enlace para ayudarlo a solucionar problemas de la puerta de enlace. De forma predeterminada, el AWS Support acceso a la puerta de enlace está desactivado. Usted proporciona este acceso a través de la consola EC2 local de Amazon. Se inicia sesión en la consola EC2 local de Amazon a través de un Secure Shell (SSH). Para iniciar sesión correctamente SSH, el grupo de seguridad de la instancia debe tener una regla que abra el TCP puerto 22.

Note

Si agrega una nueva regla a un grupo de seguridad existente, la nueva regla se aplicará a todas las instancias que utilicen ese grupo de seguridad. Para obtener más información sobre los grupos de seguridad y cómo añadir una regla de grupo de seguridad, consulte [los grupos de EC2 seguridad de Amazon](#) en la Guía del EC2 usuario de Amazon.

Para permitir la AWS Support conexión a su puerta de enlace, primero debe iniciar sesión en la consola local de la EC2 instancia de Amazon, navegar hasta la consola de Storage Gateway y, a continuación, proporcionar el acceso.

Para activar el AWS Support acceso a una puerta de enlace implementada en una EC2 instancia de Amazon

1. Inicia sesión en la consola local de tu EC2 instancia de Amazon. Para obtener instrucciones, consulta [Connect to your instance](#) en la Guía del EC2 usuario de Amazon.

Puedes usar el siguiente comando para iniciar sesión en la consola local de la EC2 instancia.

```
ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
```

Note

La **PRIVATE-KEY** es el .pem archivo que contiene el certificado privado del EC2 key pair que utilizaste para lanzar la EC2 instancia de Amazon. Para obtener más información, consulta [Cómo recuperar la clave pública de tu par de claves](#) en la Guía del EC2 usuario de Amazon.

La **INSTANCE-PUBLIC-DNS-NAME** es el nombre del Sistema de nombres de dominio público (DNS) de la EC2 instancia de Amazon en la que se ejecuta la puerta de enlace. Para obtener este DNS nombre público, seleccione la EC2 instancia de Amazon en la EC2 consola y haga clic en la pestaña Descripción.

2. En el símbolo del sistema, introduzca **6 - Command Prompt** para abrir la consola del canal de AWS Support .
3. Entra **h** para abrir la AVAILABLECOMMANDSventana.
4. Realice una de las siguientes acciones siguientes:
 - Si su puerta de enlace utiliza un punto final público, en la AVAILABLECOMMANDSventana, introduzca **open-support-channel** para conectarse al servicio de atención al cliente de Storage Gateway. Habilite el TCP puerto 22 para poder abrir un canal de soporte AWS. Cuando conecte con el servicio de atención al cliente, Storage Gateway le asignará un número de soporte. Apunte el número de soporte.
 - Si su puerta de enlace utiliza un VPC punto final, introduzca en la AVAILABLECOMMANDSventana **open-support-channel**. Si la puerta de enlace no está activada, proporcione el VPC punto final o la dirección IP para conectarse al servicio de atención al cliente de Storage Gateway. Habilite el TCP puerto 22 para poder abrir un canal de soporte AWS. Cuando 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 del Protocolo de control de transmisión/ Protocolo de datagramas de usuario (TCP/UDP). En su lugar, la puerta de enlace establece una conexión Secure Shell (SSH) (TCP22) con los servidores Storage Gateway y proporciona el canal de soporte para la conexión.

5. Una vez establecido el canal de soporte, proporcione su número de servicio de soporte para AWS Support que AWS Support pueda ayudarlo a solucionar problemas.
6. Cuando se complete la sesión de soporte, introduzca **q** para finalizarla. No cierre la sesión hasta que se le AWS Support notifique que la sesión de soporte ha finalizado.
7. Introduzca **exit** para salir de la consola de Storage Gateway.
8. Siga los menús de la consola para cerrar sesión en la instancia de Storage Gateway.

Quieres conectarte a tu instancia de gateway mediante la consola EC2 serie de Amazon

Puedes usar la consola EC2 serie de Amazon para solucionar problemas de arranque, configuración de red y otros problemas. Para obtener instrucciones y consejos de solución de problemas, consulte [Amazon EC2 Serial Console](#) en la Guía del usuario de Amazon Elastic Compute Cloud.

Solución de problemas del dispositivo de hardware

En los siguientes temas, se explican los problemas que pueden producirse con el dispositivo de hardware de Storage Gateway y 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 restablece la configuración 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 soporte, como se describe en la sección de soporte a continuación.

¿Cómo se realiza un reinicio remoto?

Si necesita realizar un reinicio remoto del dispositivo, puede hacerlo mediante la interfaz de DRAC administración Dell i. Para obtener más información, consulte [i Ciclo de alimentación DRAC9 virtual:](#)

[apague EMC PowerEdge los servidores Dell de forma remota](#) en el InfoHub sitio web de Dell Technologies.

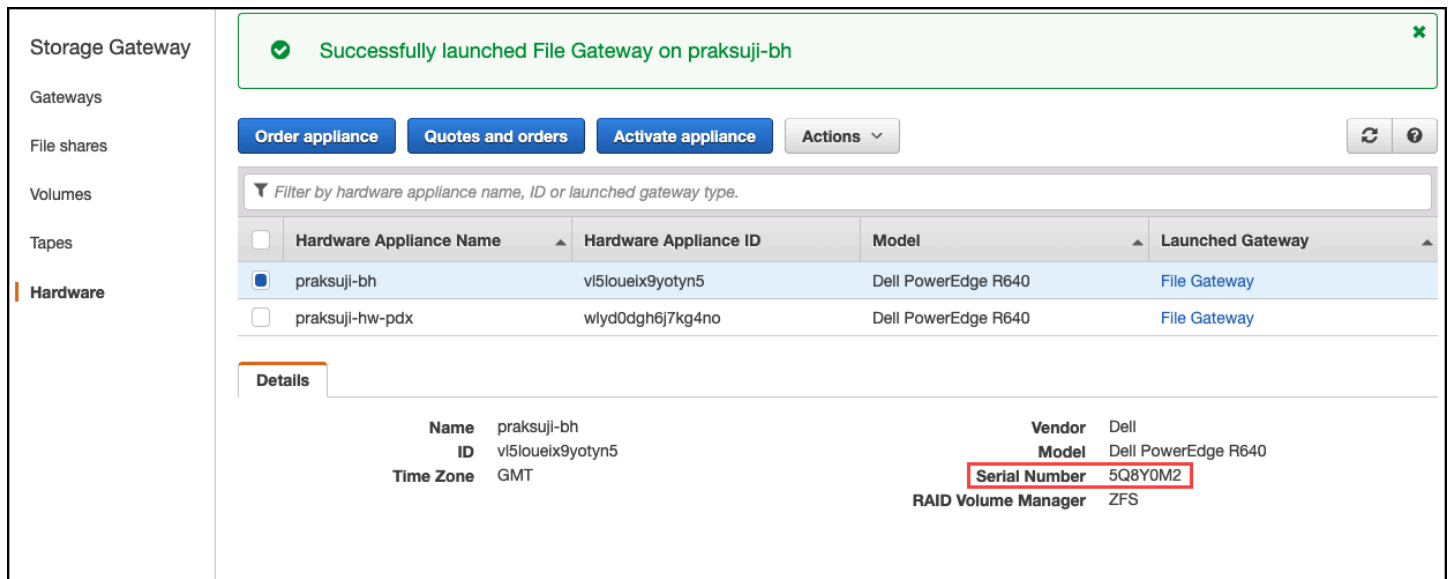
¿Dónde puede obtener el DRAC soporte Dell i?

El servidor Dell PowerEdge R640 incluye la interfaz de DRAC administración Dell i. Le recomendamos lo siguiente:

- Si utiliza la interfaz DRAC de administración i, debe cambiar la contraseña predeterminada. Para obtener más información sobre las DRAC credenciales i, consulte [Dell PowerEdge : ¿Cuáles son las credenciales de inicio de sesión predeterminadas para i? DRAC](#) .
- Asegúrese de que el firmware sea up-to-date para evitar violaciones de seguridad.
- Mover la interfaz de DRAC red i a un puerto normal (em) puede provocar problemas de rendimiento o impedir el funcionamiento normal del dispositivo.

No puede encontrar el número de serie del dispositivo hardware

Para encontrar el número de serie del dispositivo hardware, vaya a la página Información general sobre el dispositivo de hardware en la consola de Storage Gateway como se muestra a continuación. Pestaña de hardware de la consola de Storage Gateway donde se muestra el dispositivo seleccionado y los detalles.



Storage Gateway

Gateways

File shares

Volumes

Tapes

Hardware

Successfully launched File Gateway on praksuji-bh

Order appliance Quotes and orders Activate appliance Actions

Filter by hardware appliance name, ID or launched gateway type.

Hardware Appliance Name	Hardware Appliance ID	Model	Launched Gateway
<input checked="" type="checkbox"/> praksuji-bh	vi5loueix9yotyn5	Dell PowerEdge R640	File Gateway
<input type="checkbox"/> praksuji-hw-pdx	wlyd0dgh6j7kg4no	Dell PowerEdge R640	File Gateway

Details

Name	praksuji-bh	Vendor	Dell
ID	vi5loueix9yotyn5	Model	Dell PowerEdge R640
Time Zone	GMT	Serial Number	5Q8Y0M2
		RAID Volume Manager	ZFS

Pestaña de hardware de la consola de Storage Gateway donde se muestra el dispositivo seleccionado y los detalles.

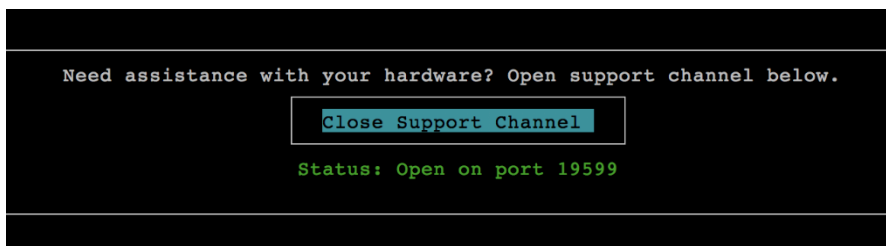
Dónde obtener soporte para el dispositivo de hardware

Para ponerse en contacto con el soporte de dispositivo de hardware de Storage Gateway, consulte [AWS Support](#).

Es posible que el AWS Support equipo le pida que active el canal de soporte para solucionar los problemas de la puerta de enlace de forma remota. No necesita que este puerto esté abierto para el funcionamiento normal de la gateway, pero es necesario para la solución de problemas. Puede activar el canal de soporte desde la consola del hardware, como se muestra en el siguiente procedimiento.

Para abrir un canal de soporte para AWS

1. Abra la consola del hardware.
2. Elija Open Support Channel (Abrir canal de soporte) como se muestra a continuación. se muestra el estado de la consola del dispositivo de hardware con el canal de soporte.



se muestra el estado de la consola del dispositivo de hardware con el canal de soporte.

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 e indíquelo en AWS Support.

Solución de problemas con cintas virtuales

A continuación encontrará información sobre las acciones que debe realizar si experimenta problemas inesperados con las cintas virtuales.

Temas

- [Recuperar una cinta virtual de una gateway no recuperable](#)
- [Solución problemas de cintas irrecuperables](#)
- [Notificaciones de estado de alta disponibilidad](#)

Recuperar una cinta virtual de una gateway no recuperable

Aunque es infrecuente, es posible que la puerta de enlace de cinta se enfrente a un error irrecuperable. Este fallo puede producirse host del hipervisor, en la propia gateway o en los discos de caché. Si se produce un error, puede seguir las instrucciones en esta sección para recuperar las cintas.

Temas

- [Necesita recuperar una cinta virtual desde una puerta de enlace de cinta que no funciona correctamente](#)
- [Necesita recuperar una cinta virtual desde un disco de caché que no funciona correctamente](#)

Necesita recuperar una cinta virtual desde una puerta de enlace de cinta que no funciona correctamente

Si su Tape Gateway o el host del hipervisor encuentran un error irrecuperable, puede recuperar cualquier dato que ya se haya cargado en otro Tape Gateway. AWS

Tenga en cuenta que es posible que los datos escritos en una cinta no se carguen completamente hasta que la cinta se haya archivado correctamente. VTS Los datos de cintas recuperadas en otra gateway de esta forma pueden estar incompletos o vacíos. Le recomendamos realizar un inventario de todas las cintas recuperadas para asegurarse de que contienen el contenido esperado.

Para recuperar una cinta en otra puerta de enlace de cinta

1. Identifique una puerta de enlace de cinta funcional para que sirva como puerta de enlace de destino de recuperación. Si no dispone de una puerta de enlace de cinta en la que recuperar las cintas, cree una nueva puerta de enlace de cinta. Para obtener información sobre cómo crear una puerta de enlace, consulte [Creación de una puerta de enlace](#).
2. Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa>.
3. En el panel de navegación, elija Puertas de enlace y, a continuación, elija la puerta de enlace de cinta desde la que desea recuperar cintas.
4. Elija la pestaña Detalles. En la pestaña se muestra un mensaje de recuperación de cinta.
5. Elija Crear cintas de recuperación para desactivar la puerta de enlace.
6. En el cuadro de diálogo que aparece, elija Disable gateway (Deshabilitar gateway).

Este proceso detiene de forma permanente el funcionamiento normal de la puerta de enlace de cinta y expone los puntos de recuperación disponibles. Para obtener instrucciones, consulte [Desactivación de la puerta de enlace de cinta](#).

- Entre las cintas que muestra la puerta de enlace desactivada, elija la cinta virtual y el punto de recuperación que desea recuperar. Una cinta virtual puede tener varios puntos de recuperación.
- Para empezar a recuperar cualquier cinta que necesite en la puerta de enlace de cinta de destino, elija Crear cintas de recuperación.
- En el cuadro de diálogo Create recovery tape (Crear cinta de recuperación), verifique el código de barras de la cinta virtual que desee recuperar.
- En Puerta de enlace, elija la puerta de enlace de cinta en la que desee recuperar la cinta virtual.
- Elija Create recovery tape (Crear cinta de recuperación).
- Elimine la puerta de enlace de cinta que produjo el error para no incurrir en cargos. Para obtener instrucciones, consulte [Eliminar la puerta de enlace y eliminar los recursos asociados](#).

Storage Gateway mueve la cinta de la puerta de enlace de cinta que produjo el error a la puerta de enlace de cinta que especificó. La puerta de enlace de cintas marca el estado de la cinta como RECOVERED.

Necesita recuperar una cinta virtual desde un disco de caché que no funciona correctamente

Si el disco de caché produce un error, la gateway impide las operaciones de lectura y escritura en cintas virtuales de la gateway. Por ejemplo, se puede producir un error cuando un disco está dañado o se ha retirado de la gateway. La consola de Storage Gateway muestra un mensaje sobre el error.

En el mensaje de error, Storage Gateway le pide que realice una de las dos acciones que pueden recuperar las cintas:

- Apagar y volver a agregar discos: adopte este enfoque si el disco tiene datos intactos y se ha retirado. Por ejemplo, si el error se ha producido porque se ha retirado un disco del host por accidente pero el disco y los datos están intactos, puede volver a agregar el disco. Para ello, consulte el procedimiento más adelante en este tema.
- Restablecer disco de caché: adopte este enfoque si el disco de caché está dañado o no permite el acceso. Si el error de disco impide el acceso al disco de caché, lo deja inutilizable o lo daña, puede restablecer el disco. Si restablece el disco de caché, las cintas que tengan datos limpios

(es decir, cintas para las que el disco de caché y Amazon S3 estén sincronizados) continuarán estando disponibles para que las utilice. Sin embargo, las cintas que tienen datos que no están sincronizados con Amazon S3 se recuperan automáticamente. El estado de estas cintas está establecido en RECOVERED, pero serán de solo lectura. Para obtener información sobre cómo retirar un disco del host, consulte [Determinación del tamaño que se va a asignar al búfer de carga](#).

⚠ Important

Si el disco de caché que está restableciendo contiene datos que no se hayan cargado aún en Amazon S3, esos datos pueden perderse. Después de restablecer discos de caché, no quedarán discos de caché en la gateway, así que debe configurar al menos un nuevo disco de caché para que la gateway funcione correctamente.

Para restablecer el disco de caché, consulte el procedimiento más adelante en este tema.

Para apagar y volver a agregar un disco

1. Apague la gateway. Para obtener información sobre cómo apagar una gateway, consulte [Como apagar la MV de la gateway](#).
2. Vuelva a agregar el disco al host y asegúrese de que el número de nodo del disco no haya cambiado. Para obtener información sobre cómo agregar un disco, consulte [Determinación del tamaño que se va a asignar al búfer de carga](#).
3. Reinicie la gateway. Para obtener información sobre cómo reiniciar una gateway, consulte [Como apagar la MV de la gateway](#).

Una vez que se reinicie la gateway, puede verificar el estado de los discos de caché. El estado de un disco puede ser uno de los siguientes:

- present: el disco está disponible para su uso.
- missing: el disco ya no está conectado a la gateway.
- mismatch: el nodo de disco está ocupado por un disco que tiene metadatos incorrectos o el contenido del disco está dañado.

Para restablecer y volver a configurar un disco de caché

1. En el mensaje de error A disk error has occurred (Se ha producido un error en el disco) que se muestra más arriba, elija Reset Cache Disk (Restablecer disco de caché).
2. En la página Configurar puerta de enlace, configure el disco para el almacenamiento en caché. Para obtener información acerca de cómo hacerlo, consulte [Configuración de la puerta de enlace de cinta](#).
3. Una vez que haya configurado el almacenamiento en caché, apague y reinicie la gateway como se describe en el procedimiento anterior.

La gateway debe recuperarse tras el reinicio. A continuación, puede comprobar el estado del disco de caché.

Para verificar el estado de un disco de caché

1. Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa>.
2. En el panel de navegación, elija Gateways y, a continuación, elija la gateway.
3. En Actions (Acciones), elija Configure Local Storage (Configurar el almacenamiento local) para mostrar el cuadro de diálogo Configure Local Storage (Configurar el almacenamiento local). Este cuadro de diálogo muestra todos los discos de la gateway.

El estado del nodo de disco de caché se muestra junto al disco.

Note

Si no completa el proceso de recuperación, la gateway muestra una pancarta que le solicita que configure almacenamiento local.

Solución problemas de cintas irrecuperables

Si la cinta virtual falla inesperadamente, Storage Gateway establece el estado de la cinta virtual fallida en IRRECOVERABLE. La acción que deberá realizar depende de las circunstancias. A continuación puede encontrar información sobre algunos problemas que pueden producirse y cómo solucionarlos.

Necesita recuperar los datos de una IRRECOVERABLE cinta

Si tiene una cinta virtual con ese estado IRRECOVERABLE y necesita trabajar con ella, pruebe una de las siguientes opciones:

- Active una nueva puerta de enlace de cinta si no tiene una activada. Para obtener más información, consulte [Creación de una puerta de enlace](#).
- Desactive la puerta de enlace de cinta que contiene la cinta irrecuperable y recupere la cinta desde un punto de recuperación en la nueva puerta de enlace de cinta. Para obtener más información, consulte [Necesita recuperar una cinta virtual desde una puerta de enlace de cinta que no funciona correctamente](#).

Note

Debe volver a configurar el SCSI iniciador i y la aplicación de backup para utilizar el nuevo Tape Gateway. Para obtener más información, consulte [Conexión de sus VTL dispositivos](#).

No necesita una IRRECOVERABLE cinta que no esté archivada

Si tiene una cinta virtual con este estado IRRECOVERABLE, no la necesita y la cinta nunca se archivó, debe eliminarla. Para obtener más información, consulte [Eliminar cintas virtuales de la puerta de enlace de cintas](#).

Un disco de caché de la gateway produce un error

Si el disco de caché produce un error, la puerta de enlace impide las operaciones de lectura y escritura en sus cintas virtuales. Para reanudar la funcionalidad normal, vuelva a configurar la puerta de enlace según se describe a continuación:

- Si el disco de caché es inaccesible o inutilizable, elimínelo de la configuración de la puerta de enlace.
- Si el disco de caché sigue siendo accesible y utilizable, vuelva a conectarlo a la puerta de enlace.

Note

Si elimina un disco de caché, las cintas o los volúmenes que tienen datos limpios (es decir, para los que se sincronizan los datos del disco de caché y Amazon S3) seguirán estando

disponibles cuando la puerta de enlace reanude la funcionalidad normal. Por ejemplo, si la puerta de enlace tiene tres discos de caché y usted elimina dos, las cintas o los volúmenes que estén limpios tendrán el AVAILABLE estado correspondiente. Las demás cintas y volúmenes tendrán este IRRECOVERABLE estado.

Si utiliza discos efímeros como discos de caché para la puerta de enlace o monta los discos de caché en una unidad efímera, estos se perderán cuando cierre la puerta de enlace. Si se cierra la puerta de enlace cuando el disco de caché y Amazon S3 no están sincronizados, se pueden perder los datos. En consecuencia, no es recomendable el uso de unidades o discos efímeros.

Notificaciones de estado de alta disponibilidad

Al ejecutar su puerta de enlace en la plataforma de VMware vSphere alta disponibilidad (HA), es posible que reciba notificaciones de estado. Para obtener más información sobre las notificaciones de estado, consulte [Solución de problemas de alta disponibilidad](#).

Solución de problemas de alta disponibilidad

A continuación puede encontrar información acerca de las acciones que debe realizar si experimenta problemas de disponibilidad.

Temas

- [Notificaciones de estado](#)
- [Métricas](#)

Notificaciones de estado

Cuando ejecuta la puerta de enlace en VMware vSphere HA, todas las puertas de enlace producen las siguientes notificaciones de estado en el grupo de registros de Amazon CloudWatch configurado. Estas notificaciones van a un flujo de registro denominado AvailabilityMonitor.

Temas

- [Notificación: reinicio](#)
- [Notificación: HardReboot](#)
- [Notificación: HealthCheckFailure](#)

- [Notificación: AvailabilityMonitorTest](#)

Notificación: reinicio

Puede recibir una notificación de reinicio cuando la MV de la gateway se reinicia. Puede reiniciar la VM de una puerta de enlace mediante la consola de gestión de hipervisor de VM o la consola de Storage Gateway. También puede llevar a cabo el reinicio de la gateway mediante el software de la gateway durante el ciclo de mantenimiento de la gateway.

Acción necesaria

Si la hora del reinicio se encuentra dentro de un periodo de 10 minutos desde la [hora de inicio de mantenimiento](#) configurada de la gateway, es probable que sea un evento normal y no sea signo de ningún problema. Si el reinicio se produce significativamente fuera del periodo de mantenimiento, compruebe si la gateway se ha reiniciado de forma manual.

Notificación: HardReboot

Puede recibir una notificación `HardReboot` cuando la MV de la gateway se reinicia de forma inesperada. Este reinicio se puede deber a una pérdida de potencia, un fallo de hardware u otro evento. En las puertas de enlace de VMware, un reinicio provocado por la supervisión de aplicaciones de alta disponibilidad de vSphere puede producir 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 ayuda adicional, póngase en contacto con AWS Support.

Notificación: `AvailabilityMonitorTest`

En una puerta de enlace de VMware vSphere HA, puede recibir una notificación de `AvailabilityMonitorTest` cuando [ejecuta una prueba](#) del sistema de [Supervisión de aplicaciones y disponibilidad](#) en VMware.

Métricas

La métrica `AvailabilityNotifications` está disponible en todas las gateways. Esta métrica es un recuento del número de notificaciones de estado relacionadas con la disponibilidad que ha generado la gateway. Utilice la estadística `Sum` para comprobar si se está produciendo algún evento relacionado con la disponibilidad en la gateway. Consulte con el grupo de CloudWatch registros configurado para obtener detalles sobre 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 imagen de máquina de Amazon (AMI) de Amazon EC2. Si la MV de la gateway no funciona correctamente, active una nueva gateway y recupere los datos para esa gateway utilizando las instrucciones siguientes.

Temas

- [Recuperación de un cierre inesperado de una máquina virtual](#)
- [Recuperación de los datos a partir de una puerta de enlace o VM que no funciona correctamente](#)

- [Recuperación de los datos desde una cinta irrecuperable](#)
- [Recuperación de los datos a partir de un disco de la caché que no funciona correctamente](#)
- [Recuperación de los datos de un centro de datos inaccesible](#)

Recuperación de un cierre inesperado de una máquina virtual

Si la MV se cierra de forma inesperada, por ejemplo, durante un corte de suministro eléctrico, el acceso a la gateway dejará de ser posible. Cuando se restablezca el suministro eléctrico y la conectividad de red, volverá a ser posible el acceso a la gateway y empezará a funcionar normalmente. A continuación se muestran algunas de las acciones que puede llevar a cabo en ese momento para facilitar la recuperación de los datos:

- Si una interrupción del suministro eléctrico provoca problemas de conectividad de red, puede solucionar el problema. Para obtener más información sobre cómo probar la conectividad de red, consulte [Prueba de conexión de la gateway a Internet](#).
- En el caso de las configuraciones de cintas, cuando sea posible el acceso a la puerta de enlace, las cintas pasarán al estado ARRANCADO. Esta funcionalidad garantiza que los datos almacenados localmente sigan sincronizados con AWS. Para obtener más información sobre este estado, consulte [Información sobre el estado de las cintas](#).
- 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 los datos a partir de una puerta de enlace o VM que no funciona correctamente

Si la puerta de enlace de cinta o el host del hipervisor encuentran un error irrecuperable, puede hacer lo siguiente para recuperar las cintas de la puerta de enlace de cinta que no funciona correctamente a otra puerta de enlace de cinta:

1. Identifique la puerta de enlace de cinta que desee utilizar como destino de la recuperación o cree una nueva.
2. Desactive la puerta de enlace que no funciona correctamente.
3. Cree cintas de recuperación para cada cinta que desee recuperar y especifique la puerta de enlace de cinta de destino.

4. Elimine la puerta de enlace de cinta que no funciona correctamente.

Para obtener información detallada sobre cómo recuperar las cintas de una puerta de enlace de cinta que no funciona correctamente a otra puerta de enlace de cinta, consulte [Necesita recuperar una cinta virtual desde una puerta de enlace de cinta que no funciona correctamente](#).

Recuperación de los datos desde una cinta irrecuperable

Si la cinta encuentra un error y el estado de la cinta es IRRECOVERABLE, le recomendamos que utilice una de las siguientes opciones para recuperar los datos o resolver el error, según la situación:

- Si necesita los datos de la cinta irrecuperable, puede recuperar la cinta en una nueva gateway.
- Si no necesita los datos de la cinta y la cinta nunca se ha archivado, puede eliminar simplemente la cinta de la puerta de enlace de cinta.

Para obtener información detallada acerca de cómo recuperar los datos o resolver el error si el estado de la cinta es IRRECOVERABLE, consulte [Solución problemas de cintas irrecuperables](#).

Recuperación de los datos a partir de un disco de la caché que no funciona correctamente

Si el disco de la caché encuentra un error, le recomendamos que haga lo siguiente para recuperar los datos en función de la situación:

- Si el error se produjo porque se retiró del host un disco de la caché, cierre la puerta de enlace, vuelva a agregar el disco y reinicie la puerta de enlace.
- 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 [Necesita recuperar una cinta virtual desde un disco de caché que no funciona correctamente](#).

Recuperación de los datos de un centro de datos inaccesible

Si una puerta de enlace o un centro de datos deja de ser accesible por algún motivo, puede recuperar los datos en otra puerta de enlace de un centro de datos diferente o en una puerta de enlace alojada en una instancia de Amazon EC2. Si no tiene acceso a otro centro de datos, le

recomendamos crear la puerta de enlace en una instancia de Amazon EC2. Los pasos que siga dependerán del tipo de gateway cuyos datos intenta recuperar.

Para recuperar datos de una puerta de enlace de cinta en un centro de datos inaccesible

1. Cree y active una nueva puerta de enlace de cinta en un host de Amazon EC2. Para obtener más información, consulte [Implementación de una EC2 instancia de Amazon para alojar su Tape Gateway](#).
2. Recupere las cintas de la puerta de enlace de origen en el centro de datos en la puerta de enlace nueva que creó en Amazon EC2. Para obtener más información, consulte [Recuperar una cinta virtual de una gateway no recuperable](#).

Las cintas deberán recuperarse en la nueva puerta de enlace de Amazon EC2.

Recursos adicionales de Storage Gateway

En esta sección se describen AWS el software, las herramientas y los recursos de terceros que pueden ayudarle a configurar o administrar su puerta de enlace, así como las cuotas de Storage Gateway.

Temas

- [Implementación y configuración del host de VM de la puerta de enlace](#)
- [Información adicional sobre los recursos de almacenamiento de Tape Gateway](#)
- [Obtención de una clave de activación para la puerta de enlace](#)
- [Conexión de SCSI iniciadores](#)
- [Uso AWS Direct Connect con Storage Gateway](#)
- [Requisitos de puerto de red para Tape Gateway](#)
- [Conexión a la gateway](#)
- [Descripción de los recursos y recursos de Storage Gateway IDs](#)
- [Etiquetado de recursos de Storage Gateway](#)
- [Uso de componentes de código abierto para AWS Storage Gateway](#)
- [AWS Storage Gateway cuotas](#)

Implementación y configuración del host de VM de la puerta de enlace

Temas

- [Configuración VMware para Storage Gateway](#)
- [Sincronización de la hora de la MV de la gateway](#)
- [Implementación de una EC2 instancia de Amazon para alojar su Tape Gateway](#)
- [Implementación de Amazon EC2 con la configuración predeterminada](#)
- [Modificar las opciones de metadatos de las EC2 instancias de Amazon](#)

Configuración VMware para Storage Gateway

Al configurar VMware Storage Gateway, asegúrese de sincronizar la hora de la máquina virtual con la hora del host, configure la máquina virtual para que utilice controladores de disco paravirtualizados al aprovisionar almacenamiento y de brindar protección contra los errores en la capa de infraestructura que soporta una máquina virtual de puerta de enlace.

Temas

- [Sincronización de la hora de la máquina virtual y el host](#)
- [Configuración de la AWS Storage Gateway máquina virtual para utilizar controladores de disco paravirtualizados](#)
- [Uso de Storage Gateway con VMware alta disponibilidad](#)

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, comprueba la hora del host y, si es necesario, establece la hora del host y configura el host para que sincronice su hora automáticamente con un servidor del Network Time Protocol (NTP).

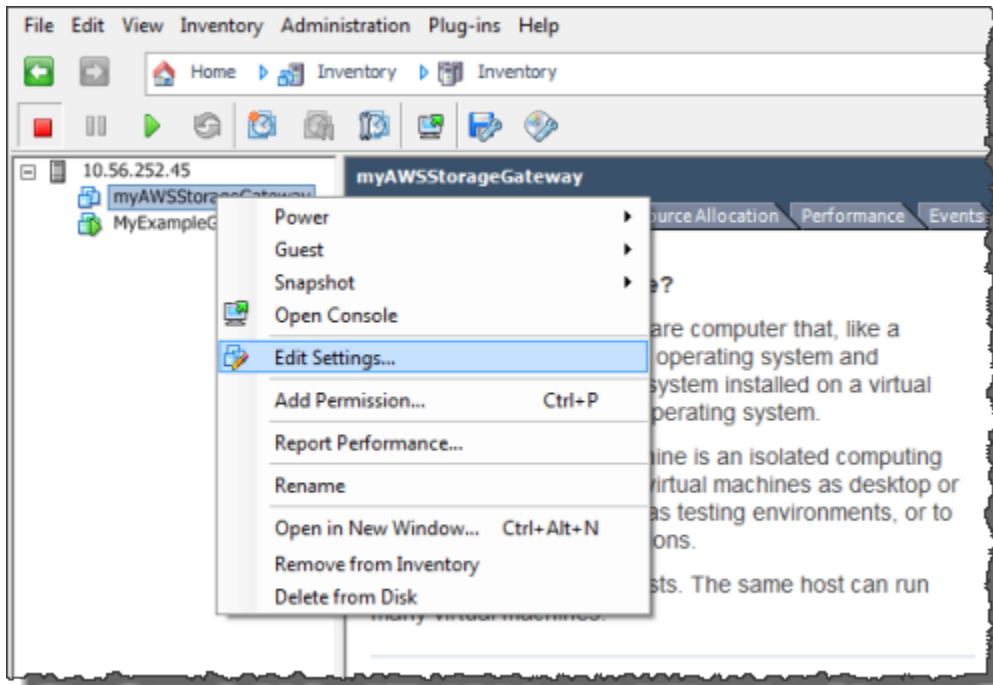
Important

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

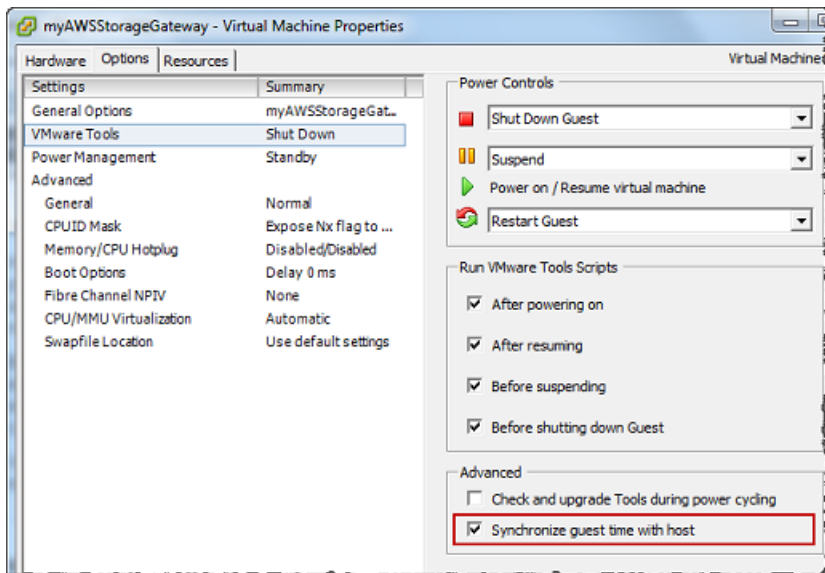
1. Configure la hora de la máquina virtual.
 - a. En el vSphere cliente, abra el menú contextual (haga clic con el botón derecho) de la máquina virtual de puerta de enlace y seleccione Editar configuración.

Se abrirá el cuadro de diálogo Virtual Machine Properties (Propiedades de la máquina virtual).



- b. Seleccione la pestaña Opciones y, en la lista de opciones, seleccione VMwareHerramientas.
- 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.

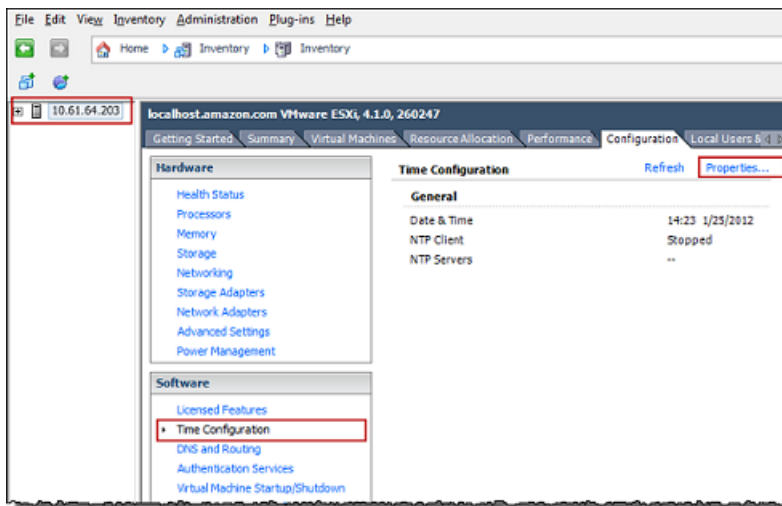


2. Configurar la hora del host.

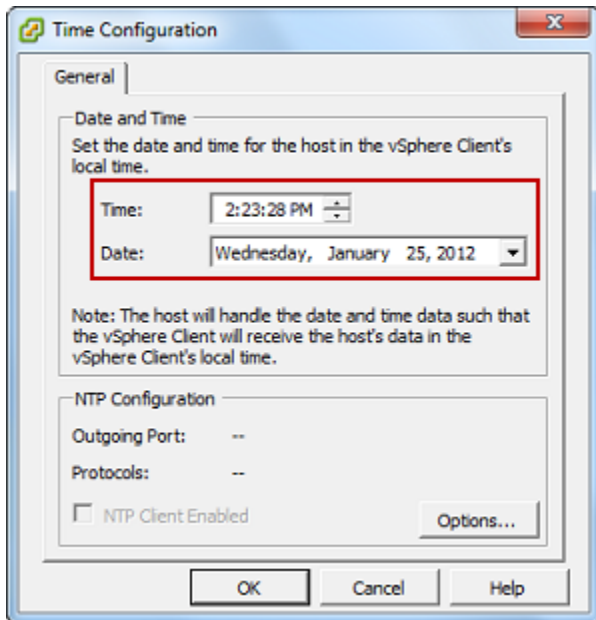
Es importante asegurarse de que el reloj del host esté establecido en la hora correcta. Si no ha configurado el reloj del host, lleve a cabo los siguientes pasos para configurarlo y sincronizarlo con un NTP servidor.

- a. En el VMware vSphere cliente, seleccione el nodo vSphere host en el panel izquierdo y, a continuación, elija la pestaña Configuración.
- b. Seleccione Time Configuration (Configuración de tiempo) en el panel Software y, a continuación, elija el enlace Properties (Propiedades).

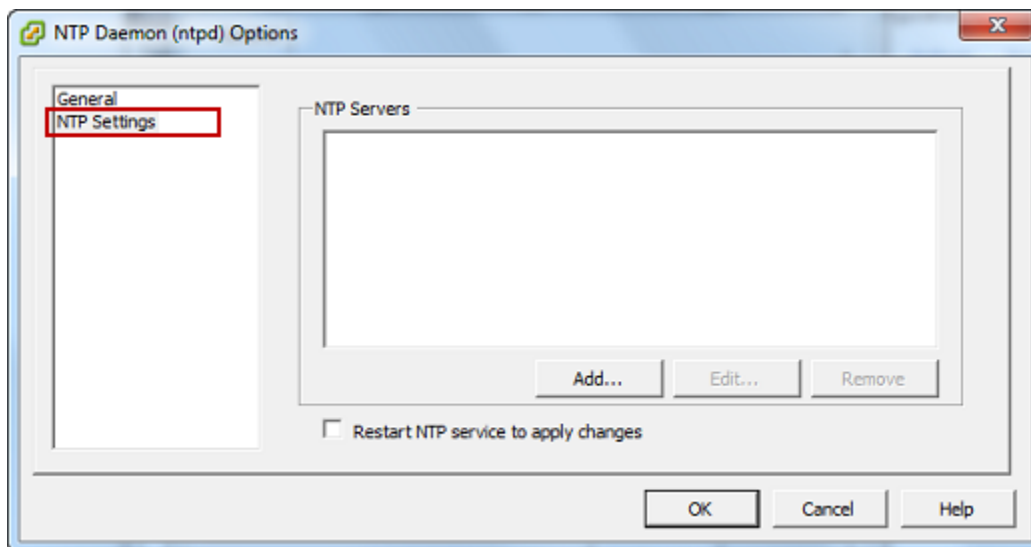
Aparecerá el cuadro de diálogo Time Configuration (Configuración de tiempo).



- c. En el panel Date and Time (Fecha y hora), establezca la fecha y la hora.

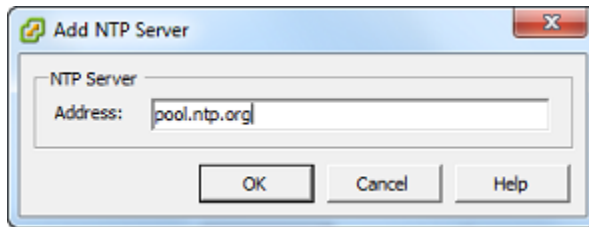


- d. Configure el host para que sincronice su hora automáticamente con un NTP servidor.
 - i. Elija Opciones en el cuadro de diálogo de configuración horaria y, a continuación, en el cuadro de diálogo Opciones de NTP Daemon (ntpd), elija NTPConfiguración en el panel izquierdo.



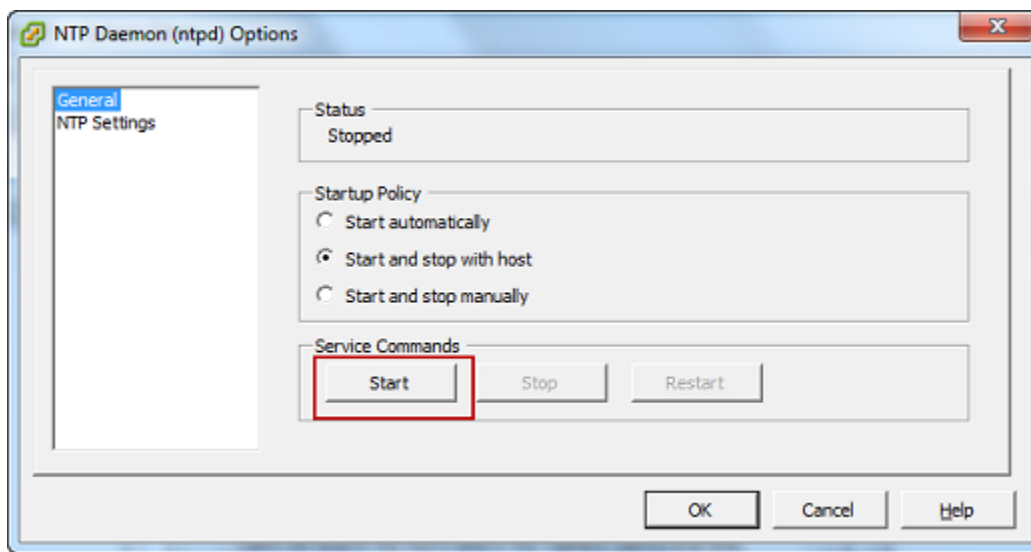
- ii. Seleccione Añadir para añadir un nuevo servidor. NTP
 - iii. En el cuadro de diálogo Agregar NTP servidor, escriba la dirección IP o el nombre de dominio completo de un NTP servidor y, a continuación, haga clic en Aceptar.

Puede utilizar `pool.ntp.org` como se muestra en el ejemplo siguiente.



- iv. En el cuadro de diálogo Opciones de NTP Daemon (ntpd), elija General 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 de NTP servidor o agrega otra más adelante, tendrá que reiniciar el servicio para usar el nuevo servidor.



- e. Pulse Aceptar para cerrar el cuadro de diálogo de opciones de NTP Daemon (ntpd).
- f. Elija OK (Aceptar) para cerrar el cuadro de diálogo Time Configuration (Configuración de tiempo).

Configuración de la AWS Storage Gateway máquina virtual para utilizar controladores de disco paravirtualizados

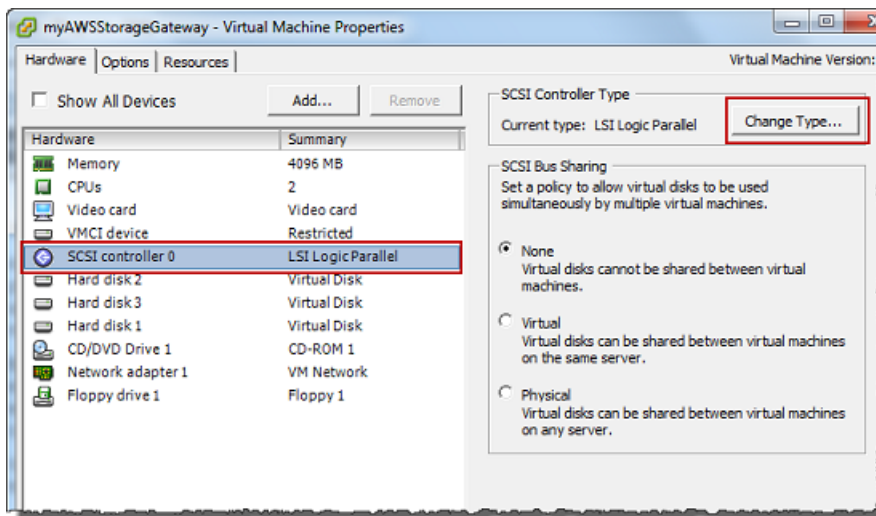
En esta tarea, debe configurar el SCSI controlador i para que la máquina virtual utilice la paravirtualización. La paravirtualización es un modo en que la máquina virtual de la gateway funciona con el sistema operativo host de tal forma que la consola pueda identificar los discos virtuales que se añaden a la máquina virtual.

Note

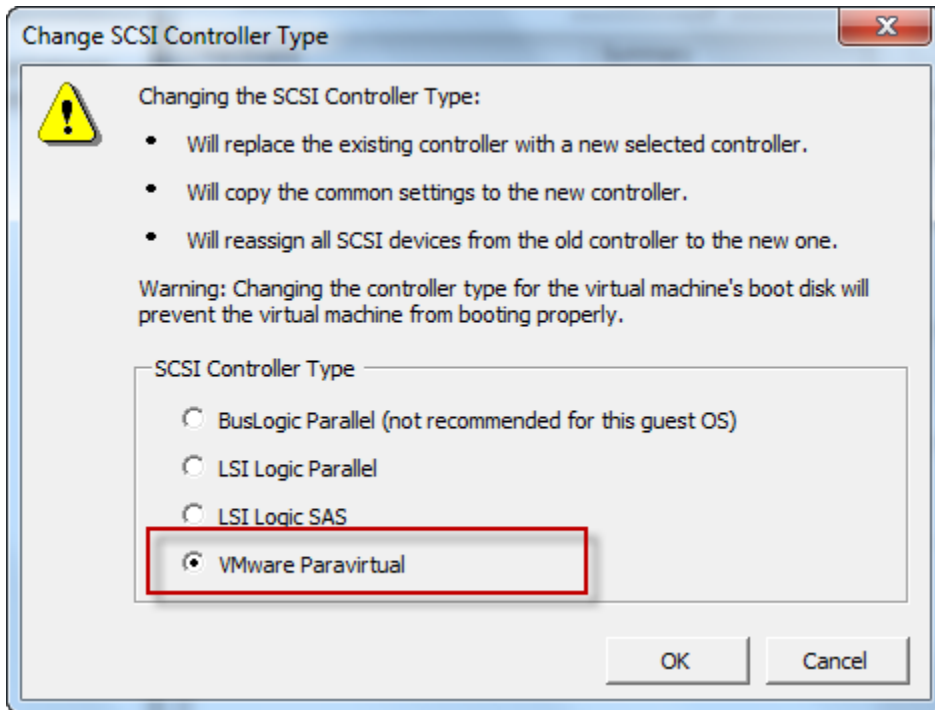
Es preciso completar este paso para evitar problemas en la identificación de estos discos cuando se configuren en la consola de gateway.

Para configurar la máquina virtual de forma que use controladores paravirtualizados

1. En el VMware vSphere cliente, abra el menú contextual (haga clic con el botón derecho) de la máquina virtual de puerta de enlace y, a continuación, seleccione Editar configuración.
2. En el cuadro de diálogo Propiedades de la máquina virtual, seleccione la pestaña Hardware, seleccione el SCSI controlador 0 y, a continuación, elija Cambiar tipo.



3. En el cuadro de diálogo Cambiar tipo de SCSI controlador, seleccione el tipo de SCSI controlador VMware paravirtual y, a continuación, elija Aceptar.



Uso de Storage Gateway con VMware alta disponibilidad

VMwareLa alta disponibilidad (HA) es un componente vSphere que puede brindar protección contra las fallas en la capa de infraestructura que soporta una máquina virtual de puerta de enlace. VMwarePara ello, HA utiliza varios hosts configurados como un clúster, de modo que si un host que ejecuta una máquina virtual de puerta de enlace falla, la máquina virtual de puerta de enlace se pueda reiniciar automáticamente en otro host del clúster. Para obtener más información sobre VMware HA, consulte [las prácticas recomendadas para los clústeres VMware vSphere de alta disponibilidad](#) en el VMware sitio web.

Para usar Storage Gateway con VMware HA, se recomienda hacer lo siguiente:

- Implemente el paquete VMware ESX .ova descargable que contiene la máquina virtual Storage Gateway en un solo host de un clúster.
- Cuando implemente el paquete .ova, seleccione un almacén de datos que no sea local para un host. En su lugar, utilice un almacén de datos accesible para todos los hosts del clúster. Si selecciona un almacén de datos local para un host y el host produce un error, es posible que la fuente de datos no permita el acceso a otros hosts del clúster y la conmutación por error a otro host no tenga éxito.

- Para evitar que el iniciador se desconecte de los objetivos de volumen de almacenamiento durante la conmutación por error, siga la SCSI configuración i recomendada para su sistema operativo. En caso de conmutación por error, es posible que pasen entre unos segundos y varios minutos hasta que la MV de una gateway se inicie en un nuevo host del clúster de conmutación por error. Los tiempos de SCSI espera recomendados para los clientes de Windows y Linux son superiores al tiempo habitual que tarda en producirse la conmutación por error. Para obtener más información sobre la personalización de ajustes de tiempo de espera de clientes Windows, consulte [Personalización de la configuración de Windows i SCSI](#). Para obtener más información sobre la personalización de ajustes de tiempo de espera de clientes Linux, consulte [Personalización de la configuración de Linux i SCSI](#).
- 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

En el caso de una puerta de enlace VMware ESXi instalada, basta con configurar la hora del host del hipervisor y sincronizar la hora de la máquina virtual con el host para evitar la pérdida de tiempo. Para obtener más información, consulte [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 una máquina virtual de puerta de enlace de hipervisor con un servidor de protocolo de tiempo de red (Network Time Protocol) NTP

1. Inicie sesión en la consola local de la gateway:
 - Para obtener más información sobre cómo iniciar sesión en la consola VMware ESXi local, consulte. [Acceder a la consola local de Gateway con VMware ESXi](#)
 - Para obtener más información sobre el inicio de sesión en la consola local de Microsoft Hyper-V, consulte [Acceso a la consola local de la gateway con Microsoft Hyper-V](#).
 - Para obtener más información sobre cómo iniciar sesión en la consola local de Virtuum Machine (KVM) basada en el kernel de Linux, consulte. [Acceso a la consola local de Gateway con Linux KVM](#)
2. En el menú principal de Configuración de Storage Gateway, introduzca **4** en Administración de la hora del sistema.

```
AWS Storage Gateway Configuration
#####
## Currently connected network adapters:
##
## eth0: 10.0.0.45
#####

1: SOCKS Proxy Configuration
2: Network Configuration
3: Test Network Connectivity
4: System Time Management
5: Gateway Console
6: View System Resource Check (0 Errors)

0: Stop AWS Storage Gateway

Press "x" to exit session

Enter command: _
```

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).

```
System Time Management

1: View and Synchronize System Time

Press "x" to exit

Enter command: _
```

4. Si el resultado indica que debe sincronizar la hora de la máquina virtual con la hora, introduzca **NTP 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.

```
System Time Management
1: View and Synchronize System Time
Press "x" to exit
Enter command: 1
Current System Time: Sat Aug 22 00:33:41 UTC 2015
Determining current NTP time (this may take a few seconds ...)
Your Storage Gateway VM system time differs from NTP time
by 0.217617 seconds
A sync is recommended if the time differs by more than 60 seconds
Do you want to sync Storage Gateway VM system time with
NTP time? [y/n]: _
```

En la siguiente captura de pantalla se muestra una MV que requiere la sincronización de la hora.

```
System Time Management
1: View and Synchronize System Time
Press "x" to exit
Enter command: 1
Current System Time: Sat Aug 22 00:33:41 UTC 2015
Determining current NTP time (this may take a few seconds ...)
Your Storage Gateway VM system time differs from NTP time
by 61.217617 seconds
A sync is recommended if the time differs by more than 60 seconds
Do you want to sync Storage Gateway VM system time with
NTP time? [y/n]: _
```

Implementación de una EC2 instancia de Amazon para alojar su Tape Gateway

Puede implementar y activar una puerta de enlace por en una instancia de Amazon Elastic Compute Cloud (AmazonEC2). AWS Storage Gateway Amazon Machine Image (AMI) está disponible como comunidadAMI.

Note

La comunidad Storage Gateway AMIs está publicada y cuenta con el apoyo total de AWS. Puede ver que el editor es AWS un proveedor verificado.

Tape Gateway AMIs utiliza la siguiente convención de nomenclatura. El número de versión adjunto al AMI nombre cambia con cada versión publicada.

`aws-storage-gateway-CLASSIC-2.9.0`

Para implementar una EC2 instancia de Amazon para alojar su Tape Gateway

1. Empiece configurando una nueva puerta de enlace mediante la consola de Storage Gateway. Para obtener instrucciones, consulte [Configuración de una puerta de enlace de cinta](#). Cuando llegue a la sección Opciones de plataforma, elija Amazon EC2 como plataforma de host y, a continuación, siga los pasos siguientes para lanzar la EC2 instancia de Amazon que alojará su Tape Gateway .
2. Elige Launch instance para abrir la AWS Storage Gateway AMI plantilla en la EC2 consola de Amazon, donde podrás configurar ajustes adicionales.

Usa Quicklaunch para lanzar la EC2 instancia de Amazon con la configuración predeterminada. Para obtener más información sobre las especificaciones predeterminadas de Amazon EC2 Quicklaunch, consulte [Especificaciones de configuración de Quicklaunch para Amazon EC2](#).

3. En Nombre, introduce un nombre para la EC2 instancia de Amazon. Una vez implementada la instancia, puedes buscar este nombre para encontrarla en las páginas de listas de la EC2 consola de Amazon.
4. En la sección Tipo de instancia, para el tipo de instancia, elija la configuración de hardware de su instancia. La configuración del hardware debe cumplir con ciertos requisitos mínimos para ser compatible con su puerta de enlace. Recomendamos comenzar por el tipo de instancia m5.xlarge, que cumple los requisitos mínimos de hardware para que la puerta de enlace funcione correctamente. Para obtener más información, consulte [Requisitos para los tipos de EC2 instancias de Amazon](#).

Puede cambiar el tamaño de la instancia después de lanzarla, si es necesario. Para obtener más información, consulta [Cómo cambiar el tamaño de una instancia](#) en la Guía del EC2 usuario de Amazon.

Note

Algunos tipos de instancias, especialmente la i3EC2, utilizan NVMe SSD discos. Estos pueden causar problemas al iniciar o detener una puerta de enlace de cinta; por ejemplo, se pueden perder datos de la caché. Supervisa la CloudWatch métrica de `CachePercentDirty` Amazon y solo inicia o detiene tu sistema cuando ese parámetro lo esté `0`. Para obtener más información sobre las métricas de monitoreo de su gateway, consulte [las métricas y dimensiones de Storage Gateway](#) en la CloudWatch documentación.

5. En la sección Par de claves (inicio de sesión), en Nombre del par de claves: obligatorio, elija el par de claves que desea usar para conectarse de forma segura a su instancia. Si es necesario, puede crear un nuevo par de claves. Para obtener más información, consulte [Crear un par de claves](#) en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux.
6. En la sección Configuración de red, revise los ajustes preconfigurados y elija Editar para realizar cambios en los siguientes campos:
 - a. En el caso de VPC: obligatorio, elige el VPC lugar en el que quieres lanzar tu EC2 instancia de Amazon. Para obtener más información, consulte [Cómo VPC funciona Amazon](#) en la Guía del usuario de Amazon Virtual Private Cloud.
 - b. (Opcional) En Subnet, elige la subred en la que quieres lanzar tu instancia de AmazonEC2.
 - c. En Auto-assign Public IP (Autoasignar IP pública), elija Enable (Habilitar).
7. En la subsección Firewall (grupos de seguridad), revise los ajustes preconfigurados. Si lo deseas, puedes cambiar el nombre y la descripción predeterminados del nuevo grupo de seguridad que se va a crear para tu EC2 instancia de Amazon, o bien optar por aplicar reglas de firewall desde un grupo de seguridad existente.
8. En la subsección Reglas de grupos de seguridad de entrada, agregue reglas de firewall para abrir los puertos que los clientes utilizarán para conectarse a su instancia. Para obtener más información sobre los puertos necesarios para puerta de enlace de cinta, consulte [Requisitos de los puertos](#). Para obtener más información sobre la agregación de reglas de firewall, consulte [Reglas del grupo de seguridad](#) en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux.

 Note

Tape Gateway requiere que el TCP puerto 80 esté abierto para el tráfico entrante y para un HTTP acceso único durante la activación de la puerta de enlace. Tras la activación, puede cerrar este puerto.

Además, debe abrir el TCP puerto 3260 para acceder a iSCSI.

9. En la subsección Configuración de red avanzada, revise los ajustes preconfigurados y realice los cambios necesarios.
10. En la sección Configurar almacenamiento, elija Agregar volumen nuevo para agregar almacenamiento a la instancia de la puerta de enlace de archivos.

 Important

Debe añadir al menos un EBS volumen de Amazon con una capacidad mínima de 165 GiB para el almacenamiento en caché y al menos un EBS volumen de Amazon con una capacidad mínima de 150 GiB para el búfer de carga, además del volumen raíz preconfigurado. Para aumentar el rendimiento, recomendamos asignar varios EBS volúmenes para el almacenamiento en caché con al menos 150 GiB cada uno.

11. En la subsección Detalles avanzados, revise los ajustes preconfigurados y realice los cambios necesarios.
12. Elija Launch instance para lanzar su nueva instancia de Amazon EC2 Gateway con los ajustes configurados.
13. Para comprobar que la nueva instancia se ha lanzado correctamente, dirígete a la página de instancias de la EC2 consola de Amazon y busca la nueva instancia por su nombre. Asegúrese de que el Estado de la instancia se muestre En ejecución con una marca de verificación verde y de que la Comprobación de estado se haya completado y muestre una marca de verificación verde.
14. Seleccione la instancia de la página de detalles. Copie la IPv4 dirección pública de la sección de resumen de la instancia y, a continuación, vuelva a la página Configurar puerta de enlace de la consola Storage Gateway para reanudar la configuración de la puerta de enlace por .

Puede determinar el AMI ID que se utilizará para lanzar una puerta de enlace por mediante la consola Storage Gateway o consultando el almacén de AWS Systems Manager parámetros.

Para determinar el AMI ID, realice una de las siguientes acciones:

- Empiece configurando una nueva puerta de enlace mediante la consola de Storage Gateway. Para obtener instrucciones, consulte [Configuración de una puerta de enlace de cinta](#). Cuando llegues a la sección de opciones de plataforma, elige Amazon EC2 como plataforma anfitriona y, a continuación, elige Launch instance para abrir la AWS Storage Gateway AMI plantilla en la EC2 consola de Amazon.

Se te redirigirá a la AMI página de la EC2 comunidad, donde podrás ver el AMI ID de tu AWS región enURL.

- Consulta del almacén de parámetros de Systems Manager. Puede usar Storage Gateway AWS CLI o Storage Gateway API para consultar el parámetro público de Systems Manager en el espacio de nombres/`aws/service/storagegateway/ami/VTL/latest`. Por ejemplo, si usa el siguiente CLI comando, se devuelve el ID actual AMI del Región de AWS que especifique.

```
aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/VTL/latest
```


El CLI comando 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/VTL/latest",
    "Name": "/aws/service/storagegateway/ami/VTL/latest",
    "Value": "ami-123c45dd67d891000"
  }
}
```

Implementación de Amazon EC2 con la configuración predeterminada

En este tema se enumeran los pasos para implementar un host de Amazon EC2 utilizando las especificaciones predeterminadas.

Puede implementar y activar una puerta de enlace de cinta en una instancia de Amazon Elastic Compute Cloud (Amazon EC2). La imagen de máquina de Amazon (AMI) de AWS Storage Gateway está disponible como una AMI de la comunidad.


 Note

Las AMI de la comunidad de Storage Gateway están publicadas y son totalmente compatibles con AWS. Puede ver que el editor es AWS un proveedor verificado.

1. Para configurar la instancia de Amazon EC2, elija Amazon EC2 como Plataforma host en la sección Opciones de plataforma del flujo de trabajo. Para obtener instrucciones sobre la configuración de la instancia de Amazon EC2, consulte [Implementación de una instancia de Amazon EC2 para alojar la puerta de enlace de cinta](#).
2. Seleccione Launch instance para abrir la plantilla AMI de AWS Storage Gateway en la consola de Amazon EC2 y personalizar ajustes adicionales, como los tipos de instancia, los ajustes de red y configurar el almacenamiento.
3. Si lo desea, puede seleccionar Usar la configuración predeterminada en la consola de Storage Gateway para implementar una instancia de Amazon EC2 con la configuración predeterminada.

La instancia de Amazon EC2 que crea Usar la configuración predeterminada tiene las siguientes especificaciones predeterminadas:

- Tipo de instancia: m5.xlarge
- Configuración de red
 - En VPC, elija la VPC en la que desea que se ejecute la instancia de EC2.
 - En Subred, especifique la subred en la que debe lanzarse la instancia de EC2.

 Note

Las subredes de VPC aparecerán en el menú desplegable solo si tienen activada la configuración de asignación automática de direcciones IPv4 públicas desde la consola de administración de VPC.

- Asignar una IP pública de forma automática: Activada

Se crea un grupo de seguridad de EC2 y se asocia a la instancia de EC2. El grupo de seguridad tiene las siguientes reglas de puerto de entrada:

Note

Necesitará que el puerto 80 esté abierto durante la activación de la puerta de enlace. El puerto se cierra inmediatamente después de la activación. A partir de entonces, solo se puede acceder a la instancia de EC2 a través de los demás puertos de la VPC seleccionada.

Solo se puede acceder a los destinos iSCSI de la puerta de enlace desde los hosts de la misma VPC que la puerta de enlace. Si es necesario acceder a los destinos iSCSI desde hosts externos a la VPC, debe actualizar las reglas del grupo de seguridad correspondientes.

Para editar los grupos de seguridad en cualquier momento, vaya a la página de detalles de la instancia de Amazon EC2, seleccione Seguridad, vaya a Detalles del grupo de seguridad y elija el ID del grupo de seguridad.

Puerto	Protocolo	Protocolo del sistema de archivos				
80	TCP	Acceso HTTP para la activación				
3260	TCP	iSCSI				

- Configurar almacenamiento

Configuración predeterminada	Volumen raíz de AMI	Caché de volumen 2	Caché de volumen 3			
Nombre de dispositivo		'/dev/sdb'	'/dev/sdc'			
Tamaño	80 GiB	165 GiB	150 GiB			
Tipo de volumen	gp3	gp3	gp3			
IOPS	3 000	3 000	3 000			
Eliminar al terminar	Sí	Sí	Sí			
Encrypted	No	No	No			
Rendimiento	125	125	125			

Modificar las opciones de metadatos de las EC2 instancias de Amazon

El servicio de metadatos de la instancia (IMDS) es un componente de la instancia que proporciona un acceso seguro a los metadatos de la EC2 instancia de Amazon. Se puede configurar una instancia para que acepte las solicitudes de metadatos entrantes que usen la IMDS versión 1 (IMDSv1) o para que todas las solicitudes de metadatos usen la IMDS versión 2 (IMDSv2). IMDSv2 utiliza solicitudes orientadas a la sesión y mitiga varios tipos de vulnerabilidades que podrían utilizarse para intentar acceder a IMDS. Para obtener más información sobre IMDSv2, consulte [Cómo funciona Instance Metadata Service versión 2](#) en la Guía del usuario de Amazon Elastic Compute Cloud.

Le recomendamos que lo requiera IMDSv2 para todas las EC2 instancias de Amazon que alojen Storage Gateway. IMDSv2 es obligatorio de forma predeterminada en todas las instancias de

gateway recién lanzadas. Si tiene instancias existentes que aún están configuradas para aceptar solicitudes de IMDSv1 metadatos, consulte [Requerir el uso de IMDSv2](#) en la Guía del usuario de Amazon Elastic Compute Cloud para obtener instrucciones sobre cómo modificar las opciones de metadatos de la instancia para requerir el uso de IMDSv2. Para aplicar este cambio no es necesario reiniciar la instancia.

Información adicional sobre los recursos de almacenamiento de Tape Gateway

Temas

- [Retirada de discos de la gateway](#)
- [Añadir y eliminar EBS volúmenes de Amazon para Amazon EC2 Gateways](#)
- [Trabajo con VTL dispositivos](#)
- [Trabajo con cintas](#)

Retirada de discos de la gateway

Aunque no es recomendable eliminar los discos subyacentes de la gateway, es posible que desee retirar un disco de la gateway, por ejemplo, si tiene un disco que presenta errores.

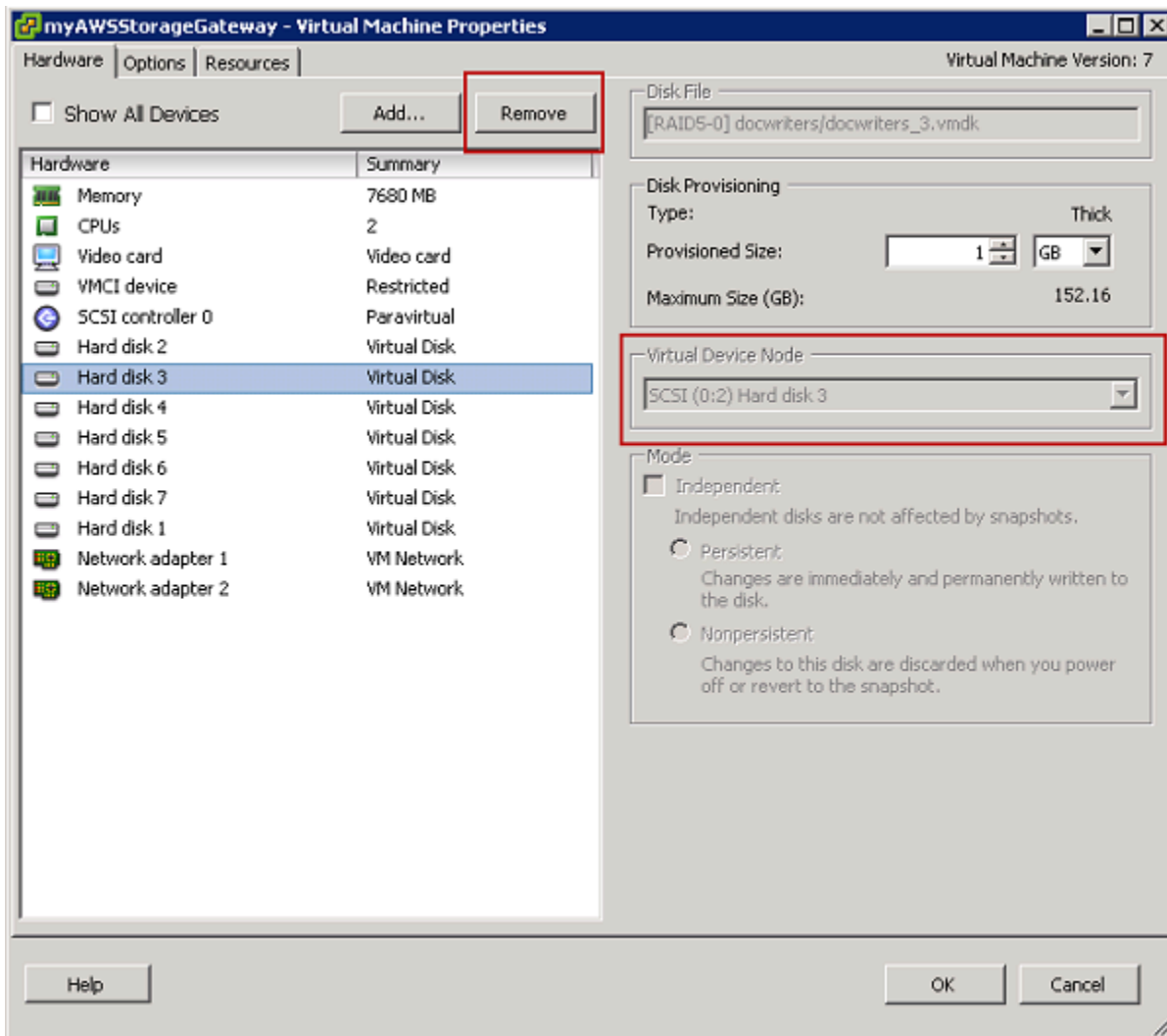
Eliminar un disco de una puerta de enlace alojada en VMware ESXi

Puede usar el siguiente procedimiento para quitar un disco de la puerta de enlace alojada en el VMware hipervisor.

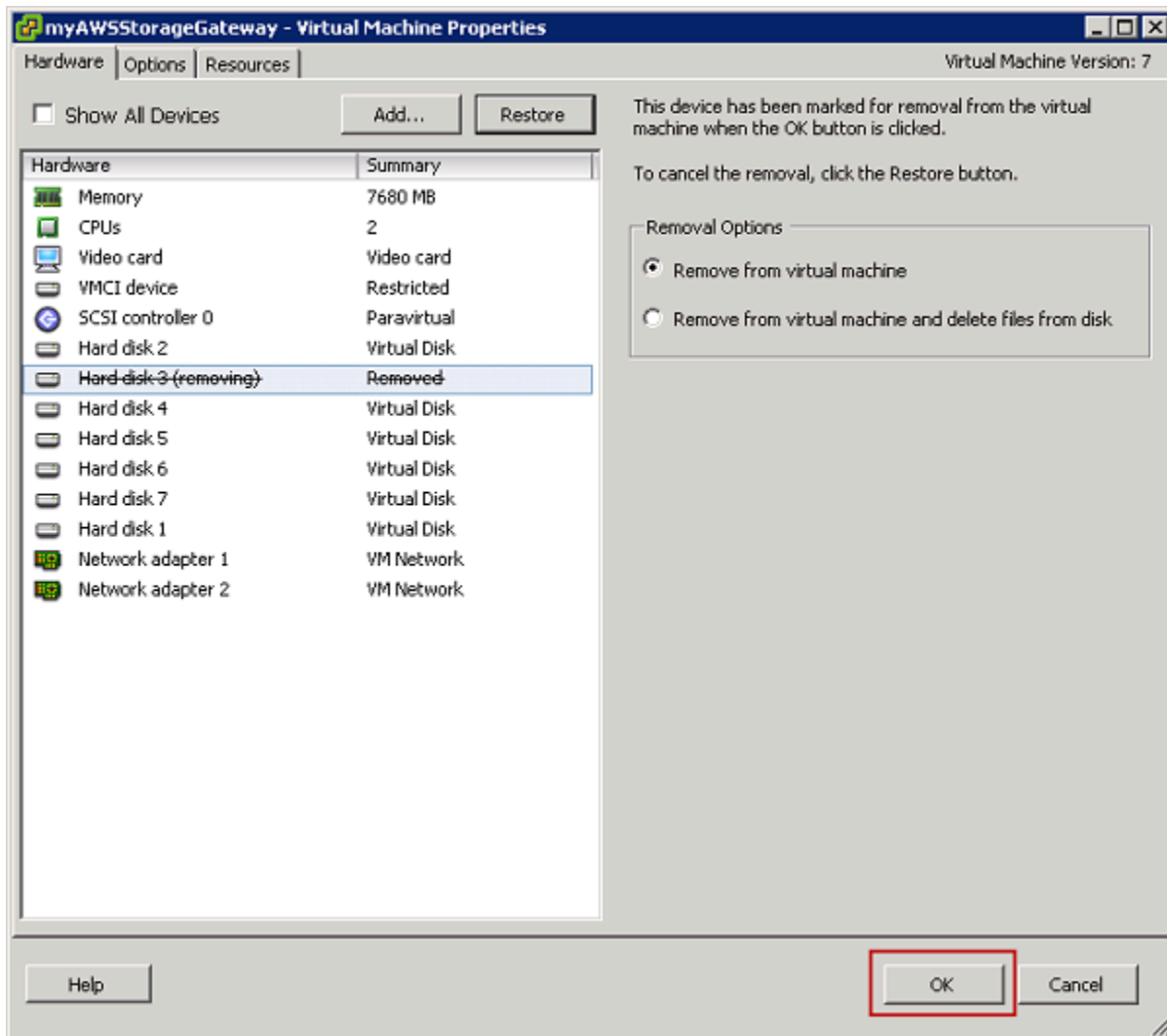
Para eliminar un disco asignado al búfer de carga () VMware ESXi

1. En el vSphere cliente, abra el menú contextual (haga clic con el botón derecho), elija el nombre de la máquina virtual de puerta de enlace y, a continuación, elija Editar configuración.
2. En la pestaña Hardware del cuadro de diálogo Virtual Machine Properties (Propiedades de la máquina virtual), seleccione el disco asignado como espacio de búfer de carga y, a continuación, seleccione Remove (Eliminar).

Compruebe que el valor de Virtual Device Node (Nodo de dispositivo virtual) en el cuadro de diálogo Virtual Machine Properties (Propiedades de la máquina virtual) tenga el mismo valor que anotó anteriormente. Esto ayuda a garantizar que se retire el disco correcto.



3. Elija una opción del panel Removal Options (Opciones de eliminación) y, a continuación, elija OK (Aceptar) para completar el proceso de retirada del disco.



Retirada de un disco de una gateway alojada en Microsoft Hyper-V

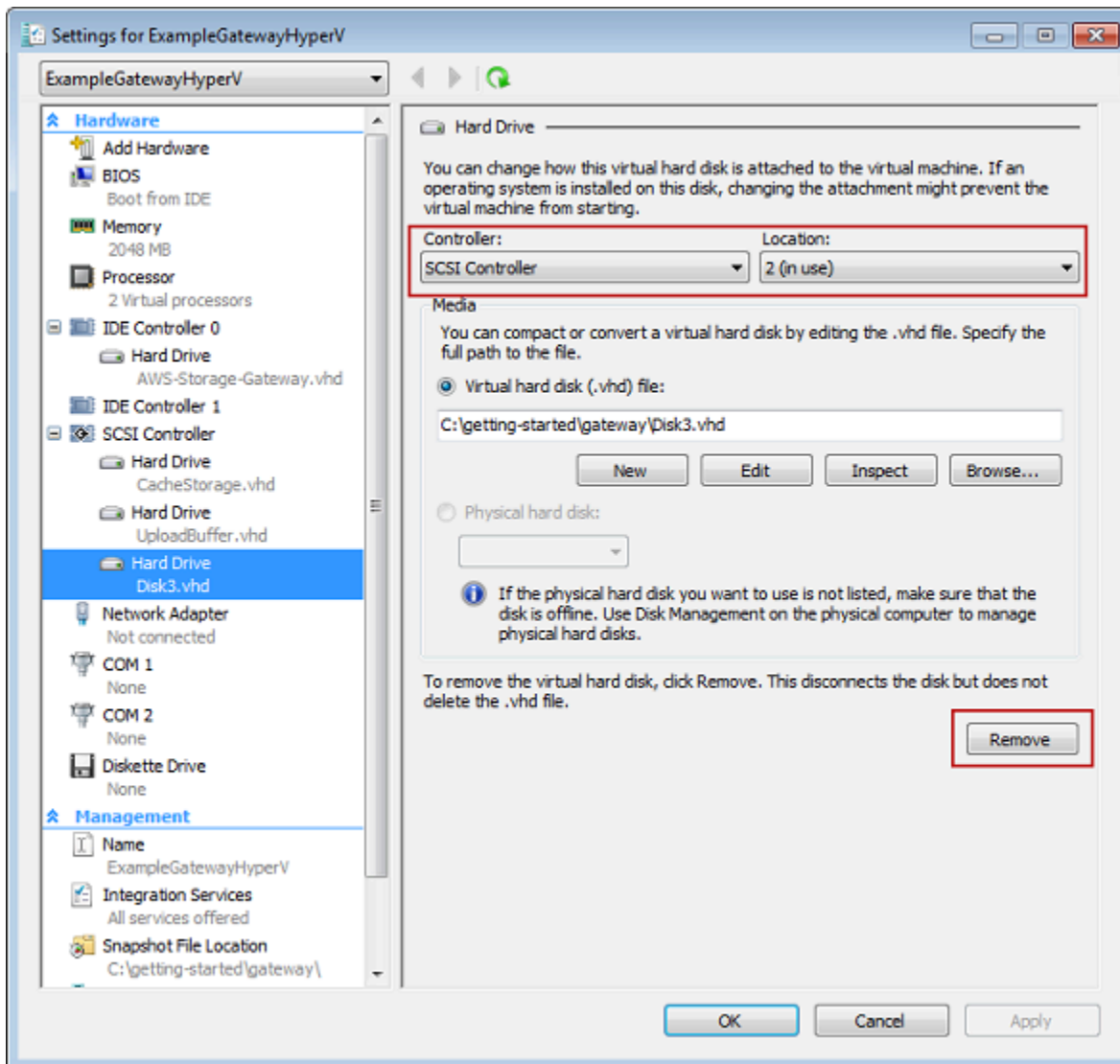
Puede utilizar el siguiente procedimiento para retirar un disco de una gateway alojada en un hipervisor Microsoft Hyper-V.

Para retirar un disco subyacente asignado al búfer de carga (Microsoft Hyper-V)

1. En Microsoft Hyper-V Manager, abra el menú contextual (haga clic con el botón secundario), elija el nombre de la máquina virtual de la gateway y, a continuación, elija Configuración.
2. En la lista Hardware del cuadro de diálogo Configuración, seleccione el disco que desee retirar y, a continuación, elija Quitar.

Los discos que añada a una puerta de enlace aparecen en la entrada SCSIControlador de la lista de hardware. Compruebe que los valores de Controladora y Ubicación sean los mismos que anotó anteriormente. Esto ayuda a garantizar que se retire el disco correcto.

El primer SCSI controlador que se muestra en el Microsoft Hyper-V Manager es el controlador 0.



3. Elija Aceptar para aplicar el cambio.

Extracción de un disco de una puerta de enlace alojada en Linux KVM

Para separar un disco de la puerta de enlace alojada en un hipervisor de máquina virtual (KVM) basado en el núcleo de Linux, puede utilizar un `virsh` comando similar al siguiente.

```
$ virsh detach-disk domain_name /device/path
```

Para obtener más información sobre la administración de KVM discos, consulte la documentación de su distribución de Linux.

Añadir y eliminar EBS volúmenes de Amazon para Amazon EC2 Gateways

Cuando configuraste inicialmente tu gateway para que se ejecutara como una EC2 instancia de Amazon, asignaste EBS volúmenes de Amazon para usarlos como búfer de carga y almacenamiento en caché. Con el tiempo, a medida que cambien las necesidades de sus aplicaciones, podrá asignar EBS volúmenes de Amazon adicionales para este uso. También puedes reducir el almacenamiento que has asignado eliminando los EBS volúmenes de Amazon previamente asignados. Para obtener más información sobre AmazonEBS, consulta [Amazon Elastic Block Store \(AmazonEBS\)](#) en la Guía del EC2 usuario de Amazon.

Antes de agregar más almacenamiento a la gateway, debe revisar cuáles son las necesidades de tamaño del búfer de carga y el almacenamiento en caché en función de las necesidades de la aplicación para una gateway. Para ello, consulte [Determinación del tamaño que se va a asignar al búfer de carga](#) y [Determinación del tamaño que se va a asignar al almacenamiento en caché](#).

Existen cuotas para el almacenamiento máximo que se puede asignar como búfer de carga y almacenamiento en caché. Puedes adjuntar tantos EBS volúmenes de Amazon a tu instancia como desees, pero solo puedes configurar estos volúmenes como búfer de carga y espacio de almacenamiento en caché hasta alcanzar estas cuotas de almacenamiento. Para obtener más información, consulte [AWS Storage Gateway cuotas](#).

Para añadir un EBS volumen de Amazon y configurarlo para su puerta de enlace

1. Crea un EBS volumen de Amazon. Para obtener instrucciones, consulta [Cómo crear o restaurar un EBS volumen de Amazon](#) en la Guía del EC2 usuario de Amazon.
2. Adjunta el EBS volumen de Amazon a tu EC2 instancia de Amazon. Para obtener instrucciones, consulta [Cómo adjuntar un EBS volumen de Amazon a una instancia](#) en la Guía del EC2 usuario de Amazon.
3. Configura el EBS volumen de Amazon que has añadido como búfer de carga o almacenamiento en caché. Para obtener instrucciones, consulte [Administración de discos locales para Storage Gateway](#).

En ocasiones, es posible que no necesite la cantidad de almacenamiento asignado al búfer de carga.

Para eliminar un EBS volumen de Amazon

Warning

Estos pasos solo se aplican a los EBS volúmenes de Amazon asignados como espacio de búfer de carga, no a los volúmenes asignados a la memoria caché. Si elimina un EBS volumen de Amazon que está asignado como almacenamiento en caché de una puerta de enlace de cintas, las cintas virtuales de la puerta de enlace tendrán ese IRRECOVERABLE estado y corre el riesgo de perder datos. Para obtener más información sobre el IRRECOVERABLE estado, consulte [Descripción de la información sobre el estado de la cinta en un VTL](#).

1. Para cerrar la gateway, siga el enfoque que se describe en la sección [Como apagar la MV de la gateway](#).
2. Separa el EBS volumen de Amazon de tu EC2 instancia de Amazon. Para obtener instrucciones, consulta [Cómo separar un EBS volumen de Amazon de una instancia](#) en la Guía del EC2 usuario de Amazon.
3. Elimina el EBS volumen de Amazon. Para obtener instrucciones, consulta [Eliminar un EBS volumen de Amazon](#) en la Guía del EC2 usuario de Amazon.
4. Para iniciar la gateway, siga el enfoque que se describe en la sección [Como apagar la MV de la gateway](#).

Trabajo con VTL dispositivos

La configuración de la puerta de enlace de cinta proporciona los siguientes SCSI dispositivos, que puede seleccionar al activar la puerta de enlace.

Temas

- [Selección de un cambiador de medios después de activar la gateway](#)
- [Actualización de la unidad de dispositivo para el cambiador de medios](#)
- [Visualización de códigos de barras para cintas en Microsoft System Center DPM](#)

En el caso de los cambiadores de medio medio, AWS Storage Gateway funciona con lo siguiente:


- AWS-Gateway- VTL — Este dispositivo se proporciona con la puerta de enlace.

- STK-L700: la emulación de este dispositivo se proporciona con la puerta de enlace.

Al activar la puerta de enlace de cinta, se selecciona la aplicación de copia de seguridad en la lista y Storage Gateway utiliza el cambiador de medios adecuado. Si la aplicación de copia de seguridad no aparece, elija Other (Otra) y, a continuación, elija el cambiador de medios que funcione con la aplicación de copia de seguridad.

El tipo de cambiador de medio que elija depende de la aplicación de copia de seguridad que vaya a utilizar. En la siguiente tabla se enumeran las aplicaciones de copia de seguridad de terceros que se han probado y que han demostrado ser compatibles con puertas de enlace de cinta. Esta tabla incluye el tipo de cambiador de medio recomendado para cada aplicación de copia de seguridad.

Aplicación de copia de seguridad	Tipo de cambiador de medio
Backup Arcserve	AWS-Gateway-VTL
Bacula Enterprise V10.x	AWS-Gateway-VTL o STK-L700
Commvault V11	STK-L700
Dell 19.5 EMC NetWorker	AWS-Gateway-VTL
IBMSpectrum Protect v8.1.10	IBM-03584L32-0402
Protector de datos Micro Focus (HPE) 9 o 11.x	AWS-Gateway-VTL
Microsoft System Center 2012 R2 o 2016 Data Protection Manager	STK-L700
NovaStor DataCenter/Network 6.4 o 7.1	STK-L700
Quest NetVault Backup 12.4 o 13.x	STK-L700
Veeam Backup & Replication 11A	AWS-Gateway-VTL
Veritas Backup Exec 2014, 15, 16, 20 o 22.x	AWS-Gateway-VTL

Aplicación de copia de seguridad	Tipo de cambiador de medio
Veritas Backup Exec 2012 <div data-bbox="147 304 808 527" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p> Note Veritas ha finalizado el soporte para Backup Exec 2012.</p> </div>	STK-L700
Veritas, NetBackup versión 7.x u 8.x	AWS-Gateway-VTL

Important

Le recomendamos encarecidamente que elija el cambiador de medio que aparece en la lista para su aplicación de copia de seguridad. Es posible que otros cambiadores de medio no funcionen correctamente. Una vez que la puerta de enlace está activada, puede elegir otro tipo de cambiador de medio. Para obtener más información, consulte [Selección de un cambiador de medios después de activar la puerta de enlace](#).

Para las unidades de cinta, Storage Gateway funciona con los siguientes dispositivos:

- IBM- ULT358 0- TD5 —Esta emulación de dispositivo se proporciona con la puerta de enlace.

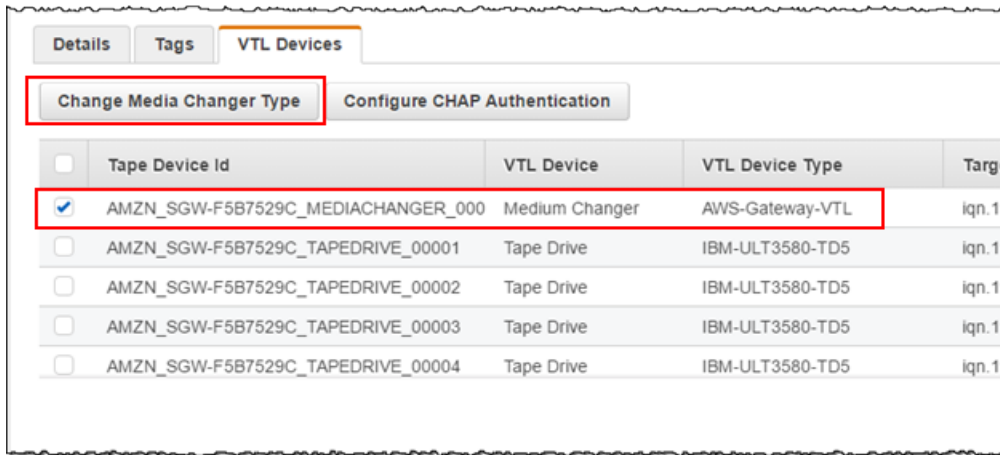
Selección de un cambiador de medios después de activar la gateway

Una vez que la gateway está activada, puede elegir otro tipo de cambiador de medios.

Para seleccionar otro tipo de cambiador de medios después de activar la gateway

1. Detenga todos los trabajos relacionados que se encuentren en ejecución en el software de copia de seguridad.
2. En el servidor Windows, abra la ventana de propiedades del SCSI iniciador i.
3. Elija la pestaña Targets (Destinos) para mostrar los destinos detectados.
4. En el panel Discovered targets, elija el cambiador de medios que desee cambiar, seleccione Disconnect (Desconectar) y, por último, haga clic en OK (Aceptar).

- En la consola de Storage Gateway, elija Puertas de enlace en el panel de navegación y, a continuación, elija la puerta de enlace cuyo cambiador de medios desee cambiar.
- Elija la pestaña VTLDispositivos, seleccione el cambiador de medio que desee cambiar y, a continuación, elija Cambiar cambiador de medio.



- En el cuadro de diálogo Change Media Changer Type (Cambiar tipo de cambiador de medios) que aparece, seleccione el cambiador de medios que desee en la lista desplegable y, a continuación, elija Save (Guardar).

Actualización de la unidad de dispositivo para el cambiador de medios

- Abra el Administrador de dispositivos del servidor de Windows y amplíe el árbol Dispositivos del cambiador de medios.
- Abra el menú contextual (haga clic con el botón derecho) de Cambiador de medio desconocido y elija Actualizar software de controlador para abrir la ventana Actualizar software de controlador - Cambiador de medios desconocido.
- En la sección ¿Cómo desea buscar el software de controlador?, elija Buscar software de controlador en el equipo.
- Elija Elegir en una lista de controladores de dispositivo en el equipo.

Note

Recomendamos utilizar el controlador Sony TSL -A500C Autoloader con el software de backup Veeam Backup & Replication 11A y Microsoft System Center Data Protection Manager. Este controlador de Sony se ha probado con estos tipos de software de copia de seguridad hasta Windows Server 2019 inclusive.

5. En la sección Seleccione el controlador de dispositivo que desea instalar para este hardware, desactive la casilla Mostrar hardware compatible, seleccione Sony en la lista de fabricantes, elija Sony - TSL -A500C Autoloader en la lista de modelos y, a continuación, elija Siguiente.
6. En el cuadro de advertencia que aparece, elija Sí. Si el controlador se ha instalado correctamente, cierre la ventana Actualizar software de controlador.

Visualización de códigos de barras para cintas en Microsoft System Center DPM

Si utiliza el controlador de cambiador de medios para el TSL cargador automático Sony -A500C, Microsoft System Center Data Protection Manager no muestra automáticamente los códigos de barras de las cintas virtuales creadas en Storage Gateway. Para mostrar correctamente los códigos de barras de las cintas, cambie el controlador del cambiador de medios a Sun/ Library. StorageTek

Para mostrar los códigos de barras

1. Asegúrese de que todos los trabajos de copia de seguridad se hayan completado y de que no haya tareas pendientes o en curso.
2. Extraiga las cintas y colóquelas en un almacenamiento sin conexión (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive) y salga de la consola de DPM administración. Para obtener información sobre cómo extraer una cinta, consulte. DPM [Archivar una cinta mediante DPM](#)
3. En Herramientas administrativas, elija Servicios y abra el menú contextual (haga clic con el botón derecho) de DPMServicio en el panel de detalles y, a continuación, elija Propiedades.
4. En la pestaña General, asegúrese de que el tipo de inicio esté establecido en Automático y seleccione Detener para detener el DPM servicio.
5. Obtenga los StorageTek controladores del [catálogo de Microsoft Update](#) en el sitio web de Microsoft.

Note

Anote los diferentes controladores para los diferentes tamaños.

Para Tamaño 18 K, elija Controladores x86.

Para Tamaño 19 K, elija Controladores x64.

6. En el servidor de Windows, abra el Administrador de dispositivos y expanda el árbol Dispositivos de cambiador de medios.

7. Abra el menú contextual (haga clic con el botón derecho) de Cambiador de medio desconocido y elija Actualizar software de controlador para abrir la ventana Actualizar software de controlador - Cambiador de medios desconocido.
8. Busque la ruta de la nueva ubicación e instalación del controlador. El controlador aparece como Sun/ StorageTek Library. Las unidades de cinta permanecen como un IBM ULT358 dispositivo TD5 SCSI secuencial 0.
9. Reinicie el DPM servidor.
10. Cree cintas en la consola de Storage Gateway.
11. Abra la consola DPM de administración, seleccione Administración y, a continuación, seleccione Volver a escanear para obtener nuevas bibliotecas de cintas. Debería ver la biblioteca Sun/ StorageTek .
12. Elija la biblioteca y seleccione Inventory (Inventario).
13. Seleccione Añadir cintas para añadir las nuevas cintas. DPM Las nuevas cintas debería mostrar ahora sus códigos de barras.

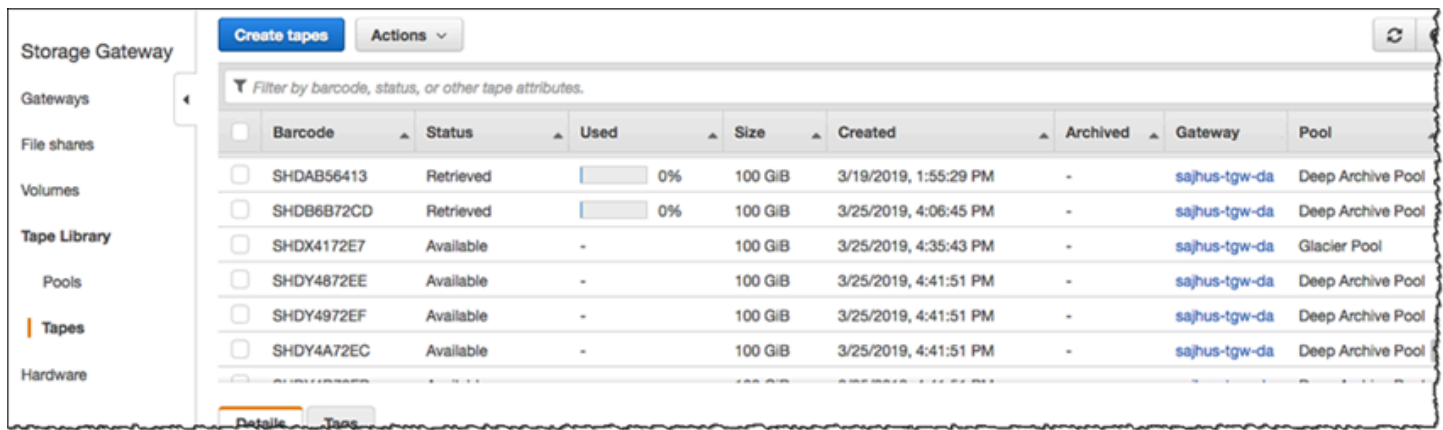
Trabajo con cintas

Storage Gateway proporciona una biblioteca de cintas virtuales (VTL) para cada puerta de enlace de cinta que active. Inicialmente, la biblioteca no contiene cintas, pero puede crear cintas siempre que lo necesite. La aplicación puede leer y escribir en cualquier cinta disponible en la puerta de enlace de cinta. El estado de una cinta debe ser AVAILABLE el mismo que para poder escribir en ella. Estas cintas están respaldadas por Amazon Simple Storage Service (Amazon S3), es decir, cuando se escribe en estas cintas, la puerta de enlace de cinta almacena los datos en Amazon S3. Para obtener más información, consulte [Descripción de la información sobre el estado de la cinta en un VTL](#).

Temas

- [Archivado de cintas](#)
- [Cancelación del archivado de cintas](#)

La biblioteca de cintas muestra las cintas de la puerta de enlace de cinta. La biblioteca muestra el código de barras de cinta, el estado, el tamaño y la cantidad de cinta utilizada, así como la gateway con la que está asociada.



	Barcode	Status	Used	Size	Created	Archived	Gateway	Pool
<input type="checkbox"/>	SHDAB56413	Retrieved	0%	100 GiB	3/19/2019, 1:55:29 PM	-	sajhus-tgw-da	Deep Archive Pool
<input type="checkbox"/>	SHDB6872CD	Retrieved	0%	100 GiB	3/25/2019, 4:06:45 PM	-	sajhus-tgw-da	Deep Archive Pool
<input type="checkbox"/>	SHDX4172E7	Available	-	100 GiB	3/25/2019, 4:35:43 PM	-	sajhus-tgw-da	Glacier Pool
<input type="checkbox"/>	SHDY4872EE	Available	-	100 GiB	3/25/2019, 4:41:51 PM	-	sajhus-tgw-da	Deep Archive Pool
<input type="checkbox"/>	SHDY4972EF	Available	-	100 GiB	3/25/2019, 4:41:51 PM	-	sajhus-tgw-da	Deep Archive Pool
<input type="checkbox"/>	SHDY4A72EC	Available	-	100 GiB	3/25/2019, 4:41:51 PM	-	sajhus-tgw-da	Deep Archive Pool

Si hay un gran número de cintas en la biblioteca, la consola permite buscar cintas por código de barras, por estado o por ambos. Cuando busque por código de barras, puede filtrar por estado y gateway.

Para buscar por código de barras, estado y gateway

1. Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa>.
2. En el panel de navegación, elija Tapes (Cintas) y, a continuación, escriba un valor en el cuadro de búsqueda. El valor puede ser el código de barras, el estado o la gateway. De forma predeterminada, Storage Gateway busca en todas las cintas virtuales. No obstante, también puede filtrar la búsqueda por estado.

Si filtra por estado, las cintas que cumplan los criterios aparecerán en la biblioteca de la consola de Storage Gateway.

Si filtra por puerta de enlace, las cintas asociadas con esa puerta de enlace aparecerán en la biblioteca de la consola de Storage Gateway.

Note

De forma predeterminada, Storage Gateway muestra todas las cintas independientemente de su estado.

Archivado de cintas

Puede archivar las cintas virtuales que se encuentran en la puerta de enlace de cinta. Cuando se archiva una cinta, Storage Gateway traslada la cinta al archivo.

Para archivar una cinta, utilice el software de copia de seguridad. El proceso de archivado en cinta consta de tres etapas, denominadas estados de la cinta IN TRANSIT TO VTS y ARCHIVING: ARCHIVED

- Para archivar una cinta, utilice el comando proporcionado por la aplicación de copia de seguridad. Cuando comienza el proceso de archivado, el estado de la cinta cambia TRANSITa IN TO VTS y la aplicación de backup ya no puede acceder a la cinta. En esta etapa, su Tape Gateway está cargando los datos a. AWS Si es necesario, puede cancelar el archivo en curso. Para obtener más información acerca de la cancelación de archivos, consulte [Cancelación del archivado de cintas](#).

Note

Los pasos para archivar una cinta dependen de la aplicación de copia de seguridad. Para obtener instrucciones detalladas, consulte la documentación de la aplicación de copia de seguridad.

- Una vez AWS finalizada la carga de datos, el estado de la cinta cambia a ARCHIVINGy Storage Gateway comienza a moverla al archivo. En este momento no se puede cancelar el proceso de archivo.
- Una vez que la cinta se mueve al archivo, su estado cambia a ARCHIVEDy usted puede recuperarla en cualquiera de sus gateways. Para obtener más información sobre la recuperación de cintas, consulte [Recuperación de cintas archivadas](#).

Los pasos para archivar una cinta dependen del software de copia de seguridad. Para obtener instrucciones sobre cómo archivar una cinta con el NetBackup software de Symantec, consulte [Archivar la](#) cinta.

Cancelación del archivado de cintas

Una vez que empiece a archivar una cinta, quizá decida que necesita recuperarla. Por ejemplo, quizá desee cancelar el proceso de archivado, recuperar la cinta porque el proceso de archivado esté tardando demasiado o leer datos de la cinta. Una cinta que se está archivando pasa por tres estados, como se muestra a continuación:

- EN TRANSITVTS: Su Tape Gateway está cargando datos a. AWS
- ARCHIVING: La carga de datos ha finalizado y la puerta de enlace de cintas está trasladando la cinta al archivo.

- ARCHIVED: La cinta se mueve y el archivo está disponible para su recuperación.

Puede cancelar el archivado solo cuando el estado de la cinta sea TO. TRANSIT VTS Según factores tales como el ancho de banda de carga y la cantidad de datos que se estén cargando, este estado puede ser visible o no en la consola de Storage Gateway. Para cancelar el archivado en cinta, utilice la [CancelRetrieval](#) acción de la referencia. API

Obtención de una clave de activación para la puerta de enlace

Para recibir una clave de activación para la puerta de enlace, realice una solicitud web a la máquina virtual (VM) de la puerta de enlace. La máquina virtual devuelve un redireccionamiento que contiene la clave de activación, la cual se transfiere como uno de los parámetros de la acción de la API de `ActivateGateway` para especificar la configuración de la puerta de enlace. Para obtener más información, consulte la referencia [ActivateGateway](#) de la API de Storage Gateway.

Note

Las claves de activación de la puerta de enlace caducan en 30 minutos si no se utilizan.

La solicitud que realiza a la máquina virtual de puerta de enlace incluye la AWS región en la que se produce la activación. La URL que devuelve el redireccionamiento en la respuesta contiene un parámetro de cadena de consulta llamado `activationkey`. Este parámetro de cadena de consulta es su clave de activación. El formato de la cadena de consulta tiene el aspecto siguiente: `http://gateway_ip_address?activationRegion=activation_region`. El resultado de esta consulta devuelve la región y la clave de activación.

La URL también incluye `vpcEndpoint`, el ID del punto de conexión de VPC para las puertas de enlace que se conectan mediante el tipo de punto de conexión de VPC.

Note

El dispositivo de hardware de Storage Gateway, las plantillas de imágenes de VM y las imágenes de máquina de Amazon (AMI) de Amazon EC2 vienen preconfigurados con los servicios HTTP necesarios para recibir y responder a las solicitudes web que se describen en esta página. No es obligatorio ni recomendable instalar ningún servicio adicional en la puerta de enlace.

Temas

- [Linux \(curl\)](#)
- [Linux \(bash/zsh\)](#)
- [Microsoft Windows PowerShell](#)
- [Mediante la consola local](#)

Linux (curl)

En los siguientes ejemplos se muestra cómo obtener una clave de activación con Linux (curl).

Note

Sustituya las variables resaltadas por valores reales de la puerta de enlace. Los valores aceptables son los siguientes:

- *gateway_ip_address*: la dirección IPv4 de la puerta de enlace, por ejemplo 172.31.29.201
- *gateway_type*: el tipo de puerta de enlace que desea activar, como, STORED, CACHEDVTL, FILE_S3 o. FILE_FSX_SMB
- *region_code*: la región en la que desea activar la puerta de enlace. Consulte [Puntos de conexión regionales](#) en la Guía de referencia general de AWS . Si no se especifica este parámetro, o si el valor proporcionado está mal escrito o no coincide con una región válida, el comando utilizará la región por defecto. us-east-1
- *vpc_endpoint*: el nombre del punto de conexión de VPC de la puerta de enlace, por ejemplo vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com.

Para obtener la clave de activación de un punto de conexión público:

```
curl "http://gateway_ip_address?activationRegion=region_code&no_redirect"
```

Para obtener la clave de activación de un punto de conexión de VPC:

```
curl "http://gateway_ip_address?  
activationRegion=region_code&vpcEndpoint=vpc_endpoint&no_redirect"
```

Linux (bash/zsh)

En el siguiente ejemplo se muestra cómo utilizar Linux (bash/zsh) para recuperar la respuesta HTTP, analizar los encabezados HTTP y obtener la clave de activación.

```
function get-activation-key() {
    local ip_address=$1
    local activation_region=$2
    if [[ -z "$ip_address" || -z "$activation_region" || -z "$gateway_type" ]]; then
        echo "Usage: get-activation-key ip_address activation_region gateway_type"
        return 1
    fi

    if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region&gatewayType=$gateway_type"); then
        activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
        echo "$activation_key_param" | cut -f2 -d=
    else
        return 1
    fi
}
```

Microsoft Windows PowerShell

El siguiente ejemplo muestra cómo utilizar Microsoft Windows PowerShell para obtener la respuesta HTTP, analizar los encabezados HTTP y obtener la clave de activación.

```
function Get-ActivationKey {
    [CmdletBinding()]
    Param(
        [parameter(Mandatory=$true)][string]$IpAddress,
        [parameter(Mandatory=$true)][string]$ActivationRegion,
        [parameter(Mandatory=$true)][string]$GatewayType
    )
    PROCESS {
        $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion&gatewayType=$GatewayType" -MaximumRedirection 0 -
ErrorAction SilentlyContinue
        if ($request) {
```

```
$activationKeyParam = $request.Headers.Location | Select-String -Pattern
"activationKey=([A-Z0-9-]+)"
    $activationKeyParam.Matches.Value.Split("=")[1]
}
}
}
```

Mediante la consola local

En el siguiente ejemplo se muestra cómo utilizar la consola local para generar y mostrar una clave de activación.

Para obtener una clave de activación para la puerta de enlace desde la consola local

1. Inicie sesión en la consola local. Si se conecta a la instancia de Amazon EC2 desde un equipo Windows, inicie sesión como admin.
2. Tras iniciar sesión y ver el menú principal Activación del dispositivo de AWS - Configuración, seleccione 0 para elegir Obtener clave de activación.
3. Seleccione Storage Gateway como opción de familia de puertas de enlace.
4. Cuando se le solicite, introduzca la AWS región en la que desee activar la puerta de enlace.
5. Introduzca 1 para punto de conexión público o 2 para punto de conexión de VPC como tipo de red.
6. Introduzca 1 para estándar o 2 estándar federal de procesamiento de información (FIPS) como tipo de punto de conexión.

Conexión de SCSI iniciadores

Al administrar su puerta de enlace, trabaja con volúmenes o dispositivos de biblioteca de cintas virtuales (VTL) que están expuestos como destinos de la interfaz de sistemas de computadoras pequeñas (iSCSI) de Internet. En el caso de las pasarelas de volumen, los SCSI objetivos i son volúmenes. En el caso de las pasarelas de cinta, los objetivos son los dispositivosVTL. Como parte de este trabajo, debe realizar tareas como conectarse a esos destinos, personalizar la SCSI configuración i, conectarse desde un cliente Red Hat Linux y configurar el Protocolo de autenticación Challenge-Handshake (). CHAP

Temas

- [Conexión de sus VTL dispositivos a un cliente de Windows](#)

- [Conexión de sus volúmenes o VTL dispositivos a un cliente Linux](#)
- [Personalización de los ajustes SCSI](#)
- [Configuración de CHAP la autenticación para sus objetivos i SCSI](#)

El SCSI estándar i es un estándar de redes de almacenamiento basado en el Protocolo de Internet (IP) para iniciar y administrar conexiones entre clientes y dispositivos de almacenamiento basados en IP. La siguiente lista define algunos de los términos que se utilizan para describir la SCSI conexión i y los componentes involucrados.

SCSIiniciador i.

El componente cliente de una SCSI red i. El iniciador envía solicitudes al SCSI objetivo i. Los iniciadores pueden implementarse en software o hardware. Storage Gateway solo admite los iniciadores de software.

i SCSI es el objetivo

El componente de servidor de la SCSI red i que recibe y responde a las solicitudes de los iniciadores. Cada uno de sus volúmenes está expuesto como un SCSI objetivo i. Connect solo un SCSI iniciador i a cada SCSI objetivo i.

Microsoft i SCSI iniciator

Programa de software de los equipos Microsoft Windows que permite conectar un equipo cliente (es decir, el equipo que ejecuta la aplicación cuyos datos desea escribir en la puerta de enlace) a una matriz externa SCSI basada en i (es decir, la puerta de enlace). La conexión se efectúa a través de la tarjeta adaptadora de red Ethernet del equipo. El SCSI iniciador Microsoft i se validó con Storage Gateway en Windows 8.1, Windows 10, Windows Server 2012 R2, Windows Server 2016 y Windows Server 2019. El iniciador está integrado en estos sistemas operativos.

Red Hat es un iniciador SCSI

El paquete `iscsi-initiator-utils` Resource Package Manager (RPM) le proporciona un SCSI iniciador i implementado en el software para Red Hat Linux. El paquete incluye un daemon de servidor para el protocolo iSCSI.

Cada tipo de puerta de enlace se puede conectar a SCSI dispositivos i y puede personalizar esas conexiones, tal y como se describe a continuación.

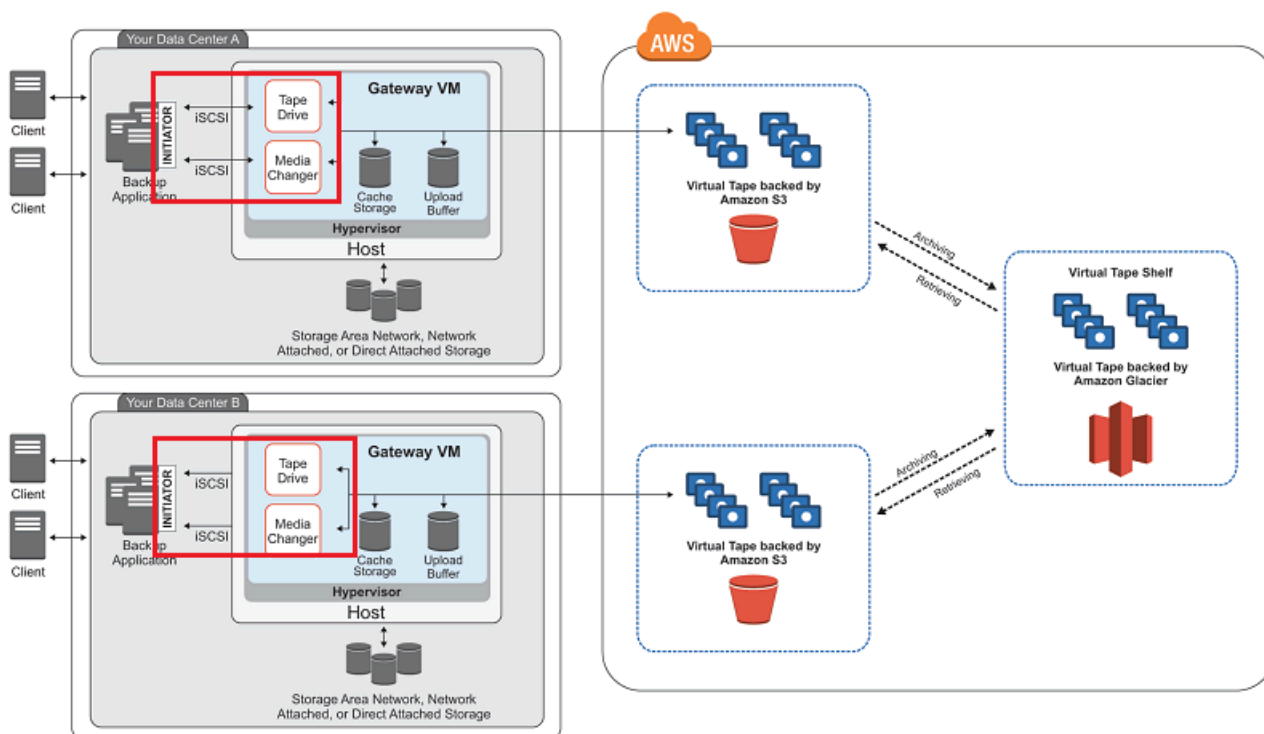
Conexión de sus VTL dispositivos a un cliente de Windows

Una puerta de enlace de cinta expone varias unidades de cinta y un cambiador de medios, denominados colectivamente VTL dispositivos, como objetivos. SCSI Para obtener más información, consulte [Requisitos para configurar Tape Gateway](#).

Note

Solo se conecta una aplicación a cada destino iSCSI.

El siguiente diagrama resalta el SCSI objetivo i en el panorama general de la arquitectura Storage Gateway. Para obtener más información sobre la arquitectura de Storage Gateway, consulte [Funcionamiento de puerta de enlace de cinta \(arquitectura\)](#).



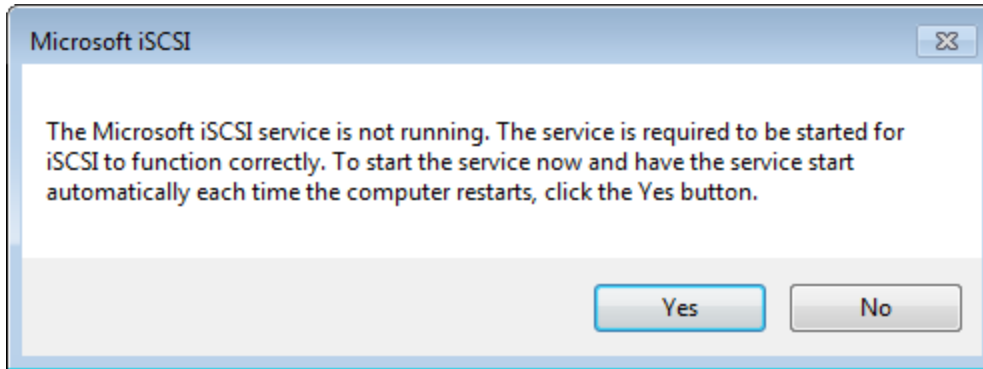
Para conectar su cliente Windows a los dispositivos VTL

1. En el menú Inicio de su equipo cliente Windows, escriba **iscsicpl.exe** en el cuadro Buscar programas y archivos, localice el programa i SCSI initiator y ejecútelo.

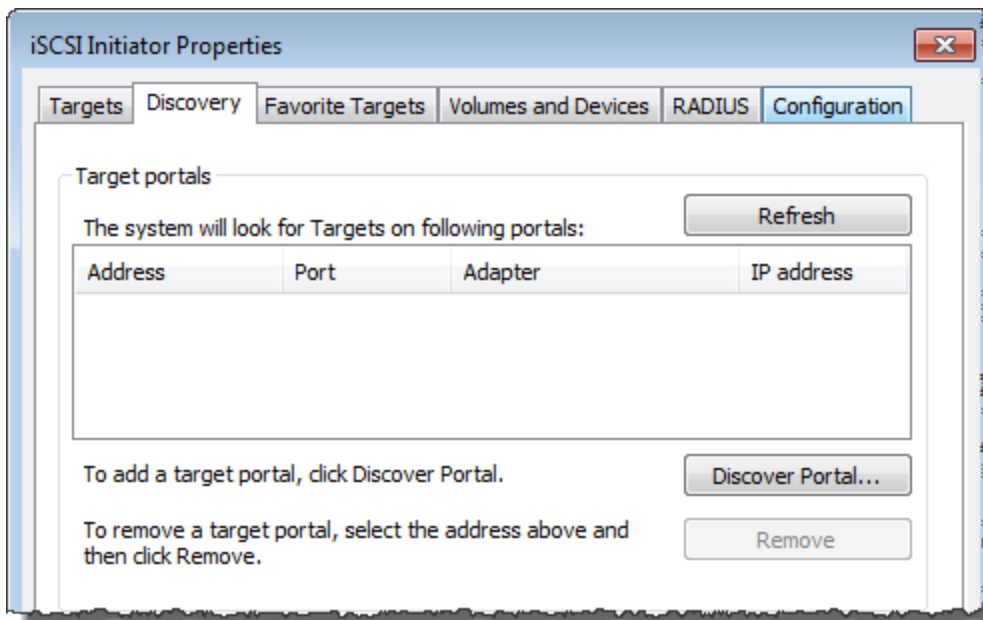
Note

Debe tener derechos de administrador en el equipo cliente para ejecutar el SCSI iniciador i.

- Si se le solicita, elija Sí para iniciar el servicio Microsoft i SCSI Initiator.

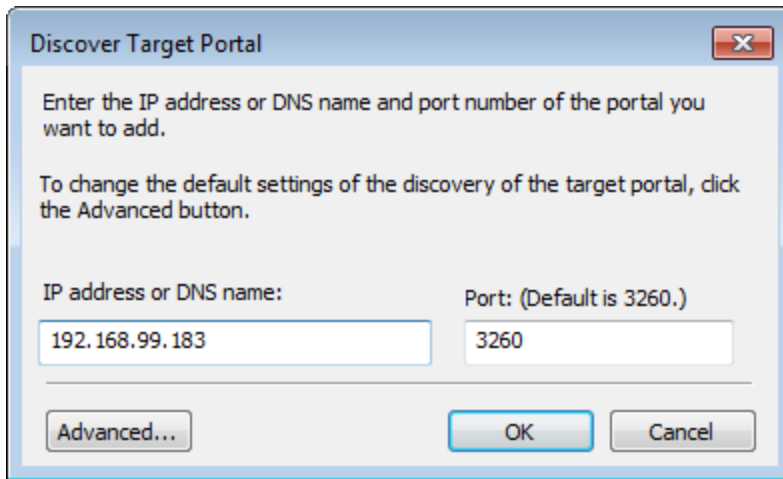


- En el cuadro de diálogo Propiedades SCSI del iniciador i, seleccione la pestaña Discovery y, a continuación, seleccione Discover Portal.



- En el cuadro de diálogo Discover Target Portal, introduzca la dirección IP de su Tape Gateway como dirección IP o DNS nombre y, a continuación, pulse Aceptar. Para obtener la dirección IP de la puerta de enlace, consulte la pestaña Puerta de enlace en la consola de Storage Gateway.

Si implementaste tu gateway en una EC2 instancia de Amazon, puedes encontrar la DNS dirección o IP pública en la pestaña Descripción de la EC2 consola de Amazon.



Discover Target Portal

Enter the IP address or DNS name and port number of the portal you want to add.

To change the default settings of the discovery of the target portal, click the Advanced button.

IP address or DNS name: 192.168.99.183

Port: (Default is 3260.) 3260

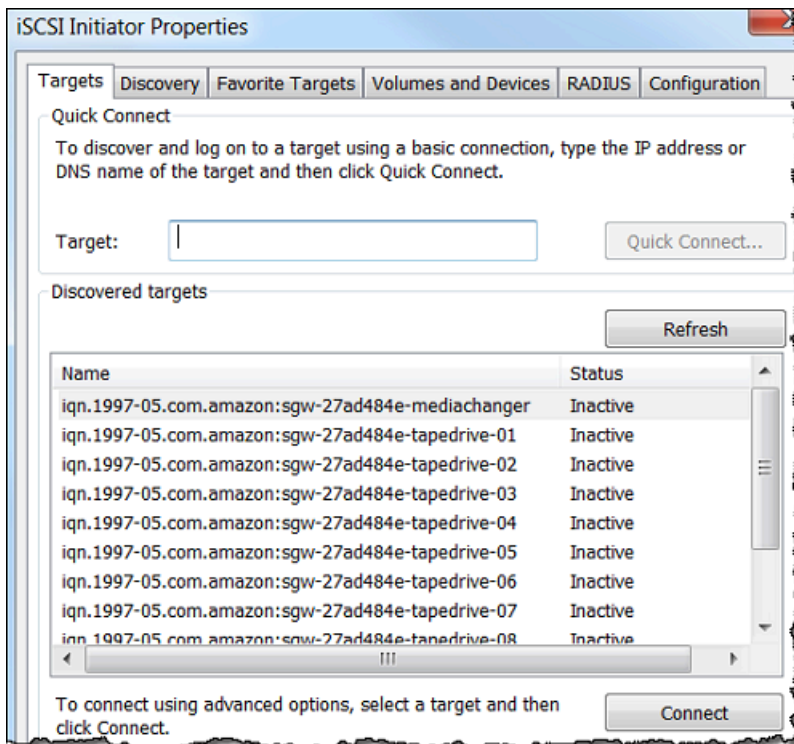
Advanced... OK Cancel

Warning

En el caso de las puertas de enlace que se implementan en una EC2 instancia de Amazon, no se admite el acceso a la puerta de enlace a través de una conexión pública a Internet. La dirección IP elástica de la EC2 instancia de Amazon no se puede utilizar como dirección de destino.

5. Elija la pestaña Targets y, a continuación, elija Refresh. Las 10 unidades de cinta y el cambiador de medios aparecen en el cuadro Destinos detectados. El estado de los destinos es Inactive.

La siguiente captura de pantalla muestra los destinos detectados.

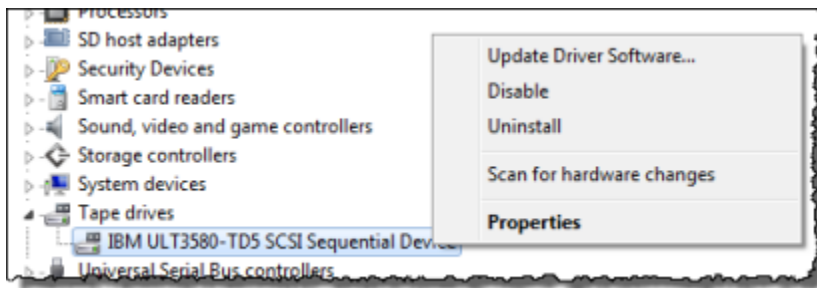


6. Seleccione el primer dispositivo y elija Conectar. Puede conectar los dispositivos de uno en uno.
7. En el cuadro de diálogo Conectarse al destino, elija Aceptar.
8. Repita los pasos 6 y 7 para cada uno de los dispositivos para conectarlos todos y, a continuación, seleccione Aceptar en el cuadro de diálogo Propiedades del SCSI iniciador i.

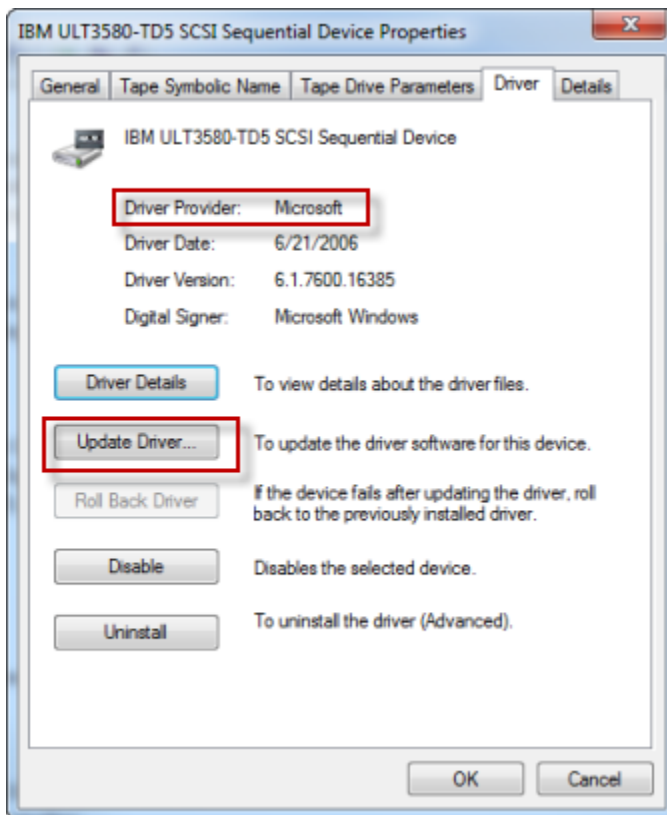
En un cliente de Windows, el proveedor de la unidad de cinta debe ser Microsoft. Utilice el siguiente procedimiento para comprobar cuál es el proveedor de la unidad y actualizarlos si es necesario.

Para comprobar el proveedor del controlador y, si es necesario, actualizar el proveedor y el controlador en un cliente Windows

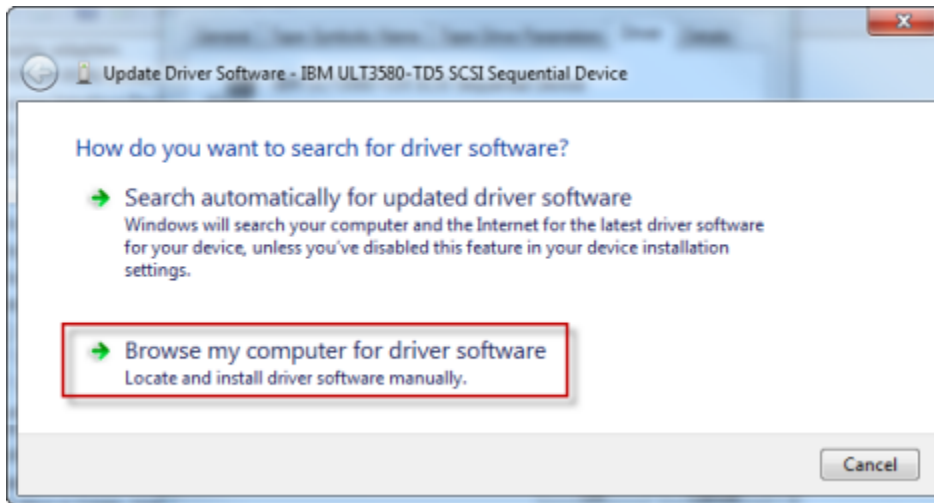
1. En el cliente de Windows, inicie el Administrador de dispositivos.
2. Expanda Unidades de cinta, elija el menú contextual (haga clic con el botón derecho) de una unidad de cinta y elija Propiedades.



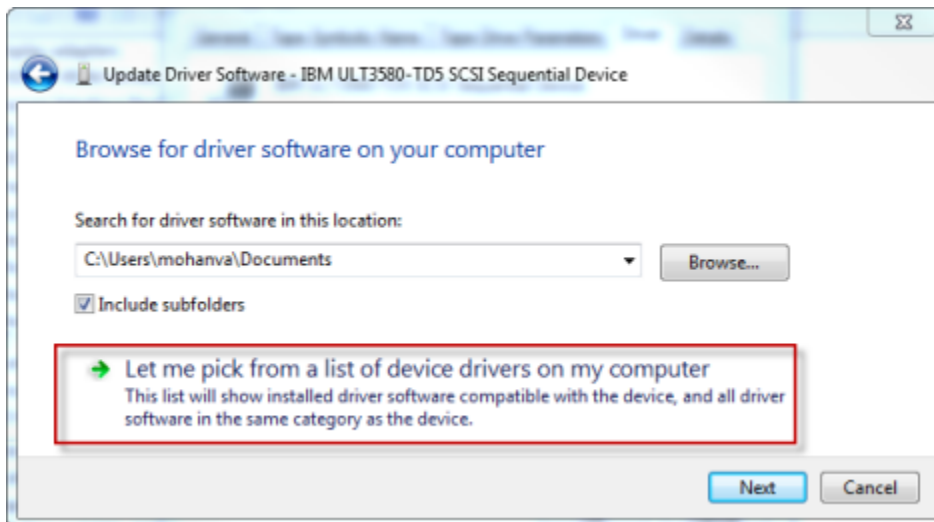
3. En la pestaña Controlador del cuadro de diálogo Propiedades del dispositivo, verifique que el Proveedor del controlador es Microsoft.



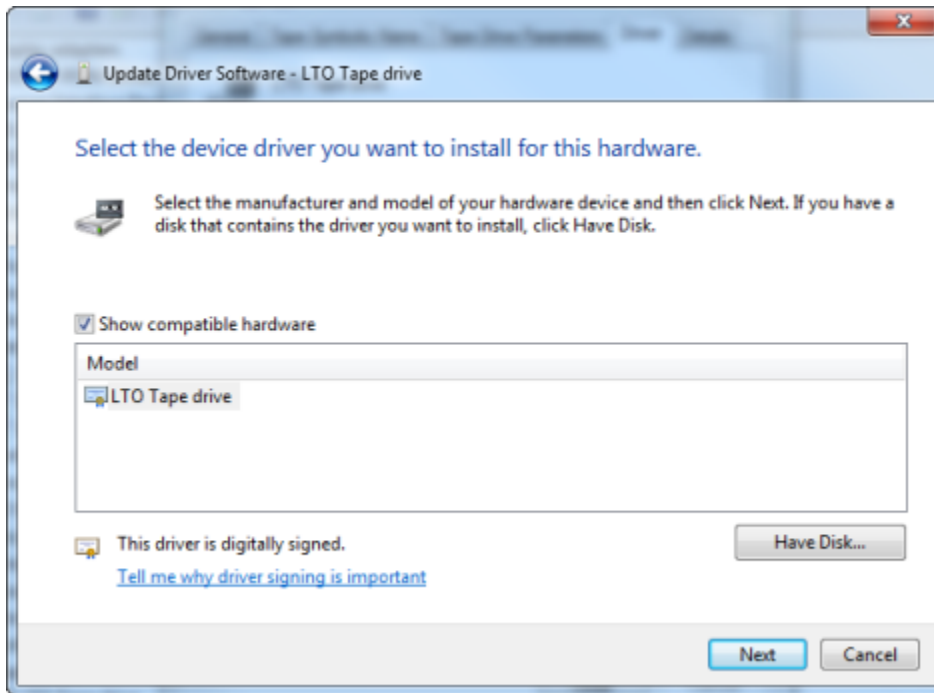
4. Si el Proveedor del controlador no es Microsoft, establezca el valor de la siguiente manera:
 - a. Elija Actualizar controlador.
 - b. En el cuadro de diálogo Update Driver Software, elija Browse my computer for driver software.



- c. En el cuadro de diálogo Update Driver Software, elija Let me pick from a list of device drivers on my computer.



- d. Seleccione Unidad de LTO cinta y elija Siguiente.



- e. Elija Cerrar para cerrar la ventana Actualizar software del controlador y verifique que el valor de Proveedor del controlador esté ahora establecido en Microsoft.
5. Repita los pasos del 4.1 al 4.5 para actualizar todas las unidades de cinta.

Conexión de sus volúmenes o VTL dispositivos a un cliente Linux

Cuando se utiliza Red Hat Enterprise Linux (RHEL), se utiliza el `iscsi-initiator-utils` RPM paquete para conectarse a los SCSI destinos de su gateway i (volúmenes o VTL dispositivos).

Para conectar un cliente Linux a los SCSI destinos i

1. Instale el `iscsi-initiator-utils` RPM paquete, si aún no está instalado en su cliente.

Puede utilizar el comando siguiente para instalar el paquete.

```
sudo yum install iscsi-initiator-utils
```

2. Asegúrese de que el SCSI daemon i esté en ejecución.
 - a. Compruebe que el SCSI daemon i se esté ejecutando mediante uno de los siguientes comandos.

Para RHEL 5 o 6, utilice el siguiente comando.

```
sudo /etc/init.d/iscsi status
```

Para RHEL 7, utilice el siguiente comando.

```
sudo service iscsid status
```

- b. Si el comando de estado no devuelve el estado en ejecución, debe iniciar el daemon mediante uno de los siguientes comandos.

Para RHEL 5 o 6, utilice el siguiente comando.

```
sudo /etc/init.d/iscsi start
```

Para RHEL 7, utilice el siguiente comando. En el RHEL caso de 7, normalmente no es necesario iniciar el `iscsid` servicio de forma explícita.

```
sudo service iscsid start
```

3. Para descubrir los objetivos de volumen o VTL dispositivo definidos para una puerta de enlace, utilice el siguiente comando de detección.

```
sudo /sbin/iscsiadm --mode discovery --type sendtargets --portal [GATEWAY_IP]:3260
```

Sustituya la dirección IP de la puerta de enlace por la `[GATEWAY_IP]` variable del comando anterior. Puede encontrar la IP de la puerta de enlace en las propiedades i SCSI Target Info de un volumen de la consola Storage Gateway.

El resultado del comando de detección tendrá un aspecto semejante al de este ejemplo.

Para puertas de enlace de volumen: `[GATEWAY_IP]:3260, 1
iqn.1997-05.com.amazon:myvolume`


Para puertas de enlace de cinta: `iqn.1997-05.com.amazon:[GATEWAY_IP]-
tapedrive-01`

Su nombre SCSI cualificado i (IQN) será diferente al que se muestra anteriormente, ya que IQN los valores son exclusivos de una organización. El nombre del destino es el especificado al crear

el volumen. También puede encontrar este nombre de destino en el panel de propiedades de iSCSI Target Info al seleccionar un volumen en la consola Storage Gateway.

4. Para conectarse a un destino, utilice el siguiente comando.

Tenga en cuenta que debe especificar el correcto `[GATEWAY_IP]` y IQN en el comando `connect`.

 Warning

En el caso de las puertas de enlace que se implementan en una EC2 instancia de Amazon, no se admite el acceso a la puerta de enlace a través de una conexión pública a Internet. La dirección IP elástica de la EC2 instancia de Amazon no se puede utilizar como dirección de destino.

```
sudo /sbin/iscsiadm --mode node --targetname  
iqn.1997-05.com.amazon:[ISCSI_TARGET_NAME] --portal [GATEWAY_IP]:3260,1 --login
```

5. Para comprobar que el volumen se encuentra asociado a la máquina cliente (el iniciador), utilice el comando siguiente.

```
ls -l /dev/disk/by-path
```

El resultado del comando tendrá un aspecto semejante al de este ejemplo.

```
lrwxrwxrwx. 1 root root 9 Apr 16 19:31 ip-[GATEWAY_IP]:3260-iscsi-  
iqn.1997-05.com.amazon:myvolume-lun-0 -> ../../sda
```

Le recomendamos encarecidamente que, después de configurar el iniciador, personalice la SCSI configuración de iSCSI tal y como se describe en [Personalización de la configuración de Linux iSCSI](#).

Personalización de los ajustes SCSI

Tras configurar el iniciador, le recomendamos encarecidamente que personalice la SCSI configuración iSCSI para evitar que el iniciador se desconecte de los destinos.

Al aumentar los valores de SCSI tiempo de espera de `i`, tal y como se muestra en los pasos siguientes, su aplicación podrá gestionar mejor las operaciones de escritura que tardan mucho tiempo y otros problemas transitorios, como las interrupciones de la red.

Note

Antes de hacer cambios en el registro, debe hacer backup del mismo. Para obtener información sobre cómo hacer una copia de seguridad y otras prácticas recomendadas a seguir al trabajar con el registro, consulte [las prácticas recomendadas del registro](#) en la TechNet biblioteca de Microsoft.

Temas

- [Personalización de la configuración de Windows i SCSI](#)
- [Personalización de la configuración de Linux i SCSI](#)
- [Personalización de la configuración del tiempo de espera del disco de Linux para las puertas de enlace de volumen](#)

Personalización de la configuración de Windows i SCSI

Para una configuración de Tape Gateway, la conexión a VTL los dispositivos mediante un SCSI iniciador Microsoft `i` es un proceso de dos pasos:

1. Conecte la puerta de enlace de cinta al cliente Windows.
2. Si está utilizando una aplicación de backup, configure la aplicación para que utilice los dispositivos.

La configuración del ejemplo de Introducción proporciona instrucciones para ambos pasos. Utiliza la aplicación de respaldo de Symantec NetBackup . Para obtener más información, consulte [Conexión de sus VTL dispositivos](#) y [Configuración de dispositivos de almacenamiento NetBackup](#) .

Para personalizar la configuración de Windows `i` SCSI

1. Aumente el tiempo máximo para las solicitudes en la cola.
 - a. Inicie el Editor del Registro (`Regedit.exe`).

- b. Navegue hasta la clave de identificación única global (GUID) de la clase de dispositivo que contiene la configuración SCSI del controlador i, como se muestra a continuación.

⚠ Warning

Asegúrese de que está trabajando en la `CurrentControlSet\Control\Class` subclave y no en otro conjunto de controles, como `ControlSet001` o `ControlSet002`.

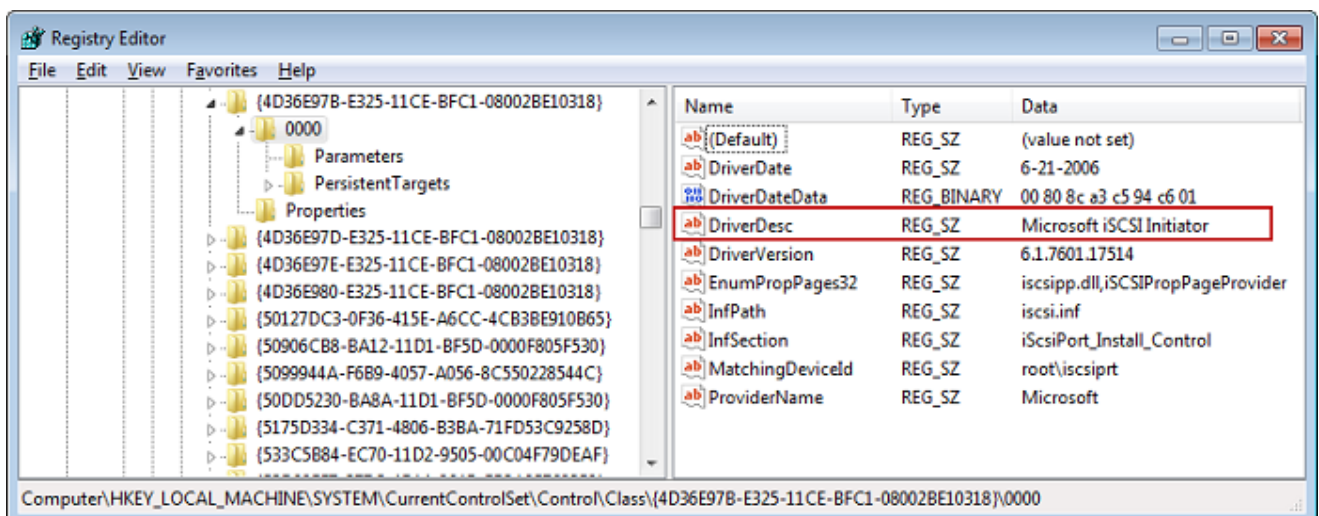
```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}
```

- c. Busque la subclave del SCSI iniciador Microsoft i, que se muestra a continuación [*Instance Number*].

La clave se representa mediante un número de cuatro dígitos, como por ejemplo `0000`.

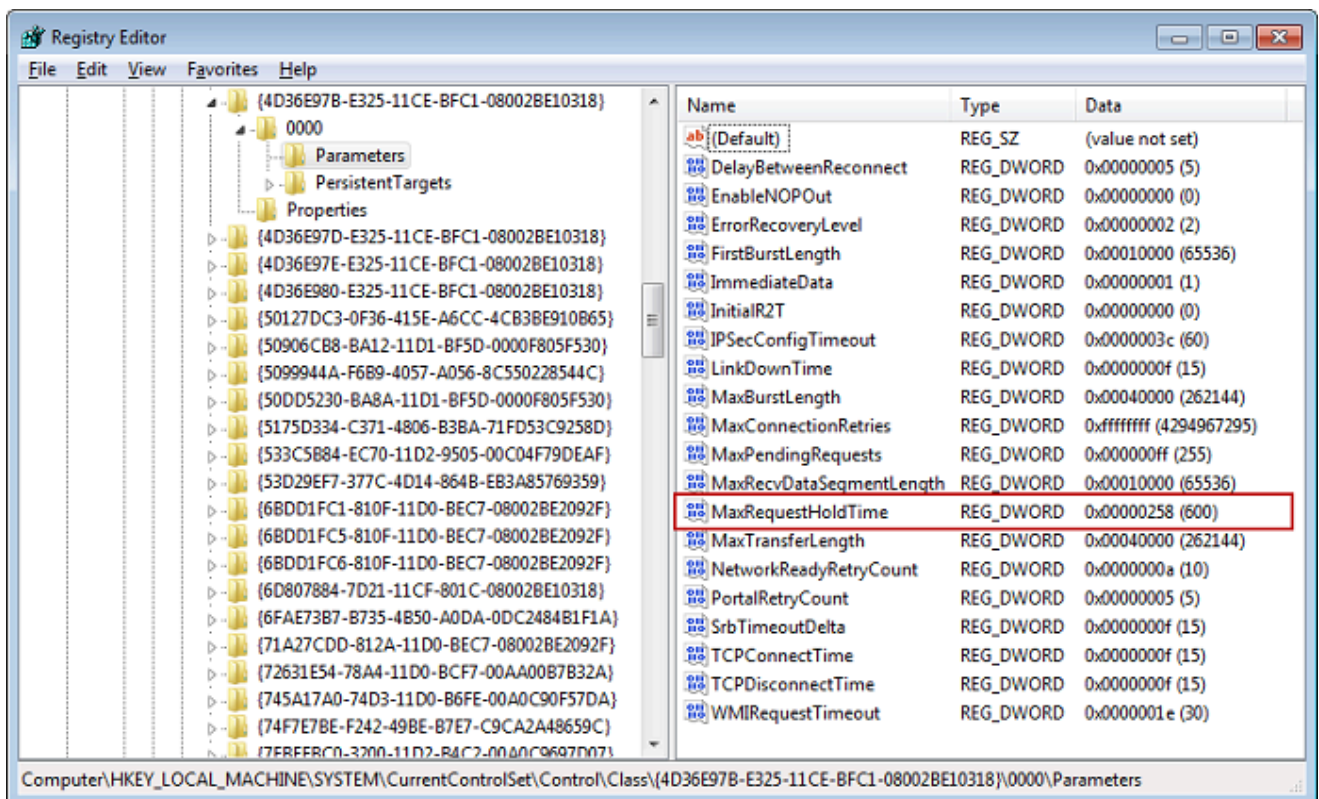
```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\[<Instance Number>
```

Según lo que esté instalado en el equipo, es posible que el SCSI iniciador Microsoft i no sea la `0000` subclave. Para asegurarse de haber seleccionado la subclave correcta, verifique que la cadena `DriverDesc` tenga el valor `Microsoft iSCSI Initiator`, como se muestra en el ejemplo siguiente.



- d. Para mostrar la SCSI configuración i, elija la subclave Parámetros.
- e. Abra el menú contextual (haga clic con el botón derecho) del valor MaxRequestHoldTimeDWORD(32 bits), elija Modificar y, a continuación, cambie el valor a **600**

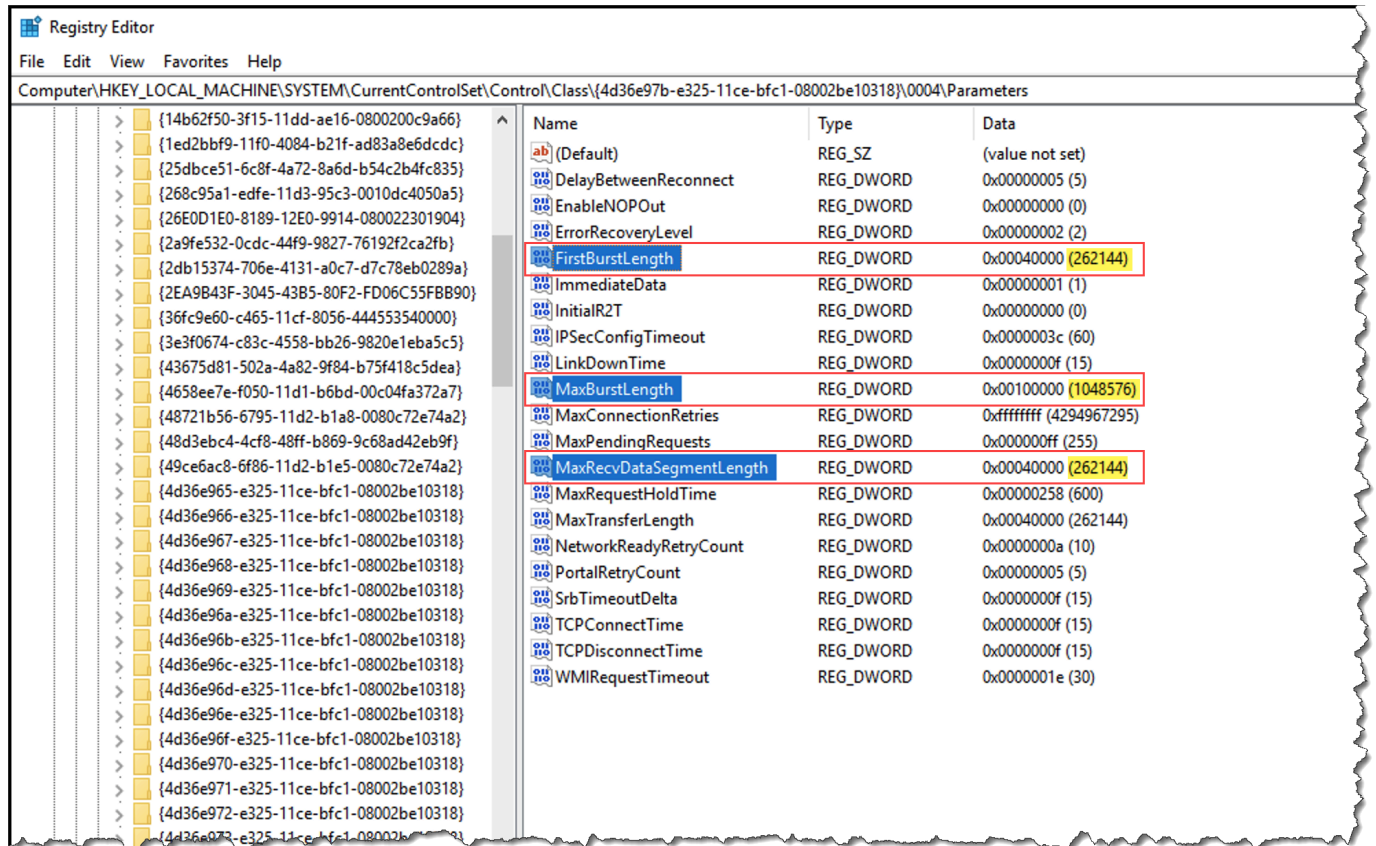
MaxRequestHoldTimeespecifica cuántos segundos debe mantener presionado el SCSI iniciador Microsoft i y volver a intentarlo los comandos pendientes antes de notificar un evento a la capa superior. Device Remove1 Este valor representa un tiempo de espera de 600 segundos, como se muestra en el siguiente ejemplo.



2. Puede aumentar la cantidad máxima de datos que se pueden enviar en SCSI paquetes i modificando los siguientes parámetros:

- FirstBurstLengthcontrola la cantidad máxima de datos que se pueden transmitir en una solicitud de escritura no solicitada. Ajuste este valor en **262144** o en el valor predeterminado del SO Windows, el que sea superior.
- MaxBurstLengthes similar a FirstBurstLength, pero establece la cantidad máxima de datos que se pueden transmitir en las secuencias de escritura solicitadas. Ajuste este valor en **1048576** o en el valor predeterminado del SO Windows, el que sea superior.

- **MaxRecvDataSegmentLength** controla el tamaño máximo del segmento de datos asociado a una sola unidad de datos de protocolo (PDU). Ajuste este valor en **262144** o en el valor predeterminado del SO Windows, el que sea superior.



Note

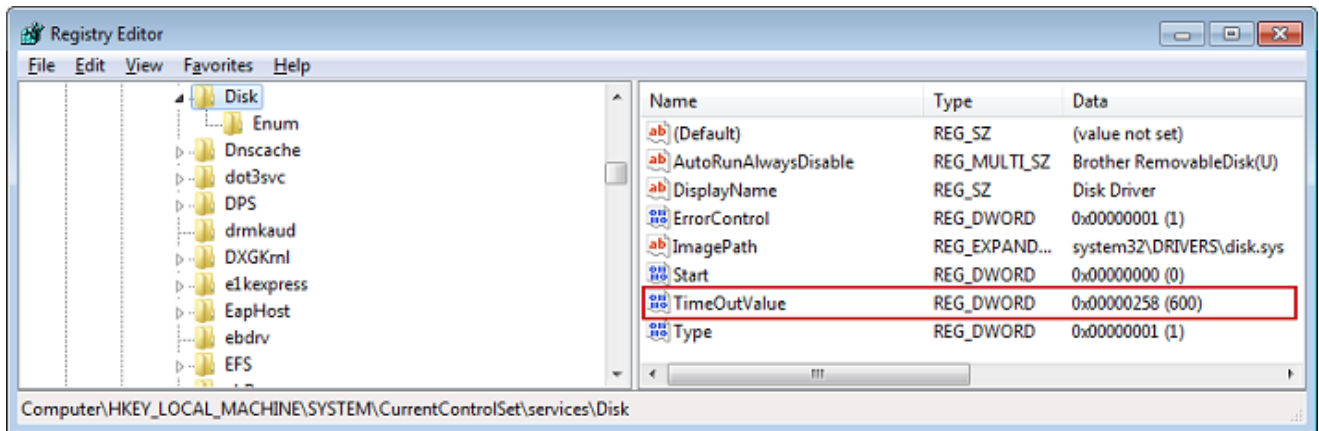
Se pueden optimizar diferentes programas de respaldo para que funcionen mejor con diferentes SCSI configuraciones i. Para comprobar los valores de estos parámetros que proporcionarán el mejor rendimiento, consulte la documentación del software de copia de seguridad.

3. Aumente el valor de tiempo de espera del disco, como se muestra a continuación:
 - a. Inicie el Editor del Registro (Regedit.exe), si no lo ha hecho ya.
 - b. Navegue hasta la subclave Disk en la subclave Services del CurrentControlSet, que se muestra a continuación.

HKEY_Local_Machine\SYSTEM\CurrentControlSet\Services\Disk

- c. Abra el menú contextual (haga clic con el botón derecho) del valor `TimeoutValue` (32 bits), elija `Modificar` y, a continuación, cambie el valor a **600**

`TimeoutValue` especifica cuántos segundos esperará el SCSI iniciador a recibir una respuesta del destino antes de intentar recuperar la sesión interrumpiendo y restableciendo la conexión. Este valor representa un período de espera de 600 segundos, como se muestra en el siguiente ejemplo.



4. Para asegurarse de que los nuevos valores de configuración surtan efecto, reinicie el sistema.

Antes de reiniciar, debe asegurarse de que los resultados de todas las operaciones de escritura en los volúmenes se vacíen. Para ello, desconecte los discos de los volúmenes de almacenamiento asignados antes de reiniciar.

Personalización de la configuración de Linux i SCSI

Tras configurar el iniciador de la puerta de enlace, le recomendamos encarecidamente que personalice la SCSI configuración de i para evitar que el iniciador se desconecte de los destinos. Al aumentar los valores de SCSI tiempo de espera de i, tal y como se muestra a continuación, su aplicación podrá gestionar mejor las operaciones de escritura que requieren mucho tiempo y otros problemas transitorios, como las interrupciones de la red.

Note

Los comandos puede ser ligeramente diferentes para otros tipos de Linux. Los siguientes ejemplos están basados en Red Hat Linux.

Para personalizar la configuración de Linux i SCSI

1. Aumente el tiempo máximo para las solicitudes en la cola.
 - a. Abra el archivo `/etc/iscsi/iscsid.conf` y busque las líneas siguientes.

```
node.session.timeo.replacement_timeout = [replacement_timeout_value]
node.conn[0].timeo.noop_out_interval = [noop_out_interval_value]
node.conn[0].timeo.noop_out_timeout = [noop_out_timeout_value]
```

- b. Establecimiento de la propiedad de `[replacement_timeout_value]` valor para **600**.

Establecimiento de la propiedad de `[noop_out_interval_value]` valor para **60**.

Establecimiento de la propiedad de `[noop_out_timeout_value]` valor para **600**.

Los tres valores está en segundos.

Note

La configuración de `iscsid.conf` debe realizarse antes de descubrir la gateway. Si ya ha descubierto la gateway, ha iniciado sesión en el destino o ambos, puede eliminar la entrada de la base de datos de descubrimiento utilizando el siguiente comando. A continuación, puede volver a descubrir o iniciar sesión de nuevo para recoger la nueva configuración.

```
iscsiadm -m discoverydb -t sendtargets -p [GATEWAY_IP]:3260 -o delete
```

2. Aumente los valores máximos para la cantidad de datos que se pueden transmitir en cada respuesta.
 - a. Abra el archivo `/etc/iscsi/iscsid.conf` y busque las líneas siguientes.


```
node.session.iscsi.FirstBurstLength = [replacement_first_burst_length_value]
node.session.iscsi.MaxBurstLength = [replacement_max_burst_length_value]
node.conn[0].iscsi.MaxRecvDataSegmentLength
= [replacement_segment_length_value]
```

- b. Recomendamos los siguientes valores para conseguir un mejor rendimiento. Es posible que el software de copia de seguridad esté optimizado para utilizar valores diferentes, por tanto, consulte la documentación del software de copia de seguridad para obtener los mejores resultados.

Establecimiento de la propiedad de *[replacement_first_burst_length_value]* valor igual **262144** o el valor predeterminado del sistema operativo Linux, el que sea superior.

Establecimiento de la propiedad de *[replacement_max_burst_length_value]* valor igual **1048576** o predeterminado del sistema operativo Linux, el que sea superior.

Establecimiento de la propiedad de *[replacement_segment_length_value]* valor igual **262144** o predeterminado del sistema operativo Linux, el que sea superior.

 Note

Se pueden optimizar distintos programas de copia de seguridad para que funcionen mejor con diferentes SCSI configuraciones i. Para comprobar los valores de estos parámetros que proporcionarán el mejor rendimiento, consulte la documentación del software de copia de seguridad.

3. Reinicie el sistema para asegurarse de que los nuevos valores de configuración surtan efecto.

Antes de reiniciar, asegúrese de que los resultados de todas las operaciones de escritura en las cintas se vacíen. Para ello, desmonte las cintas antes de reiniciar.

Personalización de la configuración del tiempo de espera del disco de Linux para las puertas de enlace de volumen

Si utiliza un Volume Gateway, puede personalizar los siguientes ajustes de tiempo de espera del disco de Linux, además de los SCSI ajustes i descritos en la sección anterior.

Para personalizar la configuración del tiempo de espera del disco de Linux

1. Aumente el valor del tiempo de espera de disco en el archivo de reglas.
 - a. Si está utilizando el iniciador RHEL 5, abra el `/etc/udev/rules.d/50-udev.rules` archivo y busque la siguiente línea.

```
ACTION=="add", SUBSYSTEM=="scsi" , SYSFS{type}=="0|7|14", \  
RUN+="/bin/sh -c 'echo [timeout] > /sys$$DEVPATH/timeout'"
```

Este archivo de reglas no existe en RHEL 6 o 7 iniciadores, por lo que debe crearlo con la siguiente regla.

```
ACTION=="add", SUBSYSTEMS=="scsi" , ATTRS{model}=="Storage Gateway", \  
RUN+="/bin/sh -c 'echo [timeout] > /sys$$DEVPATH/timeout'"
```

Para modificar el valor de tiempo de espera en RHEL 6, utilice el siguiente comando y, a continuación, añada las líneas de código que se muestran anteriormente.

```
sudo vim /etc/udev/rules.d/50-udev.rules
```

Para modificar el valor de tiempo de espera en RHEL 7, utilice el siguiente comando y, a continuación, añada las líneas de código que se muestran anteriormente.

```
sudo su -c "echo 600 > /sys/block/[device name]/device/timeout"
```

- b. Establecimiento de la propiedad de `[timeout]` valor para. **600**

Este valor representa un tiempo de espera de 600 segundos.

2. Reinicie el sistema para asegurarse de que los nuevos valores de configuración surtan efecto.

Antes de reiniciar, asegúrese de que los resultados de todas las operaciones de escritura en los volúmenes se vacíen. Para ello, desmonte los volúmenes de almacenamiento antes de reiniciar.

3. Puede probar la configuración mediante el siguiente comando.

```
udevadm test [PATH_TO_ISCSI_DEVICE]
```

Este comando muestra las reglas udev que se aplican al SCSI dispositivo `i`.

Configuración de CHAP la autenticación para sus objetivos i SCSI

Storage Gateway admite la autenticación entre la puerta de enlace y SCSI los iniciadores i mediante el Protocolo de autenticación Challenge-Handshake (). CHAP proporciona protección contra los ataques de reproducción al verificar periódicamente la identidad de un SCSI iniciador i autenticado para acceder a un volumen y un dispositivo objetivo. VTL

Note

CHAP la configuración es opcional, pero se recomienda encarecidamente.

Para configurarlo CHAP, debe configurarlo tanto en la consola Storage Gateway como en el software i SCSI initiator que utiliza para conectarse al destino. Storage Gateway usa la CHAP conexión mutua, que es cuando el iniciador autentica el destino y el destino autentica al iniciador.

Para configurar el mutuo para sus objetivos CHAP

1. CHAP Configúrelo en la consola Storage Gateway, tal y como se describe en [CHAP Para configurar un destino de VTL dispositivo en la consola Storage Gateway](#).
2. En el software iniciador del cliente, complete la CHAP configuración:
 - Para configurar Mutual CHAP en un cliente de Windows, consulte [Para configurar la conexión mutua CHAP en un cliente de Windows](#).
 - Para configurar CHAP la conexión mutua en un cliente Red Hat Linux, consulte [Para configurar Mutual CHAP en un cliente Red Hat Linux](#).

CHAP Para configurar un destino de VTL dispositivo en la consola Storage Gateway

En este procedimiento, debe especificar dos claves secretas que se utilizan para leer y escribir en una cinta virtual. Estas mismas claves se utilizan en el procedimiento para configurar el iniciador del cliente.

1. En el panel de navegación, seleccione Puertas de enlace.
2. Elija su puerta de enlace y, a continuación, elija la pestaña VTL Dispositivos para ver todos los VTL dispositivos.
3. Elige el dispositivo para el que quieres CHAP configurarlo.

4. Proporcione la información solicitada en el cuadro de diálogo Configurar la CHAP autenticación.
 - a. En Nombre del iniciador, introduzca el nombre del SCSI iniciador i. Este nombre es un nombre SCSI cualificado de Amazon i (IQN) que va `iqn.1997-05.com.amazon:` precedido del nombre de destino. A continuación, se muestra un ejemplo.

`iqn.1997-05.com.amazon:your-tape-device-name`

Para encontrar el nombre del iniciador, utilice el software i SCSI initiator. Por ejemplo, para los clientes de Windows, el nombre es el valor de la pestaña Configuración del iniciador iSCSI. Para obtener más información, consulte [Para configurar la conexión mutua CHAP en un cliente de Windows](#).

 Note


Para cambiar el nombre de un iniciador, primero debe desactivarlo CHAP, cambiar el nombre del iniciador en el software del iniciador i SCSI y, a continuación, activarlo CHAP con el nuevo nombre.

- b. En Secreto que se utiliza para autenticar el iniciador, escriba la clave secreta solicitada.

Esta clave secreta debe tener 12 caracteres como mínimo y 16 como máximo. Este valor es la clave secreta que el iniciador (es decir, el cliente de Windows) debe conocer para poder participar en el destino. CHAP

- c. En Secret used to authenticate Target (mutuoCHAP), introduzca el secreto solicitado.

Esta clave secreta debe tener 12 caracteres como mínimo y 16 como máximo. Este valor es la clave secreta que el objetivo debe conocer para poder participar CHAP con el iniciador.

 Note

La clave secreta que se utiliza para autenticar el destino debe ser diferente de la que se usa para autenticar el iniciador.

- d. Seleccione Guardar.

5. En la pestaña VTLD dispositivos, confirme que el campo de SCSI CHAP autenticación i esté establecido en true.

Para configurar la conexión mutua CHAP en un cliente de Windows

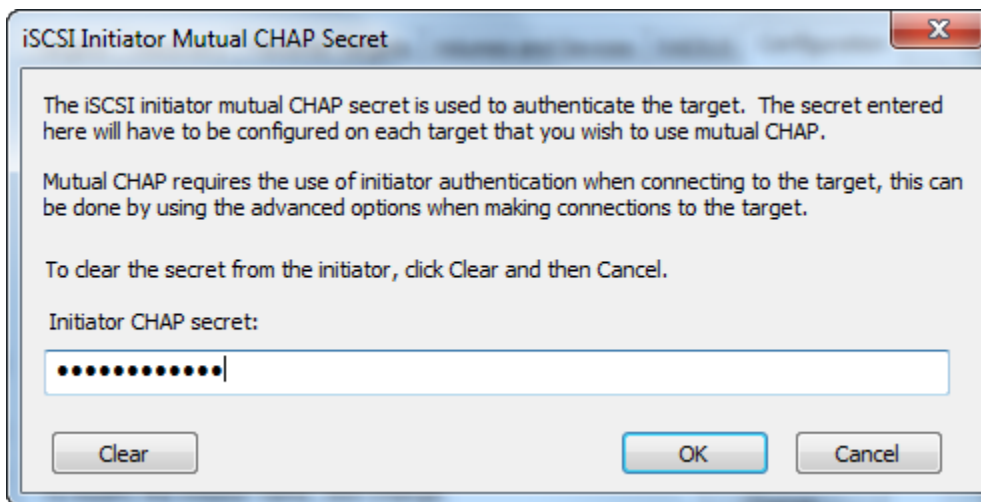
En este procedimiento, se configura CHAP en el SCSI iniciador Microsoft i con las mismas teclas que se usaron CHAP para configurar el volumen de la consola.

1. Si el SCSI iniciador i aún no está iniciado, en el menú Inicio del equipo cliente Windows, elija Ejecutar, enter y, a continuación **iscsicpl.exe**, elija Aceptar para ejecutar el programa.
2. Configure la CHAP configuración mutua para el iniciador (es decir, el cliente de Windows):
 - a. Elija la pestaña Configuración.

Note

El valor de Nombre de iniciador es exclusivo del iniciador en su empresa. El nombre que se muestra antes es el valor que utilizó en el cuadro de diálogo Configurar CHAP autenticación de la consola Storage Gateway.
El nombre que se muestra en el ejemplo de la imagen solo tiene fines ilustrativos.

- b. Elija CHAP.
- c. En el cuadro de diálogo i SCSI Initiator Mutual Chap Secret, introduzca el valor del CHAP secreto mutuo.

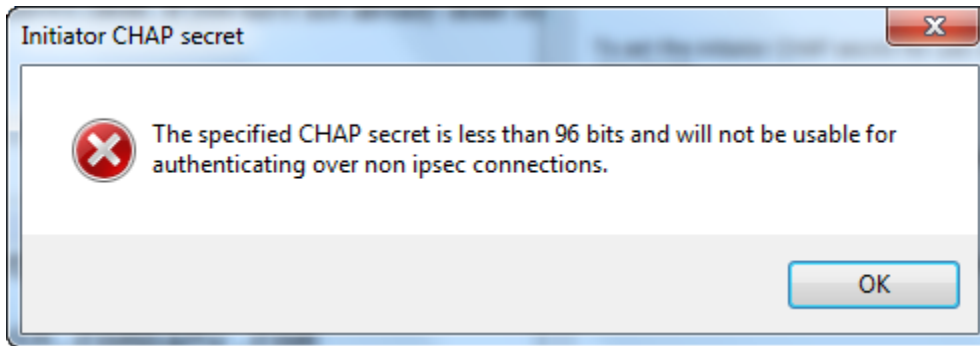


En este cuadro de diálogo, especifique la clave secreta que el iniciador (el cliente de Windows) utiliza para autenticar el destino (el volumen de almacenamiento). Esta clave secreta permite que el destino lea y escriba en el iniciador. Este secreto es el mismo que el introducido en el cuadro Secreto utilizado para autenticar el destino (mutuoCHAP)

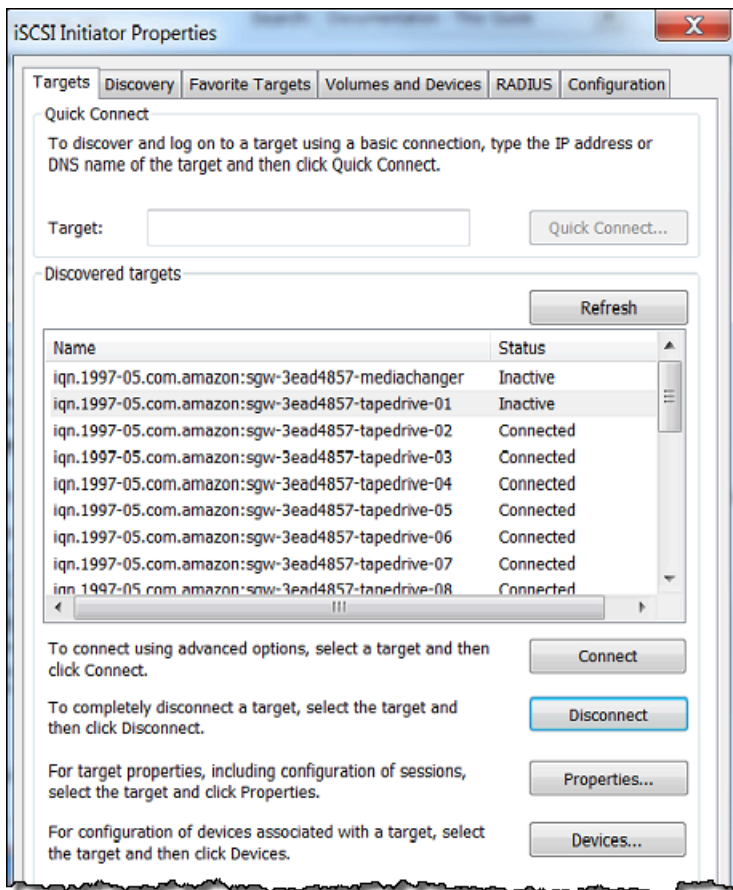
del cuadro de diálogo Configurar CHAP la autenticación. Para obtener más información, consulte [Configuración de CHAP la autenticación para sus objetivos i SCSI](#).

- d. Si la clave que ha introducido tiene menos de 12 caracteres o más de 16 caracteres, aparece un cuadro de diálogo de error relacionado con el CHAPsecreto del iniciador.

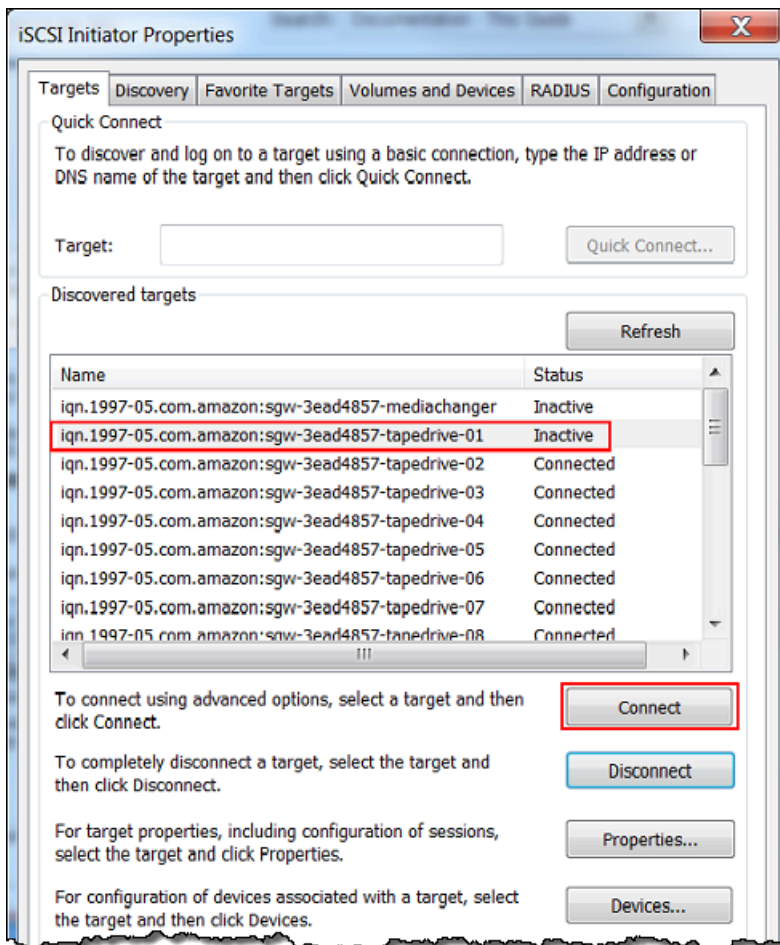
Elija Aceptar y vuelva a introducir la clave.



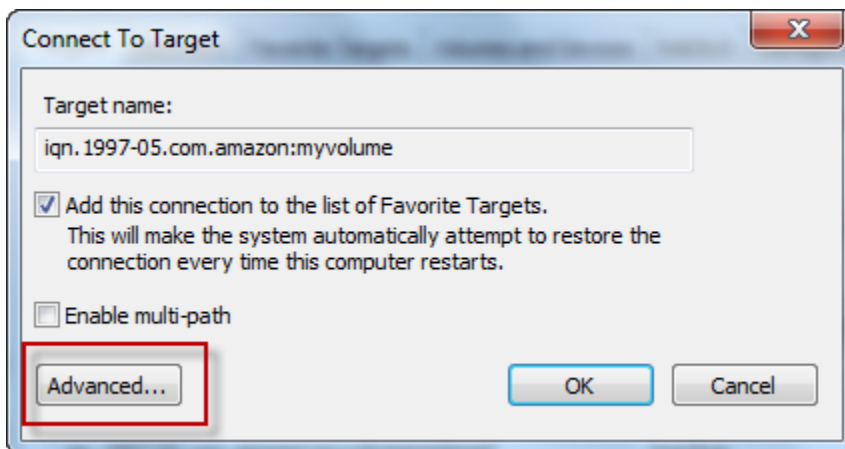
3. Configure el objetivo con el secreto del iniciador para completar la configuración mutua. CHAP
 - a. Elija la pestaña Destinos.



- b. Si el objetivo para el que desea configurar CHAP está conectado actualmente, desconéctelo seleccionándolo y eligiendo Desconectar.
- c. Seleccione el destino para el que desea configurar yCHAP, a continuación, elija Connect.

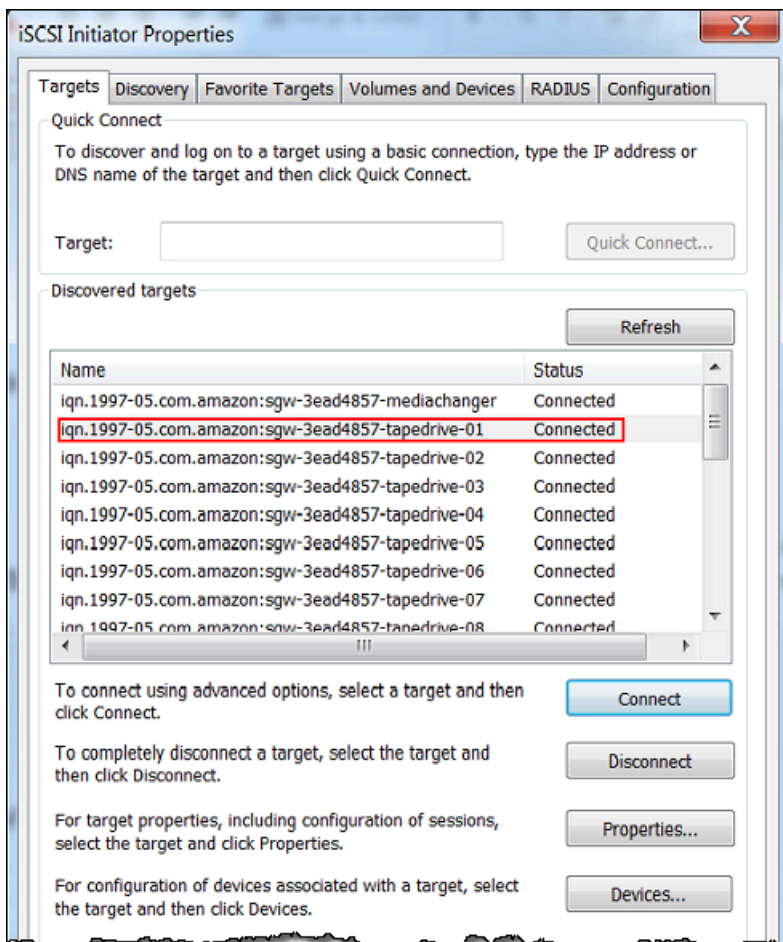


- d. En el cuadro de diálogo Conectarse al destino, elija Opciones avanzadas.



- e. En el cuadro de diálogo Configuración avanzada, configure CHAP.
- i. Seleccione Activar CHAP inicio de sesión.

- ii. Introduzca la clave secreta que se requiere para autenticar el iniciador. Este secreto es el mismo que el escrito en el cuadro Secreto utilizado para autenticar el iniciador del cuadro de diálogo Configurar la CHAP autenticación. Para obtener más información, consulte [Configuración de CHAP la autenticación para sus objetivos i SCSI](#).
 - iii. Seleccione Realizar autenticación mutua.
 - iv. Para aplicar los cambios, elija Aceptar.
- f. En el cuadro de diálogo Conectarse al destino, elija Aceptar.
4. Si ha proporcionado la clave secreta correcta, el destino mostrará el estado Conectado.



Para configurar Mutual CHAP en un cliente Red Hat Linux

En este procedimiento, se configura CHAP en el SCSI iniciador Linux i con las mismas claves que se usaron CHAP para configurar el volumen en la consola Storage Gateway.

1. Asegúrese de que el SCSI daemon `i` esté en ejecución y de que ya se haya conectado a un destino. Si no ha completado estas dos tareas, consulte [Conexión a un cliente Linux](#).
2. Desconecte y elimine cualquier configuración existente del destino para el que va a configurar CHAP.
 - a. Para encontrar el nombre del destino y asegurarse de que se trate de una configuración definida, enumere las configuraciones mediante el siguiente comando.

```
sudo /sbin/iscsiadm --mode node
```

- b. Desconéctese del destino.

El siguiente comando se desconecta del destino nombrado **myvolume** que está definido en el nombre SCSI calificado de Amazon `i` (IQN). Cambie el nombre del objetivo y IQN según sea necesario para su situación.

```
sudo /sbin/iscsiadm --mode node --logout GATEWAY_IP:3260,1  
iqn.1997-05.com.amazon:myvolume
```

- c. Elimine la configuración del destino.

El siguiente comando elimina la configuración del destino **myvolume**.

```
sudo /sbin/iscsiadm --mode node --op delete --targetname  
iqn.1997-05.com.amazon:myvolume
```

3. Edite el archivo SCSI de configuración `i` para activarlo CHAP.
 - a. Obtenga el nombre del iniciador (es decir, el cliente que está utilizando).

El siguiente comando obtiene el nombre de iniciador del archivo `/etc/iscsi/initiatorname.iscsi`.

```
sudo cat /etc/iscsi/initiatorname.iscsi
```

La salida de este comando tiene este aspecto:

```
InitiatorName=iqn.1994-05.com.redhat:8e89b27b5b8
```

- b. Abra el archivo `/etc/iscsi/iscsid.conf`.

- c. Elimine los comentarios de las siguientes líneas del archivo y especifique los valores correctos para *username*, *password*, *username_in*, y *password_in*.

```
node.session.auth.authmethod = CHAP
node.session.auth.username = username
node.session.auth.password = password
node.session.auth.username_in = username_in
node.session.auth.password_in = password_in
```

Para obtener instrucciones sobre qué valores debe especificar, consulte la siguiente tabla.

Opción de configuración	Valor
<i>username</i>	Nombre del iniciador que obtuvo en el paso anterior de este procedimiento. El valor comienza por iqn. Por ejemplo, iqn.1994-05.com.redhat:8e89b27b5b8 es un valor válido <i>username</i> valor.
<i>password</i>	Clave secreta que se utiliza para autenticar el iniciador (el cliente que está utilizando) cuando se comunica con el volumen.
<i>username_in</i>	El IQN del volumen objetivo. El valor comienza por iqn y termina por el nombre del destino. Por ejemplo, iqn.1997-05.com.amazon:myvolume es válido <i>username_in</i> valor.
<i>password_in</i>	Clave secreta que se utiliza para autenticar el destino (el volumen) cuando se comunica con el iniciador.

- d. Guarde los cambios en el archivo de configuración y, a continuación, ciérrelo.
4. Detecte el destino e inicie sesión en él. Para ello, siga los pasos que se indican en [Conexión a un cliente Linux](#).

Uso AWS Direct Connect con Storage Gateway

AWS Direct Connect vincula su red interna a la nube de Amazon Web Services. Al usarlo AWS Direct Connect con Storage Gateway, puede crear una conexión para las necesidades de carga de trabajo de alto rendimiento, proporcionando una conexión de red dedicada entre su puerta de enlace local y AWS.

Storage Gateway utiliza puntos de conexión públicos. Con una AWS Direct Connect conexión establecida, puede crear una interfaz virtual pública para permitir que el tráfico se enrute a los puntos finales de Storage Gateway. La interfaz virtual pública omite a los proveedores de Internet en su ruta de acceso a la red. El punto final público del servicio Storage Gateway puede estar en la misma AWS región que la AWS Direct Connect ubicación o en una AWS región diferente.

En la siguiente ilustración se muestra un ejemplo de cómo AWS Direct Connect funciona con Storage Gateway.

arquitectura de red que muestra Storage Gateway conectado a la nube mediante conexión AWS directa.

En el siguiente procedimiento se supone que ha creado una gateway funcional.

Para usar AWS Direct Connect con Storage Gateway

1. Cree y establezca una AWS Direct Connect conexión entre su centro de datos local y su terminal Storage Gateway. Para obtener más información sobre cómo crear una conexión, consulte [Introducción a AWS Direct Connect](#) en la Guía del usuario de AWS Direct Connect .
2. Conecte el dispositivo Storage Gateway local al AWS Direct Connect router.
3. Cree una interfaz virtual pública y configure su router local según sea necesario. Incluso con Direct Connect, VPC los puntos finales se deben crear con HAProxy. Para obtener más información, consulte [Creación de una interfaz virtual](#) en la Guía del usuario de AWS Direct Connect .

Para obtener más información AWS Direct Connect, consulte [¿Qué es? AWS Direct Connect](#) en la Guía AWS Direct Connect del usuario.

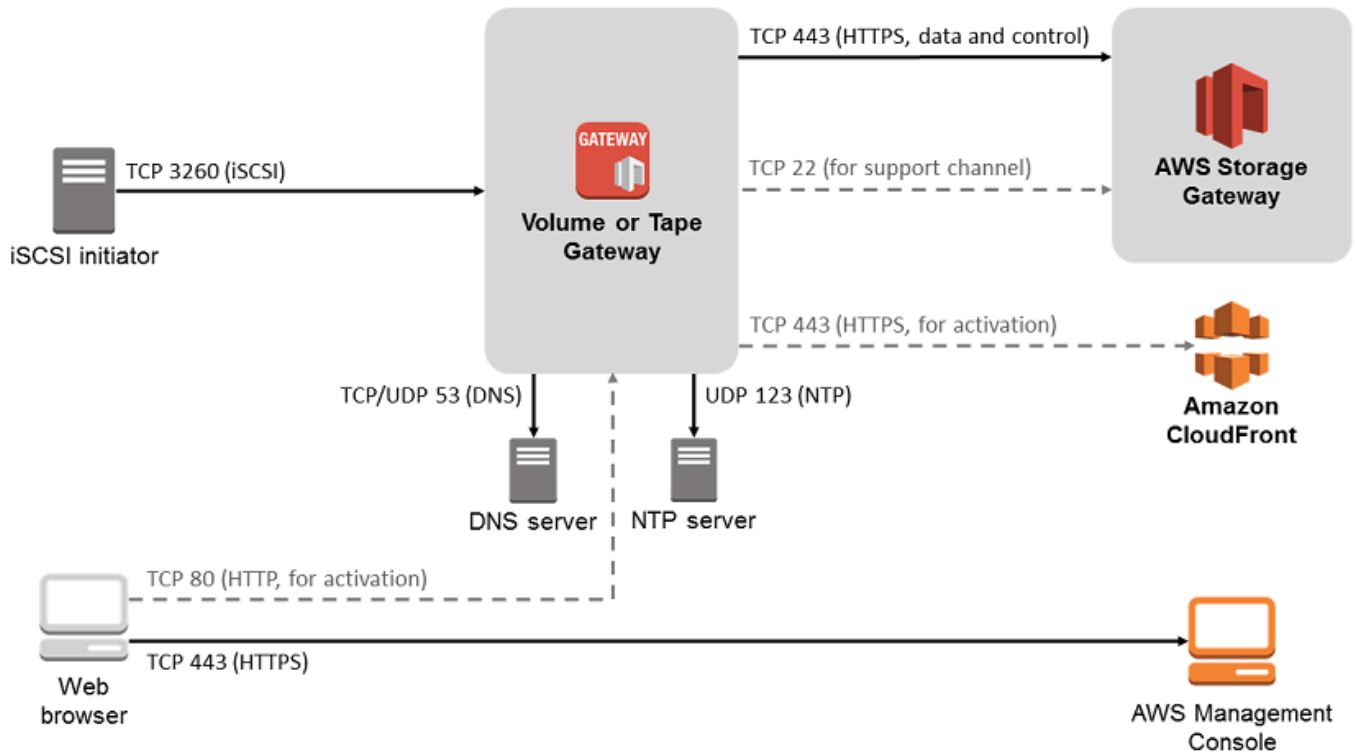
Requisitos de puerto de red para Tape Gateway

Storage Gateway requiere los siguientes puertos para su funcionamiento. Algunos puertos son comunes y obligatorios para todos los tipos de puerta de enlace. Otros puertos son exigidos por

tipos de gateway específicos. En esta sección, encontrará una ilustración y una lista de los puertos necesarios para la puerta de enlace de cinta.

Puerta de enlace de cinta

En la siguiente ilustración se muestran los puertos que se deben abrir para la correcta operación de la puerta de enlace de cinta.



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

De	Para	Protocolo	Puerto	Cómo se utiliza
VM de Storage Gateway	AWS	Protocolo de control de transmisión (TCP)	43 (HTTPS)	Para la comunicación desde una máquina virtual saliente de Storage Gateway

De	Para	Protocolo	Puerto	Cómo se utiliza	
				a un punto final AWS de servicio. Para obtener más información acerca de los puntos de enlace de servicio, consulte Permitir el AWS Storage Gateway acceso a través de firewalls y enrutadores.	

De	Para	Protocolo	Puerto	Cómo se utiliza	
El navegador web	VM de Storage Gateway	TCP	80 () HTTP	<p>Por los sistemas locales para obtener la clave de activación de Storage Gateway. El puerto 80 solo se utiliza durante la activación de un dispositivo de Storage Gateway.</p> <p>La máquina virtual de Storage Gateway no requiere que el puerto 80 sea accesible públicamente. El nivel de acceso exigido al puerto 80 depende de la configuración de la red. Si activa la puerta de enlace desde</p>	

De	Para	Protocolo	Puerto	Cómo se utiliza
				la consola de administración de Storage Gateway, el host desde el que se conecta a la consola debe tener acceso al puerto 80 de la puerta de enlace.
VM de Storage Gateway	Servidor del Servicio de nombres de dominio (DNS)	Protocolo de datagramas de usuario (UDP)/UDP	53 () DNS	Para la comunicación entre una máquina virtual Storage Gateway y el DNS servidor.

De	Para	Protocolo	Puerto	Cómo se utiliza	
VM de Storage Gateway	AWS	TCP	22 (canal de soporte)	Permite acceder AWS Support a su puerta de enlace para ayudarlo a solucionar los problemas de la puerta de enlace. No necesita este puerto abierto para el funcionamiento normal de la gateway, pero se exige para la solución de problemas.	

De	Para	Protocolo	Puerto	Cómo se utiliza
VM de Storage Gateway	Servidor Network Time Protocol (NTP)	UDP	123 (NTP)	<p>Lo utilizan los sistemas locales para sincronizar la hora de la VM con la hora del host. Una máquina virtual Storage Gateway está configurada para usar los siguientes NTP servidores:</p> <ul style="list-style-type: none">• 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 del Protocolo de transferencia de hipertexto (HTTP)	TCP	8080 () HTTP	Se necesita brevemente para la activación.	

Además de los comunes, la puerta de enlace de cinta requiere los siguientes puertos.

De	Para	Protocolo	Puerto	Cómo se utiliza	
i iniciadores SCSI	VM de Storage Gateway	TCP	3260 (i) SCSI	Mediante sistemas locales para conectarse a los SCSI objetivos i expuestos por una puerta de enlace.	

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. En el caso de EC2 las pasarelas de Amazon, también puede obtener la dirección IP de su EC2 instancia de Amazon en Amazon EC2 Management Console. Para encontrar información cómo obtener la dirección IP de la gateway, consulte uno de los siguientes enlaces:

- VMwareanfitrión: [Acceder a la consola local de Gateway con VMware ESXi](#)
- Host HyperV: [Acceso a la consola local de la gateway con Microsoft Hyper-V](#)
- Host de máquina virtual basada en el kernel de Linux (KVM): [Acceso a la consola local de Gateway con Linux KVM](#)
- EC2anfitrión: [Obtener una dirección IP de un EC2 host de Amazon](#)

Cuando encuentre la dirección IP, anótela. A continuación, vuelva a la consola de Storage Gateway y escriba la dirección IP en la consola.

Obtener una dirección IP de un EC2 host de Amazon

Para obtener la dirección IP de la EC2 instancia de Amazon en la que está desplegada tu puerta de enlace, inicia sesión en la consola local de la EC2 instancia. A continuación, obtenga la dirección IP de la parte superior de la página de la consola. Para obtener instrucciones, consulte [Inicio de sesión en la consola local de Amazon EC2 Gateway](#).

También puede obtener la dirección IP de Amazon EC2 Management Console. Le recomendamos que utilice la dirección IP pública para la activación. Para obtener la dirección IP pública, utilice el procedimiento 1. Si, en su lugar, decide utilizar la dirección IP elástica, consulte el procedimiento 2.

Procedimiento 1: conectarse a la gateway mediante la dirección IP pública

1. Abra la EC2 consola de Amazon en <https://console.aws.amazon.com/ec2/>.
2. En el panel de navegación, elija Instances y, a continuación, seleccione la EC2 instancia en la que está desplegada la puerta de enlace.
3. Elija la pestaña Description en la parte inferior y, a continuación, anote la dirección IP pública. Utilice esta dirección IP para conectar con la gateway. Vuelva a la consola de Storage Gateway y escriba la dirección IP.

Si desea utilizar la dirección IP elástica para la activación, utilice el procedimiento siguiente.

Procedimiento 2: conectarse a la gateway mediante la dirección IP elástica

1. Abra la EC2 consola de Amazon en <https://console.aws.amazon.com/ec2/>.
2. En el panel de navegación, elija Instances y, a continuación, seleccione la EC2 instancia en la que está desplegada la puerta de enlace.

3. Elija la pestaña Description en la parte inferior y, a continuación, anote el valor de Elastic IP. Utilice esta dirección IP elástica para conectar con la gateway. Vuelva a la consola de Storage Gateway y escriba la dirección IP elástica.
4. Una vez activada la puerta de enlace, elija la puerta de enlace que acaba de activar y, a continuación, elija la pestaña de VTL dispositivos en el panel inferior.
5. Obtén los nombres de todos tus VTL dispositivos.
6. Ejecute el siguiente comando para configurar cada uno de los destinos.

```
iscsiadm -m node -o new -T [$TARGET_NAME] -p [$Elastic_IP]:3260
```

7. Ejecute el siguiente comando para iniciar sesión en cada uno de los destinos.

```
iscsiadm -m node -p [$ELASTIC_IP]:3260 --login
```

La puerta de enlace ahora está conectada mediante la dirección IP elástica de la EC2 instancia.

Descripción de los recursos y recursos de Storage Gateway IDs

En Storage Gateway, el recurso principal es una puerta de enlace, pero otros tipos de recursos incluyen: volumen, cinta virtual, SCSI destino i y dispositivo 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 (ARNs) exclusivos asociados a ellos, como se muestra en la siguiente tabla.

Tipo de recurso	ARNFormato
Puerta de enlace ARN	arn:aws:storagegateway: <i>region:account-id</i> :gateway/ <i>gateway-id</i>
Cinta ARN	arn:aws:storagegateway: <i>region:account-id</i> :tape/ <i>tapebarcode</i>
Objetivo ARN (en el SCSI objetivo)	arn:aws:storagegateway: <i>region:account-id</i> :gateway/ <i>gateway-id</i> /target/ <i>iSCSITarget</i>

Tipo de recurso	ARNFormato
VTLDispositivo ARN	arn:aws:storagegateway: <i>region</i> : <i>account-id</i> :gateway/ <i>gateway-id</i> /device/ <i>vtldevice</i>

Storage Gateway también admite el uso de EC2 instancias, EBS volúmenes e instantáneas. Estos recursos son recursos de Amazon EC2 que se utilizan en Storage Gateway.

Trabajando con un recurso IDs

Cuando se crea un recurso, Storage Gateway asigna al recurso un ID de recurso único. Este identificador de recurso forma parte del recursoARN. 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.

IDsLos recursos de Storage Gateway están en mayúsculas. Sin embargo, cuando utilizas estos recursos IDs con Amazon EC2API, Amazon EC2 espera que el recurso esté IDs en minúsculas. Debes cambiar tu ID de recurso a minúsculas para usarlo con. EC2 API Por ejemplo, en Storage Gateway el ID para un volumen podría ser `vol-1122AABB`. Si usa este ID con EC2API, debe cambiarlo a `vol-1122aabb` De lo contrario, es EC2 API posible que no se comporte como se esperaba.

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.

Las etiquetas no tiene ningún significado semántico, sino que se interpretan como cadenas de caracteres.

Se aplican las siguientes restricciones a las etiquetas:

- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas.
- El número máximo de etiquetas para cada recurso es de 50.
- Las etiquetas no pueden empezar por aws : . Este prefijo se reserva para uso de AWS .
- Los caracteres válidos para la propiedad clave son UTF -8 letras y números, espacios y caracteres especiales + - = . _:/y @.

Trabajo con etiquetas

Puede trabajar con etiquetas mediante la consola Storage Gateway, Storage Gateway API o la [interfaz de línea de comandos de Storage Gateway \(CLI\)](#). Los siguientes procedimientos muestran cómo agregar, editar y eliminar una etiqueta de la consola.


Para agregar una etiqueta

1. Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa>.
2. En el panel de navegación , elija el recurso que desea etiquetar.

Por ejemplo, para etiquetar una gateway, elija Gateways y, a continuación, elija la gateway que desee etiquetar en la lista de gateways.

3. Elija Tags (Etiquetas) y, a continuación, elija Add/edit tags (Añadir o editar etiquetas).
4. En el cuadro de diálogo Add/edit tags (Añadir o editar etiquetas), elija Create tag (Crear etiqueta).

5. Escriba una clave para Key (Clave) y un valor para Value (Valor). Por ejemplo, puede escribir **Department** para la clave y **Accounting** para el valor.

 Note

Puede dejar en blanco el cuadro Value (Valor).

6. Elija Create Tag (Crear etiqueta) para agregar más etiquetas. Puede agregar varias etiquetas a un recurso.
7. Cuando haya acabado de agregar etiquetas, elija Save (Guardar).

Para editar una etiqueta

1. Abra la consola Storage Gateway en <https://console.aws.amazon.com/storagegateway/casa>.
2. Elija el recurso cuya etiqueta desea editar.
3. Elija Tags (Etiquetas) para abrir el cuadro de diálogo Add/edit tags (Añadir o editar etiquetas).
4. 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 en <https://console.aws.amazon.com/storagegateway/casa>.
2. Elija el recurso cuya etiqueta desea eliminar.
3. Elija Tags (Etiquetas) y, a continuación, elija Add/edit tags (Añadir o editar etiquetas) para abrir el cuadro de diálogo Add/edit tags (Añadir o editar etiquetas).
4. Elija el icono X situado junto a la etiqueta que desea eliminar y, a continuación, elija Save (Guardar).

Uso de componentes de código abierto para AWS Storage Gateway

En esta sección, se describen las herramientas y licencias de terceros de las que dependemos para ofrecer la funcionalidad de Storage Gateway.

El código fuente de algunos componentes de software de código abierto que se incluyen con el software AWS Storage Gateway está disponible para su descarga en las siguientes ubicaciones:

- [Para las puertas de enlace implementadas en VMwareESXi, descargue sources.tar](#)
- Para gateways implementadas en Microsoft Hyper-V, descargue [sources_hyperv.tar](#)
- [Para las puertas de enlace implementadas en una máquina virtual basada en el kernel de Linux \(KVM\), descargue sources_ .tar KVM](#)

[Este producto incluye software desarrollado por Open SSL Project para su uso en el Open Toolkit \(http://www.openssl.org/\). SSL](#) Para obtener las licencias pertinentes para todas las herramientas de terceros dependientes, consulte [Licencias de terceros](#).

AWS Storage Gateway cuotas

En este tema, encontrará información sobre los límites que se aplican en Storage Gateway a los volúmenes, las cuotas de cintas, la configuración y el rendimiento.

Temas

- [Cuotas para las cintas](#)
- [Tamaños de disco local recomendados para la puerta de enlace](#)

Cuotas para las cintas

En la siguiente tabla se muestran las cuotas para las cintas.

Descripción	Gateway de cinta
Tamaño mínimo de una cinta virtual	100 GiB
Tamaño máximo de una cinta virtual	15 TiB
Número máximo de cintas virtuales asignadas a una puerta de enlace	1500
Tamaño total de todas las cintas asignadas a una puerta de enlace	1 PiB

Descripción	Gateway de cinta
Número máximo de cintas virtuales en un archivo	Sin límite
Tamaño total de todas las cintas en archivo	Sin límite

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)	Búfer de carga (mínimo)	Búfer de carga (máximo)	Otros discos locales necesarios
Puerta de enlace de cinta	150 GiB	64 TiB	150 GiB	2 TiB	—

Note

Puede configurar una o más unidades locales para la memoria caché y el búfer de carga hasta la capacidad máxima.

Al añadir caché o búfer de carga a una puerta de enlace existente, es importante crear nuevos discos en el host (hipervisor o EC2 instancia de Amazon). No cambie el tamaño de los discos si se han asignado previamente como caché o como búfer de carga.

API Referencia para Storage Gateway

Además de utilizar la consola, puede utilizarla para configurar y AWS Storage Gateway API administrar las puertas de enlace mediante programación. En esta sección se describen las AWS Storage Gateway operaciones, la firma de solicitudes para la autenticación y la gestión de errores. Para obtener información acerca de las regiones y los puntos de enlace disponibles para Storage Gateway, consulte [Puntos de enlace y cuotas de AWS Storage Gateway](#) en la Referencia general de AWS.

Note

También puede utilizarla AWS SDKs cuando desarrolle aplicaciones con AWS Storage Gateway. El AWS SDKs para Java, .NET, y PHP envuelva lo subyacente AWS Storage Gateway API, simplificando sus tareas de programación. Para obtener información sobre la descarga de las SDK bibliotecas, consulte [Ejemplos de bibliotecas de códigos](#).

Temas

- [Encabezados de solicitud obligatorios para Storage Gateway](#)
- [Firmar solicitudes](#)
- [Respuestas de error](#)
- [Acciones](#)

Encabezados de solicitud obligatorios para Storage Gateway

En esta sección se describen los encabezados necesarios que debe enviar con cada POST solicitud a Storage Gateway. Incluye HTTP encabezados para identificar la información clave sobre la solicitud, incluida 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 deben incluirse en POST las solicitudes a Storage Gateway. Los encabezados que se muestran a continuación y que comienzan por «x-amz» son encabezados específicos. AWS Todos los demás encabezados de la lista son encabezados comunes que se utilizan en las transacciones. HTTP

Encabezado	Descripción
Authorization	<p>El encabezado de autorización contiene varios elementos de información sobre la solicitud que permite a Storage Gateway determinar 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):</p> <pre> Authorization: AWS4-HMAC_SHA456 Credentials= <i>YourAccessKey</i> /<i>yyyymmdd</i>/<i>region</i>/storagegateway/aw s4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-targ et, Signature= <i>CalculatedSignature</i> </pre> <p>En la sintaxis anterior, se especifican el año <i>YourAccessKey</i>, el mes y el día (<i>aaaaammdd</i>), la región y el. <i>CalculatedSignature</i> El formato del encabezado de autorización viene determinado por los requisitos del proceso de firma de la versión 4. AWS Los detalles de la firma se tratan en el tema Firmar solicitudes.</p>
Content-Type	Utilice <code>application/x-amz-json-1.1</code> como tipo de contenido para todas las solicitudes a Storage Gateway.

Encabezado	Descripción
	<pre>Content-Type: application/x-amz-json-1.1</pre>
Host	<p>Utilice el encabezado de host para especificar el punto de conexión de Storage Gateway donde desea enviar la solicitud. Por ejemplo, <code>storagegateway.us-east-2.amazonaws.com</code> es el punto de conexión de la región Este de EE. UU. (Ohio). Para obtener más información acerca de los puntos de enlace disponibles para Storage Gateway, consulte Puntos de enlace y cuotas de AWS Storage Gateway en la Referencia general de AWS.</p> <pre>Host: storagegateway. <i>region</i>.amazonaws.com</pre>
x-amz-date	<p>Debe proporcionar la marca de tiempo en el HTTP Date encabezado o en el AWS x-amz-date encabezado. (Algunas bibliotecas HTTP cliente no permiten configurar el Date encabezado). Cuando hay un encabezado x-amz-date presente, Storage Gateway hace caso omiso de cualquier encabezado Date durante la autenticación de la solicitud. El x-amz-date formato debe ser ISO8601 Basic en formato YYYYMMDD «THHMMSS» y «Z». Si se utilizan Date tanto el x-amz-date encabezado como el encabezado, el formato del encabezado de fecha no tiene que ser ISO8601.</p> <pre>x-amz-date: <i>YYYYMMDD'T'HHMMSS'Z'</i></pre>
x-amz-target	<p>Este encabezado especifica la versión API y la operación que está solicitando. Los valores del encabezado objetivo se forman concatenando la API versión con el API nombre y tienen el siguiente formato.</p> <pre>x-amz-target: StorageGateway_ <i>APIversion</i> .<i>operationName</i></pre> <p>El operationNamevalor (por ejemplo, "ActivateGateway«) se encuentra en la API lista, APIReferencia para Storage Gateway</p>

Firmar solicitudes

Storage Gateway requiere que se firmen todas las solicitudes enviadas para autenticarlas. Para firmar una solicitud, se calcula una firma digital mediante una función hash criptográfica. Un hash criptográfico es una función que devuelve un valor hash único basado en la entrada. La entrada a la función hash incluye el texto de la solicitud y la clave de acceso secreta. La función hash devuelve un valor hash que se incluye en la solicitud como la firma. La firma forma parte del encabezado de la `Authorization` de la solicitud.

Tras recibir la solicitud, Storage Gateway recalcula la firma utilizando la misma función hash y los datos especificados para firmar la solicitud. Si la firma resultante coincide con la firma de la solicitud, Storage Gateway procesa la solicitud. De lo contrario, la solicitud se rechaza.

Storage Gateway admite la autenticación mediante [AWS Signature Version 4](#). El proceso para calcular una firma se puede dividir en tres tareas:

- [Tarea 1: Creación de una solicitud canónica](#)

Reorganiza tu HTTP solicitud en un formato canónico. Es preciso utilizar un formato canónico, ya que Storage Gateway utiliza el mismo formato canónico cuando recalcula una firma para compararla con la que se ha enviado.

- [Tarea 2: Creación de una cadena para firmar](#)

Crear una cadena que se utilizará como uno de los valores de entrada de la función hash criptográfica. La cadena, denominada cadena para firmar, es una concatenación del nombre del algoritmo hash, la fecha de la solicitud, una cadena de ámbito de credenciales y la solicitud en formato canónico de la tarea anterior. La cadena del ámbito de credenciales es una concatenación de fecha, región e información del servicio.

- [Tarea 3: Crear una firma](#)

Cree una firma para su solicitud mediante una función hash criptográfica que acepte dos cadenas de entrada: la cadena para firmar y una clave derivada. La clave derivada se calcula empezando por la clave de acceso secreta y utilizando la cadena del ámbito de las credenciales para crear una serie de códigos de autenticación de mensajes basados en Hash (`HMACs`).

Ejemplo de cálculo de firma

En el siguiente ejemplo, se explican 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 horaria de la solicitud es «Mon, 10 de septiembre de 2012 00:00:00». GMT
- El punto de conexión es la región Este de EE. UU. (Ohio).

La sintaxis general de la solicitud (incluido el JSON cuerpo) 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 otro Storage GatewayAPIs).

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
92c0effa6f9224ac752ca179a04cecbde3038b0959666a8160ab452c9e51b3e
```

La primera línea de la cadena para firmar es el algoritmo, la segunda es la marca temporal, la tercera es el ámbito de credenciales y la última es el hash de la solicitud canónica de la tarea 1.

En [Tarea 3: Crear una firma](#), la clave derivada se puede representar como sigue:

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey, "20120910"), "us-
east-2"), "storagegateway"), "aws4_request")
```

Si se utiliza la clave de acceso secreta, wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY, la firma calculada es:

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

El último paso consiste en construir el encabezado `Authorization`. Para la clave de acceso de demostración `AKIAIOSFODNN7EXAMPLE`, el encabezado (con saltos de línea agregados para facilitar la lectura) 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 proporciona información de referencia sobre AWS Storage Gateway los errores. Estos errores se representan mediante una excepción de error y un código de error de operación. Por ejemplo, cualquier API respuesta devuelve la excepción `InvalidSignatureException` de error si hay algún problema con la firma de la solicitud. Sin embargo, el código de error de la operación solo `ActivationKeyInvalid` se devuelve para [ActivateGateway](#) API.

Según el tipo de error, Storage Gateway puede devolver solamente una excepción o puede devolver una excepción y un código de error de operación. Ejemplos de respuestas de error se muestran en [Respuestas de error](#).

Excepciones

En la siguiente tabla se enumeran las AWS Storage Gateway API excepciones. Cuando una AWS Storage Gateway operación devuelve una respuesta de error, el cuerpo de la respuesta contiene una de estas excepciones. Las excepciones `InternalServerError` e `InvalidGatewayRequestException` devuelven uno de los códigos de mensaje [Códigos de error de operación](#) de los códigos de error de operación que proporcionan el código de error de operación específico.

Excepción	Mensaje	HTTPCódigo de estado
<code>IncompleteSignatureException</code>	La firma especificada está incompleta.	400: solicitud maligna
<code>InternalFailure</code>	El procesamiento de la solicitud ha fallado debido a un error o una excepción desconocidos.	500 Error de servidor interno
<code>InternalServerError</code>	Uno de los mensajes de código de error de operación Códigos de error de operación .	500 Error de servidor interno
<code>InvalidAction</code>	La acción u operación solicitada no es válida.	400: solicitud maligna
<code>InvalidClientTokenId</code>	El certificado X.509 o el identificador de clave de AWS acceso proporcio	403: prohibido

Excepción	Mensaje	HTTPCódigo de estado
	nados no existen en nuestros registros.	
<code>InvalidGatewayRequestException</code>	Uno de los mensajes de código de error de operación de Códigos de error de operación .	400: solicitud maligna
<code>InvalidSignatureException</code>	La firma de solicitud que calculamos no coincide con la firma que proporcionó. Compruebe su clave de AWS acceso y su método de firma.	400: solicitud maligna
<code>MissingAction</code>	Falta un parámetro de operación o acción en la solicitud.	400: solicitud maligna
<code>MissingAuthenticationToken</code>	La solicitud debe contener un identificador de clave de AWS acceso válido (registrado) o un certificado X.509.	403: prohibido
<code>RequestExpired</code>	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
<code>SerializationException</code>	Se ha producido un error durante la serialización. Comprueba que la JSON carga útil esté bien formada.	400: solicitud maligna
<code>ServiceUnavailable</code>	La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.	503 Service Unavailable
<code>SubscriptionRequiredException</code>	El identificador de clave de AWS acceso necesita una suscripción al servicio.	400: solicitud maligna

Excepción	Mensaje	HTTPCódigo de estado
ThrottlingException	Tasa superada.	400: solicitud maligna
TooManyRequests	Demasiadas solicitudes.	429 Demasiadas solicitudes
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

La siguiente tabla muestra el mapeo entre los códigos de error de AWS Storage Gateway operación y los APIs 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

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
ActivationKeyInvalid	La clave de activación especificada no es válida.	ActivateGateway
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

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
DiskSizeNotGigAligned	El disco especificado no está alineado en gigabytes.	CreateStorediSCSIVolume
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

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
GatewayInternalError	Se produjo un error interno de la gateway.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
GatewayNotConnected	La gateway especificada no está conectada.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
GatewayNotFound	La gateway especificada no se ha encontrado.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
		ListLocalDisks
		ListVolumes
		ListVolumeRecoveryPoints
		ShutdownGateway
		StartGateway
		UpdateBandwidthRateLimit
		UpdateChapCredentials
		UpdateMaintenanceStartTime
		UpdateGatewaySoftwareNow
		UpdateSnapshotSchedule

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
GatewayProxyNetworkConnectionBusy	La conexión de red proxy de la gateway especificada está ocupada.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
InternalError	Se ha producido un error interno.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
		DescribeWorkingStorage
		ListLocalDisks
		ListGateways
		ListVolumes
		ListVolumeRecoveryPoints
		ShutdownGateway
		StartGateway
		UpdateBandwidthRateLimit
		UpdateChapCredentials
		UpdateMaintenanceStartTime
		UpdateGatewayInformation
		UpdateGatewaySoftwareNow
		UpdateSnapshotSchedule

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
InvalidParameters	La solicitud especificada contiene parámetros incorrectos.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
LocalStorageLimitExceeded	El límite de almacenamiento local se ha superado.	AddCache AddUploadBuffer AddWorkingStorage
LunInvalid	Lo especificado LUN es incorrecto.	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
NetworkConfigurationChanged	La configuración de red de la gateway ha cambiado.	CreateCachediSCSIVolume CreateStorediSCSIVolume

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
NotSupported	La operación especificada no es compatible.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
OutdatedGateway	La gateway especificada está obsoleta.	ActivateGateway
SnapshotInProgressException	La snapshot especificada está en curso.	DeleteVolume
SnapshotIdInvalid	La instantánea especificada 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
<code>UnsupportedOperationForGatewayType</code>	La operación especificada no es válida para el tipo de gateway.	AddCache AddWorkingStorage CreateCachediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteSnapshotSchedule DescribeCache DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
<code>VolumeAlreadyExists</code>	El volumen especificado ya existe.	CreateCachediSCSIVolume CreateStorediSCSIVolume
<code>VolumeIdInvalid</code>	El volumen especificado no es válido.	DeleteVolume
<code>VolumeInUse</code>	El volumen especificado ya se está usando.	DeleteVolume

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
VolumeNotFound	El volumen especificado no se ha encontrado.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint DeleteVolume DescribeCachediSCSIVolumes DescribeSnapshotSchedule DescribeStorediSCSIVolumes UpdateSnapshotSchedule
VolumeNotReady	El volumen especificado no está listo.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

Respuestas de error

Cuando se produce un error, la información de encabezado de la respuesta contiene:

- Tipo de contenido: application/-1.1 x-amz-json
- Un código apropiado o de estado 4xx 5xx HTTP

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 siguiente tabla se explican los campos de respuesta a JSON errores que se muestran en la sintaxis anterior.

`__type`

Una de las excepciones de [Excepciones](#).

Tipo: cadena

`error`

Contiene detalles API de error específicos. En los errores generales (es decir, no específicos de ningunoAPI), no se muestra esta información de error.

Tipo: recopilación

`errorCode`

Uno de los códigos de error de operación .

Tipo: cadena

`errorDetails`

Este campo no se utiliza en la versión actual deAPI.

Tipo: cadena

`message`

Uno de los mensajes de código de error de operación.

Tipo: cadena

Ejemplos de respuestas de error

Se devuelve el siguiente JSON cuerpo si utiliza DescribeStoredi SCSIVolumes API y especifica una entrada de ARN solicitud de puerta de enlace que no existe.

```
{
```

```
"__type": "InvalidGatewayRequestException",
"message": "The specified volume was not found.",
"error": {
  "errorCode": "VolumeNotFound"
}
}
```

Si Storage Gateway calcula una firma que no coincide con la firma enviada con una solicitud, se devuelve el siguiente JSON cuerpo.

```
{
  "__type": "InvalidSignatureException",
  "message": "The request signature we calculated does not match the signature you
provided."
}
```

Operaciones en Storage Gateway

Para obtener una lista de las operaciones de Storage Gateway, consulte [Acciones](#) en la AWS Storage Gateway API referencia.

Historial de documentos de la Guía del usuario de puerta de enlace de cinta

- API versión: 30 de junio de 2013
- Última actualización de la documentación: 24 de noviembre de 2020

En la siguiente tabla se describen los cambios importantes en cada versión de la Guía del usuario de AWS Storage Gateway posteriores a abril de 2018. Para recibir notificaciones sobre las actualizaciones de esta documentación, puede suscribirse a un feed. RSS

Cambio	Descripción	Fecha
Se ha añadido la opción de activar o desactivar las actualizaciones de mantenimiento	Storage Gateway recibe actualizaciones de mantenimiento periódicas que pueden incluir actualizaciones del sistema operativo y del software, correcciones para mejorar la estabilidad, el rendimiento y la seguridad, y acceso a nuevas funciones . Ahora puede configurar un ajuste para activar o desactivar estas actualizaciones para cada puerta de enlace individual de su implementación. Para obtener más información, consulte Administrar las actualizaciones de la puerta de enlace mediante la AWS Storage Gateway consola .	6 de junio de 2024

[Soporte obsoleto para Tape Gateway en Snowball Edge](#)

Ya no es posible alojar Tape Gateway en los dispositivos Snowball Edge.

14 de marzo de 2024

[Instrucciones actualizadas para probar la configuración de la puerta de enlace mediante aplicaciones de terceros](#)

Las instrucciones para probar la configuración de la puerta de enlace mediante aplicaciones de terceros ahora describen el comportamiento esperado si la puerta de enlace se reinicia durante un trabajo de copia de seguridad en curso. Para obtener más información, consulte [Uso de su software de copia de seguridad para comprobar la configuración de la gateway.](#)

24 de octubre de 2023

[Alarmas recomendadas CloudWatch actualizadas](#)

La CloudWatch HealthNotifications alarma ahora se aplica y se recomienda para todos los tipos de puertas de enlace y plataformas host. Los ajustes de configuración recomendados también se han actualizado para HealthNotifications y AvailabilityNotifications . Para obtener más información, consulte [Descripción de CloudWatch las alarmas](#) .

2 de octubre de 2023

[Se aumentó el tamaño máximo de cinta a 15 TiB para las puertas de enlace de cinta](#)

Además, para las puertas de enlace de cinta, el tamaño máximo de cinta virtual ha aumentado de 5 TiB a 15 TiB. Para obtener más información, consulte [Cuotas para las cintas](#) en la Guía del usuario de Storage Gateway.

4 de octubre de 2022

[Guías del usuario separadas para puerta de enlace de cinta y de volumen](#)

La Guía del usuario de Storage Gateway, que anteriormente incluía información sobre los tipos de puerta de enlace de cinta y de volumen, se ha dividido en la Guía del usuario de puerta de enlace de cinta y la Guía del usuario de puerta de enlace de volumen, cada una de las cuales contiene información sobre un solo tipo de puerta de enlace. Para obtener más información, consulte la [Guía del usuario de puerta de enlace de cinta](#) y la [Guía del usuario de puerta de enlace de volumen](#).

23 de marzo de 2022

[Actualización de procedimientos de creación de puerta de enlace](#)

Se han actualizado los procedimientos para crear todos los tipos de puertas de enlace mediante la consola de Storage Gateway. Para obtener más información, consulte [Creación de la puerta de enlace](#).

18 de enero de 2022

[Nueva interfaz de cintas](#)

Se ha actualizado la página de información general sobre las cintas de la AWS Storage Gateway consola con nuevas funciones de búsqueda y filtrado. Todos los procedimientos relevantes de esta guía se han actualizado para describir la nueva funcionalidad. Para obtener más información, consulte [Administración de la puerta de enlace de cinta](#).

23 de septiembre de 2021

[Soporte para Quest NetVault Backup 13 para Tape Gateway](#)

Las puertas de enlace de cinta ahora son compatibles con Quest NetVault Backup 13 que se ejecuta en Microsoft Windows Server 2012 R2 o Microsoft Windows Server 2016. Para obtener más información, consulte [Probar su configuración mediante Quest NetVault Backup](#).

22 de agosto de 2021

[Los temas de una puerta de enlace de archivo de S3 se han eliminado de las guías de puerta de enlace de cinta y de volumen](#)

Para facilitar el uso de las guías de usuario de puerta de enlace de cinta y puerta de enlace de volumen a los clientes que configuran sus respectivos tipos de puerta de enlace, se han eliminado algunos temas innecesarios.

21 de julio de 2021

[Support para IBM Spectrum Protect 8.1.10 en Windows y Linux para Tape Gateway](#)

Las puertas de enlace de cinta ahora son compatibles con la versión 8.1.10 de IBM Spectrum Protect que se ejecuta en Microsoft Windows Server y Linux. Para obtener más información, consulte [Probar la configuración mediante IBM Spectrum Protect](#).

24 de noviembre de 2020

[Cumplimiento de la RAMP normativa](#)

Storage Gateway ahora cumple con la RAMP normativa de la Reserva Federal. Para obtener más información, consulte [Validación de conformidad para Storage Gateway](#).

24 de noviembre de 2020

[Limitación del ancho de banda basada en la programación](#)

Storage Gateway ahora admite la limitación del ancho de banda basada en la programación para las puertas de enlace de cinta y de volumen. Para obtener más información, consulte [Programación de la limitación del ancho de banda mediante la consola de Storage Gateway](#).

9 de noviembre de 2020

[El volumen en caché y el almacenamiento en caché local de puertas de enlace de cinta se han cuadruplicado](#)

Storage Gateway ahora admite una caché local de hasta 64 TB para las puertas de enlace de cinta y de volumen almacenadas en caché, lo que mejora el rendimiento de las aplicaciones en las instalaciones al proporcionar acceso de baja latencia a conjuntos de datos de trabajo más grandes. Para obtener más información, consulte [Tamaños de disco local recomendados para la puerta de enlace.](#)

9 de noviembre de 2020

[Migración de puerta de enlace](#)

Storage Gateway ahora admite la migración de puertas de enlace de volumen almacenadas en caché a nuevas máquinas virtuales. Para obtener más información, consulte [Traslado de volúmenes en caché a una nueva máquina virtual de puerta de enlace de volumen en caché.](#)

10 de septiembre de 2020

[Support para el bloqueo de retención de la cinta y write-once-read-many \(WORM\) la protección de la cinta](#)

19 de agosto de 2020

Storage Gateway admite el bloqueo de retención de cintas en las cintas virtuales y la escritura una vez, lectura múltiple (WORM). El bloqueo de retención de cinta le permite especificar el modo y el período de retención de las cintas virtuales archivadas, lo que evita que se eliminen durante un período fijo de tiempo de hasta 100 años. Incluye controles de permisos sobre quién puede eliminar las cintas o modificar la configuración de retención. Para obtener más información, consulte [Uso de un bloqueo de retención de cintas](#). WORM-las cintas virtuales activadas ayudan a garantizar que los datos de las cintas activas de su biblioteca de cintas virtuales no se puedan sobrescribir ni borrar. Para obtener más información, consulte Protección en cintas para [escribir una vez, leer muchas \(WORM\)](#).

[Pedir el dispositivo de hardware a través de la consola](#)

Ahora puede solicitar el dispositivo de hardware a través de la AWS Storage Gateway consola. Para obtener más información, consulte [Uso del dispositivo de hardware de Storage Gateway](#).

12 de agosto de 2020

[Support for Federal Information Processing Standard \(FIPS\) endpoints in new Regions AWS](#)

Ahora puede activar una puerta de enlace con FIPS puntos de conexión 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, consulte [Puntos de conexión y cuotas de AWS Storage Gateway](#) en la Referencia general de AWS.

31 de julio de 2020

[Migración de puerta de enlace](#)

Storage Gateway ahora admite la migración de puertas de enlace de cinta y de volumen almacenadas a nuevas máquinas virtuales. Para obtener más información, consulte [Transferir los datos a una nueva puerta de enlace](#).

31 de julio de 2020

[Vea CloudWatch las alarmas de Amazon en la consola Storage Gateway](#)

Ahora puede ver CloudWatch las alarmas en la consola Storage Gateway. Para obtener más información, consulte [Descripción de CloudWatch las alarmas](#).

29 mayo de 2020

[Support for Federal Information Processing Standard \(FIPS\) endpoints](#)

Ahora puede activar una puerta de enlace con FIPS puntos finales en las AWS GovCloud (US) regiones. Para elegir un FIPS punto final para un Volume Gateway, consulte [Elegir un punto final de servicio](#). Para elegir un FIPS punto final para una puerta de enlace de cinta, consulte [Conectar una puerta de enlace de cinta a AWS](#).

22 de mayo de 2020

[Nuevas AWS regiones](#)

Storage Gateway ya está disponible en las regiones de África (Ciudad del Cabo) y Europa (Milán). Para obtener más información, consulte [Puntos de conexión y cuotas de AWS Storage Gateway](#) en la Referencia general de AWS.

7 de mayo de 2020

[Compatibilidad con la clase de almacenamiento S3 Intelligent-Tiering](#)

Storage Gateway ahora admite la clase de almacenamiento S3 Intelligent-Tiering. La clase de almacenamiento S3 Intelligent-Tiering optimiza los costos de almacenamiento mediante el desplazamiento automático de los datos a la capa de acceso de almacenamiento más rentable, sin que afecte al rendimiento ni se produzca sobrecarga operativa. Para obtener más información, consulte [Clase de almacenamiento para optimizar automáticamente los objetos a los que se obtiene acceso de forma frecuente e infrecuente](#) en la Guía del usuario de Amazon Simple Storage Service.

30 de abril de 2020

[Duplicación del rendimiento de escritura y lectura de la puerta de enlace de cinta](#)

Storage Gateway duplica el rendimiento de lectura y escritura en cintas virtuales en la puerta de enlace de cinta, lo que le permite realizar copias de seguridad y recuperaciones de forma más rápida que antes. Para obtener más información, consulte [Directrices de rendimiento para las puertas de enlaces de cinta](#) en la Guía del usuario de Storage Gateway.

23 de abril de 2020

[Compatibilidad con la creación automática de cintas](#)

Storage Gateway ahora proporciona la capacidad de crear automáticamente nuevas cintas virtuales. La puerta de enlace de cinta crea automáticamente nuevas cintas virtuales para mantener el número mínimo de cintas disponibles que configura y, después, permite que la aplicación de copia de seguridad importe esas nuevas cintas, por lo que los trabajos de copia de seguridad podrán ejecutarse sin interrupción. Para obtener más información, consulte [Creación automática de cintas](#) en la Guía del usuario de Storage Gateway.

23 de abril de 2020

[Nueva AWS región](#)

Storage Gateway ya está disponible en la región AWS GovCloud (EE. UU. Este). Para obtener más información, consulte [Puntos de enlace y cuotas de AWS Storage Gateway](#) en la Referencia general de AWS.

12 de marzo de 2020

[Support para el hipervisor Virtual Machine \(\) KVM basado en Linux Kernel](#)

Storage Gateway ahora ofrece la posibilidad de implementar una puerta de enlace local en la plataforma de KVM virtualización. Las pasarelas implementadas en KVM ellas tienen todas las mismas funciones y características que las pasarelas locales existentes. Para obtener más información, consulte [Hipervisores compatibles y requisitos de host](#) en la Guía del usuario de Storage Gateway.

4 de febrero de 2020

[Support for VMware vSphere High Availability](#)

Storage Gateway ahora admite la alta disponibilidad para ayudar VMware a proteger las cargas de trabajo de almacenamiento contra fallas de hardware, hipervisor o red. Para obtener más información, consulte [Uso de la VMware vSphere alta disponibilidad con Storage Gateway](#) en la Guía del usuario de Storage Gateway. Esta versión también incluye mejoras de rendimiento. Para obtener más información, consulte [Rendimiento](#) en la Guía del usuario de Storage Gateway.

20 de noviembre de 2019

[Nueva AWS región para Tape Gateway](#)

La puerta de enlace de cinta ahora está disponible en la región América del Sur (São Paulo). Para obtener más información, consulte [Puntos de enlace y cuotas de AWS Storage Gateway](#) en la Referencia general de AWS.

24 de septiembre de 2019

[Support para la versión 7.1.9 de IBM Spectrum Protect en Linux y para Tape Gateways, un tamaño máximo de cinta aumentado a 5 TiB](#)

Los Tape Gateways ahora son compatibles con la versión 7.1.9 de IBM Spectrum Protect (Tivoli Storage Manager) que se ejecuta en Linux, además de en Microsoft Windows. Para obtener más información, consulte [Probar la configuración mediante IBM Spectrum Protect](#) en la Guía del usuario de Storage Gateway. . Además, para las puertas de enlace de cinta, el tamaño máximo de cinta virtual ha aumentado de 2,5 TiB a 5 TiB. Para obtener más información, consulte [Cuotas para las cintas](#) en la Guía del usuario de Storage Gateway.

10 de septiembre de 2019

[Support para Amazon CloudWatch Logs](#)

Ahora puede configurar File Gateways con Amazon CloudWatch Log Groups para recibir notificaciones sobre los errores y el estado de su puerta de enlace y sus recursos. Para obtener más información, consulte [Cómo recibir notificaciones sobre el estado y los errores de Gateway con Amazon CloudWatch Log Groups](#) en la Guía del usuario de Storage Gateway.

4 de septiembre de 2019

[Nueva AWS región](#)

Storage Gateway ya está disponible en la región Asia Pacífico (Hong Kong). Para obtener más información, consulte [Puntos de enlace y cuotas de AWS Storage Gateway](#) en la Referencia general de AWS.

14 de agosto de 2019

[Nueva AWS región](#)

Storage Gateway ya está disponible en la región Medio Oriente (Baréin). Para obtener más información, consulte [Puntos de enlace y cuotas de AWS Storage Gateway](#) en la Referencia general de AWS.

29 de julio de 2019

[Support para activar una puerta de enlace en una nube privada virtual \(VPC\)](#)

Ahora puede activar una puerta de enlace en unVPC. Puede crear una conexión privada entre su dispositivo de software local y una infraestructura de almacenamiento basada en la nube. Para obtener más información, consulte [Activación de una puerta de enlace en una nube virtual privada](#).

20 de junio de 2019

[Posibilidad de mover cintas virtuales de S3 Glacier Flexible Retrieval a S3 Glacier Deep Archive](#)

Ahora puede mover cintas virtuales que están archivadas en la clase de almacenamiento S3 Glacier Flexible Retrieval a la clase de almacenamiento S3 Glacier Deep Archive para conseguir una retención de datos rentable a largo plazo. Para obtener más información, consulte [Traslado de una cinta desde S3 Glacier Flexible Retrieval a S3 Glacier Deep Archive](#).

28 de mayo de 2019

[SMBsoporte para compartir archivos para Microsoft Windows ACLs](#)

En el caso de las puertas de enlace de archivos, ahora puede utilizar las listas de control de acceso de Microsoft Windows (ACLs) para controlar el acceso a los recursos compartidos de archivos del bloque de mensajes del servidor (SMB). Para obtener más información, consulte [Uso de Microsoft Windows ACLs para controlar el acceso a un recurso compartido de SMB archivos](#).

8 de mayo de 2019

[Integración con S3 Glacier Deep Archive](#)

La puerta de enlace de cinta se integra con S3 Glacier Deep Archive. Ahora puede archivar cintas virtuales en S3 Glacier Deep Archive para la retención de datos a largo plazo. Para obtener más información, consulte [Archivado de cintas virtuales](#).

27 de marzo de 2019

[Disponibilidad del dispositivo de hardware de Storage Gateway en Europa](#)

El dispositivo de hardware de Storage Gateway ya está disponible en Europa. Para obtener más información, consulte [Regiones de dispositivo de hardware de AWS Storage Gateway](#) en la Referencia general de AWS. Además, ahora puede aumentar el almacenamiento utilizable en el dispositivo de hardware 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

[Integración con AWS Backup](#)

Storage Gateway se integra con AWS Backup. Ahora puede utilizarlo AWS Backup para hacer copias de seguridad de aplicaciones empresariales locales que utilizan volúmenes de Storage Gateway para almacenamiento respaldado en la nube. Para obtener más información, consulte [Realización de la copia de seguridad de los volúmenes](#).

16 de enero de 2019

[Support para Bacula Enterprise y IBM Spectrum Protect](#)

Las pasarelas de cinta ahora son compatibles con Bacula Enterprise y Spectrum Protect. IBM Storage Gateway ahora también es compatible con las versiones más recientes de Veritas NetBackup, Veritas Backup Exec y Quest Backup. NetVault Ahora puede utilizar estas aplicaciones de copia de seguridad para hacer copias de seguridad de los datos en Amazon S3 y archivarlos directamente en el almacenamiento sin conexión (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). Para obtener más información, consulte [Uso de su software de copia de seguridad para comprobar la configuración de la gateway](#).

13 de noviembre de 2018

[Compatibilidad con el dispositivo de hardware de 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 puertas de enlace de archivos, cintas y volúmenes. Para obtener más información, consulte [Uso del dispositivo de hardware de Storage Gateway](#).

18 de septiembre de 2018

[Compatibilidad con Microsoft System Center 2016 Data Protection Manager \(DPM\)](#)

Las pasarelas de cinta ahora son compatibles con Microsoft System Center 2016 Data Protection Manager (DPM). Ahora puede usar Microsoft DPM para hacer copias de seguridad de sus datos en Amazon S3 y archivarlos directamente en un almacenamiento sin conexión (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). Para obtener más información, consulte [Prueba de la configuración utilizando Microsoft System Center Data Protection Manager](#).

18 de julio de 2018

[Soporte para el protocolo Server Message Block \(SMB\)](#)

File Gateways agregó compatibilidad con el protocolo Server Message Block (SMB) a los recursos compartidos de archivos. Para obtener más información, consulte [Creación de un recurso compartido de archivos](#).

20 de junio de 2018

[Compatibilidad con recursos compartidos de archivos, volúmenes en caché y cifrado de cintas virtuales](#)

Ahora puede usar AWS Key Management Service (AWS KMS) para cifrar los datos escritos en un recurso compartido de archivos, un volumen en caché o una cinta virtual. Actualmente, puede hacerlo mediante

AWS Storage Gateway API. Para obtener más información, consulte [Cifrado de datos mediante AWS KMS](#).

12 de junio de 2018

[Support for NovaStor DataCenter /Network](#)

Las pasarelas de cinta ahora son compatibles con /Network. NovaStor DataCenter Ahora puede usar las versiones 6.4 o 7.1 de NovaStor DataCenter /Network para hacer copias de seguridad de sus datos en Amazon S3 y archivarlos directamente en un almacenamiento sin conexión (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). Para obtener más información, consulte [Probar la configuración mediante NovaStor DataCenter /Network](#).

24 de mayo de 2018

Actualizaciones anteriores

En la siguiente tabla, se describen los cambios importantes de cada versión de la Guía del usuario de AWS Storage Gateway anteriores a mayo de 2018.

Cambio	Descripción	Fecha de modificación
Soporte para clase de almacenamiento S3 One Zone-IA	En las puertas de enlace de archivo, 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 permite almacenar los datos de objetos en una única zona de disponibilidad en Amazon S3. Para obtener más información, consulte Creación de un recurso compartido de archivos .	4 de abril de 2018
Nueva región de	La puerta de enlace de cinta ahora está disponible en la región Asia Pacífico (Singapur). Para obtener información detallada, consulte Regiones de AWS compatibles con Storage Gateway .	3 de abril de 2018
Support para actualizar la memoria caché, pagar el solicitante y almacenar buckets ACLs de Amazon S3.	<p>Las puertas de enlace de archivo ahora le permiten recibir una notificación cuando la puerta de enlace termine de actualizar la caché para el bucket de Amazon S3. Para obtener más información, consulte RefreshCache.html en Storage Gateway API Reference.</p> <p>Las puertas de enlace de archivo ahora permiten que el pago por los cargos de acceso lo realice el solicitante o el lector en lugar del propietario del bucket.</p> <p>Las puertas de enlace de archivos ahora le permiten otorgar el control total al propietario del bucket de S3 que se asigna al recurso compartido de NFS archivos.</p> <p>Para obtener más información, consulte Creación de un recurso compartido de archivos.</p>	1 de marzo de 2018
Support para Dell EMC NetWorker V9.x	Las pasarelas de cinta ahora son compatibles con Dell V9.x. EMC NetWorker Ahora puede usar Dell EMC NetWorker V9.x para hacer copias de seguridad	27 de febrero de 2018

Cambio	Descripción	Fecha de modificación
	de sus datos en Amazon S3 y archivarlos directamente en un almacenamiento sin conexión (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). Para obtener más información, consulte Probar la configuración con Dell . EMC NetWorker	
Nueva región de	Storage Gateway ya está disponible en la región Europa (París). Para obtener información detallada, consulte Regiones de AWS compatibles con Storage Gateway .	18 de diciembre de 2017
Support para la notificación de carga de archivos y la adivinación del tipo MIME	<p>File Gateways ahora puede notificarle cuando todos los archivos escritos en su recurso compartido de NFS archivos se hayan cargado en Amazon S3. Para obtener más información, consulte NotifyWhenUploaded Storage Gateway API Reference.</p> <p>Las pasarelas de archivos ahora permiten adivinar el MIME tipo de objetos cargados en función de las extensiones de los archivos. Para obtener más información, consulte Creación de un recurso compartido de archivos.</p>	21 de noviembre de 2017
Support for VMware ESXi Hypervisor versión 6.5	AWS Storage Gateway ahora es compatible con la versión 6.5 de VMware ESXi Hypervisor. Esta se suma a las versiones 4.1, 5.0, 5.1, 5.5 y 6.0. Para obtener más información, consulte Hipervisores compatibles y requisitos de host .	13 de septiembre de 2017

Cambio	Descripción	Fecha de modificación
Compatibilidad con Commvault 11	Las puertas de enlace de cinta ahora son compatibles con Commvault 11. Ahora puede utilizar Commvault para hacer copias de seguridad de los datos en Amazon S3 y archivarlos directamente en el almacenamiento sin conexión (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). Para obtener más información, consulte Comprobación de la configuración mediante Commvault .	12 de septiembre de 2017
Compatibilidad de la puerta de enlace de archivo con el hipervisor Microsoft Hyper-V	A partir de ahora, se puede implementar una puerta de enlace de archivo en un hipervisor Microsoft Hyper-V. Para obtener más información, consulte Hipervisores compatibles y requisitos de host .	22 de junio de 2017
Compatibilidad con la recuperación desde archivo de cintas de entre tres y cinco horas	En una puerta de enlace de cinta, ahora puede recuperar cintas del archivo en un tiempo de entre tres y cinco horas. También puede determinar la cantidad de datos que se graban en la cinta desde la aplicación de respaldo o la biblioteca de cintas virtuales (VTL). Para obtener más información, consulte Visualizar el uso de cintas .	23 de mayo de 2017
Nueva región de	Storage Gateway ya está disponible en la región Asia-Pacífico (Bombay). Para obtener información detallada, consulte Regiones de AWS compatibles con Storage Gateway .	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	<p>Las puertas de enlace de archivo ahora incorporan opciones de montaje a la configuración de recursos compartidos de archivos. A partir de ahora, puede establecer opciones de agrupación y de solo lectura para el recurso compartido de archivos. Para obtener más información, consulte Creación de un recurso compartido de archivos.</p> <p>Las puertas de enlace de archivo ahora son capaces de encontrar objetos en el bucket de Amazon S3 que se han agregado o quitado después de que la puerta de enlace elaborase la última lista del contenido del bucket y almacenase en caché el resultado. Para obtener más información, consulte RefreshCachela API Referencia.</p>	28 de marzo de 2017
Compatibilidad con la clonación de volúmenes	En el caso de las pasarelas de volumen almacenadas en caché, AWS Storage Gateway ahora se admite la posibilidad de clonar un volumen a partir de un volumen existente. Para obtener más información, consulte Clonación de un volumen .	16 de marzo de 2017

Cambio	Descripción	Fecha de modificación
Support para File Gateways en Amazon EC2	<p>AWS Storage Gateway ahora ofrece la posibilidad de implementar un File Gateway en AmazonEC2. Puede lanzar una puerta de enlace de archivos en Amazon EC2 utilizando la Amazon Machine Image (AMI) de Storage Gateway, que ahora está disponible como comunidadAMI. Para obtener información sobre cómo crear una puerta de enlace de archivos e implementarla en una EC2 instancia, consulte Crear y activar una puerta de enlace de archivos Amazon S3 o Crear y activar una puerta de enlace de FSx archivos de Amazon. Para obtener información sobre cómo lanzar una puerta de enlace de archivosAMI, consulte Implementación de una puerta de enlace de archivos S3 en un EC2 host de Amazon o Implementación de una puerta de enlace de FSx archivos en un EC2 host de Amazon.</p>	08 de febrero de 2017
Compatibilidad con Arcserve 17	<p>Las puertas de enlace de cinta ahora son compatibles con Arcserve 17. A partir de ahora, puede utilizar Arcserve para realizar una copia de seguridad de los datos en Amazon S3 y archivarlos directamente en S3 Glacier Flexible Retrieval. Para obtener más información, consulte Prueba de la configuración con Arcserve Backup r17.0.</p>	17 de enero de 2017
Nueva región de	<p>Storage Gateway ya está disponible en la región UE (Londres). Para obtener información detallada, consulte Regiones de AWS compatibles con Storage Gateway.</p>	13 de diciembre de 2016
Nueva región de	<p>Storage Gateway ya está disponible en la región Canadá (centro). Para obtener información detallada, consulte Regiones de AWS compatibles con Storage Gateway.</p>	08 de diciembre de 2016

Cambio	Descripción	Fecha de modificación
Compatibilidad con la puerta de enlace de archivos	Además de puerta de enlace de volumen y puerta de enlace de cinta, Storage Gateway ahora ofrece puerta de enlace de archivo. File Gateway combina un servicio y un dispositivo de software virtual, lo que le permite almacenar y recuperar objetos en Amazon S3 mediante protocolos de archivos estándares del sector, como Network File System (NFS). La puerta de enlace proporciona acceso a los objetos de Amazon S3 como archivos en un punto de NFS montaje.	29 de noviembre de 2016
Backup Exec 16	La puerta de enlace de cinta ahora es compatible con Backup Exec 16. Ahora puede utilizar Backup Exec 16 para hacer copias de seguridad de los datos en Amazon S3 y archivarlos directamente en el almacenamiento sin conexión (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). Para obtener más información, consulte Comprobación de la configuración mediante Veritas Backup Exec .	7 de noviembre de 2016
Compatibilidad con Micro Focus (HPE) Data Protector 9.x	Tape Gateway ahora es compatible con Micro Focus (HPE) Data Protector 9.x. Ahora puede usar HPE Data Protector para hacer copias de seguridad de sus datos en Amazon S3 y archivarlos directamente en S3 Glacier Flexible Retrieval. Para obtener más información, consulte Probar la configuración con Micro Focus (HPE) Data Protector .	2 de noviembre de 2016
Nueva región de	Storage Gateway ya está disponible en la región Este de EE. UU. (Ohio). Para obtener información detallada, consulte Regiones de AWS compatibles con Storage Gateway .	17 de octubre de 2016

Cambio	Descripción	Fecha de modificación
Rediseño de la consola de Storage Gateway	La consola de administración de Storage Gateway se ha rediseñado para que resulte más fácil configurar, administrar y supervisar las puertas de enlace, los volúmenes y las cintas virtuales. La interfaz de usuario ahora proporciona vistas que se pueden filtrar y proporciona enlaces directos a AWS servicios integrados como CloudWatch AmazonEBS. Para obtener más información, consulte Inscríbase en AWS Storage Gateway .	30 de agosto de 2016
Compatibilidad con Veeam Backup & Replication V9 Update 2 o posterior	Las puertas de enlace de cinta ahora admiten Veeam Backup & Replication V9 actualización 2 o versiones posteriores (es decir, la versión 9.0.0.1715 o posteriores). Ahora puede utilizar Veeam Backup Replication V9 actualización 2 o posterior para hacer copias de seguridad de los datos en Amazon S3 y archivarlos directamente en el almacenamiento sin conexión (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). Para obtener más información, consulte Prueba de la configuración con Veeam Backup & Replication .	15 de agosto de 2016
Mayor volumen e instantánea IDs	Storage Gateway presenta una versión más larga IDs para volúmenes e instantáneas. Puede activar el formato de ID más largo para sus volúmenes, instantáneas y otros recursos compatibles AWS . Para obtener más información, consulte Descripción de los recursos y recursos de Storage Gateway IDs .	25 de abril de 2016

Cambio	Descripción	Fecha de modificación
<p>Nueva región de</p> <p>Compatibilidad con almacenamiento de hasta 512 TiB para volúmenes almacenados</p> <p>Otras actualizaciones de la puerta de enlace y mejoras de la consola local de Storage Gateway</p>	<p>La puerta de enlace de cinta ahora está disponibles en la región Asia Pacífico (Seúl). Para obtener más información, consulte Regiones de AWS compatibles con Storage Gateway.</p> <p>Para los volúmenes almacenados, ahora puede crear hasta 32 volúmenes de almacenamiento con un tamaño de hasta 16 TiB cada uno, para un máximo de 512 TiB de almacenamiento. Para obtener más información, consulte Arquitectura de volúmenes almacenados y AWS Storage Gateway cuotas.</p> <p>El tamaño total de todas las cintas de una biblioteca de cintas virtuales se aumenta a 1 PiB. Para obtener más información, consulte AWS Storage Gateway cuotas.</p> <p>Ahora puede establecer la contraseña de la consola local de la máquina virtual en la consola de Storage Gateway. Para obtener más información, consulte Ajuste de la contraseña de la consola local desde la consola de Storage Gateway.</p>	<p>21 de marzo de 2016</p>
<p>Compatibilidad con Dell 8.x EMC NetWorker</p>	<p>Tape Gateway ahora es compatible con Dell EMC NetWorker 8.x. Ahora puede usar Dell EMC NetWorker para hacer copias de seguridad de sus datos en Amazon S3 y archivarlos directamente en un almacenamiento sin conexión (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). Para obtener más información, consulte Probar la configuración con Dell EMC NetWorker.</p>	<p>29 de febrero de 2016</p>

Cambio	Descripción	Fecha de modificación
Support para VMware ESXi Hypervisor versión 6.0 y el iniciador Red Hat Enterprise Linux 7 i SCSI	AWS Storage Gateway Ahora es compatible con la versión 6.0 del VMware ESXi hipervisor y el iniciador Red Hat Enterprise Linux 7 i. SCSI Para obtener más información, consulte Hypervisores compatibles y requisitos de host y Compatible con SCSI iniciadores .	20 de octubre de 2015
Reestructuración del contenido	Esta versión incluye esta mejora: la documentación ahora incluye una sección de administración de la gateway activada, que combina las tareas de administración que son comunes a todas las soluciones de gateway. A continuación, encontrará instrucciones sobre cómo administrar la gateway después de haberla implementado y activado. Para obtener más información, consulte Administración de la gateway .	

Cambio	Descripción	Fecha de modificación
<p>Compatibilidad con almacenamiento de hasta 1024 TiB para volúmenes en caché</p> <p>Support para el tipo de adaptador de red VMXNET3 (10 GbE) en el VMware ESXi hipervisor</p> <p>Mejoras de desempeño</p> <p>Diversas mejoras y actualizaciones de la consola local de Storage Gateway</p>	<p>Para los volúmenes en caché, ahora puede crear hasta 32 volúmenes de almacenamiento de hasta 32 TiB cada uno, para un máximo de 1024 TiB de almacenamiento. Para obtener más información, consulte Arquitectura de volúmenes en caché y AWS Storage Gateway cuotas.</p> <p>Si la puerta de enlace está alojada en un VMware ESXi hipervisor, puede volver a configurar la puerta de enlace para que utilice el VMXNET3 tipo de adaptador . Para obtener más información, consulte Configuración de adaptadores de red para la gateway.</p> <p>La velocidad de carga máxima para Storage Gateway ha aumentado a 120 MB por segundo y la velocidad de descarga máxima ha aumentado a 20 MB por segundo.</p> <p>La consola local de Storage Gateway se ha actualizado y mejorado con características adicionales que le ayudarán a llevar a cabo tareas de mantenimiento. Para obtener más información, consulte Configuración de red de la gateway.</p>	<p>16 de septiembre de 2015</p>
<p>Compatibilidad con el etiquetado</p>	<p>Storage Gateway ya es compatible con el etiquetado de recursos. A partir de ahora, puede agregar etiquetas a las gateways, los volúmenes y las cintas virtuales, para facilitar su administración. Para obtener más información, consulte Etiquetado de recursos de Storage Gateway.</p>	<p>2 de septiembre de 2015</p>

Cambio	Descripción	Fecha de modificación
Compatibilidad con Quest (anteriormente Dell) NetVault Backup 10.0	Tape Gateway ahora es compatible con Quest NetVault Backup 10.0. Ahora puede usar Quest NetVault Backup 10.0 para hacer copias de seguridad de sus datos en Amazon S3 y archivarlos directamente en un almacenamiento sin conexión (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). Para obtener más información, consulte Probar su configuración mediante Quest NetVault Backup .	22 de junio de 2015

Cambio	Descripción	Fecha de modificación
Compatibilidad con volúmenes de almacenamiento de 16 TiB para configuraciones de gateways de volúmenes almacenados	Storage Gateway ahora es compatible con volúmenes de almacenamiento de 16 TiB para configuraciones de puerta de enlace de volumen almacenados. A partir de ahora, puede crear 12 volúmenes de almacenamiento de 16 TiB para un máximo de 192 TiB de almacenamiento. Para obtener más información, consulte Arquitectura de volúmenes almacenados .	3 de junio de 2015
Compatibilidad con comprobaciones de recursos del sistema en la consola local de Storage Gateway	Ahora puede determinar si los recursos de su sistema (CPU núcleos virtuales, tamaño del volumen raíz y RAM) son suficientes para que su puerta de enlace funcione correctamente. Para obtener más información, consulte Visualización del estado de los recursos de sistema de la gateway o Visualización del estado de los recursos de sistema de la gateway .	
Support para el SCSI iniciador Red Hat Enterprise Linux 6 i	Storage Gateway ahora es compatible con el SCSI iniciador Red Hat Enterprise Linux 6 i. Para obtener más información, consulte Requisitos para configurar Tape Gateway .	
	<p>Esta versión incluye las siguientes mejoras y actualizaciones de Storage Gateway:</p> <ul style="list-style-type: none"> • Desde la consola de Storage Gateway, ahora puede ver la fecha y la hora en que se aplicó a la puerta de enlace la última actualización de software correcta. Para obtener más información, consulte Administrar las actualizaciones de la pasarela. • Storage Gateway ahora proporciona y API puede usar para enumerar SCSI los iniciadores conectado 	

Cambio	Descripción	Fecha de modificación
	<p>s a sus volúmenes de almacenamiento. Para obtener más información, consulte ListVolum eInitiators la API referencia.</p>	
<p>Compatibilidad con las versiones 2012 y 2012 R2 del hipervisor Microsoft Hyper-V</p>	<p>Storage Gateway ya es compatible con las versiones 2012 y 2012 R2 del hipervisor Microsoft Hyper-V. Esto se suma a la compatibilidad con el hipervisor Microsoft Hyper-V versión 2008 R2. Para obtener más información, consulte Hipervisores compatibles y requisitos de host.</p>	<p>30 de abril de 2015</p>
<p>Compatibilidad con Symantec Backup Exec 15</p>	<p>La puerta de enlace de cinta ahora es compatible con Symantec Backup Exec 15. Ahora puede utilizar Symantec Backup Exec 15 para hacer copias de seguridad de los datos en Amazon S3 y archivarlos directamente en el almacenamiento sin conexión (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). Para obtener más información, consulte Comprobación de la configuración mediante Veritas Backup Exec.</p>	<p>6 de abril de 2015</p>
<p>CHAP soporte de autenticación para volúmenes de almacenamiento</p>	<p>Storage Gateway ahora admite la configuración de CHAP la autenticación para los volúmenes de almacenamiento. Para obtener más información, consulte Configurar la CHAP autenticación para sus volúmenes.</p>	<p>2 de abril de 2015</p>
<p>Support para las versiones 5.1 y 5.5 de VMware ESXi Hypervisor</p>	<p>Storage Gateway ahora es compatible con las versiones 5.1 y 5.5 de VMware ESXi Hypervisor. Esto se suma a la compatibilidad con las versiones 4.1 y 5.0 de VMware ESXi Hypervisor. Para obtener más información, consulte Hipervisores compatibles y requisitos de host.</p>	<p>30 de marzo de 2015</p>

Cambio	Descripción	Fecha de modificación
CHKDSKUtilidad Support for Windows	Storage Gateway ahora es compatible con la CHKDSK utilidad de Windows. Puede utilizar esta utilidad para comprobar la integridad de los volúmenes y corregir errores en ellos. Para obtener más información, consulte la Solución de problemas con volúmenes .	04 de marzo de 2015
Integración con AWS CloudTrail para capturar API llamadas	<p>Storage Gateway ahora está integrado con AWS CloudTrail. AWS CloudTrail captura API las llamadas realizadas por Storage Gateway o en su nombre en su cuenta de Amazon Web Services y entrega los archivos de registro a un bucket de Amazon S3 que especifique. Para obtener más información, consulte Inicio de sesión y supervisión AWS Storage Gateway.</p> <p>Esta versión incluye la siguiente mejora y actualización de Storage Gateway:</p> <ul style="list-style-type: none">Ahora, las cintas virtuales que tienen datos incorrectos en el almacenamiento en caché (es decir, que incluyen contenido que no se ha cargado en AWS) se recuperan cuando cambia la unidad en caché de una puerta de enlace. Para obtener más información, consulte Recuperar una cinta virtual de una puerta de enlace no recuperable.	16 de diciembre de 2014

Cambio	Descripción	Fecha de modificación
<p>Compatibilidad con software de backup adicional y cambiador de medios</p>	<p>La puerta de enlace de cinta ahora es compatible con el software de copia de seguridad siguiente:</p> <ul style="list-style-type: none"> • Symantec Backup Exec 2014 • Microsoft System Center 2012 R2 Data Protection Manager • Veeam Backup & Replication V7 • Veeam Backup & Replication V8 <p>Ahora puede usar estos cuatro productos de software de respaldo con la biblioteca de cintas virtuales Storage Gateway (VTL) para realizar copias de seguridad en Amazon S3 y archivarlas directamente en un almacenamiento fuera de línea (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). Para obtener más información, consulte Uso de su software de copia de seguridad para comprobar la configuración de la gateway.</p> <p>A partir de ahora, Storage Gateway ofrece un cambiador de medios adicional que funciona con el nuevo software de copia de seguridad.</p> <p>Esta versión incluye varias mejoras y actualizaciones. AWS Storage Gateway</p>	<p>3 de noviembre de 2014</p>
<p>Región de Europa (Fráncfort)</p>	<p>Ahora Storage Gateway también está disponible en la región de Europa (Fráncfort). Para obtener información detallada, consulte Regiones de AWS compatibles con Storage Gateway.</p>	<p>23 de octubre de 2014</p>

Cambio	Descripción	Fecha de modificación
Reestructuración del contenido	Se ha creado una sección de introducción que es común a todas las soluciones de gateway. A continuación, encontrará instrucciones para descargar , implementar y activar una gateway. Después de implementar y activar una puerta de enlace, puede consultar más instrucciones específicas de volúmenes almacenados, volúmenes en caché y configuraciones de puerta de enlace de cinta. Para obtener más información, consulte Creación de una puerta de enlace de cinta .	19 de mayo de 2014
Compatibilidad con Symantec Backup Exec 2012	La puerta de enlace de cinta ahora es compatible con Symantec Backup Exec 2012. Ahora puede utilizar Symantec Backup Exec 2012 para hacer copias de seguridad de los datos en Amazon S3 y archivarlos directamente en el almacenamiento sin conexión (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). Para obtener más información, consulte Comprobación de la configuración mediante Veritas Backup Exec .	28 de abril de 2014

Cambio	Descripción	Fecha de modificación
<p>Compatibilidad con Clústeres de conmutación por error de Windows Server</p> <p>Support for VMware ESX initiator</p> <p>Compatibilidad con la realización de tareas de configuración en la consola local de Storage Gateway</p>	<ul style="list-style-type: none"> • Storage Gateway ahora admite la conexión de varios hosts al mismo volumen si los hosts coordinan el acceso mediante el clúster de conmutación por error de Windows Server (WSFC). Sin embargo, no puede conectar varios hosts al mismo volumen sin usarlos. WSFC • Storage Gateway ahora le permite administrar la conectividad de almacenamiento directamente a través de su ESX host. Esto ofrece una alternativa al uso de iniciadores residentes en el sistema operativo huésped de su VMs empresa. • Storage Gateway ahora es compatible con la realización de tareas de configuración en la consola local de Storage Gateway. Para obtener información sobre cómo realizar tareas de configuración en gateways implementadas on-premise, consulte Realización de tareas en la consola local de la MV de o Realización de tareas en la consola local de la MV de . Para obtener información sobre cómo realizar tareas de configuración en las puertas de enlace implementadas en una EC2 instancia, consulte Realización de tareas en la consola EC2 local de Amazon o Realización de tareas en la consola EC2 local de Amazon 	<p>31 de enero de 2014</p>

Cambio	Descripción	Fecha de modificación
<p>Support para biblioteca de cintas virtuales (VTL) e introducción de la API versión 2013-06-30</p>	<p>Storage Gateway conecta un dispositivo de software local con un almacenamiento basado en la nube para integrar el entorno de TI local con la infraestructura AWS de almacenamiento. Además de Volume Gateways (volúmenes en caché y volúmenes almacenados), Storage Gateway ahora admite gateway—biblioteca de cintas virtuales (). VTL Puede configurar una puerta de enlace de cinta con hasta 10 unidades de cinta virtuales por puerta de enlace. Cada unidad de cinta virtual responde al conjunto de SCSI comandos, por lo que las aplicaciones de backup locales existentes funcionarán sin modificaciones. Para obtener más información, consulte los siguientes temas en la Guía del usuario de AWS Storage Gateway .</p> <ul style="list-style-type: none"> • Para obtener una descripción general de la arquitectura, consulte Funcionamiento de puerta de enlace de cinta (arquitectura). • Para empezar a utilizar puerta de enlace de cinta, consulte Creación de una puerta de enlace de cinta. 	<p>5 de noviembre de 2013</p>
<p>Compatibilidad con Microsoft Hyper-V</p>	<p>A partir de ahora, Storage Gateway permite implementar una puerta de enlace en las instalaciones en la plataforma de virtualización Microsoft Hyper-V. Las puertas de enlace implementadas en Microsoft Hyper-V tienen las mismas funcionalidades y características que la Storage Gateway en las instalaciones existente . Para comenzar a implementar una gateway con Microsoft Hyper-V, consulte Hipervisores compatibles y requisitos de host.</p>	<p>10 de abril de 2013</p>

Cambio	Descripción	Fecha de modificación
Support para implementar una puerta de enlace en Amazon EC2	Storage Gateway ahora ofrece la posibilidad de implementar una puerta de enlace en Amazon Elastic Compute Cloud (AmazonEC2). Puede lanzar una instancia de gateway en Amazon EC2 mediante el Storage Gateway AMI disponible en AWS Marketplace . Para empezar a implementar una puerta de enlace mediante Storage GatewayAMI, consulte Implementación de una EC2 instancia de Amazon para alojar su Tape Gateway .	15 de enero de 2013

Cambio	Descripción	Fecha de modificación
Support para volúmenes en caché e introducción de la API versión 2012-06-30	<p>En esta versión, Storage Gateway presenta la compatibilidad con los volúmenes en caché. Los volúmenes en caché reducen al mínimo la necesidad de escalar la infraestructura de almacenamiento on-premise a la vez que proporcionan a sus aplicaciones acceso de baja latencia a los datos activos. Puede crear volúmenes de almacenamiento de hasta 32 TiB y montarlos como SCSI dispositivos i desde sus servidores de aplicaciones locales. Los datos grabados en los volúmenes en caché se almacenan en Amazon Simple Storage Service (Amazon S3), en la memoria caché se mantienen únicamente los datos grabados y leídos recientemente y que están almacenados en su hardware local en las instalaciones. Los volúmenes en caché permiten utilizar Amazon S3 para los datos cuando son aceptables latencias de recuperación más altas (por ejemplo, para datos más antiguos o a los que se obtiene acceso de forma infrecuente), mientras se mantiene el almacenamiento en las instalaciones para los datos que requieren acceso de baja latencia.</p> <p>En esta versión, Storage Gateway también presenta una nueva API versión que, además de admitir las operaciones actuales, proporciona nuevas operaciones para admitir los volúmenes en caché.</p> <p>Para obtener más información sobre las dos soluciones de Storage Gateway, consulte Funcionamiento de puerta de enlace de cinta (arquitectura).</p> <p>También puede probar una configuración de prueba. Para obtener instrucciones, consulte Creación de una puerta de enlace de cinta.</p>	29 de octubre de 2012

Cambio	Descripción	Fecha de modificación
API soporte IAM	<p>En esta versión, Storage Gateway presenta el API soporte y el soporte para AWS Identity and Access Management(IAM).</p> <ul style="list-style-type: none"> • APIsoporte: ahora puede configurar y administrar mediante programación los recursos de Storage Gateway. Para obtener más información al respectoAPI, consulte la APIReferencia para Storage Gateway Guía del AWS Storage Gateway usuario. • IAMsupport — AWS Identity and Access Management (IAM) le permite crear usuarios y administrar el acceso de los usuarios a sus recursos de Storage Gateway mediante IAM políticas. Para ver algunos ejemplos de políticas de IAM, consulte Identity and Access Management para AWS Storage Gateway. Para obtener más información al respectoIAM, consulte la página de detalles de AWS Identity and Access Management (IAM). 	9 de mayo de 2012
Compatibilidad con direcciones IP estáticas	A partir de ahora, puede especificar una dirección IP estática para la gateway local. Para obtener más información, consulte Configuración de red de la gateway .	5 de marzo de 2012
Nueva guía	Esta es la primera versión de la Guía de usuario de AWS Storage Gateway .	24 de enero de 2012

Notas de la versión del software del dispositivo Tape Gateway

Estas notas de la versión describen las funciones, mejoras y correcciones nuevas y actualizadas que se incluyen en cada versión del dispositivo Tape Gateway . Cada versión de software se identifica por su fecha de lanzamiento y un número de versión único.

Para determinar el número de versión del software de una puerta de enlace, consulte su página de detalles en la consola de Storage Gateway o llame a la [DescribeGatewayInformation](#) API acción mediante un AWS CLI comando similar al siguiente:

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

El número de versión se devuelve en el SoftwareVersion campo de la API respuesta.

Note

Una puerta de enlace no proporcionará información sobre la versión del software en las siguientes circunstancias:

- La puerta de enlace está fuera de línea.
- La puerta de enlace ejecuta un software antiguo que no admite la generación de informes de versiones.
- El tipo de puerta de enlace es FSx File Gateway.

Para obtener más información sobre las actualizaciones de Tape Gateway , incluida la forma de modificar la programación automática predeterminada de mantenimiento y actualización de una puerta de enlace, consulte [Administración de las actualizaciones de la puerta de enlace mediante la consola AWS Storage Gateway](#) .

Fecha de lanzamiento	Versión del software	Notas de la versión
2024-07-29	2.10.0	<ul style="list-style-type: none">• Actualizaciones del sistema operativo para las puertas

Fecha de lanzamiento	Versión del software	Notas de la versión
		<p>de enlace nuevas y existentes</p> <ul style="list-style-type: none">• Mejoras y correcciones de errores varias
-17 de junio de 2024	2.9.2	<ul style="list-style-type: none">• Actualizaciones del sistema operativo para las puertas de enlace nuevas y existentes
28 de mayo de 2022	2.9.0	<ul style="list-style-type: none">• Reducción del tiempo de reinicio de la puerta de enlace durante las actualizaciones de software• Se ha reducido la cantidad de datos transferidos para estimar el ancho de banda de la red
08-05-2022	2.8.3	<ul style="list-style-type: none">• Se solucionó el problema de conectividad a la nube al usar un proxy SOCKS5• Se solucionó el problema de degradación del rendimiento de carga en determinadas condiciones (por ejemplo, un gran número de operaciones de borrado de cintas)

Fecha de lanzamiento	Versión del software	Notas de la versión
10 de abril de 2022	2.8.1	<ul style="list-style-type: none">• Se solucionó un problema de uso de memoria introducido en la versión 2.8.0• Actualizaciones de los parches de seguridad• Proceso de actualización de software mejorado• Se solucionó la falta del componente Network Time Protocol (NTP) para las nuevas puertas de enlace
06/03/2022	2.8.0	<ul style="list-style-type: none">• Actualizaciones del sistema operativo para las nuevas puertas de enlace• Actualizaciones de parches de seguridad• Rendimiento mejorado para cargas de trabajo simultáneas de Backup y Restore
19 de diciembre de 2021	2.7.0	<ul style="list-style-type: none">• Actualizaciones del sistema operativo para las nuevas puertas de enlace
14 de diciembre de 2023	2.6.6	<ul style="list-style-type: none">• Se ha corregido un problema con el posicionamiento relativo en cintas de más de 5 TiB

Fecha de lanzamiento	Versión del software	Notas de la versión
19 de octubre de 2023	2.6.5	<ul style="list-style-type: none">• Se agregaron medidas de protección contra la sobrescritura de cintas por parte de los clientes después de reiniciar la puerta de enlace