Guía del usuario de puerta de enlace de volumen

AWS Storage Gateway

Versión de API 2013-06-30

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

Table of Contents

¿Qué es una puerta de enlace de volumen?

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.

Puede implementar Storage Gateway de forma local como un dispositivo de máquina virtual que se ejecute en VMware ESXi un hipervisor KVM o Microsoft Hyper-V, como un dispositivo de hardware o como una instancia de Amazon. AWS EC2 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 la amplia gama de casos de uso que AWS Storage Gateway ayudan a hacerlo posible, consulte. AWS Storage Gateway Para obtener información actualizada sobre los precios, consulte Precios en la página de detalles de AWS Storage Gateway .

AWS Storage Gateway ofrece soluciones de almacenamiento basadas en archivos (S3 File Gateway y FSx File Gateway), basadas en volúmenes (Volume Gateway) y en cintas (Tape Gateway).

Esta guía del usuario proporciona información relacionada con puerta de enlace de volumen.

Una puerta de enlace de volumen proporciona volúmenes de almacenamiento respaldados por la nube que puede montar como dispositivos de interfaz de sistemas informáticos pequeños de Internet (iSCSI) desde los servidores de aplicaciones en las instalaciones.

La puerta de enlace de volumen es compatible con las siguientes configuraciones de volumen:

- Volúmenes en caché: almacene los datos en Amazon Simple Storage Service (Amazon S3) y conserve una copia local de los subconjuntos de datos de acceso frecuente. Los volúmenes almacenados en caché ofrecen ahorros importantes en el almacenamiento principal y minimizan la necesidad de escalar el almacenamiento on-premises. También puede mantener un acceso de baja latencia a los datos de acceso frecuente.
- Volúmenes almacenados: si necesita acceso de baja latencia a todo el conjunto de datos, configure primero la puerta de enlace en las instalaciones para almacenar todos los datos localmente. A continuación, haga una copia de seguridad asíncrona de point-in-time las instantáneas de estos datos en Amazon S3. Esta configuración proporciona copias de seguridad externas duraderas y económicas que puede recuperar en su centro de datos local o en Amazon

Elastic Compute Cloud (Amazon EC2). Por ejemplo, si necesita capacidad de reemplazo para la recuperación ante desastres, puede recuperar las copias de seguridad en Amazon EC2.

Para ver información general sobre la arquitectura, consulte Funcionamiento de puerta de enlace de volumen.

En esta guía del usuario, puede encontrar una sección de introducción que incluye la información de configuración común a todos los tipos de puertas de enlace. Puede también encontrar los requisitos de configuración de puerta de enlace de volumen y las secciones que describen cómo implementar, activar, configurar y administrar la puerta de enlace de volumen.

Los procedimientos de esta guía del usuario se centran principalmente en realizar operaciones de puerta de enlace mediante la AWS Management Console. Si desea realizar estas operaciones mediante programación, consulte la Referencia de la API de AWS Storage Gateway.

Funcionamiento de puerta de enlace de volumen

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

Gateways de volúmenes

Para las puertas de enlace de volúmenes, puede utilizar volúmenes en caché o volúmenes almacenados.

Temas

- Arquitectura de volúmenes en caché
- Arquitectura de volúmenes almacenados

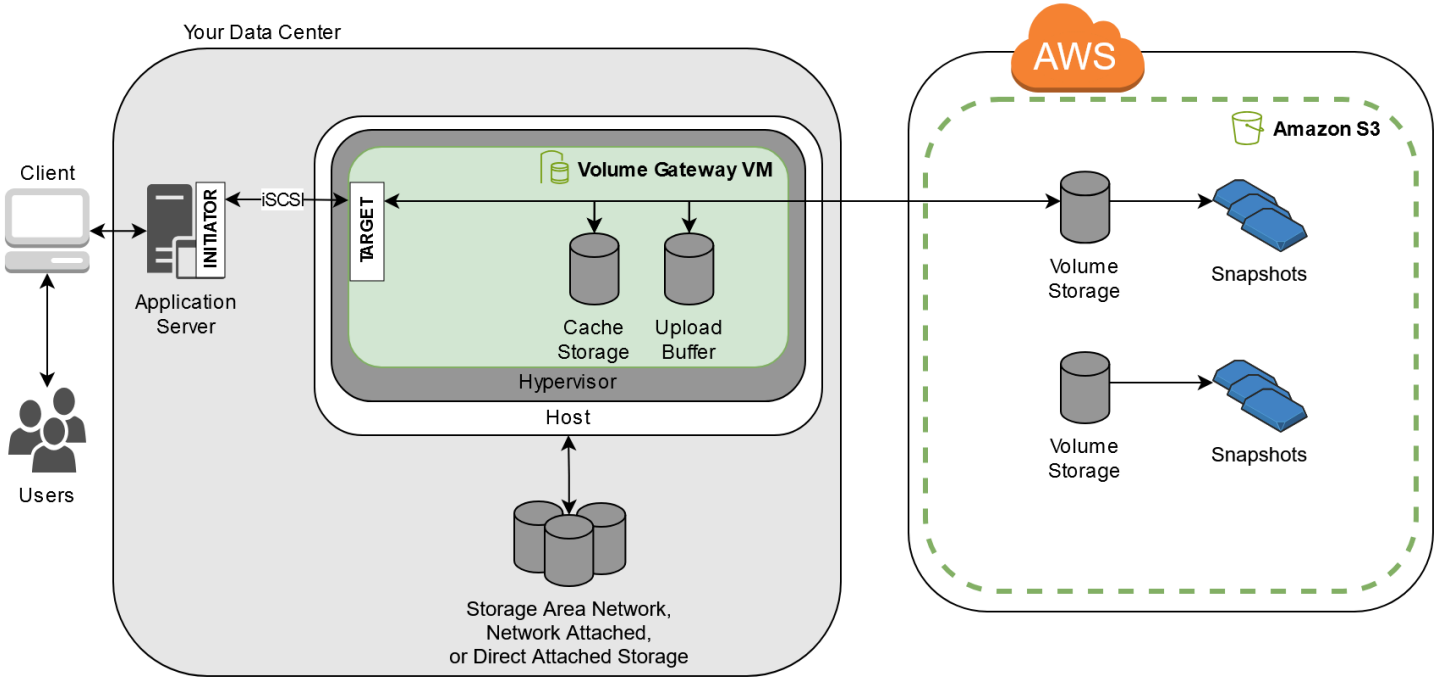
Arquitectura de volúmenes en caché

Mediante el uso de volúmenes en caché, puede usar Amazon S3 como almacenamiento de datos principal manteniendo localmente los datos de acceso frecuente en Storage Gateway. Los volúmenes almacenados en caché reducen al mínimo la necesidad de escalar la infraestructura de almacenamiento local a la vez que proporcionan a sus aplicaciones acceso de baja latencia a los datos de acceso frecuente. Puede crear volúmenes de almacenamiento con un tamaño de hasta 32 TiB y asociarlos como dispositivos iSCSI desde los servidores de aplicaciones locales. La puerta de enlace almacena los datos que se escriben en estos volúmenes en Amazon S3 y

conserva los datos leídos recientemente en la caché de Storage Gateway en las instalaciones y en el almacenamiento del búfer de carga.

Los volúmenes almacenados en caché pueden ir de 1 GiB a 32 TiB de tamaño y deben redondearse al GiB más próximo. Cada gateway configurada para volúmenes almacenados en caché admite hasta 32 volúmenes para un volumen de almacenamiento máximo de 1 024 TiB (1 PiB).

En la solución de volúmenes en caché, Storage Gateway almacena todos los datos de las aplicaciones en las instalaciones en un volumen de almacenamiento en Amazon S3. En el diagrama siguiente se proporciona información general de la implementación de los volúmenes almacenados en caché.



Tras instalar el dispositivo de software Storage Gateway (la máquina virtual) en un host de su centro de datos y activarlo, lo utilizará AWS Management Console para aprovisionar volúmenes de almacenamiento respaldados por Amazon S3. También puede aprovisionar volúmenes de almacenamiento mediante programación mediante la API Storage Gateway o las bibliotecas del AWS SDK. A continuación, puede montar estos volúmenes de almacenamiento en servidores de aplicaciones on-premises como dispositivos iSCSI.

También puede asignar discos on-premises para la MV. Estos discos on-premises sirven para los siguientes propósitos:

- Discos para que la puerta de enlace los utilice como almacenamiento en caché: a medida que las aplicaciones escriben datos en los volúmenes de almacenamiento AWS, la puerta de enlace

primero almacena los datos en los discos locales que se utilizan para el almacenamiento en caché. A continuación, la puerta de enlace carga los datos en Amazon S3. El almacenamiento en caché funciona como un almacén en las instalaciones permanente para los datos que están a la espera de cargarse desde el búfer de carga en Amazon S3.

El almacenamiento en caché también permite que la gateway almacene los datos de acceso reciente de la aplicación on-premises para un acceso de baja latencia. Si la aplicación solicita datos, la puerta de enlace los busca en el almacenamiento en caché antes que en Amazon S3.

Puede utilizar las siguientes directrices para determinar la cantidad de espacio en disco que se asigna para el almacenamiento en caché. Por lo general, debe asignar al menos el 20 por ciento del tamaño del almacén de archivos existente como almacenamiento en caché. El almacenamiento en caché, además, debe ser mayor que el búfer de carga. Esta última directriz contribuye a garantizar que el almacenamiento en caché sea suficientemente grande para almacenar todos los datos en el búfer de carga que aún no se hayan cargado en Amazon S3.

- Discos utilizados por la puerta de enlace como búfer de carga: para preparar la carga en Amazon S3, la puerta de enlace también almacena datos de entrada en un área de concentración que se denomina búfer de carga. Su puerta de enlace carga estos datos del búfer a través de una conexión Secure Sockets Layer (SSL) cifrada AWS, donde se almacenan cifrados en Amazon S3.

Se pueden hacer copias de seguridad incrementales, denominadas instantáneas, de los volúmenes de almacenamiento en Amazon S3. Estas point-in-time instantáneas también se almacenan en Amazon S3 como instantáneas de Amazon EBS. Cuando se toma una nueva instantánea, solo se almacenan los datos modificados desde la última instantánea. Cuando se toma la instantánea, la puerta de enlace carga los cambios hasta el punto de la instantánea y, a continuación, crea la nueva instantánea mediante Amazon EBS. Puede iniciar las instantáneas de manera programada o puntual. Un solo volumen admite poner en cola varias instantáneas en rápida sucesión, pero cada instantánea debe terminar de crearse antes de poder tomar la siguiente. Cuando se elimina una instantánea, solo se borran los datos que no son necesarios para ninguna otra instantánea. Para obtener información sobre las instantáneas de Amazon EBS, consulte Instantáneas de Amazon EBS.

Puede restaurar una instantánea de Amazon EBS en un volumen de almacenamiento de puerta de enlace si necesita recuperar una copia de seguridad de los datos. Para instantáneas de hasta 16 TiB de tamaño, también puede utilizar la instantánea como punto de partida para un nuevo volumen de Amazon EBS. A continuación, puede adjuntar este nuevo volumen de Amazon EBS a una EC2 instancia de Amazon.

Todos los datos de puerta de enlace y de instantáneas de los volúmenes en caché se almacenan en Amazon S3 y se cifran en reposo mediante cifrado del servidor (SSE). Sin embargo, no puede obtener acceso a estos datos con la API de Amazon S3 u otras herramientas como la consola de administración de Amazon S3.

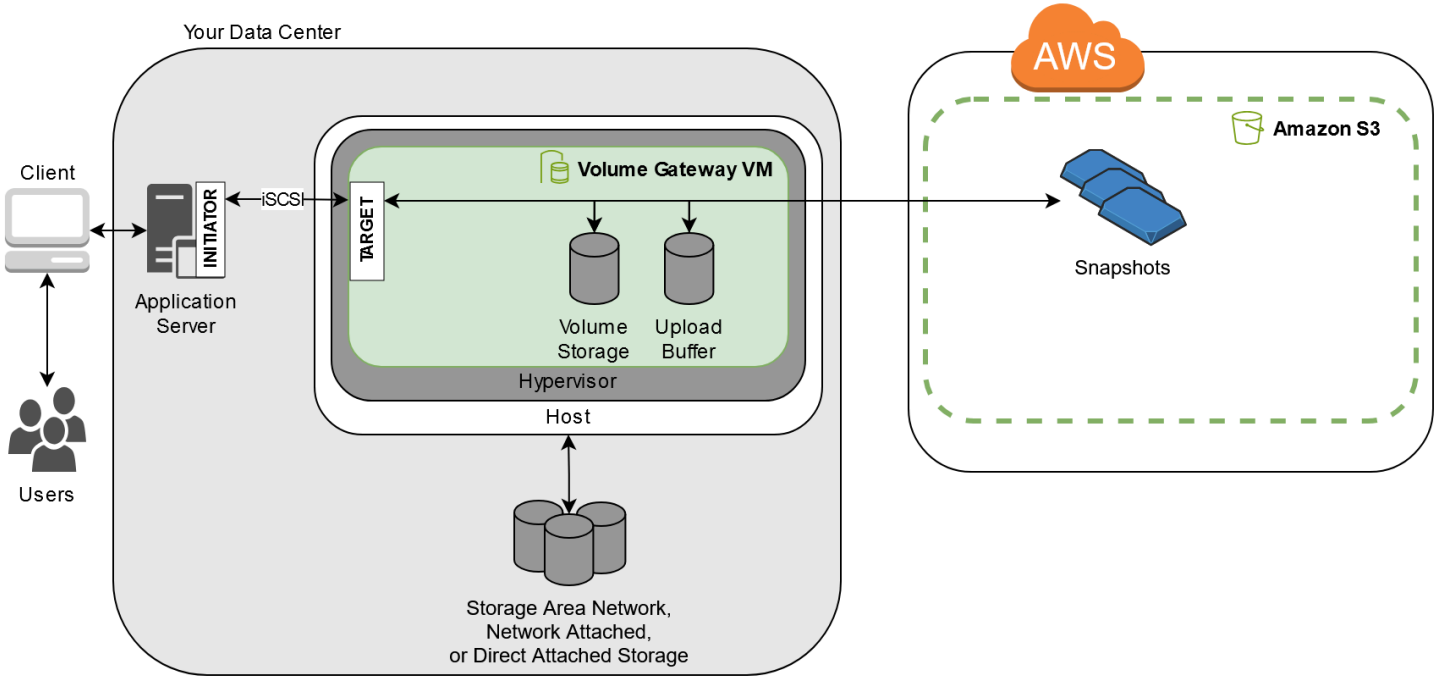
Arquitectura de volúmenes almacenados

Al utilizar volúmenes almacenados, puede almacenar sus datos principales de forma local y, al mismo tiempo, realizar copias de seguridad de esos datos de forma asíncrona. AWS Los volúmenes almacenados proporcionan aplicaciones locales con acceso de baja latencia a conjuntos de datos completos. Asimismo, proporcionan copias de seguridad duraderas externas. Puede crear volúmenes de almacenamiento y montarlos como dispositivos iSCSI desde los servidores de aplicaciones on-premises. Los datos escritos en los volúmenes almacenados se almacenan en el hardware de almacenamiento on-premises. Se realiza una copia de seguridad de estos datos de forma asíncrona en Amazon S3 como instantáneas de Amazon Elastic Block Store (Amazon EBS).

Los volúmenes almacenados pueden ir de 1 GiB a 16 TiB de tamaño y deben redondearse al GiB más próximo. Cada gateway configurada para volúmenes almacenados en la gateway admite hasta 32 volúmenes y un almacenamiento de volumen total de 512 TiB (0,5 PiB).

Con los volúmenes almacenados, mantiene el almacenamiento de volumen on-premises en el centro de datos. Es decir, almacena todos los datos de aplicación en hardware de almacenamiento on-premises. A continuación, la puerta de enlace utiliza características que ayudan a mantener la seguridad de los datos para cargarlos en Amazon Web Services Cloud para una copia de seguridad económica y una rápida recuperación de desastres. Esta solución es ideal si desea mantener los datos localmente en las instalaciones, porque necesite un acceso de baja latencia a todos los datos y, además, mantener copias de seguridad en AWS.

En el diagrama siguiente se proporciona información general de la implementación de los volúmenes almacenados.



Después de instalar el dispositivo de software de Storage Gateway (la máquina virtual) en un host del centro de datos y una vez activado, puede crear volúmenes de almacenamiento de la puerta de enlace. A continuación, deberá asignarlos a un sistema de almacenamiento local conectado directamente (DAS) o a discos de la red del área de almacenamiento (SAN). Puede comenzar con discos nuevos o discos que ya contengan datos. A continuación, puede montar estos volúmenes de almacenamiento en servidores de aplicaciones on-premises como dispositivos iSCSI. A medida que las aplicaciones on-premises escriben y leer datos en un volumen de almacenamiento de la gateway, estos datos se almacenan y se recuperan en el volumen de disco asignado.

Para preparar los datos para la carga en Amazon S3, la puerta de enlace almacena también los datos entrantes en un área de almacenamiento transitorio, que se denomina búfer de carga. Puede utilizar discos DAS o SAN on-premises para el almacenamiento de trabajo. La puerta de enlace carga datos desde el búfer de carga a través de una conexión de capa de conexión segura (SSL) cifrada en el servicio de Storage Gateway que se ejecuta en Amazon Web Services Cloud. A continuación, el servicio almacena los datos cifrados en Amazon S3.

Puede hacer copias de seguridad incrementales, denominadas instantáneas, de los volúmenes de almacenamiento. La puerta de enlace almacena estas instantáneas en Amazon S3 como instantáneas de Amazon EBS. Cuando se toma una nueva instantánea, solo se almacenan los datos modificados desde la última instantánea. Cuando se toma la instantánea, la puerta de enlace carga los cambios hasta el punto de la instantánea y, a continuación, crea la nueva instantánea mediante Amazon EBS. Puede iniciar las instantáneas de manera programada o puntual. Un solo volumen

admite poner en cola varias instantáneas en rápida sucesión, pero cada instantánea debe terminar de crearse antes de poder tomar la siguiente. Cuando se elimina una instantánea, solo se eliminan los datos que no son necesarios para ninguna otra instantánea.

Puede restaurar una instantánea de Amazon EBS en un volumen de almacenamiento de puerta de enlace en las instalaciones si necesita recuperar una copia de seguridad de los datos. También puede usar la instantánea como punto de partida para un nuevo volumen de Amazon EBS, que luego podrá adjuntar a una EC2 instancia de Amazon.

Empezar con AWS Storage Gateway

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

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

Temas

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

Inscríbase en AWS Storage Gateway

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

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

Para suscribirte a una Cuenta de AWS

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

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

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

También recomendamos que exija a sus usuarios que utilicen credenciales temporales al acceder AWS. Para proporcionar credenciales temporales, puede utilizar una federación y un proveedor de identidad, como el AWS IAM Identity Center. Si su empresa ya utiliza un proveedor de identidad, puede utilizarlo junto con la federación para simplificar el acceso a los recursos de su AWS cuenta.

Creación de un usuario de IAM con privilegios de administrador

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

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

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

Warning

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

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

Acceder AWS Storage Gateway

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

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

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

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

Regiones de AWS compatibles con Storage Gateway

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

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

- Storage Gateway: para ver AWS las regiones compatibles y una lista de los puntos de enlace de AWS servicio que puede usar con Storage Gateway, consulte 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 puerta de enlace de volumen

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

Temas

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.
- En el caso de la puerta de enlace de volumen, el hardware debe dedicar las siguientes cantidades de RAM:
  - 16 GiB de RAM reservados para puertas de enlace con un tamaño de caché de hasta 16 TiB
  - 32 GiB de RAM reservados para puertas de enlace con un tamaño de caché de 16 TiB a 32 TiB
  - 48 GiB de RAM reservados para puertas de enlace con un tamaño de caché de 32 TiB a 64 TiB
- 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 Optimizing Gateway Performance. 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 (Amazon EC2), el tamaño de la instancia debe ser al menos xlarge para que la puerta de enlace funcione. Sin embargo, para la familia de instancias optimizadas para computación, el tamaño debe ser como mínimo 2xlarge.

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

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

- 16 GiB de RAM reservados para puertas de enlace con un tamaño de caché de hasta 16 TiB
- 32 GiB de RAM reservados para puertas de enlace con un tamaño de caché de 16 TiB a 32 TiB
- 48 GiB de RAM reservados para puertas de enlace con un tamaño de caché de 32 TiB a 64 TiB

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

. Recomendado para volúmenes en caché

- Familia de instancias de uso general: tipo de instancia m4, m5 o m6.
- Familia de instancias optimizada para la informática: tipos de instancias c4, c5, c6 o c7. Seleccione el tamaño de instancia 2xlarge o superior para cumplir los requisitos de RAM necesarios.
- Familia de instancias optimizada para memoria: tipos de instancias r3, r5, r6 o r7.
- Familia de instancias optimizada para el almacenamiento: tipos de instancias i3, i4 o i7.

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
Puerta de enlace de volumen en caché	150 GiB	64 TiB	150 GiB	2 TiB	—
Puerta de enlace de volumen almacenado	—	—	150 GiB	2 TiB	1 o más para el volumen o los volúmenes almacenados

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

Para poder implementar y operar correctamente, Volume Gateway requiere que puertos específicos pasen a través de la seguridad de la red. Algunos puertos son necesarios para todas las puertas de enlace, mientras que otros solo son necesarios para configuraciones específicas, como cuando se conecta a puntos finales de VPC.

Requisitos de puerto para Gateway Volume Gateway

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

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

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

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

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

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

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

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

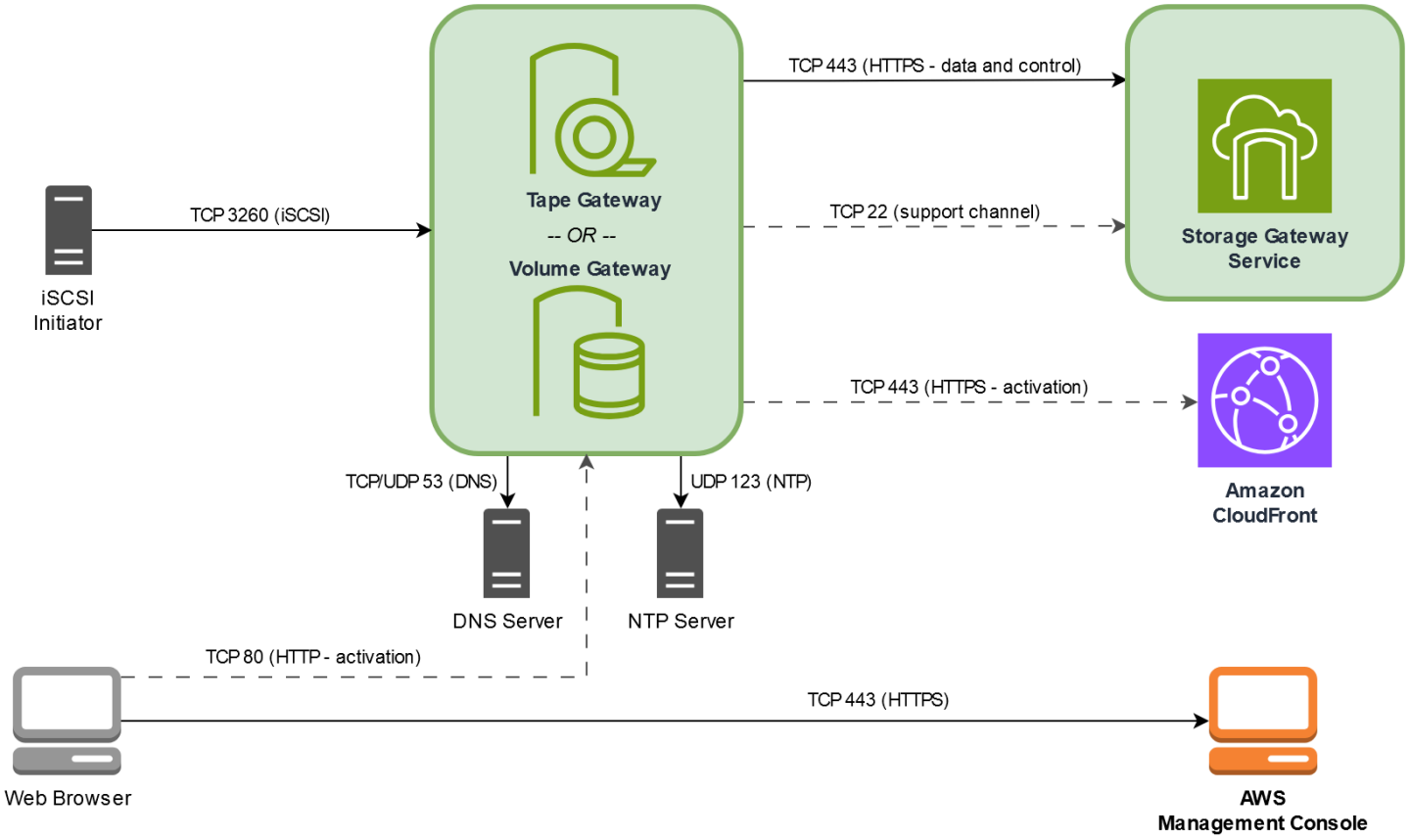
Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
VPC	VM de Storage Gateway	AWS	TCP HTTPS	443	✓	✓	✓*	Control de administración *Necesario solo cuando se utilizan puntos finales de VPC
VPC	VM de Storage Gateway	AWS	TCP HTTPS	1026		✓	✓*	Punto final del plano de control *Necesario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

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

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
VPC	VM de Storage Gateway	AWS	TCP HTTPS	1031		✓	✓*	Plano de datos *Necesario solo cuando se utilizan puntos finales de VPC
VPC	VM de Storage Gateway	AWS	TCP HTTPS	2222		✓	✓*	Canal de soporte SSH para VPCe *Necesario solo para abrir un canal de soporte cuando se utilizan puntos finales de VPC

Elemento de red	De	Para	Protocolo	Puerto	Entrada	Salida	Obligatorio	Notas
VPC	VM de Storage Gateway	AWS	TCP HTTPS	443	✓	✓	✓*	Control de administración *Necesario solo cuando se utilizan puntos finales de VPC
Cliente iSCSI	Cliente iSCSI	VM de Storage Gateway	TCP	3260	✓	✓	✓	Para que los sistemas locales se conecten a los destinos iSCSI expuestos por la puerta de enlace.

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



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

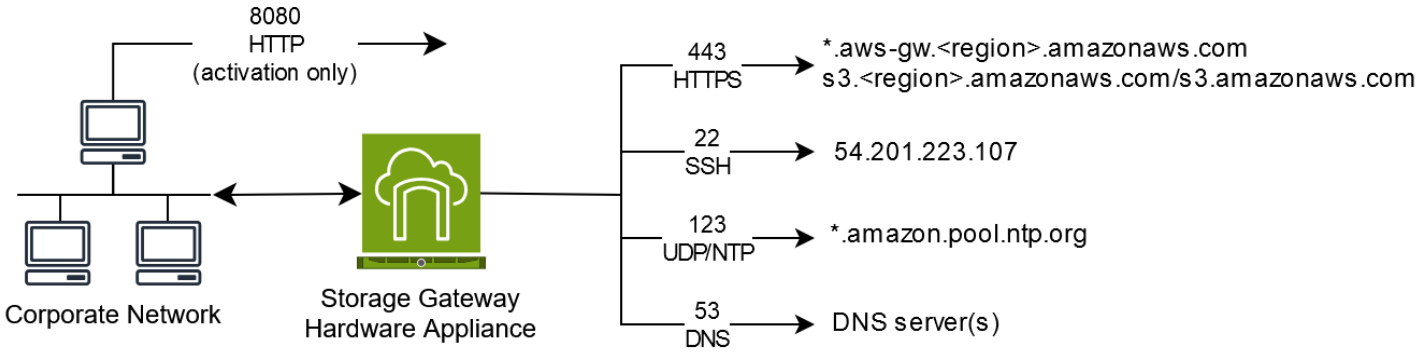
Cada dispositivo de hardware de Storage Gateway requiere los siguientes servicios de red:

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

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

1. iDRAC
2. em1
3. em2
4. em3
5. em4

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



Un dispositivo de hardware requiere los siguientes puertos para funcionar.

Protocolo	Puerto	Dirección	Origen	Destino	Cómo se utiliza
SSH	22	Salida	Dispositivo de hardware	`54.201.223.107`	canal de soporte
DNS	53	Salida	Dispositivo de hardware	Servidores DNS	Resolución de nombres
UDP/NTP	123	Salida	Dispositivo de hardware	`*.amazon.pool.ntp.org`	Sincronización horaria
HTTPS	443	Salida	Dispositivo de hardware	`*.amazonaws.com`	Transferencia de datos

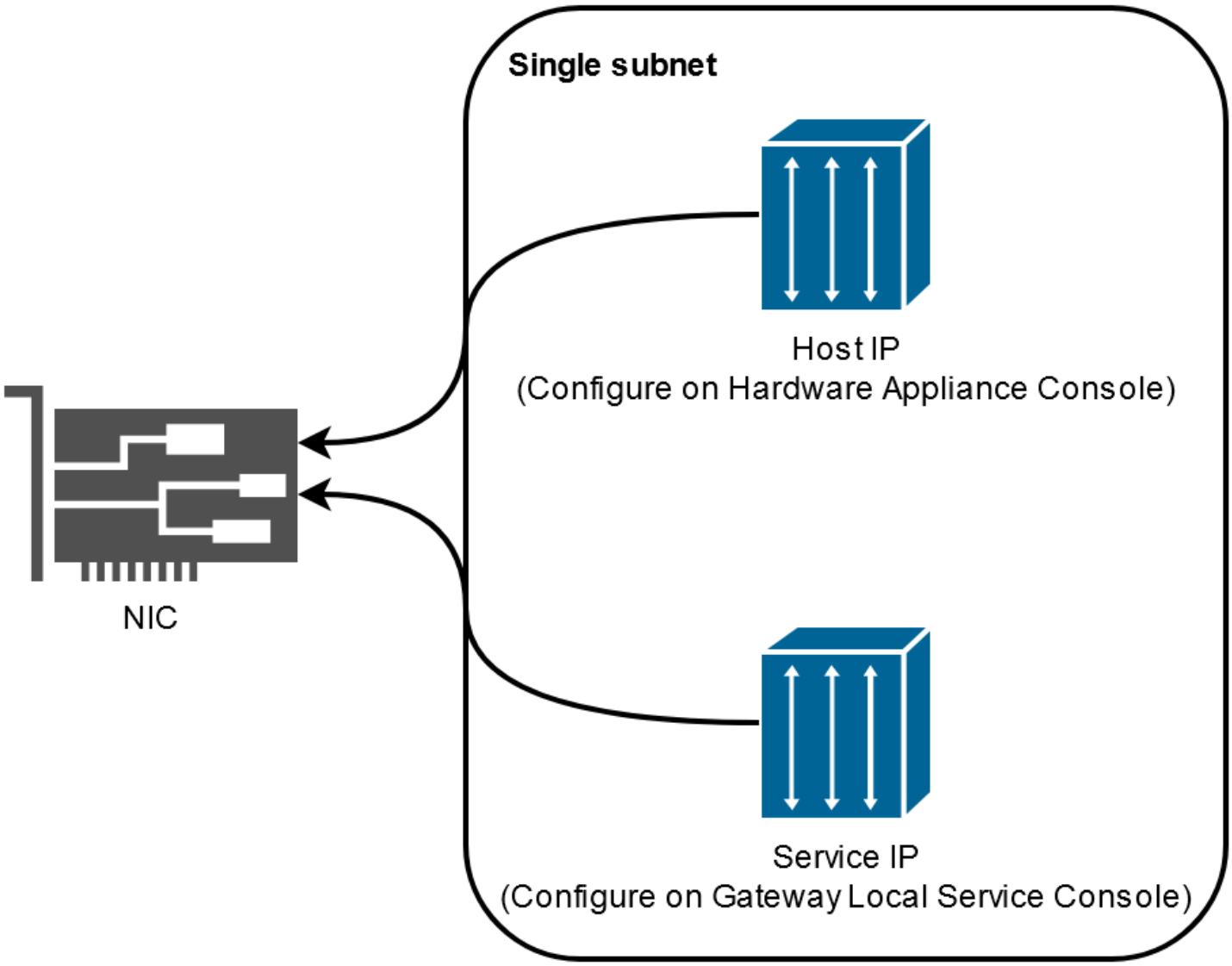
Protocolo	Puerto	Dirección	Origen	Destino	Cómo se utiliza
HTTP	8080	Entrada	AWS	Dispositivo de hardware	Activación (solo brevemente)

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

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

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

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



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

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

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

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

> **Important**
>
> Según la AWS región de la puerta de enlace, sustituya *region* el extremo del servicio por la cadena de región correcta.

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
```

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

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

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

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

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

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

- Storage Gateway: para 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 necesita permitir que se conecten instancias con la gateway desde el exterior de su grupo de seguridad, le recomendamos que solo permita conexiones en los puertos 3260 (para conexiones iSCSI) y 80 (para la activación).
- Si quieres activar tu puerta de enlace desde un EC2 host de Amazon ajeno al grupo de seguridad de la puerta de enlace, permite las conexiones entrantes en el puerto 80 desde la dirección IP de ese host. Si no puede determinar la dirección IP del host de activación, puede abrir el puerto 80, activar la gateway y, a continuación, cerrar el acceso en el puerto 80 tras completar la activación.
- Permita el acceso al puerto 22 solo si lo utiliza Soporte para solucionar problemas. Para obtener más información, consulte ¿Desea ayudar Soporte a solucionar los problemas de su puerta de enlace EC2 .

En algunos casos, puede utilizar una EC2 instancia de Amazon como iniciador (es decir, para conectarse a destinos iSCSI en una puerta de enlace que haya implementado en Amazon). EC2 En tal caso, se recomienda un enfoque de dos pasos:

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

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

Hipervisores compatibles y requisitos de host

Puede ejecutar Storage Gateway de forma local 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 cliente VMware vSphere para conectarse al host.
- Microsoft Hyper-V Hypervisor (2012 R2, 2016, 2019 o 2022): hay una versión gratuita independiente de Hyper-V disponible en el Centro de descarga de Microsoft. Para esta configuración, necesitará Microsoft Hyper-V Manager en un equipo cliente Microsoft Windows para conectarse al host.
- Máquina virtual basada en el kernel (KVM) de Linux: tecnología de virtualización gratuita y de código abierto. KVM está incluida en todas las versiones de Linux 2.6.20 y posteriores. Storage Gateway se ha probado y es compatible con las distribuciones CentOS/RHEL 7.7, Ubuntu 16.04 LTS y Ubuntu 18.04 LTS. Cualquier otra distribución moderna de Linux puede funcionar, pero la funcionalidad o el rendimiento no están garantizados. Recomendamos esta opción si ya tiene un entorno KVM en funcionamiento y ya está familiarizado con el funcionamiento de KVM.
- 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, consulteImplemente una EC2 instancia de Amazon personalizada para Volume 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 su Amazon EC2 AMI. Si la MV de la gateway no funciona correctamente, active una nueva gateway y recupere los datos para esa gateway. Para obtener más información, consulte Recuperación de un cierre inesperado de una máquina virtual.
> Storage Gateway no es compatible con la memoria dinámica ni con la asignación dinámica (ballooning) de memoria virtual.

Iniciadores iSCSI compatibles

Al implementar una puerta de enlace de volumen almacenado o en caché, puede crear volúmenes de almacenamiento iSCSI en la puerta de enlace.

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

- Microsoft Windows Server 2022
- Red Hat Enterprise Linux 8
- Red Hat Enterprise Linux 9
- VMware ESX Initiator, que ofrece una alternativa al uso de iniciadores en los sistemas operativos invitados de su VMs

> **Important**
>
> Storage Gateway no es compatible con Microsoft Multipath I/O (MPIO) desde clientes Windows.
> Storage Gateway permite conectar varios hosts al mismo volumen si los hosts coordinan el acceso mediante Clústeres de conmutación por error de Windows Server (WSFC). Sin embargo, no se pueden conectar varios hosts a ese mismo volumen (por ejemplo, compartir un sistema de archivos NTFS/ext4 no en clúster) sin usar WSFC.

Uso del dispositivo de hardware de Storage Gateway

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

El 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 gestionar los dispositivos de hardware de su implementación desde la página de información general sobre los dispositivos de hardware de la AWS Storage Gateway consola.

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

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

En las secciones siguientes, puede encontrar instrucciones sobre cómo instalar, montar un bastidor, activar, configurar, lanzar, usar y eliminar un dispositivo de hardware de Storage Gateway.

Temas

- Configuración de los parámetros de red del dispositivo de hardware
- Activación del dispositivo de hardware de Storage Gateway
- Creación de una puerta de enlace en el dispositivo de hardware
- Configuración de una dirección IP de puerta de enlace en el dispositivo de hardware
- Eliminación del software de puerta de enlace del dispositivo de hardware
- Eliminación del dispositivo de hardware de Storage Gateway

Configuración del dispositivo de hardware de Storage Gateway

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

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

Para instalar y configurar su dispositivo de hardware

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

4. Cree una puerta de enlace en el dispositivo de hardware. Para obtener más información, consulte Creación de una gateway de volumen.

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

Como aumentar el almacenamiento en caché utilizable

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

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

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

Opciones de tarjeta interfaz de red

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

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

Instalación física del dispositivo de hardware

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

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

Requisitos previos

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

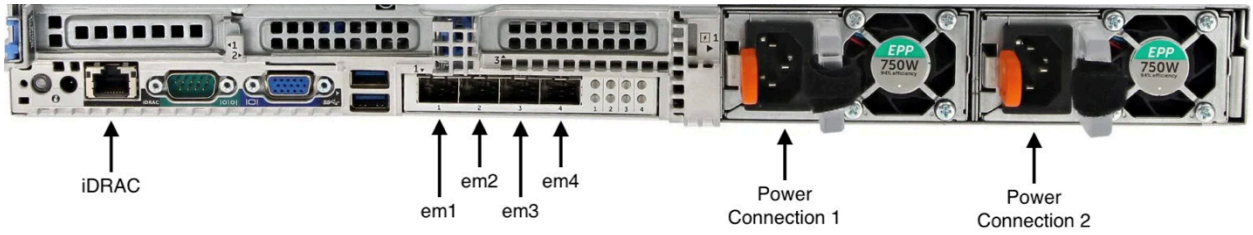
- Cables de alimentación: se necesita uno pero se recomienda tener dos.
- Cableado de red compatible (según la tarjeta de interfaz de red [NIC] que se incluya en el dispositivo de hardware). DAC de cobre Twinax, módulo óptico SFP+ (compatible con Intel) o transceptor de cobre SFP a Base-T.
- Un teclado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

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

Instalación física del dispositivo de hardware

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

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

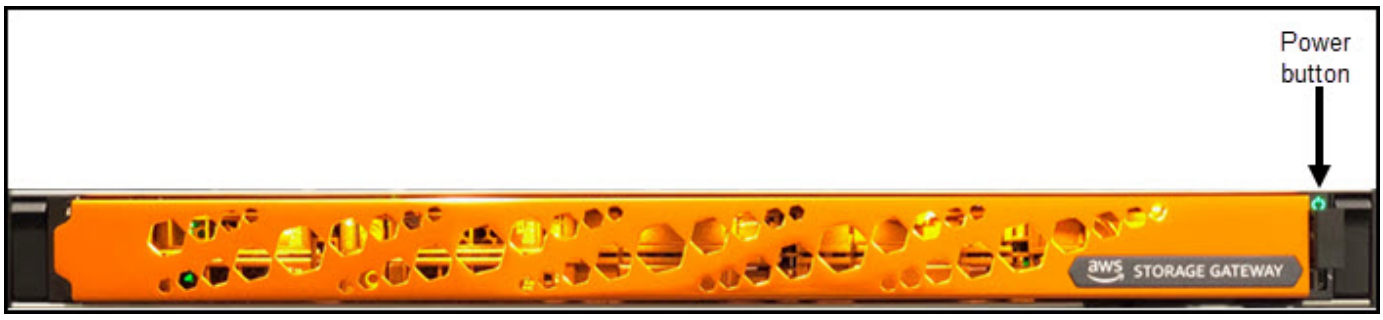


una parte trasera del dispositivo de hardware con etiquetas de conectores de red y alimentación.

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

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

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



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

Paso siguiente

[Acceso a la consola del dispositivo de hardware]

Acceso a la consola del dispositivo de hardware

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

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

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

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

Establecimiento de una contraseña de administrador

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

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

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

Paso siguiente

Configuración de los parámetros de red del dispositivo de hardware

Configuración de los parámetros de red del dispositivo de hardware

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

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

Para establecer una dirección de red

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

2. Para la interfaz em1, realice una de las acciones siguientes:

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

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

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

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

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

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

Para cerrar sesión en la consola de hardware

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

Paso siguiente

[Activación del dispositivo de hardware de Storage Gateway]

Activación del dispositivo de hardware de Storage Gateway

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

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

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

Para activar 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.
   > - Su firewall debe permitir el acceso HTTP al puerto 8080 del dispositivo para el tráfico de entrada.

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

Para obtener más información sobre la configuración de la dirección IP, consulte Configuración de parámetros de red.

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

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

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

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

Paso siguiente

Creación de una puerta de enlace en el dispositivo de hardware

Creación de una puerta de enlace en el dispositivo de hardware

> **Note**
>
> Aviso de fin de disponibilidad: a partir del 12 de mayo de 2025, el dispositivo de AWS Storage Gateway hardware dejará de estar disponible. Los clientes actuales que dispongan del dispositivo de AWS Storage Gateway hardware pueden seguir utilizándolo y recibiendo asistencia hasta mayo de 2028. Como alternativa, puede utilizar el AWS Storage Gateway

servicio para ofrecer a sus aplicaciones un acceso local y en la nube a un almacenamiento en la nube prácticamente ilimitado.

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

Para crear una puerta de enlace en su dispositivo de hardware

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

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

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

Paso siguiente

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

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

> **Note**
>
> Aviso de fin de disponibilidad: a partir del 12 de mayo de 2025, el dispositivo de AWS Storage Gateway hardware dejará de estar disponible. Los clientes actuales que dispongan del dispositivo de AWS Storage Gateway hardware pueden seguir utilizándolo y recibiendo asistencia hasta mayo de 2028. Como alternativa, puede utilizar el AWS Storage Gateway

servicio para ofrecer a sus aplicaciones un acceso local y en la nube a un almacenamiento en la nube prácticamente ilimitado.

Antes de activar el dispositivo de hardware, asignó una dirección IP a su interfaz de red física. Ahora que ha activado el dispositivo e iniciado el Storage Gateway en él, debe asignar otra dirección IP a la máquina virtual de Storage Gateway que se ejecuta en el dispositivo de hardware. Para asignar una dirección IP estática a una puerta de enlace instalada en el dispositivo de hardware, configure la dirección IP desde la consola local de la puerta de enlace para esa puerta de enlace. Las aplicaciones (como los clientes de NFS o SMB) se conectan a esta dirección IP. Puede acceder a la consola local de la puerta de enlace desde la consola del dispositivo de hardware con la opción Abrir consola de servicio.

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

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

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

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

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

   - Configuración de un proxy SOCKS o HTTP
   - Configuración de red

- Prueba de la conectividad de red
- Vista de una comprobación de recursos del sistema
- Administración de la hora del sistema
- Información sobre licencias
- Símbolo del sistema

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

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

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

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

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

Para salir de la consola local de la gateway

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

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

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

Eliminación del software de puerta de enlace del dispositivo de hardware

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

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

Eliminar una gateway de un dispositivo de hardware

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

Aparece el cuadro de diálogo de confirmación.

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

> **Note**
>
> Después de eliminar el software de la puerta de enlace, no podrá deshacer la acción. En determinados tipos de gateway, puede perder datos tras su eliminación, sobre todo datos almacenados. Para obtener más información sobre la eliminación de una gateway, consulte Eliminación de la puerta de enlace y eliminación de los recursos asociados.

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

Eliminación del dispositivo de hardware de Storage Gateway

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

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

> **Note**
>
> Para mover el dispositivo a una AWS cuenta diferente o Región de AWS, primero debe eliminarlo mediante el siguiente procedimiento y, a continuación, abrir el canal de soporte y el contacto de la puerta de enlace Soporte para realizar un restablecimiento parcial. Para

obtener más información, consulte activar el Soporte acceso para ayudar a solucionar los problemas de la puerta de enlace alojada en las instalaciones.

Para eliminar el dispositivo de hardware

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

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

Creación de la puerta de enlace

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

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

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

Descripción general: activación de una puerta de enlace

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

Configuración de una puerta de enlace

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

Connect to AWS

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

Revisión y activación

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

Descripción general: configuración de la puerta de enlace

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

Descripción general: recursos de almacenamiento

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

Creación de una gateway de volumen

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

Temas

Configuración de una puerta de enlace de volumen

Para configurar una nueva puerta de enlace de volumen

1. Abre AWS Management Console at https://console.aws.amazon.com/storagegateway/home/ y elige Región de AWS dónde 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 volumen y, a continuación, elija el tipo de volumen que usará su puerta de enlace. Puede elegir entre las siguientes opciones:

    - Volúmenes en memoria caché: almacena sus datos principales en Amazon S3 y conserva los datos a los que se accede con frecuencia de forma local en la memoria caché para un acceso más rápido.
    - Volúmenes almacenados: almacena todos los datos de forma local y, al mismo tiempo, realiza copias de seguridad de los estos de forma asíncrona en Amazon S3. Las pasarelas que utilizan este tipo de volumen no se pueden implementar en Amazon EC2.

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:

      - VMware ESXi- Descargue, implemente y configure la máquina virtual de puerta de enlace mediante VMware ESXi.
      - Microsoft Hyper-V: descargue, implemente y configure la máquina virtual de puerta de enlace mediante Microsoft Hyper-V.
      - Linux KVM: descargue, implemente y configure la máquina virtual de puerta de enlace mediante Linux KVM.
      - 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. 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 Volume Gateway a AWS.

Conexión de la puerta de enlace de volumen a AWS

Para conectar un nuevo Volume Gateway a AWS

1. Complete el procedimiento que se describe en Configuración de una puerta de enlace de volumen 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, marque la casilla de verificación del Punto de conexión habilitado para el Estándar federal de procesamiento de información (FIPS) para especificar si la conexión debe cumplir los estándares federales de procesamiento de información (FIPS).

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

- Alojada en la VPC: la puerta de enlace se comunica con AWS a través de una conexión privada, lo que le permite controlar la configuración de la red. Si selecciona esta opción, debe especificar un punto de conexión de VPC existente; para ello, elija su ID de punto de conexión de VPC en el menú desplegable o proporcione el nombre de DNS o la dirección IP de su punto de conexión de VPC.

3. En la sección Opciones de conexión de puerta de enlace, en Opciones de conexión, elija cómo identificar la puerta de enlace en AWS. Puede elegir entre las siguientes opciones:

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

     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 volumen.

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

Para activar una nueva puerta de enlace de volumen

1. Complete los procedimientos que se describen en los siguientes temas si aún no lo ha hecho:

   - Configuración de una puerta de enlace de volumen
   - Conecta tu Volume 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 crear 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 volumen.

Configuración de la puerta de enlace de volumen

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

1. Complete los procedimientos que se describen en los siguientes temas si aún no lo ha hecho:

   - Configuración de una puerta de enlace de volumen
   - Conecta tu Volume Gateway a AWS

- Revisión de la configuración y activación de la puerta de enlace de volumen

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 para ALMACENAMIENTO EN CACHÉ y al menos un disco con una capacidad mínima de 150 GiB para BÚFER DE CARGA. 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. *highlighted section*Sustitúyala por la información ResourceArn del grupo de registros específico para su implementación.

```
"Sid": "AWSLogDeliveryWrite20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "delivery.logs.amazonaws.com"
        ]
      },
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
```

```
        ],
        "Resource": "arn:aws:logs:eu-west-1:1234567890:log-group:/foo/bar:log-
stream:*"
```

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

4. En la sección de CloudWatch alarmas, elige cómo configurar 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. Selecciona Crear alarma para definir las métricas y especificar las acciones de alarma en la CloudWatch consola de Amazon. Para obtener instrucciones, consulta Uso de CloudWatch alarmas de Amazon en la Guía del CloudWatch usuario de Amazon.
   - Sin alarma: no reciba CloudWatch notificaciones sobre las métricas de su pasarela.

5. (Opcional) En la sección Etiquetas, 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 un volumen para utilizarla. Para obtener instrucciones, consulte Creación de un volumen.

Creación de un volumen de almacenamiento

Anteriormente, ha asignado discos locales que agregó al almacenamiento en caché de la máquina virtual (VM) y al búfer de carga. Ahora, cree un volumen de almacenamiento en el que sus aplicaciones puedan leer y escribir datos. La puerta de enlace mantiene los datos del volumen a los que se ha tenido acceso recientemente en el almacenamiento en caché local y trasfiere los datos de forma asincrónica a Amazon S3. Para los volúmenes almacenados, ha asignado discos locales que agregó al búfer de carga de la máquina virtual y a los datos de la aplicación.

> **Note**
>
> Puede usar AWS Key Management Service (AWS KMS) para cifrar los datos escritos en un volumen en caché almacenado en Amazon S3. Actualmente, puede hacerlo mediante la Referencia de la API de AWS Storage Gateway . Para obtener más información, consulte CreateCachediSCSIVolume o create-cached-iscsi-volume.

Para crear un volumen

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. En la consola de Storage Gateway, elija Crear volumen.
3. En el cuadro de diálogo Create volume, elija una gateway en Gateway.
4. En el caso de los volúmenes en caché, introduzca la capacidad en Capacidad.

   Para los volúmenes almacenados, seleccione un valor de Disk ID de la lista.
5. En Contenido del volumen, su elección depende del tipo de puerta de enlace para la que vaya a crear el volumen.

   En el caso de los volúmenes en caché, dispone de las siguientes opciones:

- Create a new empty volume.
- Crear un volumen basado en una instantánea de Amazon EBS. Si elige esta opción, proporcione un valor para EBS snapshot ID.

> **Note**
>
> Storage Gateway no admite la creación de volúmenes en caché a partir de instantáneas de volúmenes de AWS Marketplace .

- Clone from last volume recovery point. Si elige esta opción, elija un ID de volumen para Source volume. Si no hay volúmenes en la región, esta opción no se muestra.

En el caso de los volúmenes almacenados, dispone de las siguientes opciones:

- Create a new empty volume.
- Create a volume based on a snapshot. Si elige esta opción, proporcione un valor para EBS snapshot ID.
- Preserve existing data on the disk.

6. Escriba el nombre para el Nombre de destino iSCSI.

   El nombre de destino puede contener minúsculas, números, puntos (.) y guiones (-). Este nombre de destino aparece como nombre de iSCSI target node en la pestaña Targets de la interfaz de usuario de iSCSI Microsoft initiator después de la detección. Por ejemplo, el nombre `target1` aparece como `iqn.1007-05.com.amazon:target1`. Asegúrese de que el nombre de destino sea globalmente exclusivo dentro de la red de área de almacenamiento (SAN).

7. Compruebe que en Network interface esté seleccionada la dirección IP o elija una dirección IP para la Network interface. En Network interface, aparece una dirección IP para cada adaptador configurado para la máquina virtual de la gateway. Si la máquina virtual de la gateway está configurada para un solo adaptador de red, no aparecerá ninguna lista de Network interface porque solo habrá una dirección IP.

   El destino de iSCSI estará disponible en el adaptador de red que elija.

   Si ha definido la gateway para que utilice varios adaptadores de red, elija la dirección IP que las aplicaciones de almacenamiento deben usar para obtener acceso al volumen. Para obtener más

información acerca de cómo configurar varios adaptadores de red, consulte Configuración de su puerta de enlace para varios NICs.

> **Note**
>
> Después de elegir un adaptador de red, no puede cambiar esta configuración.

8. (Opcional) En Tags (Etiquetas), introduzca una clave y un valor para añadir una etiqueta al volumen. Una etiqueta es un par clave-valor que distingue entre mayúsculas y minúsculas y que le ayuda a administrar, filtrar y buscar volúmenes.
9. Seleccione Create volume (Crear volumen).

   Si ha creado volúmenes en esta región anteriormente, aparecerán listados en la consola de Storage Gateway.

   Aparecerá el cuadro de diálogo Configure CHAP Authentication (Configurar la autenticación CHAP). En este punto, puede configurar el protocolo CHAP (Challenge-Handshake Authentication Protocol) para el volumen o puede elegir Cancelar y configurar el CHAP más tarde. Para obtener más información sobre la configuración de CHAP, consulte Configuración de la autenticación CHAP para los volúmenes.

Si no desea configurar CHAP, empiece a utilizar su volumen. Para obtener más información, consulte Conexión de los volúmenes al cliente.

Configuración de la autenticación CHAP para los volúmenes

El protocolo CHAP ofrece protección contra ataques que requieren autenticación para el acceso a los destinos de los volúmenes de almacenamiento. En el cuadro de diálogo Configure CHAP Authentication, proporcione la información para configurar CHAP para sus volúmenes.

Para configurar CHAP

1. Seleccione el volumen para el que quiere configurar CHAP.
2. En Actions, elija Configure CHAP authentication.
3. En Nombre del iniciador, introduzca el nombre del iniciador.
4. En Secreto del iniciador, introduzca la frase secreta que usó para autenticar el iniciador de iSCSI.

5. En Secreto del destino, introduzca la frase secreta que usó para autenticar el destino para el protocolo CHAP mutuo.
6. Elija Save para guardar las entradas.

   Para obtener más información acerca de la autenticación CHAP, consulte Configuración de la autenticación CHAP para los destinos iSCSI.

Paso siguiente

Conexión de los volúmenes al cliente

Conexión de los volúmenes al cliente

Puede utilizar el iniciador iSCSI del cliente para conectarse a los volúmenes. Al final del siguiente procedimiento, los volúmenes pasan a estar disponibles como dispositivos locales en el cliente.

> **Important**
>
> Con Storage Gateway, puede conectar varios hosts al mismo volumen si los hosts coordinan el acceso mediante Clústeres de conmutación por error de Windows Server (WSFC). No puede conectar varios hosts al mismo volumen sin usar WSFC (por ejemplo, compartir un sistema de archivos NTFS/ext4 no en clúster).

Temas

- Conexión a un cliente Microsoft Windows
- Conexión a un cliente Red Hat Enterprise 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 obtener más información, consulte Conexión de iniciadores iSCSI.

Para conectarse a un cliente de Windows

1. Inicie iscsicpl.exe.

2. En el cuadro de diálogo iSCSI Initiator Properties (Propiedades del iniciador ISCSI), elija la pestaña Discovery (Detección) y, a continuación, elija Discovery Portal (Portal de detección).
3. En el cuadro de diálogo Discover Target Portal (Portal de destino de detección), escriba la dirección IP del destino iSCSI para la dirección IP o el nombre de DNS.
4. Conecte el nuevo portal de destino al destino del volumen de almacenamiento en la gateway.
5. Seleccione el destino y, a continuación, elija Connect (Conectar).
6. En la pestaña Targets (Destinos), asegúrese de que el estado del destino tenga el valor Connected (Conectado), que indica que el destino se encuentra conectado, y elija OK (Aceptar).

Conexión a un cliente Red Hat Enterprise Linux

El siguiente procedimiento muestra un resumen de los pasos que deberá seguir para conectarse a un cliente Red Hat Enterprise Linux (RHEL). Para obtener más información, consulte Conexión de iniciadores iSCSI.

Para conectar un cliente Linux a destinos iSCSI

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

   Puede utilizar el comando siguiente para instalar el paquete.

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

2. Asegúrese de que el daemon iSCSI se encuentre en ejecución.

   Para RHEL 5 o 6, utilice el comando siguiente.

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

   Para RHEL 7, 8 o 9, utilice el comando siguiente.

   ```
   sudo service iscsid status
   ```

3. Detecte los objetivos de dispositivo VTL o de volumen definidos para una gateway. 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 IQN correcto `[GATEWAY_IP]` y el 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
   ```

   Tras configurar el iniciador, es muy recomendable que personalice la configuración de iSCSI como se explica en Personalización de la configuración de iSCSI de Linux.

Inicialización y formateo del volumen

Después de utilizar el iniciador iSCSI en su cliente para conectarse a los volúmenes, inicialice y formatee su volumen.

Temas

- Inicialización y formateo del volumen en Microsoft Windows
- Inicialización y formateo del volumen en Red Hat Enterprise Linux

Inicialización y formateo del volumen en Microsoft Windows

Utilice el siguiente procedimiento para inicializar y formatear su volumen en Windows.

Para inicializar y formatear su volumen de almacenamiento

1. Inicie **`diskmgmt.msc`** para abrir la consola Disk Management.
2. En el cuadro de diálogo Initialize Disk, inicialice el volumen como una partición MBR (Master Boot Record). Al seleccionar el estilo de partición, debe tener en cuenta el tipo de volumen al que está conectado (en caché o almacenado), como se muestra en la siguiente tabla.

Estilo de partición	Condiciones en que se utiliza
MBR (Master Boot Record)	• Si la gateway es un volumen almacenado y su tamaño de almacenamiento está limitado a 1 TiB. • Si la gateway es un volumen en caché y su tamaño de almacenamiento es inferior a 2 TiB.
GPT (GUID Partition Table)	Si el volumen de almacenamiento de la gateway tiene un tamaño de 2 TiB o más.

3. Cree un volumen simple:
   a. Ponga en línea el volumen para inicializarlo. Todos los volúmenes disponibles se muestran en la consola de administración de discos.
   b. Abra el menú contextual (haga clic con el botón derecho) del disco y elija New Simple Volume.

      > **Important**
      >
      > Tenga cuidado de no formatear un disco incorrecto. Asegúrese de que el tamaño del disco que va a formatear coincida con el tamaño del disco local que ha asignado a la máquina virtual de gateway y de que su estado sea Unallocated.

   c. Especifique el tamaño máximo de disco.
   d. Asigne una ruta o letra de unidad al volumen y formatéelo eligiendo Perform a quick format.

> **Important**
>
> Es absolutamente recomendable que use Perform a quick format para los volúmenes en caché. De esta forma, se reducirán las operaciones de E/S de inicialización, se reducirá el tamaño de la instantánea inicial y el volumen estará listo para su uso en menor tiempo. También evitará la utilización de espacio del volumen almacenado en caché para el proceso completo de formateo.

> **Note**
>
> El tiempo que se tarda en formatear el volumen depende del tamaño de este. El proceso puede tardar varios minutos en completarse.

Inicialización y formateo del volumen en Red Hat Enterprise Linux

Utilice el siguiente procedimiento para inicializar y formatear su volumen en Red Hat Enterprise Linux (RHEL).

Para inicializar y formatear su volumen de almacenamiento

1. Cambie el directorio a la carpeta `/dev`.
2. Ejecute el comando `sudo cfdisk`.
3. Identifique el nuevo volumen con el comando siguiente. Para buscar nuevos volúmenes, muestre el diseño de la partición de los volúmenes.

   ```
   $ lsblk
   ```

   Se muestra un error de "etiqueta de volumen no reconocida" para el nuevo volumen sin particionar.
4. Inicialice el nuevo volumen. Cuando seleccione el estilo de partición, debe tener en cuenta el tamaño y el tipo de volumen al que se va a conectar (en caché o almacenado), como se muestra en la siguiente tabla.

Estilo de partición	Condiciones en que se utiliza
MBR (Master Boot Record)	• Si la gateway es un volumen almacenado y su tamaño de almacenamiento está limitado a 1 TiB. • Si la gateway es un volumen en caché y su tamaño de almacenamiento es inferior a 2 TiB.
GPT (GUID Partition Table)	Si el volumen de almacenamiento de la gateway tiene un tamaño de 2 TiB o más.

Para una partición MBR, utilice el siguiente comando: `sudo parted /dev/your volume mklabel msdos`

Para una partición GPT, utilice el siguiente comando: `sudo parted /dev/your volume mklabel gpt`

5. Cree una partición con el siguiente comando.

   ```
   sudo parted -a opt /dev/your volume mkpart primary file system 0% 100%
   ```

6. Asigne una letra de unidad a la partición y cree un sistema de archivos con el siguiente comando.

   ```
   sudo mkfs -L datapartition /dev/your volume
   ```

7. Monte el sistema de archivos con el siguiente comando.

   ```
   sudo mount -o defaults /dev/your volume /mnt/your directory
   ```

Prueba de la puerta de enlace

Para probar la configuración de la puerta de enlace de volumen, realice las siguientes tareas:

1. Escriba datos en el volumen.
2. Realice una instantánea.
3. Restaure la instantánea en otro volumen.

Para verificar la configuración de una puerta de enlace, haga una copia de seguridad instantánea del volumen y almacene la instantánea en ella AWS. A continuación, restaure la instantánea en un nuevo volumen. La puerta de enlace copia los datos de la instantánea especificada en AWS el nuevo volumen.

> **Note**
>
> No se admite la restauración de datos de volúmenes de Amazon Elastic Block Store (Amazon EBS) que estén cifrados.

Para crear una instantánea de Amazon EBS de un volumen de almacenamiento en Microsoft Windows

1. En el equipo Windows, copie datos en el volumen de almacenamiento asignado.

   La cantidad de datos copiados no es importante para esta demostración. Un archivo pequeño es suficiente para demostrar el proceso de restauración.
2. En el panel de navegación de la consola de Storage Gateway, elija Volúmenes.
3. Seleccione el volumen de almacenamiento que ha creado para la gateway.

   Esta gateway solo debe tener un volumen de almacenamiento. Al seleccionar el volumen se muestran sus propiedades.
4. En Actions (Acciones), elija Create EBS snapshot (Crear instantánea de EBS) para crear una instantánea del volumen.

   Dependiendo de la cantidad de datos del disco y del ancho de banda de carga, es posible que tarde unos segundos en completar la instantánea. Tenga en cuenta que el ID del volumen desde el que se crea una instantánea. Utilizará el ID para encontrar la instantánea.
5. En el cuadro de diálogo Create EBS Snapshot (Crear instantánea de EBS), proporcione una descripción de la instantánea.
6. (Opcional) En Tags (Etiquetas), escriba una clave y un valor para añadir una etiqueta a la instantánea. Una etiqueta es un par clave-valor que distingue entre mayúsculas y minúsculas y que le ayuda a administrar, filtrar y buscar instantáneas.
7. Elija Create Snapshot (Crear instantánea). La instantánea se almacena como una instantánea de Amazon EBS. Tome nota del ID de la instantánea. El número de instantáneas creadas para el volumen se muestra en la columna de instantáneas.

8. En la columna Instantáneas de EBS, elija el enlace del volumen para el que creó la instantánea para ver la instantánea de EBS en la consola de Amazon. EC2

Para restaurar una instantánea en otro volumen

Consulte Creación de un volumen de almacenamiento.

Realización de la copia de seguridad de los volúmenes

Al utilizar Storage Gateway, puede ayudar a proteger sus aplicaciones de negocio en las instalaciones que utilizan volúmenes de Storage Gateway para almacenamiento respaldado por la nube. Puede hacer copias de seguridad de los volúmenes de Storage Gateway en las instalaciones mediante el programador de instantáneas nativas en Storage Gateway o AWS Backup. En ambos casos, las copias de seguridad de los volúmenes de Storage Gateway se almacenan como instantáneas de Amazon EBS en Amazon Web Services.

Temas

- Uso de Storage Gateway para realizar copias de seguridad de los volúmenes
- Se usa AWS Backup para hacer copias de seguridad de sus volúmenes

Uso de Storage Gateway para realizar copias de seguridad de los volúmenes

Puede utilizar la consola de administración de Storage Gateway para realizar una copia de seguridad de los volúmenes realizando instantáneas de Amazon EBS y almacenando las instantáneas en Amazon Web Services. Puede realizar una instantánea única o configurar un programa de instantáneas administrado por Storage Gateway. Luego, puede restaurar la instantánea en un nuevo volumen mediante la consola de Storage Gateway. Para obtener información acerca de cómo hacer copias de seguridad y administrar su copia de seguridad a partir del Storage Gateway, consulte los siguientes temas:

- Prueba de la puerta de enlace
- Creación de una instantánea de recuperación
- Clonación de un volumen en caché desde un punto de recuperación

Se usa AWS Backup para hacer copias de seguridad de sus volúmenes

AWS Backup es un servicio de copia de seguridad centralizado que le permite realizar copias de seguridad de los datos de sus aplicaciones de forma sencilla y rentable en todos AWS los servicios, tanto en la nube de Amazon Web Services como en las instalaciones. De este modo, podrá cumplir con sus requisitos empresariales y normativos de conformidad con las copias de seguridad. AWS Backup simplifica la protección AWS de sus volúmenes de almacenamiento, bases de datos y sistemas de archivos al proporcionar un lugar central donde puede hacer lo siguiente:

- Configure y audite los AWS recursos de los que desea hacer una copia de seguridad.
- Automatizar la programación de copias de seguridad.
- Establecer políticas de retención.
- Monitorizar toda la actividad reciente de copias de seguridad y restauración.

Como Storage Gateway se integra con AWS Backup, permite AWS Backup a los clientes realizar copias de seguridad de las aplicaciones empresariales locales que utilizan volúmenes de Storage Gateway para el almacenamiento respaldado por la nube. AWS Backup admite la copia de seguridad y la restauración de volúmenes almacenados y en caché. Para obtener más información al respecto AWS Backup, consulte la AWS Backup documentación. Para obtener información al respecto AWS Backup, consulte ¿Qué es AWS Backup? en la Guía AWS Backup del usuario.

Puede administrar las operaciones de respaldo y recuperación de los volúmenes de Storage Gateway con scripts personalizados AWS Backup y evitar la necesidad de crear scripts personalizados o administrar point-in-time los respaldos manualmente. Con él AWS Backup, también puede supervisar sus copias de seguridad por volumen locales junto con sus AWS recursos en la nube desde un único panel de control. AWS Backup Puede utilizarla AWS Backup para crear una copia de seguridad única y bajo demanda o para definir un plan de copia de seguridad que se gestione de forma integrada. AWS Backup

Las copias de seguridad de volúmenes de Storage Gateway tomadas se AWS Backup almacenan en Amazon S3 como instantáneas de Amazon EBS. Puede ver las copias de seguridad de los volúmenes de Storage Gateway desde la AWS Backup consola o la consola de Amazon EBS.

Puede restaurar fácilmente los volúmenes de Storage Gateway que se administran AWS Backup a través de cualquier puerta de enlace local o puerta de enlace en la nube. También puede restaurar dicho volumen en un volumen de Amazon EBS que pueda usar con las EC2 instancias de Amazon.

Ventajas del uso AWS Backup para realizar copias de seguridad de los volúmenes de Storage Gateway

Las ventajas de utilizarlo AWS Backup para hacer copias de seguridad de los volúmenes de Storage Gateway son que puede cumplir con los requisitos de conformidad, evitar la carga operativa y centralizar la administración de las copias de seguridad. AWS Backup le permite hacer lo siguiente:

- Establecer políticas de copia de seguridad programadas personalizables que satisfacen los requisitos de copia de seguridad.
- Establezca reglas de retención y caducidad de las copias de seguridad para que ya no tenga que desarrollar scripts personalizados ni administrar manualmente las point-in-time copias de seguridad de sus volúmenes.
- Administre y supervise las copias de seguridad en múltiples puertas de enlace y otros AWS recursos desde una vista centralizada.

Para usar AWS Backup para crear copias de seguridad de sus volúmenes

> **Note**
>
> AWS Backup requiere que elija un rol AWS Identity and Access Management (de IAM) que AWS Backup consuma. Debe crear este rol porque AWS Backup no lo crea por usted. También debe crear una relación de confianza entre este rol de IAM AWS Backup y este. Para obtener información sobre cómo hacerlo, consulte la Guía del usuario de AWS Backup . Para obtener información acerca de cómo hacerlo, consulte Creación de un plan de copia de seguridad en la AWS Backup Guía del usuario de .

1. Abra la consola de Storage Gateway y elija Volúmenes desde el panel de navegación a la izquierda.
2. En Acciones, selecciona Crear copia de seguridad bajo demanda con AWS Backup o Crear un plan de AWS copia de seguridad.

   Si desea crear una copia de seguridad bajo demanda del volumen de Storage Gateway, elija Crear copia de seguridad bajo demanda con AWS Backup. Se le dirigirá a la AWS Backup consola.

   Si quieres crear un AWS Backup plan nuevo, selecciona Crear un plan AWS de respaldo. Se le dirigirá a la AWS Backup consola.

En la AWS Backup consola, puede crear un plan de respaldo, asignar un volumen de Storage Gateway al plan de respaldo y crear un respaldo. También puede hacer las tareas de administración de copia de seguridad en curso.

Búsqueda y restauración de los volúmenes desde AWS Backup

Puede buscar y restaurar los volúmenes de Storage Gateway de respaldo desde la AWS Backup consola. Para obtener más información, consulte la AWS Backup Guía del usuario de . Para obtener más información, consulte Puntos de recuperación en la Guía del usuario de AWS Backup .

Para buscar y restaurar los volúmenes

1. Abra la AWS Backup consola y busque la copia de seguridad del volumen de Storage Gateway que desee restaurar. Puede restaurar la copia de seguridad del volumen de Storage Gateway en un volumen de Amazon EBS o en un volumen de Storage Gateway. Elija la opción apropiada para sus requisitos de restauración.
2. En Tipo de restauración, elija restaurar un volumen de Storage Gateway almacenado o almacenado en caché y proporcione la información necesaria:
   - Para un volumen almacenado, facilite la información de Gateway name (Nombre de gateway), Disk ID (ID de disco) y iSCSI target name (Nombre de destino iSCSI).
   - Para un volumen almacenado en caché, facilite la información de Gateway name (Nombre de gateway), Capacity (Capacidad) y iSCSI target name (Nombre de destino iSCSI).
3. Elija Restore resource (Restaurar recurso) para restaurar el volumen.

> **Note**
>
> No puede usar la consola de Amazon EBS para eliminar una instantánea creada por AWS Backup.

¿Qué tengo que hacer ahora?

En las secciones anteriores, ha creado y aprovisionado una gateway y, a continuación, ha conectado el host Windows al volumen de almacenamiento de la gateway. Ha añadido datos al volumen iSCSI

de la gateway, ha tomado una instantánea del volumen y la ha restaurado en un nuevo volumen, se ha conectado al nuevo volumen y ha verificado que los datos se muestran en él.

Después de finalizar el ejercicio, tenga en cuenta lo siguiente:

- Si piensa seguir utilizando la gateway, lea lo relativo al ajuste del tamaño adecuado del búfer de carga para cargas de trabajo del mundo real. Para obtener más información, consulte Ajuste del tamaño de almacenamiento de la gateway de volúmenes para cargas de trabajo del mundo real.

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

- Para obtener más información sobre los volúmenes de almacenamiento y cómo administrarlos, consulte Administración de la gateway de volúmenes.
- Si no piensa seguir utilizando la gateway, considere la posibilidad de eliminar la gateway para evitar gastos. Para obtener más información, consulte Limpieza de recursos innecesarios.
- Para resolver problemas con la gateway, consulte Solución de problemas de la gateway.
- Para optimizar la gateway, consulte Optimizing Gateway Performance.
- Para obtener información sobre las métricas de Storage Gateway y cómo supervisar el rendimiento de la puerta de enlace, consulte Supervisión de Storage Gateway.
- Para obtener más información sobre la configuración de destinos iSCSI de la gateway para almacenar datos, consulte Conexión a los volúmenes de un cliente de Windows.

Para obtener más información sobre el tamaño de almacenamiento de la puerta de enlace de volumen para cargas de trabajo del mundo real y cómo limpiar los recursos que no necesita, consulte las secciones siguientes.

Ajuste del tamaño de almacenamiento de la gateway de volúmenes para cargas de trabajo del mundo real

En este momento, tiene una gateway sencilla y funcional. Sin embargo, los supuestos utilizados para crear esta gateway no son suficientes para cargas de trabajo del mundo real. Si desea utilizar esta gateway para cargas de trabajo del mundo real, debe hacer dos cosas:

1. Ajustar un tamaño suficiente para el búfer de carga.
2. Configure la monitorización del búfer de carga, si aún no lo ha hecho.

A continuación se muestra cómo realizar ambas tareas. Si ha activado una puerta de enlace para volúmenes en caché, también debe ajustar el tamaño del almacenamiento caché para cargas de trabajo del mundo real.

Para ajustar el tamaño del búfer de carga y el almacenamiento en caché para una configuración de gateway almacenada en caché

- Utilice la fórmula que se muestra en Determinación del tamaño que se va a asignar al búfer de carga para ajustar el tamaño del búfer de carga. Recomendamos encarecidamente que asigne al menos 150 GiB para el búfer de carga. Si la fórmula del búfer de carga genera un valor inferior a 150 GiB, utilice 150 GiB como búfer de carga asignado.

  La fórmula del búfer de carga tiene en cuenta la diferencia entre el rendimiento de la aplicación a la puerta de enlace y el rendimiento de la puerta de enlace a AWS, multiplicada por el tiempo que espera escribir los datos. Por ejemplo, supongamos que sus aplicaciones escriben texto en la gateway a una velocidad de 40 MB por segundo durante 12 horas al día y su rendimiento de red es de 12 MB por segundo. Suponiendo un factor de compresión de 2:1 para los datos de texto, la fórmula especifica que debe asignar aproximadamente 675 GiB de espacio de búfer de carga.

Para ajustar el tamaño del búfer de carga para una configuración almacenada

- Utilice la fórmula que se ha tratado en Determinación del tamaño que se va a asignar al búfer de carga. Recomendamos encarecidamente que asigne al menos 150 GiB para el búfer de carga. Si la fórmula del búfer de carga genera un valor inferior a 150 GiB, utilice 150 GiB como búfer de carga asignado.

  La fórmula del búfer de carga tiene en cuenta la diferencia entre el rendimiento de la aplicación a la puerta de enlace y el rendimiento de la puerta de enlace a la misma AWS, multiplicada por el tiempo que espera escribir los datos. Por ejemplo, supongamos que sus aplicaciones escriben texto en la gateway a una velocidad de 40 MB por segundo durante 12 horas al día y su rendimiento de red es de 12 MB por segundo. Suponiendo un factor de compresión de 2:1 para los datos de texto, la fórmula especifica que debe asignar aproximadamente 675 GiB de espacio de búfer de carga.

Para monitorizar el búfer de carga

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

2. Elija la pestaña Gateway, elija la pestaña Details (Detalles) y busque el campo Upload Buffer Used (Búfer de carga usado) para ver el búfer de carga actual de la gateway.
3. Establezca una o más alarmas para que le informen del uso del búfer de carga.

   Te recomendamos encarecidamente que crees una o más alarmas de búfer de carga en la CloudWatch consola de Amazon. Por ejemplo, puede establecer una alarma para un nivel de uso del que desee que se le avise y una alarma para un nivel de uso que, si se supera, provoque una acción. Las acciones podrían consistir en añadir más espacio de búfer de carga. Para obtener más información, consulte Para establecer una alarma de umbral superior para el búfer de carga de una gateway.

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

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

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

Temas

- Creación de un punto de conexión de VPC para Storage Gateway

Creación de un punto de conexión de VPC para Storage Gateway

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

Para crear un punto de conexión de VPC para Storage Gateway

1. Inicie sesión en la consola de Amazon VPC AWS Management Console y ábrala en. https://console.aws.amazon.com/vpc/
2. En el panel de navegación, elija Endpoints (Puntos de enlace) y, a continuación, elija Create Endpoint (Crear punto de enlace).
3. En la página Crear punto de conexión, elija Servicios de AWS en Categoría de servicio.
4. En Service Name (Nombre de servicio), seleccione `com.amazonaws.region.storagegateway`, Por ejemplo, `com.amazonaws.us-east-2.storagegateway`.
5. En VPC, elija su VPC y anote sus zonas de disponibilidad y subredes.
6. Compruebe que la opción Enable Private DNS Name (Habilitar nombre de DNS privado) no esté seleccionada.
7. En Security group (Grupo de seguridad), elija el grupo de seguridad que desea utilizar para su VPC. Puede aceptar el grupo de seguridad predeterminado. Compruebe que los siguientes puertos TCP están permitidos en su grupo de seguridad:
   - TCP 443
   - TCP 1026
   - TCP 1027
   - TCP 1028
   - TCP 1031
   - TCP 2222
8. Elija Crear punto de conexión. El estado inicial del punto de enlace espending (pendiente). Cuando se crea el punto de enlace, anote el ID del punto de enlace de la VPC que acaba de crear.
9. Cuando se cree el punto de enlace, elija Endpoints (Puntos de enlace) y, a continuación, elija el nuevo punto de enlace de la VPC.
10. En la pestaña Detalles del punto de conexión de Storage Gateway seleccionado, en Nombres de DNS, utilice el primer nombre de DNS que no especifique

una zona de disponibilidad. El nombre de la DNS tiene un aspecto similar a este: `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

Ahora que ha creado un punto de enlace de la VPC, puede crear su gateway. Para obtener más información, consulte Creación de una puerta de enlace.

Administración de la gateway de volúmenes

La administración de la puerta de enlace incluye tareas como la configuración del almacenamiento en caché y el espacio del búfer de carga, el trabajo con volúmenes y la realización el mantenimiento general. Si no ha creado una gateway, consulte Empezar con AWS Storage Gateway.

Los volúmenes en caché son volúmenes en Amazon Simple Storage Service (Amazon S3) expuestos como destinos iSCSI en los que puede almacenar los datos de la aplicación. Podrá encontrar información sobre cómo agregar y eliminar volúmenes para la configuración almacenada en caché. También puedes aprender a añadir y eliminar volúmenes de Amazon Elastic Block Store (Amazon EBS) en Amazon Gateways. EC2

> **Important**
>
> Si un volumen en caché mantiene los datos principales en Amazon S3, debe evitar procesos que lean o escriban todos los datos del volumen completo. Por ejemplo, no recomendamos utilizar software de detección de virus que explore todo el volumen almacenado en la memoria caché. Tal exploración, tanto si se hace bajo petición como de manera programada, hace que todos los datos almacenados en Amazon S3 se descarguen localmente para explorarlos, lo que provoca un uso elevado de ancho de banda. En lugar de realizar una exploración completa del disco, puede utilizar la detección de virus en tiempo real, es decir, explorar los datos a medida que se lean o se escriban en el volumen almacenado en caché.

El cambio de tamaño de un volumen no se admite. Para cambiar el tamaño de un volumen, cree una instantánea del volumen y, a continuación, cree un nuevo volumen almacenado en caché a partir de la instantánea. El nuevo volumen puede ser mayor que el volumen a partir del cual se creó la instantánea. Para ver pasos que describen cómo eliminar un volumen, consulte Para eliminar un volumen. Para ver pasos que describen cómo agregar un volumen y conservar datos existentes, consulte Eliminación de volúmenes de almacenamiento.

Todos los datos de volúmenes en caché y los datos de instantáneas almacenados se almacenan en Amazon S3 y se cifran en reposo mediante cifrado del servidor (SSE). Sin embargo, no puede obtener acceso a estos datos a través de la API de Amazon S3 u otras herramientas como, por ejemplo, la consola de administración de Amazon S3.

A continuación, puede encontrar información acerca de cómo administrar los recursos de Puerta de enlace de volumen.

Temas

- Edición de información básica de la puerta de enlace- Aprenda a usar la consola Storage Gateway para editar la información básica de una puerta de enlace existente, incluidos el nombre de la puerta de enlace, la zona horaria y el grupo de CloudWatch registros.
- Agregación y ampliación de volúmenes: obtenga información sobre cómo agregar más volúmenes a la puerta de enlace o ampliar el tamaño de los volúmenes existentes a medida que aumenten las necesidades de la aplicación.
- Clonación de un volumen en caché desde un punto de recuperación: obtenga información sobre cómo crear un volumen nuevo a partir del punto de recuperación de un volumen existente, que es un punto guardado en el tiempo cuando todos los datos del volumen son coherentes.
- Visualización del uso del volumen: obtenga información sobre cómo ver la cantidad de datos almacenados en un volumen mediante la consola de Storage Gateway.
- Eliminación de volúmenes de almacenamiento: obtenga información sobre cómo eliminar un volumen si es necesario modificar la aplicación; por ejemplo, si migra una aplicación para que utilice un volumen de almacenamiento mayor.
- Mover los volúmenes a una gateway diferente: obtenga información sobre cómo separar y volver a conectar volúmenes, lo que resulta útil si necesita mover los volúmenes a una puerta de enlace de volumen diferente a medida que cambian sus necesidades de rendimiento.
- Creación de una instantánea de recuperación: obtenga información sobre cómo crear una instantánea de recuperación desde un punto de recuperación de volumen para una puerta de enlace y dónde encontrar esa instantánea en la consola de Storage Gateway después de crearla.
- Edición de un programa de instantáneas: obtenga información sobre cómo personalizar la programación de las instantáneas cambiando la hora en que se producen las instantáneas cada día o la frecuencia con la que se toman las instantáneas.
- Eliminación de instantáneas de los volúmenes de almacenamiento: obtenga información sobre cómo eliminar instantáneas innecesarias cuando ya no las necesite.
- Funcionamiento de los estados de volúmenes y las transiciones: obtenga información sobre los distintos valores de estado de los volúmenes de los que informa Storage Gateway para ayudar a determinar si un volumen funciona con normalidad o si hay algún problema que pueda requerir la adopción de medidas por su parte.
- Transferir los datos a una nueva puerta de enlace: obtenga información sobre cómo mover datos entre puertas de enlace a medida que aumenten sus necesidades de datos y rendimiento o si recibe una notificación de AWS para migrar la puerta de enlace.

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. En Nombre de la puerta de enlace, introduzca un nombre para la puerta de enlace. Puede buscar este nombre para encontrar la puerta de enlace en las páginas de la lista de la consola de Storage Gateway.

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

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

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

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

Agregación y ampliación de volúmenes

A medida que la aplicación necesite crecer, es posible que tenga que agregar más volúmenes a la puerta de enlace o ampliar el tamaño de los volúmenes existentes. Cuando agregue o amplíe los volúmenes, debe tener en cuenta el tamaño del almacenamiento en caché y del búfer de carga que asignó a la puerta de enlace. La gateway debe tener suficiente espacio de búfer y caché para los nuevos volúmenes. Para obtener más información, consulte Determinación del tamaño que se va a asignar al búfer de carga.

Puede agregar volúmenes mediante la consola de Storage Gateway o la API de Storage Gateway. Para obtener instrucciones sobre cómo agregar un volumen mediante la consola de Storage Gateway, consulte Creación de un volumen de almacenamiento. Para obtener información sobre el uso de la API Storage Gateway para añadir volúmenes, consulte CreateCachediSCSIVolume.

Puede ampliar el tamaño de los volúmenes existentes mediante cualquiera de los siguientes métodos:

- Crear una instantánea del volumen que desee ampliar y, a continuación, usar la instantánea para crear un nuevo volumen de mayor tamaño. Para obtener información sobre cómo crear una instantánea, consulte Creación de una instantánea de recuperación. Para obtener información sobre cómo usar una instantánea para crear un nuevo volumen, consulte Creación de un volumen de almacenamiento.
- Utilice el volumen almacenado en caché que desee ampliar para clonar un nuevo volumen de mayor tamaño. Para obtener información sobre cómo clonar un volumen, consulte Clonación de un volumen en caché desde un punto de recuperación. Para obtener información sobre cómo crear un volumen, consulte Creación de un volumen de almacenamiento.

Clonación de un volumen en caché desde un punto de recuperación

Puede crear un volumen nuevo a partir de cualquier volumen almacenado en caché existente en la misma AWS región. El nuevo volumen se crea desde el punto de recuperación más reciente del volumen seleccionado. Un punto de recuperación de volumen es un momento en el que todos los datos del volumen son coherentes. Para clonar un volumen, puede seleccionar la opción Clone from last recovery point (Clonar a partir del último punto de recuperación) del cuadro de diálogo Create volume (Crear volumen) y, a continuación, seleccionar el volumen que desee utilizar como origen.

Clonar a partir de un volumen existente es más rápido y rentable que crear una instantánea de Amazon EBS. La clonación hace una byte-to-byte copia de los datos del volumen de origen al nuevo volumen, utilizando el punto de recuperación más reciente del volumen de origen. Storage Gateway crea automáticamente puntos de recuperación para los volúmenes en caché. Para ver cuándo se creó el último punto de recuperación, consulta la `TimeSinceLastRecoveryPoint` métrica en Amazon CloudWatch.

El volumen clonado es independiente del volumen de origen. Es decir, los cambios realizados en cualquier volumen tras la clonación no afectan a los demás. Por ejemplo, si elimina el volumen de origen, no tendrá efecto sobre el volumen clonado. Puede clonar un volumen de origen mientras haya iniciadores conectados y en uso activo. Hacerlo así no afecta al rendimiento del volumen de origen. Para obtener información sobre cómo clonar un volumen, consulte Creación de un volumen de almacenamiento.

También puede utilizar el proceso de clonación en situaciones de recuperación. Para obtener más información, consulte La gateway almacenada en la caché es inaccesible y desea recuperar los datos.

El siguiente procedimiento muestra cómo utilizar y clonar un volumen a partir de un punto de recuperación de volumen.

Para clonar y utilizar un volumen de una gateway que no permite el acceso

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. En la consola de Storage Gateway, elija Crear volumen.
3. En el cuadro de diálogo Create volume, elija una gateway en Gateway.
4. En Capacity (Capacidad), escriba la capacidad del volumen. La capacidad debe ser al menos del mismo tamaño que el volumen de origen.
5. Elija Clone from last recovery point (Clonar a partir del último punto de recuperación) y seleccione un ID de volumen para Source volume (Volumen de origen). El volumen de origen puede ser cualquier volumen en caché de la AWS región seleccionada.
6. Escriba el nombre para el iSCSI target name.

   El nombre de destino puede contener minúsculas, números, puntos (.) y guiones (-). Este nombre de destino aparece como nombre de iSCSI target node en la pestaña Targets de la interfaz de usuario de iSCSI Microsoft initiator después de la detección. Por ejemplo, el nombre `target1` aparece como `iqn.1007-05.com.amazon:target1`. Asegúrese de que el nombre de destino sea globalmente exclusivo dentro de la red de área de almacenamiento (SAN).

7. Compruebe que la configuración de Network interface (Interfaz de red) sea la dirección IP de la gateway o elija una dirección IP para Network interface (Interfaz de red).

   Si ha definido la gateway para utilizar varios adaptadores de red, elija la dirección IP que las aplicaciones de almacenamiento usan para obtener acceso al volumen. Cada adaptador de red definido para una gateway representa una dirección IP que puede elegir.

   Si la máquina virtual de la gateway está configurada para más de un adaptador de red, el cuadro de diálogo Create volume (Crear volumen) muestra una lista desplegable para Network interface (Interfaz de red). En esta lista, aparece una dirección IP para cada adaptador configurado para la MV de la gateway. Si la MV de la gateway está configurada para un solo adaptador de red, no aparecerá ninguna lista porque solo habrá una dirección IP.

8. Seleccione Create volume (Crear volumen). Aparecerá el cuadro de diálogo Configure CHAP Authentication (Configurar la autenticación CHAP). Puede configurar CHAP más tarde. Para obtener más información, consulte Configuración de la autenticación CHAP para los destinos iSCSI.

El siguiente paso consiste en conectar el volumen al cliente. Para obtener más información, consulte Conexión de los volúmenes al cliente.

Visualización del uso del volumen

Al escribir datos en un volumen, puede ver la cantidad de datos almacenados en dicho volumen desde la consola de administración de Storage Gateway. La pestaña Details (Detalles) de cada volumen muestra información sobre su uso.

Para ver la cantidad de datos grabados en un volumen

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. En el panel de navegación, elija Volumes (Volúmenes) y seleccione el volumen de su interés.
3. Elija la pestaña Detalles.

   En los campos siguientes se muestra información del volumen:

   - Size (Tamaño): la capacidad total del volumen seleccionado.
   - Used (En uso): el tamaño de los datos almacenados en el volumen.

> **Note**
>
> Estos valores no están disponibles para volúmenes creados antes del 13 de mayo de 2015, hasta que almacene datos en dichos volúmenes.

Eliminación de volúmenes de almacenamiento

Es posible que tenga que eliminar un volumen cuando sea necesario modificar la aplicación; por ejemplo, si migra la aplicación para que utilice un volumen de almacenamiento mayor. Antes de eliminar un volumen, asegúrese de que no haya aplicaciones escribiendo en el volumen. Además, asegúrese de que no haya instantáneas en curso para el volumen. Si se ha definido una programación de instantáneas para el volumen, puede consultarlo en la pestaña Programación de instantáneas) de la consola de Storage Gateway. Para obtener más información, consulte Edición de un programa de instantáneas.

Puede eliminar volúmenes mediante la consola de Storage Gateway o la API de Storage Gateway. Para obtener información sobre el uso de la API de Storage Gateway para eliminar volúmenes, consulte Eliminar volumen. El siguiente procedimiento demuestra el uso de la consola.

Antes de eliminar un volumen, haga una copia de seguridad de los datos o una instantánea de los datos más importantes. en el caso de los volúmenes almacenados, los discos locales no se borran. Una vez eliminado un volumen, no podrá recuperarlo.

Para eliminar un volumen

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Elija Volúmenes y, a continuación, seleccione uno o más volúmenes para eliminar.
3. En Acciones, elija Eliminar volumen. Aparece el cuadro de diálogo de confirmación.
4. Compruebe que desea eliminar los volúmenes especificados, escriba la palabra eliminar en el cuadro de confirmación y seleccione Eliminar.

Mover los volúmenes a una gateway diferente

A medida que necesita aumentar los datos y el rendimiento, es posible que desee trasladar los volúmenes a otra puerta de enlace de volumen. Para ello, puede desconectar y asociar un volumen mediante la API o la consola de Storage Gateway.

Al desconectar y asociar un volumen, puede hacer lo siguiente:

- Mueva sus volúmenes a mejores plataformas de alojamiento o a EC2 instancias de Amazon más nuevas.
- Actualizar el hardware subyacente para el servidor.
- Mover los volúmenes entre tipos de hipervisor.

Al desconectar un volumen, la puerta de enlace carga y almacena los metadatos y los datos de volumen con el servicio de Storage Gateway en AWS. Puede asociar fácilmente con posterioridad un volumen desconectado a una gateway en cualquier plataforma de host admitida.

> **Note**
>
> Un volumen desconectado se factura a la tarifa estándar de almacenamiento de volumen hasta que lo elimine. Para obtener más información sobre cómo reducir su factura, consulte Cómo reducir la cantidad de almacenamiento facturado en un volumen.

> **Note**
>
> Existen algunas limitaciones para asociar y desconectar volúmenes:
>
> - La desconexión de un volumen puede llevar mucho tiempo. Al separar un volumen, la pasarela carga todos los datos del volumen AWS antes de separarlo. El tiempo que tarda la carga en completarse depende de la cantidad de datos que tiene que cargar y su conectividad de red en AWS.
> - Si desconecta un volumen almacenado en caché, no puede vuelva a asociarlo como volumen almacenado.
> - Si desconecta un volumen almacenado, no puede vuelva a asociarlo como volumen almacenado en caché.
> - Un volumen desconectado no se puede utilizar hasta que se asocia a una gateway.

- Cuando se asocia un volumen almacenado, tiene que restaurarse por completo antes de poder asociarlo a una gateway.
- Cuando empieza a asociar o desconectar un volumen, tiene que esperar hasta que la operación se haya completado antes de utilizar el volumen.
- En la actualidad, la eliminación de manera forzada de un volumen solo se admite en la API.
- Si elimina una gateway mientras el volumen se está desconectando de dicha gateway, se produce una pérdida de datos. Espere hasta que se complete la operación de desconexión del volumen antes de eliminar la gateway.
- Si una gateway almacenada está en estado de restauración, no puede desconectar un volumen de la misma.

Los siguientes pasos le muestran cómo desconectar y asociar un volumen mediante la consola de Storage Gateway. Para obtener más información sobre cómo hacerlo con la API, consulta DetachVolumeo consulta la Referencia AttachVolumede la AWS Storage Gateway API.

Para desconectar un volumen de una gateway

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Elija Volúmenes y, a continuación, seleccione uno o más volúmenes para desconectar.
3. En Actions (Acciones), elija Detach volume (Desconectar volumen). Aparece el cuadro de diálogo de confirmación.
4. Compruebe que desea desconectar los volúmenes especificados, escriba la palabra desconectar en el cuadro de confirmación y seleccione Desconectar.

> **Note**
>
> Si un volumen que desconecta tiene una gran cantidad de datos, pasa del estado Attached (Asociado) a Detaching (Desconectando) hasta que termina de cargar todos los datos. A continuación, el estado cambia a Detached (Desconectado). Para pequeñas cantidades de datos, es posible que no vea el estado Detaching (Desconectando). Si el volumen no tiene datos, el estado cambia de Attached (Asociado) a Detached (Desconectado).

Ahora puede asociar el volumen a una gateway distinta.

Para asociar un volumen a una gateway

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. En el panel de navegación, seleccione Volumes (Volúmenes). El estado de cada volumen que está desconectado se muestra como Detached (Desconectado).
3. En la lista de volúmenes desconectados, seleccione el volumen que desea asociar. Solo puede asociar los volúmenes de uno en uno.
4. En Actions (Acciones), elija Attach volume (Asociar volumen).
5. En el cuadro de diálogo Attach Volume (Asociar volumen), elija la gateway a la que desea asociar el volumen y, a continuación, introduzca el destino iSCSI al que desea asociar el volumen.

   Si está asociando un volumen almacenado, introduzca su identificador de disco en Disk ID (ID de disco).
6. Elija Attach volume (Asociar volumen). Si un volumen que asocia tiene muchos datos, pasa de Detached (Desconectado) a Attached (Asociado) si la operación `AttachVolume` se realiza correctamente.
7. En el asistente Configurar autenticación de CHAP que aparece, introduzca Initiator name (Nombre del iniciador), Initiator secret (Secreto del iniciador) y Target secret (Secreto de destino) y, a continuación, seleccione Save (Guardar). Para obtener más información acerca del uso de la autenticación del Protocolo de autenticación por desafío mutuo (CHAP), consulte Configuración de la autenticación CHAP para los destinos iSCSI.

Creación de una instantánea de recuperación

El siguiente procedimiento le muestra cómo crear una instantánea de recuperación desde un punto de recuperación de volumen para una puerta de enlace y dónde encontrar esa instantánea en la consola de Storage Gateway después de crearla. Puede realizar instantáneas de recuperación una sola vez y según las necesidades o puede configurar un programa de instantáneas para tomar instantáneas recurrentes del volumen a los intervalos regulares que especifique.

Creación y uso de una instantánea de recuperación de un volumen a partir de una puerta de enlace existente

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

2. En el panel de navegación del lado izquierdo de la página de la consola, elija Puertas de enlace.
3. Elija la puerta de enlace para la que desea crear una instantánea y, a continuación, elija la pestaña Detalles.

   La pestaña Detalles muestra un mensaje de instantánea de recuperación para la puerta de enlace seleccionada.
4. Elija Create recovery snapshot (Crear instantánea de recuperación) para abrir el cuadro de diálogo Create recovery snapshot (Crear instantánea de recuperación).
5. En la lista de volúmenes que se muestra, elija el volumen que desea recuperar y, a continuación, elija Crear instantáneas.

   Storage Gateway inicia el proceso de instantáneas para el volumen especificado. Cuando se complete el proceso de instantáneas, puede encontrar la instantánea mostrada en la columna Instantáneas al ver el volumen en la página Volúmenes de la consola de Storage Gateway.

Edición de un programa de instantáneas

Para los volúmenes almacenados, AWS Storage Gateway crea una programación de instantáneas predeterminada de una vez al día.

> **Note**
>
> No puede eliminar el programa de instantáneas predeterminado. Los volúmenes almacenados requieren al menos un programa de instantáneas. No obstante, puede cambiar el programa de instantáneas especificando la hora a la se realiza la instantánea cada día o la frecuencia (cada 1, 2, 4, 8, 12 o 24 horas), o incluso ambos parámetros.

Para los volúmenes en caché, AWS Storage Gateway no crea una programación de instantáneas predeterminada. No se crea un programa de instantáneas predeterminado porque los datos se almacenan en Amazon S3. Por lo tanto, no se necesitan instantáneas ni un programa de instantáneas con fines de recuperación de desastres. Sin embargo, puede configurar un programa de instantáneas en cualquier momento si lo necesita. La creación de una instantánea para el volumen almacenado en caché proporciona una manera adicional de recuperar los datos, si es necesario.

Puede hacer lo siguiente para editar el programa de instantáneas para un volumen.

Para editar el programa de instantáneas para un volumen

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. En el panel de navegación, elija Volumes (Volúmenes) y, a continuación, elija el volumen a partir del cual se creó la instantánea.
3. En Actions (Acciones), elija Edit snapshot schedule (Editar programa de instantáneas).
4. En el cuadro de diálogo Edit snapshot schedule (Editar programa de instantáneas), modifique el programa y, a continuación, elija Save (Guardar).

Eliminación de instantáneas de los volúmenes de almacenamiento

Es posible eliminar instantáneas del volumen de almacenamiento. Quizá desee hacerlo si, por ejemplo, ha tomado muchas instantáneas de un volumen de almacenamiento y no necesita las más antiguas. Dado que las instantáneas son copias de seguridad incrementales, si se elimina una instantánea, solo se eliminarán los datos que no se necesiten en otras instantáneas.

Temas

- Eliminación de instantáneas utilizando el AWS SDK para Java
- Eliminación de instantáneas utilizando el AWS SDK para .NET
- Eliminación de instantáneas utilizando el AWS Tools for Windows PowerShell

En la consola de Amazon EBS, puede eliminar instantáneas de una en una. Para obtener información sobre cómo eliminar instantáneas mediante la consola de Amazon EBS, consulte Eliminar una instantánea de Amazon EBS en la Guía del usuario de Amazon EC2 .

Para eliminar varias instantáneas a la vez, puede usar una de las AWS SDKs que sea compatible con las operaciones de Storage Gateway. Para ver ejemplos, consulte Eliminación de instantáneas utilizando el AWS SDK para Java, Eliminación de instantáneas utilizando el AWS SDK para .NET y Eliminación de instantáneas utilizando el AWS Tools for Windows PowerShell.

Eliminación de instantáneas utilizando el AWS SDK para Java

Para eliminar muchas instantáneas asociadas con un volumen, puede utilizar un enfoque programático. En el ejemplo siguiente se muestra cómo eliminar instantáneas utilizando el AWS SDK para Java. Para utilizar el código del ejemplo, debe haberse familiarizado con la ejecución de aplicaciones de la consola de Java. Para obtener más información, consulte Introducción en la Guía

para desarrolladores de AWS SDK para Java. Si solo necesita iluminar algunas instantáneas, utilice la consola como se describe en Eliminación de instantáneas de los volúmenes de almacenamiento.

Example : Eliminar instantáneas mediante el AWS SDK para Java

En el siguiente ejemplo de código Java se muestran las instantáneas para cada volumen de una gateway y si la hora de inicio de la instantánea es anterior o posterior a una fecha especificada. Utiliza la API de AWS SDK for Java para Storage Gateway y Amazon EC2. La EC2 API de Amazon incluye operaciones para trabajar con instantáneas.

Actualice el código para proporcionar el punto de enlace de servicio, el Nombre de recurso de Amazon (ARN) de la gateway y el número de días pasados cuyas instantáneas desea guardar. Las instantáneas realizadas antes de la fecha más antigua se eliminan. También debe especificar el valor booleano `viewOnly`, que indica si desea ver las instantáneas que se vayan a eliminar o realizar realmente las eliminaciones de instantáneas. Primero ejecute el código solo con la opción de vista (es decir, con `viewOnly` con el valor `true`) para ver qué elimina el código. 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 java.util.ArrayList;
import java.util.Calendar;
import java.util.Collection;
import java.util.Date;
import java.util.GregorianCalendar;
import java.util.List;

import com.amazonaws.auth.PropertiesCredentials;
import com.amazonaws.services.ec2.AmazonEC2Client;
import com.amazonaws.services.ec2.model.DeleteSnapshotRequest;
import com.amazonaws.services.ec2.model.DescribeSnapshotsRequest;
import com.amazonaws.services.ec2.model.DescribeSnapshotsResult;
import com.amazonaws.services.ec2.model.Filter;
import com.amazonaws.services.ec2.model.Snapshot;
import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
import com.amazonaws.services.storagegateway.model.ListVolumesRequest;
import com.amazonaws.services.storagegateway.model.ListVolumesResult;
import com.amazonaws.services.storagegateway.model.VolumeInfo;

public class ListDeleteVolumeSnapshotsExample {

    public static AWSStorageGatewayClient sgClient;
```

```
    public static AmazonEC2Client ec2Client;
    static String serviceURLSG = "https://storagegateway.us-east-1.amazonaws.com";
    static String serviceURLEC2 = "https://ec2.us-east-1.amazonaws.com";

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

    // The number of days back you want to save snapshots. Snapshots before this cutoff
are deleted
    // if viewOnly = false.
    public static int daysBack = 10;

    // true = show what will be deleted; false = actually delete snapshots that meet
the daysBack criteria
    public static boolean viewOnly = true;

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

        // Create a Storage Gateway and amazon ec2 client
        sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(

ListDeleteVolumeSnapshotsExample.class.getResourceAsStream("AwsCredentials.properties")));

        sgClient.setEndpoint(serviceURLSG);

        ec2Client = new AmazonEC2Client(new PropertiesCredentials(

ListDeleteVolumeSnapshotsExample.class.getResourceAsStream("AwsCredentials.properties")));
        ec2Client.setEndpoint(serviceURLEC2);

        List<VolumeInfo> volumes = ListVolumesForGateway();
        DeleteSnapshotsForVolumes(volumes, daysBack);

    }
    public static List<VolumeInfo> ListVolumesForGateway()
    {
        List<VolumeInfo> volumes = new ArrayList<VolumeInfo>();

        String marker = null;
        do {
            ListVolumesRequest request = new
ListVolumesRequest().withGatewayARN(gatewayARN);
            ListVolumesResult result = sgClient.listVolumes(request);
            marker = result.getMarker();
```

```
            for (VolumeInfo vi : result.getVolumeInfos())
            {
                volumes.add(vi);
                System.out.println(OutputVolumeInfo(vi));
            }
        } while (marker != null);

        return volumes;
    }
    private static void DeleteSnapshotsForVolumes(List<VolumeInfo> volumes,
            int daysBack2) {

        // Find snapshots and delete for each volume
        for (VolumeInfo vi : volumes) {

            String volumeARN = vi.getVolumeARN();
            String volumeId =
volumeARN.substring(volumeARN.lastIndexOf("/")+1).toLowerCase();
            Collection<Filter> filters = new ArrayList<Filter>();
            Filter filter = new Filter().withName("volume-id").withValues(volumeId);
            filters.add(filter);

            DescribeSnapshotsRequest describeSnapshotsRequest =
                new DescribeSnapshotsRequest().withFilters(filters);
            DescribeSnapshotsResult describeSnapshotsResult =
                ec2Client.describeSnapshots(describeSnapshotsRequest);

            List<Snapshot> snapshots = describeSnapshotsResult.getSnapshots();
            System.out.println("volume-id = " + volumeId);
            for (Snapshot s : snapshots){
                StringBuilder sb = new StringBuilder();
                boolean meetsCriteria = !CompareDates(daysBack, s.getStartTime());
                sb.append(s.getSnapshotId() + ", " + s.getStartTime().toString());

                sb.append(", meets criteria for delete? " + meetsCriteria);
                sb.append(", deleted? ");
                if (!viewOnly & meetsCriteria) {
                    sb.append("yes");
                    DeleteSnapshotRequest deleteSnapshotRequest =
                        new DeleteSnapshotRequest().withSnapshotId(s.getSnapshotId());
                    ec2Client.deleteSnapshot(deleteSnapshotRequest);
                }
                else {
```

```
                    sb.append("no");
                }
                System.out.println(sb.toString());
            }
        }
    }

    private static String OutputVolumeInfo(VolumeInfo vi) {

        String volumeInfo = String.format(
                 "Volume Info:\n" +
                 "  ARN: %s\n" +
                 "  Type: %s\n",
                 vi.getVolumeARN(),
                 vi.getVolumeType());
        return volumeInfo;
     }

    // Returns the date in two formats as a list
    public static boolean CompareDates(int daysBack, Date snapshotDate) {
        Date today = new Date();
        Calendar cal = new GregorianCalendar();
        cal.setTime(today);
        cal.add(Calendar.DAY_OF_MONTH, -daysBack);
        Date cutoffDate = cal.getTime();
        return (snapshotDate.compareTo(cutoffDate) > 0) ? true : false;
    }

}
```

Eliminación de instantáneas utilizando el AWS SDK para .NET

Para eliminar muchas instantáneas asociadas con un volumen, puede utilizar un enfoque programático. En el ejemplo siguiente se muestra cómo eliminar instantáneas utilizando el AWS SDK para .NET versión 2 y 3. Para utilizar el código del ejemplo, debe haberse familiarizado con la ejecución de aplicaciones de la consola de .NET. Para obtener más información, consulte Introducción en la Guía para desarrolladores de AWS SDK para .NET. Si solo necesita iluminar algunas instantáneas, utilice la consola como se describe en Eliminación de instantáneas de los volúmenes de almacenamiento.

Example : Eliminar instantáneas mediante el AWS SDK para .NET

En el siguiente ejemplo de código en C#, un AWS Identity and Access Management usuario puede enumerar las instantáneas de cada volumen de una puerta de enlace. Eso permite al usuario determinar si la hora de inicio de la instantánea es anterior o posterior a una fecha especificada (periodo de retención) y eliminar las instantáneas que hayan superado el periodo de retención. En el ejemplo, se usa la API de AWS SDK for .NET para Storage Gateway y Amazon EC2. La EC2 API de Amazon incluye operaciones para trabajar con instantáneas.

En el siguiente ejemplo de código se utiliza el AWS SDK para las versiones 2 y 3 de S.NET. Puede migrar las versiones más antiguas de .NET a la versión más reciente. Para obtener más información, consulte Migración de un proyecto para el AWS SDK para .NET.

Actualice el código para proporcionar el punto de enlace de servicio, el Nombre de recurso de Amazon (ARN) de la gateway y el número de días pasados cuyas instantáneas desea guardar. Las instantáneas realizadas antes de la fecha más antigua se eliminan. También debe especificar el valor booleano `viewOnly`, que indica si desea ver las instantáneas que se vayan a eliminar o realizar realmente las eliminaciones de instantáneas. Primero ejecute el código solo con la opción de vista (es decir, con `viewOnly` con el valor `true`) para ver qué elimina el código. 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

En primer lugar, cree un usuario y asocie la política de IAM mínima al usuario. A continuación, programe instantáneas automatizadas para la gateway.

El siguiente código crea la política mínima que permite a un usuario eliminar instantáneas. En este ejemplo, la política se denomina **`sgw-delete-snapshot`**.

JSON

```
{
      "Version": "2012-10-17",
      "Statement": [
          {
              "Sid": "StmtEC2Snapshots",
              "Effect": "Allow",
              "Action": [
                  "ec2:DeleteSnapshot",
                  "ec2:DescribeSnapshots"
              ],
```

```
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "StmtSgwListVolumes",
            "Effect": "Allow",
            "Action": [
                "storagegateway:ListVolumes"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

El siguiente código de C# comprueba todas las instantáneas de la gateway especificada que coinciden con los volúmenes y el periodo de corte especificado y las elimina.

```
using System;
using System.Collections.Generic;
using System.Text;
using Amazon.EC2;
using Amazon.EC2.Model;
using Amazon.StorageGateway.Model;
using Amazon.StorageGateway;

namespace DeleteStorageGatewaySnapshotNS
{
    class Program
    {
        /*
         * Replace the variables below to match your environment.
         */

         /* IAM AccessKey */
        static String AwsAccessKey = "AKIA...............";

        /* IAM SecretKey */
        static String AwsSecretKey = "******************************";
```

```
        /* Account number, 12 digits, no hyphen */
        static String OwnerID = "123456789012";

        /* Your Gateway ARN. Use a Storage Gateway ID, sgw-XXXXXXXX* */
        static String GatewayARN = "arn:aws:storagegateway:ap-
southeast-2:123456789012:gateway/sgw-XXXXXXXX";

        /* Snapshot status: "completed", "pending", "error" */

        static String SnapshotStatus = "completed";

        /* Region where your gateway is activated */
        static String AwsRegion = "ap-southeast-2";

        /* Minimum age of snapshots before they are deleted (retention policy) */
        static int daysBack = 30;

        /*
         * Do not modify the four lines below.
         */
        static AmazonEC2Config ec2Config;
        static AmazonEC2Client ec2Client;
        static AmazonStorageGatewayClient sgClient;
        static AmazonStorageGatewayConfig sgConfig;

        static void Main(string[] args)
        {
            // Create an EC2 client.
            ec2Config = new AmazonEC2Config();
            ec2Config.ServiceURL = "https://ec2." + AwsRegion + ".amazonaws.com";
            ec2Client = new AmazonEC2Client(AwsAccessKey, AwsSecretKey, ec2Config);

            // Create a Storage Gateway client.
            sgConfig = new AmazonStorageGatewayConfig();
            sgConfig.ServiceURL = "https://storagegateway." + AwsRegion +
 ".amazonaws.com";
            sgClient = new AmazonStorageGatewayClient(AwsAccessKey, AwsSecretKey,
 sgConfig);

            List<VolumeInfo> StorageGatewayVolumes = ListVolumesForGateway();
            List<Snapshot> StorageGatewaySnapshots =
 ListSnapshotsForVolumes(StorageGatewayVolumes,
                                                    daysBack);
            DeleteSnapshots(StorageGatewaySnapshots);
```

```
        }

        /*
         * List all volumes for your gateway
         * returns: A list of VolumeInfos, or null.
         */
        private static List<VolumeInfo> ListVolumesForGateway()
        {
            ListVolumesResponse response = new ListVolumesResponse();
            try
            {
                ListVolumesRequest request = new ListVolumesRequest();
                request.GatewayARN = GatewayARN;
                response = sgClient.ListVolumes(request);

                foreach (VolumeInfo vi in response.VolumeInfos)
                {
                    Console.WriteLine(OutputVolumeInfo(vi));
                }
            }
            catch (AmazonStorageGatewayException ex)
            {
                Console.WriteLine(ex.Message);
            }
            return response.VolumeInfos;
        }

        /*
         * Gets the list of snapshots that match the requested volumes
         * and cutoff period.
         */
        private static List<Snapshot> ListSnapshotsForVolumes(List<VolumeInfo> volumes,
int snapshotAge)
        {
            List<Snapshot> SelectedSnapshots = new List<Snapshot>();
            try
            {
                foreach (VolumeInfo vi in volumes)
                {
                    String volumeARN = vi.VolumeARN;
                    String volumeID = volumeARN.Substring(volumeARN.LastIndexOf("/") +
1).ToLower();
```

```
                    DescribeSnapshotsRequest describeSnapshotsRequest = new
DescribeSnapshotsRequest();

                    Filter ownerFilter = new Filter();
                    List<String> ownerValues = new List<String>();
                    ownerValues.Add(OwnerID);
                    ownerFilter.Name = "owner-id";
                    ownerFilter.Values = ownerValues;
                    describeSnapshotsRequest.Filters.Add(ownerFilter);

                    Filter statusFilter = new Filter();
                    List<String> statusValues = new List<String>();
                    statusValues.Add(SnapshotStatus);
                    statusFilter.Name = "status";
                    statusFilter.Values = statusValues;
                    describeSnapshotsRequest.Filters.Add(statusFilter);

                    Filter volumeFilter = new Filter();
                    List<String> volumeValues = new List<String>();
                    volumeValues.Add(volumeID);
                    volumeFilter.Name = "volume-id";
                    volumeFilter.Values = volumeValues;
                    describeSnapshotsRequest.Filters.Add(volumeFilter);

                    DescribeSnapshotsResponse describeSnapshotsResponse =
                      ec2Client.DescribeSnapshots(describeSnapshotsRequest);

                    List<Snapshot> snapshots = describeSnapshotsResponse.Snapshots;
                    Console.WriteLine("volume-id = " + volumeID);
                    foreach (Snapshot s in snapshots)
                    {
                        if (IsSnapshotPastRetentionPeriod(snapshotAge, s.StartTime))
                        {
                            Console.WriteLine(s.SnapshotId + ", " + s.VolumeId + ",
                               " + s.StartTime + ", " + s.Description);
                            SelectedSnapshots.Add(s);
                        }
                    }
                }
            }
            catch (AmazonEC2Exception ex)
            {
                Console.WriteLine(ex.Message);
            }
```

```
            return SelectedSnapshots;
        }

        /*
         * Deletes a list of snapshots.
         */
        private static void DeleteSnapshots(List<Snapshot> snapshots)
        {
            try
            {
                foreach (Snapshot s in snapshots)
                {

                    DeleteSnapshotRequest deleteSnapshotRequest = new
DeleteSnapshotRequest(s.SnapshotId);
                    DeleteSnapshotResponse response =
ec2Client.DeleteSnapshot(deleteSnapshotRequest);
                    Console.WriteLine("Volume: " +
                              s.VolumeId +
                              " => Snapshot: " +
                              s.SnapshotId +
                              " Response: "
                              + response.HttpStatusCode.ToString());
                }
            }
            catch (AmazonEC2Exception ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /*
         * Checks if the snapshot creation date is past the retention period.
         */
        private static Boolean IsSnapshotPastRetentionPeriod(int daysBack, DateTime
snapshotDate)
        {
            DateTime cutoffDate = DateTime.Now.Add(new TimeSpan(-daysBack, 0, 0, 0));
            return (DateTime.Compare(snapshotDate, cutoffDate) < 0) ? true : false;
        }

        /*
         * Displays information related to a volume.
         */
```

```
        private static String OutputVolumeInfo(VolumeInfo vi)
        {
            String volumeInfo = String.Format(
                "Volume Info:\n" +
                "  ARN: {0}\n" +
                "  Type: {1}\n",
                vi.VolumeARN,
                vi.VolumeType);
            return volumeInfo;
        }
    }
}
```

Eliminación de instantáneas utilizando el AWS Tools for Windows PowerShell

Para eliminar muchas instantáneas asociadas con un volumen, puede utilizar un enfoque programático. En el ejemplo siguiente se muestra cómo eliminar instantáneas utilizando el AWS Tools for Windows PowerShell. Para usar el script de ejemplo, debe estar familiarizado con la ejecución de un PowerShell script. Para obtener más información, consulte Introducción en la AWS Tools for Windows PowerShell. Si solo necesita iluminar algunas instantáneas, utilice la consola como se describe en Eliminación de instantáneas de los volúmenes de almacenamiento.

Example : Eliminar instantáneas mediante el AWS Tools for Windows PowerShell

El siguiente ejemplo de PowerShell script muestra las instantáneas de cada volumen de una puerta de enlace y indica si la hora de inicio de la instantánea es anterior o posterior a una fecha especificada. Utiliza los AWS Tools for Windows PowerShell cmdlets de Storage Gateway y Amazon. EC2 La EC2 API de Amazon incluye operaciones para trabajar con instantáneas.

Deberá actualizar el código del script para proporcionar el Nombre de recurso de Amazon (ARN) de la gateway y el número de días pasados cuyas instantáneas desea guardar. Las instantáneas realizadas antes de la fecha más antigua se eliminan. También debe especificar el valor booleano `viewOnly`, que indica si desea ver las instantáneas que se vayan a eliminar o realizar realmente las eliminaciones de instantáneas. Primero ejecute el código solo con la opción de vista (es decir, con `viewOnly` con el valor `true`) para ver qué elimina el código.

```
<#
.DESCRIPTION
    Delete snapshots of a specified volume that match given criteria.
```

```
.NOTES
    PREREQUISITES:
    1) AWS Tools for Windows PowerShell from https://aws.amazon.com/powershell/
    2) Credentials and AWS 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_DeleteSnapshots.ps1
#>

# Criteria to use to filter the results returned.
$daysBack = 18
$gatewayARN = "*** provide gateway ARN ***"
$viewOnly = $true;

#ListVolumes
$volumesResult = Get-SGVolume -GatewayARN $gatewayARN
$volumes = $volumesResult.VolumeInfos
Write-Output("`nVolume List")
foreach ($volumes in $volumesResult)
  { Write-Output("`nVolume Info:")
    Write-Output("ARN:  " + $volumes.VolumeARN)
    write-Output("Type: " + $volumes.VolumeType)
  }

Write-Output("`nWhich snapshots meet the criteria?")
foreach ($volume in $volumesResult)
  {
    $volumeARN = $volume.VolumeARN

    $volumeId = ($volumeARN-split"/")[3].ToLower()

    $filter = New-Object Amazon.EC2.Model.Filter
    $filter.Name = "volume-id"
    $filter.Value.Add($volumeId)

    $snapshots = get-EC2Snapshot -Filter $filter
    Write-Output("`nFor volume-id = " + $volumeId)
    foreach ($s in $snapshots)
    {
       $d = ([DateTime]::Now).AddDays(-$daysBack)
       $meetsCriteria = $false
```

```
      if ([DateTime]::Compare($d, $s.StartTime) -gt 0)
      {
           $meetsCriteria = $true
      }

      $sb = $s.SnapshotId + ", " + $s.StartTime + ", meets criteria for delete? " +
$meetsCriteria
      if (!$viewOnly -AND $meetsCriteria)
      {
          $resp = Remove-EC2Snapshot -SnapshotId $s.SnapshotId
          #Can get RequestId from response for troubleshooting.
          $sb = $sb + ", deleted? yes"
      }
      else {
          $sb = $sb + ", deleted? no"
      }
      Write-Output($sb)
   }
 }
```

Funcionamiento de los estados de volúmenes y las transiciones

Cada volumen tiene una indicación de estado asociado que permite ver de inmediato en qué estado se encuentra. En la mayoría de los casos, el estado indica que el volumen funciona normalmente y que no se requiere ninguna intervención por parte del usuario. En ocasiones, el estado indica algún problema con el volumen; en este caso, podría o no ser preciso que intervenga. A continuación encontrará información que le ayudará a decidir cuándo debe intervenir. Puede ver el estado del volumen en la consola de Storage Gateway o mediante una de las operaciones de la API de Storage Gateway, por ejemplo, DescribeCachediSCSIVolumeso DescribeStorediSCSIVolumes.

Temas

- Información sobre el estado de los volúmenes
- Información sobre el estado de la conexión
- Cómo funcionan las transiciones de estado de volúmenes almacenados en caché
- Cómo funcionan las transiciones de estado de volúmenes almacenados

Información sobre el estado de los volúmenes

La tabla siguiente muestra el estado del volumen en la consola de Storage Gateway. El estado del volumen aparece en la columna Status (Estado) de cada volumen de almacenamiento de la gateway. El estado de un volumen que funciona normalmente es Available (Disponible).

En la tabla siguiente, encontrará una descripción de cada estado de volumen de almacenamiento y si debe hacer algo según cada estado y cuándo. El estado Available (Disponible) es el estado normal de un volumen. El estado de un volumen debe ser AVAILABLE la totalidad o la mayor parte del tiempo que se esté usando.

Estado	Significado
Disponible	El volumen está disponible para su uso. Este es el estado normal de funcionamiento para un volumen. Cuando finaliza una fase Bootstrapping (Proceso de arranque), el volumen vuelve al estado Available (Disponible). Es decir, la gateway ha sincronizado los cambios realizados en el volumen desde que pasó al estado Pass Through (Acceso directo).
Bootstrapping (Proceso de arranque)	La puerta de enlace sincroniza los datos de forma local con una copia de los datos almacenados en AWS ella. Por lo general, este estado no requiere ninguna acción, ya que el volumen de almacenamiento suele detectar el estado Available (Disponible) automáticamente. En las situaciones siguientes, el estado de un volumen es Bootstrapping (Proceso de arranque): • Una gateway se ha cerrado de forma inesperada. • Un búfer de carga de la gateway se ha superado. En este caso, el proceso de arranque se produce cuando el volumen tiene el estado Pass Through (Acceso directo) y la cantidad de búfer de carga libre aumenta lo suficiente. Puede proporcionar más espacio de búfer de carga como una forma de aumentar el porcentaje de espacio de búfer de carga libre. En este caso concreto, el volumen de almacenam iento va del estado Pass Through (Acceso directo) a Bootstrapping

Estado	Significado
	(Proceso de arranque) a Available (Disponible). Puede seguir utilizando este volumen durante este periodo de arranque. Sin embargo, en este momento no puede tomar instantáneas del volumen. • Está creando una puerta de enlace de volumen almacenado y preservando los datos del disco local existente. En este escenario, la puerta de enlace comienza a cargar todos los datos en. AWS El volumen tiene el estado de arranque hasta que se copien todos los datos del disco local. AWS Puede utilizar el volumen durante este periodo de arranque. Sin embargo, en este momento no puede tomar instantáneas del volumen.
Creando	El volumen se está creando y no está listo para utilizarlo. El estado Creating (Creando) es transitorio. No hay que hacer nada más.
Eliminando	El volumen está siendo eliminado. El estado Deleting (Eliminando) es transitorio. No hay que hacer nada más.
Irrecoverable (Irrecuperable)	Se ha producido un error de que el volumen no se puede recuperar . Para obtener información acerca de qué hacer en esta situación, consulte Solución de problemas con volúmenes.

Estado	Significado
Pass Through (Acceso directo)	Los datos guardados localmente no están sincronizados con los datos almacenados en él. AWS Los datos que se escriben en un volumen mientras este se encuentra en estado Pass Through (Acceso directo) permanecen en la caché hasta que el estado del volumen es Bootstrap ping (Proceso de arranque). Estos datos comienzan a cargarse AWS cuando comienza el estado de arranque. El estado Pass Through (Acceso directo) puede producirse por varios motivos, que se enumeran a continuación: • El estado Pass Through (Acceso directo) se produce si la gateway se ha quedado sin espacio de búfer de carga. Las aplicaciones pueden continuar leyendo y escribiendo datos en los volúmenes de almacenamiento mientras los volúmenes tienen el estado Pass Through (Acceso directo). Sin embargo, la puerta de enlace no escribe los datos del volumen en el búfer de carga ni los carga en AWS. La gateway continúa cargando todos los datos escritos en el volumen antes de que este entre en el estado Pass Through (Acceso directo). Cualquier instantánea pendiente o programada de un volumen de almacenamiento producirá un error mientras el volumen tenga el estado Pass Through (Acceso directo). Para obtener información sobre qué hacer cuando el volumen de almacenamiento tenga el estado Pass Through (Acceso directo) porque se haya superado el búfer de carga, consulte Solución de problemas con volúmenes. Para volver al estado ACTIVE, un volumen en Pass Through (Acceso directo) debe completar la fase Bootstrapping (Proceso de arranque) . Durante el arranque, el volumen restablece la sincronización interna AWS para poder reanudar el registro (registro) de los cambios en el volumen y activar la funcionalidad. `CreateSnapshot` Durante Bootstrapping (Proceso de arranque), lo que se escribe en el volumen se registra en el búfer de carga. •

Estado	Significado
	El estado Pass Through (Acceso directo) se produce cuando hay más de un volumen de almacenamiento arrancando a la vez. Solo puede arrancar un volumen de almacenamiento de gateway a la vez. Por ejemplo, supongamos que crea dos volúmenes de almacenamiento y elige conservar los datos existentes en ambos. En este caso, el estado del segundo volumen de almacenamiento es Pass Through (Acceso directo) hasta que el primer volumen de almacenamiento termina el proceso de arranque. En este caso, no tiene que hacer nada. El estado de cada volumen de almacenamiento cambia automáticamente Available (Disponible) al terminar de crearse. Puede leer y escribir en el volumen de almacenamiento mientras tenga el estado Pass Through (Acceso directo) o Bootstrapping (Proceso de arranque). • De manera infrecuente, el estado Pass Through (Acceso directo) puede indicar que un disco asignado al búfer de carga ha producido un error. Para obtener información sobre qué hacer en este caso, consulte Solución de problemas con volúmenes. • El estado Pass Through (Acceso directo) puede producirse cuando un volumen tiene el estado Active (Activo) o Bootstrapping (Proceso de arranque). En este caso, el volumen recibe una escritura, pero el búfer de carga no tiene capacidad suficiente para registrarla. • El volumen pasa al estado Pass Through (Acceso directo) cuando se encuentra en cualquier estado y la gateway no se cierra perfectam ente. Este tipo de cierre puede ocurrir porque el software se bloquea o la MV se apaga. En este caso, un volumen en cualquier estado pasa al estado Pass Through (Acceso directo).

Estado	Significado
Restauración	El volumen se está restaurando a partir de una instantánea existente . Este estado se aplica únicamente a volúmenes almacenados. Para obtener más información, consulte Funcionamiento de puerta de enlace de volumen. Si restaura dos volúmenes de almacenamiento al mismo tiempo, ambos volúmenes de almacenamiento mostrarán el estado Restoring (Restaurándose). El estado de cada volumen de almacenamiento cambia automáticamente Available (Disponible) al terminar de crearse. Puede leer y escribir en un volumen de almacenamiento y tomar una instantánea del mismo mientras tenga el estado Restoring (Restaurá ndose).
Restoring Pass Through (Restaura ndo acceso directo)	El volumen se está restaurando a partir de una instantánea existente y ha encontrado un problema del búfer de carga. Este estado se aplica únicamente a volúmenes almacenados. Para obtener más información, consulte Funcionamiento de puerta de enlace de volumen. Un motivo para el estado Restoring Pass Through (Restaurando acceso directo) es que la gateway se haya quedado sin espacio en el búfer de almacenamiento. Las aplicaciones pueden continuar leyendo y escribien do datos en los volúmenes de almacenamiento mientras tienen el estado Restoring Pass Through (Restaurando acceso directo). Sin embargo, no puede tomar instantáneas de un volumen de almacenamiento mientras su estado sea Restoring Pass Through (Restaurando acceso directo). Para obtener información sobre la acción a realizar cuando el volumen de almacenamiento tenga el estado Restoring Pass Through (Restaura ndo acceso directo) porque se haya superado la capacidad del búfer de carga, consulte Solución de problemas con volúmenes. De manera infrecuente, el estado Restoring Pass Through (Restaurando acceso directo) puede indicar que un disco asignado para un búfer de carga ha producido un error. Para obtener información sobre qué hacer en este caso, consulte Solución de problemas con volúmenes.

Estado	Significado
Upload Buffer Not Configured (Búfer de carga no configurado)	No puede crear ni utilizar el volumen, porque la gateway no tiene un búfer de carga configurado. Para obtener más información sobre cómo agregar capacidad de búfer de carga para volúmenes en una configuración de volúmenes en caché, consulte Determinación del tamaño que se va a asignar al búfer de carga. Para obtener más información sobre cómo agregar capacidad de búfer de carga para volúmenes en una configuración de volúmenes almacenados, consulte Determinación del tamaño que se va a asignar al búfer de carga.

Información sobre el estado de la conexión

Puede desconectar un volumen de una gateway o asociarlo a la gateway mediante la API o la consola de Storage Gateway. La tabla siguiente muestra el estado de conexión del volumen en la consola de Storage Gateway. El estado de conexión del volumen aparece en la columna Attachment status (Estado de la conexión) de cada volumen de almacenamiento en la gateway. Por ejemplo, un volumen que se desconecta de una gateway tiene un estado de Detached (Desconectado). Para obtener información sobre cómo desconectar y asociar un volumen, consulte Mover los volúmenes a una gateway diferente.

Estado	Significado
Attached (Asociado)	El volumen se asocia a una gateway.
Detached (Desvinculado)	El volumen se desconecta de una gateway.
Detaching (Desconectar)	El volumen se está desconectando de una gateway. Cuando se desconecta un volumen y el volumen no tiene datos, es posible que no vea este estado.

Cómo funcionan las transiciones de estado de volúmenes almacenados en caché

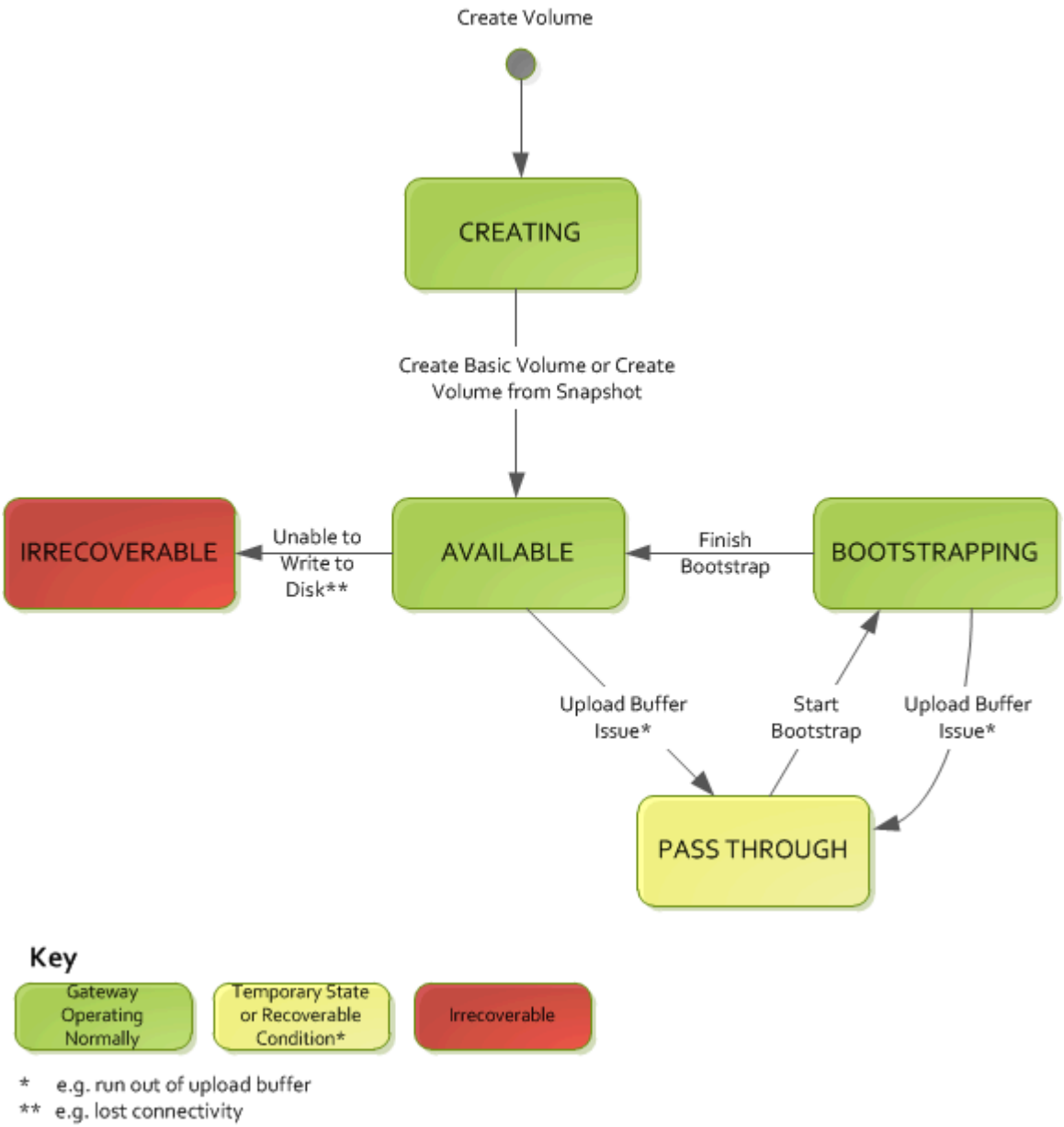
Consulte el siguiente diagrama de estado para comprender las transiciones más comunes entre estados de volúmenes en gateways almacenadas en caché. No es necesario conocer el diagrama de forma detallada para utilizar la gateway de forma eficaz. En su lugar, el diagrama ofrece información detallada si le interesa obtener más información acerca de cómo funcionan las puertas de enlace de volumen.

El diagrama no muestra el estado Upload Buffer Not Configured (Búfer de carga no configurado) ni el estado Deleting (Eliminando). Los estados de volumen del diagrama se representan con cuadros verdes, amarillos y rojos. Los colores se pueden interpretar de la manera siguiente.

Color	Estado de volumen
Green (Verde)	La gateway funciona con normalidad. El estado del volumen es Available (Disponible) o pasará a Available (Disponible).
Yellow (Amarillo)	El volumen tiene estado Pass Through (Acceso directo) que indica que existe un problema potencial con el volumen de almacenamiento. Si este estado aparece porque el espacio de búfer de carga está lleno, en algunos casos, el espacio del búfer vuelve a estar disponible. En ese momento, el volumen de almacenamiento se corrige automáticamente al estado Available (Disponible). En otros casos, es posible que tenga que agregar más espacio de búfer de carga a la gateway para permitir que el estado del volumen de almacenamiento pase a ser Available (Disponible). Para obtener informaci ón sobre cómo solucionar un caso cuando se supere la capacidad del búfer de carga, consulte Solución de problemas con volúmenes . Para obtener información sobre cómo agregar capacidad al búfer de carga, consulte Determina

Color	Estado de volumen
	ción del tamaño que se va a asignar al búfer de carga.
Rojo	El volumen de almacenamiento tiene el estado Irrecoverable (Irrecuperable). En este caso, debe eliminar el volumen. Para obtener información sobre cómo hacerlo, consulte Para eliminar un volumen.

En el diagrama, se representa una transición entre dos estados con una línea etiquetada. Por ejemplo, la transición desde el estado Creating (Creando) al estado Available (Disponible) está etiquetada como Create Basic Volume or Create Volume from Snapshot (Crear un volumen básico o crear un volumen a partir de una instantánea). La transición representa la creación de un volumen almacenado en caché. Para obtener más información sobre la creación de volúmenes de almacenamiento, consulte Agregación y ampliación de volúmenes.



> **Note**
>
> El estado Pass Through (Acceso directo) del volumen aparece como amarillo en este diagrama. Sin embargo, esto no coincide con el color de este icono de estado en el cuadro Estado de la consola de Storage Gateway.

Cómo funcionan las transiciones de estado de volúmenes almacenados

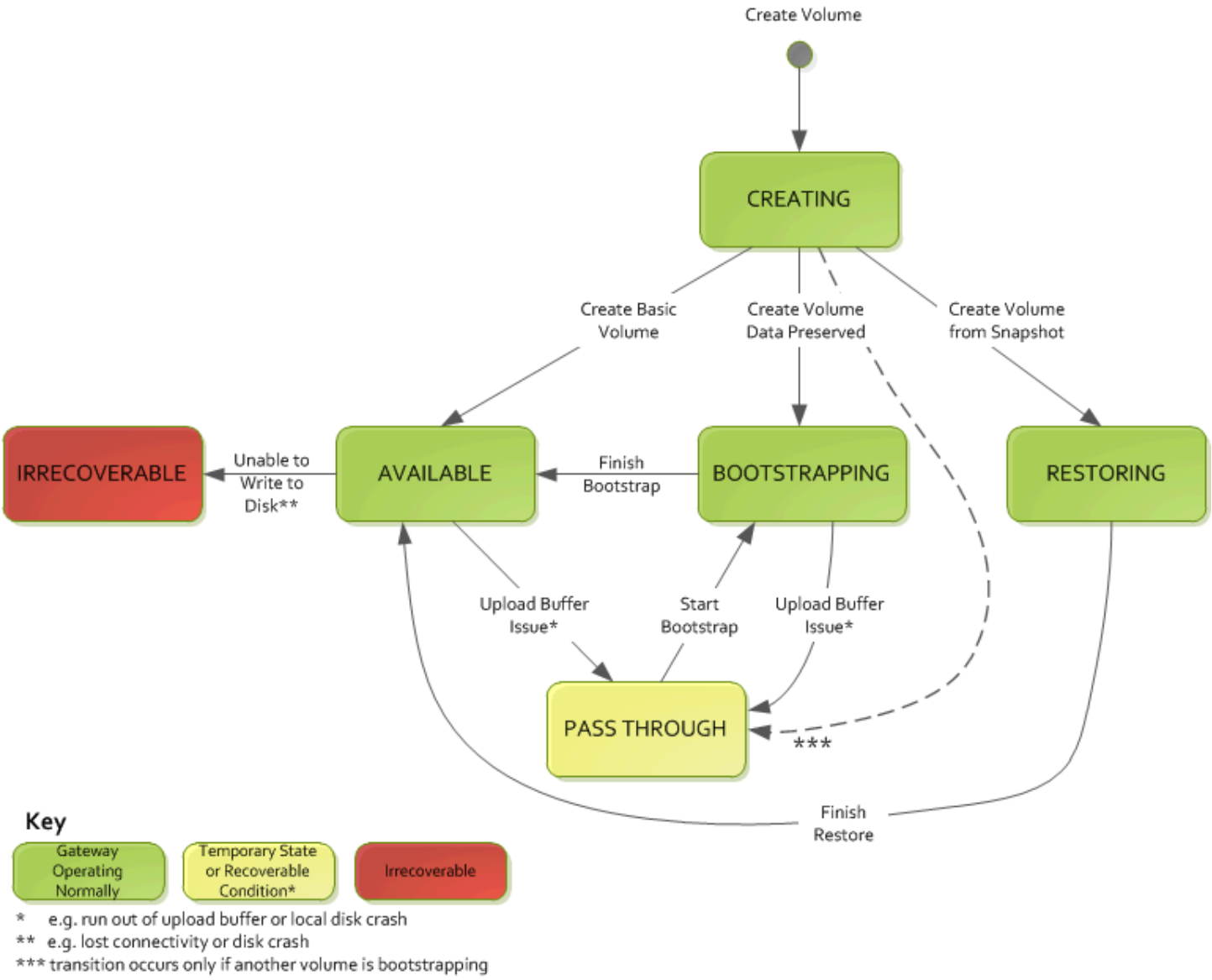
Consulte el siguiente diagrama de estado para comprender las transiciones más comunes entre estados de volúmenes en gateways almacenadas. No es necesario conocer el diagrama de forma detallada para utilizar la gateway de forma eficaz. En su lugar, el diagrama ofrece información detallada si le interesa conocer más información acerca de cómo funcionan las puertas de enlace de volumen.

El diagrama no muestra el estado Upload Buffer Not Configured (Búfer de carga no configurado) ni el estado Deleting (Eliminando). Los estados de volumen del diagrama se representan con cuadros verdes, amarillos y rojos. Los colores se pueden interpretar de la manera siguiente.

Color	Estado de volumen
Green (Verde)	La gateway funciona con normalidad. El estado del volumen es Available (Disponible) o pasará a Available (Disponible).
Yellow (Amarillo)	Cuando se crea un volumen de almacenamiento y se conservan los datos, la ruta desde el estado Creating (Creando) al estado Pass Through (Acceso directo) se produce si hay otro volumen arrancando. En este caso, el volumen con el estado Pass Through (Acceso directo) pasa al estado Bootstrapping (Proceso de arranque) y, a continuación, al estado Available (Disponible) cuando el primer volumen termina de arrancar. Aparte de la situación específica mencionada, el amarillo (estado Pass Through (Acceso directo)) indica que existe un problema potencial con el volumen de almacenamiento, el más común de los cuales es un problema del búfer de carga. Si la capacidad del búfer de carga se ha superado, en algunos casos, el espacio del búfer vuelve a estar disponible. En ese momento, el volumen de almacenamiento se corrige automáticamente al estado Available (Disponible). En otros casos, es posible que tenga que agregar más capacidad

Color	Estado de volumen
	de búfer de carga a la gateway para devolver el volumen de almacenamiento al estado Available (Disponible). Para obtener información sobre cómo solucionar un caso cuando se supere la capacidad del búfer de carga, consulte Solución de problemas con volúmenes. Para obtener información sobre cómo agregar capacidad al búfer de carga, consulte Determinación del tamaño que se va a asignar al búfer de carga.
Rojo	El volumen de almacenamiento tiene el estado Irrecoverable (Irrecuperable). En este caso, debe eliminar el volumen. Para obtener información sobre cómo hacerlo, consulte Eliminación de volúmenes de almacenamiento.

En el siguiente diagrama, se representa una transición entre dos estados con una línea etiquetada. Por ejemplo, la transición desde el estado Creating (Creando) al estado Available (Disponible) está etiquetada como Create Basic Volume (Crear un volumen básico). Esta transición representa la creación de un volumen de almacenamiento sin conservar datos ni crear el volumen a partir de una instantánea.



> **Note**
>
> El estado Pass Through (Acceso directo) del volumen aparece como amarillo en este diagrama. Sin embargo, esto no coincide con el color de este icono de estado en el cuadro Estado de la consola de Storage Gateway.

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 los volúmenes almacenados a una nueva puerta de enlace de volumen almacenada

Para trasladar los volúmenes almacenados a una nueva puerta de enlace de volumen almacenado

1. Detenga cualquier aplicación que esté escribiendo en la antigua puerta de enlace de volumen almacenado.
2. Siga estos pasos para crear una instantánea del volumen y espere a que se complete.
   a. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
   b. En el panel de navegación, elija Volúmenes y, a continuación, elija el volumen del que desea crear la instantánea.
   c. En Actions (Acciones), seleccione Create alias (Crear alias).
   d. En el cuadro de diálogo Crear instantánea, introduzca una descripción de la instantánea y, a continuación, elija Crear instantánea.

Para verificar que la instantánea se creó, utilice la consola. Si los datos se siguen cargando en el volumen, espere a que la carga haya finalizado antes de proceder al siguiente paso. Para ver el estado de las instantáneas y comprobar que no hay ninguna pendiente, seleccione los enlaces a las instantáneas en los volúmenes.

3. Siga estos pasos para detener la antigua puerta de enlace de volumen almacenado:

   a. En el panel de navegación, elija Puertas de enlace y, a continuación, elija la puerta de enlace de volumen almacenado 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 el gateway se esté deteniendo, puede que aparezca un mensaje que indica el estado de la gateway. Cuando la puerta de enlace se apague, aparecerán un mensaje y el botón Iniciar puerta de enlace en la pestaña Detalles. Cuando la puerta de enlace se cierra, el estado de la puerta de enlace es Cerrado.

   c. Apague la máquina virtual mediante los controles del hipervisor.

   Para obtener más información acerca de detener una puerta de enlace, consulte Inicio y detención de una puerta de enlace de volumen.

4. Separe los discos de almacenamiento asociados a los volúmenes almacenados de la VM de puerta de enlace. Esto excluye el disco raíz de la VM.

5. Active un nuevo Volume Gateway almacenado con una nueva imagen de máquina virtual de hipervisor disponible en la consola de Storage Gateway de https://console.aws.amazon.com/storagegateway/su casa.

6. Conecte los discos de almacenamiento físico que desconectó de la antigua VM de la puerta de enlace de volumen almacenado en el paso 5.

7. Para conservar los datos existentes en el disco, siga los siguientes pasos para crear los volúmenes almacenados.

   a. En la consola de Storage Gateway, elija Crear volumen.

   b. En el cuadro de diálogo Crear volumen, seleccione la puerta de enlace de volumen almacenado que creó en el paso 5.

   c. Seleccione un valor de ID del disco en la lista.

d. En Contenido de volumen, elija la opción Conservar los datos existentes en el disco.

Para obtener más información sobre la creación de volúmenes, consulte Creación de un volumen de almacenamiento.

8. (Opcional) En el asistente Configurar la autenticación de CHAP que aparece, introduzca los datos de Nombre del iniciador, Secreto del iniciador y Secreto de destino; a continuación, elija Guardar.

   Para obtener más información acerca del uso de la autenticación del Protocolo de autenticación por desafío mutuo (CHAP), consulte Configuración de la autenticación CHAP para los destinos iSCSI.

9. Inicie la aplicación que escribe en el volumen almacenado.

10. Cuando haya confirmado que la nueva puerta de enlace de volumen almacenado funciona correctamente, puede eliminar la antigua puerta de enlace de volumen almacenado.

> ⚠ Important
>
> Antes de eliminar una puerta de volumen, asegúrese de que no haya aplicaciones escribiendo en el los volúmenes de la puerta de enlace. Si elimina la puerta de enlace mientras se esté utilizando, puede producirse pérdida de datos.

Siga estos pasos para eliminar la antigua puerta de enlace de volumen almacenado:

> ⚠ 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 de volumen almacenado anterior que desea eliminar.

b. En Actions (Acciones), elija Delete gateway (Eliminar la gateway).

c. En el cuadro de diálogo de confirmación que aparece, active la casilla de verificación para confirmar la eliminación. Asegúrese de que el ID de la puerta de enlace que aparece especifica la puerta de enlace de volumen que desea eliminar y, a continuación, elija Eliminar.

11. Eliminar la VM de puerta de enlace anterior. Para obtener información acerca de cómo eliminar una VM, consulte la documentación de su hipervisor.

Traslado de volúmenes en caché a una nueva máquina virtual de puerta de enlace

Para trasladar volúmenes en caché a una nueva máquina virtual (VM) de puerta de enlace de volumen en caché

1. Detenga cualquier aplicación que esté escribiendo en la antigua puerta de enlace de volumen en caché.
2. Desmonte o desconecte los volúmenes iSCSI de cualquier cliente que los utilice. Esto ayuda a mantener la coherencia de los datos de esos volúmenes al evitar que los clientes cambien o agreguen datos a esos volúmenes.
3. Siga estos pasos para crear una instantánea del volumen y espere a que se complete.

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

    b. En el panel de navegación, elija Volúmenes y, a continuación, elija el volumen del que desea crear la instantánea.

    c. En Actions (Acciones), seleccione Create alias (Crear alias).

    d. En el cuadro de diálogo Crear instantánea, introduzca una descripción de la instantánea y, a continuación, elija Crear instantánea.

    Para verificar que la instantánea se creó, utilice la consola. Si los datos se siguen cargando en el volumen, espere a que la carga haya finalizado antes de proceder al siguiente paso. Para ver el estado de las instantáneas y comprobar que no hay ninguna pendiente, seleccione los enlaces a las instantáneas en los volúmenes.

    Para obtener más información sobre la comprobación del estado del volumen, consulte Funcionamiento de los estados de volúmenes y las transiciones. Para obtener información sobre el estado del volumen en caché, consulte Cómo funcionan las transiciones de estado de volúmenes almacenados en caché .

4. Siga estos pasos para detener la antigua puerta de enlace de volumen en caché:

a. En el panel de navegación, elija Puertas de enlace y, a continuación, elija la puerta de enlace de volumen en caché 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. Anote el ID de la puerta de enlace, ya que será necesario en un paso posterior.

   Aunque la puerta de enlace se esté deteniendo, puede que aparezca un mensaje que indica el estado de la puerta de enlace. Cuando la puerta de enlace se apague, aparece un mensaje y el botón Iniciar puerta de enlace en la pestaña Detalles. Cuando la puerta de enlace se cierra, el estado de la puerta de enlace es Cerrado.

c. Apague la VM anterior mediante los controles del hipervisor. Para obtener más información sobre cómo cerrar una EC2 instancia de Amazon, consulta Cómo detener e iniciar las instancias en la Guía del EC2 usuario de Amazon. Para obtener más información sobre cómo apagar una máquina virtual KVM o Hyper-V VMware, consulte la documentación del hipervisor.

Para obtener más información acerca de detener una puerta de enlace, consulte Inicio y detención de una puerta de enlace de volumen.

5. Separe todos los discos, incluidos el disco raíz, los discos de memoria caché y los discos de búfer de carga, de la VM de puerta de enlace anterior.

> **Note**
>
> Anote el ID de volumen del disco raíz, así como el ID de puerta de enlace asociado a ese disco raíz. Desconectará este disco del nuevo hipervisor de Storage Gateway en un paso posterior. (Consulte el paso 11.)

Si utiliza una EC2 instancia de Amazon como máquina virtual para su Volume Gateway en caché, consulte Separar un volumen de Amazon EBS de una instancia de Linux en la Guía del usuario de Amazon EC2 . Para obtener información sobre cómo separar discos de una máquina virtual KVM o Hyper-V VMware, consulte la documentación del hipervisor.

6. Cree una nueva instancia de VM de hipervisor Storage Gateway, pero no la active como puerta de enlace. Para obtener más información sobre la creación de una nueva VM de hipervisor de

Storage Gateway, consulte Configuración de una puerta de enlace de volumen. Esta nueva puerta de enlace asumirá la identidad de la puerta de enlace anterior.

> **Note**
>
> No agregue discos para la memoria caché ni el búfer de carga a la nueva VM. La nueva VM utilizará los mismos discos de memoria caché y búfer de carga que utilizaba la VM anterior.

7. La nueva instancia de VM de hipervisor de Storage Gateway debe usar la misma configuración de red que la VM anterior. La configuración de red predeterminada de la gateway es DHCP (Dynamic Host Configuration Protocol). Con DHCP, a la gateway se le asigna automáticamente una dirección IP.

   Si necesita configurar manualmente una dirección IP estática para la nueva VM, consulte Configuración de red de la gateway para obtener más información. Si su puerta de enlace debe usar un proxy Socket Secure versión 5 (SOCKS5) para conectarse a Internet, consulte para obtener más información. Configuración de un SOCKS5 proxy para su puerta de enlace local
8. Inicie la nueva VM.
9. Adjunte los discos que desconectó de la antigua VM de puerta de enlace de volumen en caché en el paso 5 a la nueva VM de puerta de enlace de volumen en caché. Adjúntelos a la nueva VM de puerta de enlace en el mismo orden en que estaban en la VM de puerta de enlace anterior.

   Todos los discos deben realizar la transición sin cambios. No cambie el tamaño de los volúmenes, ya que eso provocará que los metadatos se vuelvan incoherentes.
10. Inicie el proceso de migración de la puerta de enlace conectándose a la nueva VM con una URL que utilice el siguiente formato.

    ```
    http://your-VM-IP-address/migrate?gatewayId=your-gateway-ID
    ```

    Puede volver a utilizar la misma dirección IP para la nueva VM de puerta de enlace que utilizaba para la VM de puerta de enlace anterior. La URL debe ser similar al siguiente ejemplo.

    ```
    http://198.51.100.123/migrate?gatewayId=sgw-12345678
    ```

    Utilice esta URL desde un navegador o desde la línea de comandos utilizando `curl` para iniciar el proceso de migración.

Cuando el proceso de migración de la puerta de enlace se haya iniciado correctamente, verá el siguiente mensaje:

```
Successfully imported Storage Gateway information. Please refer to
Storage Gateway documentation to perform the next steps to complete the
migration.
```

11. Desconecte el disco raíz de la antigua puerta de enlace, cuyo ID de volumen indicó en el paso 5.
12. Inicie la puerta de enlace.

    Siga estos pasos para iniciar la nueva puerta de enlace de volumen en caché:

    a. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
    b. En el panel de navegación, elija Puertas de enlace y, a continuación, elija la puerta de enlace que desee iniciar. El estado de la gateway es Shutdown (Apagada).
    c. Elija Detalles y, a continuación, Iniciar puerta de enlace.

    Para obtener más información acerca de iniciar una puerta de enlace, consulte Inicio y detención de una puerta de enlace de volumen.
13. Los volúmenes ahora deberían estar disponibles para sus aplicaciones en la dirección IP de la nueva VM de puerta de enlace.
14. Confirme que los volúmenes estén disponibles y elimine la VM de puerta de enlace anterior. Para obtener información acerca de cómo eliminar una VM, consulte la documentación de su hipervisor.

Supervisión de Storage Gateway

En esta sección se describe cómo monitorizar una Storage Gateway, 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 al respecto CloudWatch, consulta la Guía CloudWatch del usuario de Amazon.

Para obtener información específica sobre la supervisión de una puerta de enlace de volumen y sus recursos asociados, consulte Supervisión de la puerta de enlace de volumen.

Temas

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`	Número de notificaciones de estado relacionadas con la disponibilidad que ha generado la gateway. 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, compruebe el grupo de CloudWatch registros configurado. Unidad: número

Métrica	Descripción	
`CacheHitPercent`	Porcentaje de lecturas de aplicación servidas desde la caché. La muestra se obtiene al final del período de notificación. Unidad: porcentaje	
`CachePercentDirty`	El porcentaje total de la memoria caché de la puerta de enlace que no se ha conservado. AWS La muestra se obtiene al final del período de notificación. Utilice esta métrica con la `Sum` estadística. Lo ideal sería que esta métrica permaneciera baja. Unidad: porcentaje	
`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. Unidad: bytes	
`IoWaitPercent`	Porcentaje de tiempo que la gateway está esperando una respuesta del disco local. Unidad: porcentaje	

Métrica	Descripción	
MemTotalBytes	Cantidad de RAM aprovisionada para la máquina virtual de la gateway, en bytes. Unidad: bytes	
MemUsedBytes	Cantidad de RAM utilizada actualmente por la máquina virtual de la gateway, en bytes. Unidad: bytes	
QueuedWrites	Normalmente, este valor representa el número de bytes almacenados localmente en espera de ser escritos AWS, pero también refleja el proceso de sincronización que se produce entre los datos locales y los datos en la nube durante el «arranque», que se produce cada vez que se reinicia una puerta de enlace. Unidad: bytes	

Métrica	Descripción	
ReadBytes	El número total de bytes leídos de las aplicaciones on-premises en el período de notificación para todos los volúmenes de la gateway. Utilice esta métrica con la estadística Sum para medir la velocidad y con la estadísti ca Samples para medir las operaciones de entrada/salida por segundo (IOPS). Unidad: bytes	
ReadTime	El número total de milisegun dos empleados en operacion es de lectura desde las aplicaciones on-premises en el período de notificación para todos los volúmenes de la gateway. Use esta métrica con la estadística Average para medir la latencia. Unidad: milisegundos	

Métrica	Descripción
`TimeSinceLastRecoveryPoint`	El tiempo desde el último punto de recuperación disponible. Para obtener más información, consulte La gateway almacenada en la caché es inaccesible y desea recuperar los datos. Unidad: segundos
`TotalCacheSize`	El tamaño total de la caché en bytes. La muestra se obtiene al final del período de notificación. Unidad: bytes
`UploadBufferPercentUsed`	Porcentaje de uso del búfer de carga de la gateway. La muestra se obtiene al final del período de notificación. Unidad: porcentaje
`UploadBufferUsed`	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. Unidad: bytes

Métrica	Descripción	
UserCpuPercent	Porcentaje de tiempo de CPU empleado en el procesamiento de la gateway. Se calcula el promedio en todos los núcleos. Unidad: porcentaje	
WorkingStorageFree	La cantidad total de espacio no utilizado en el almacenamiento de trabajo de la gateway. La muestra se obtiene al final del período de notificación. Unidad: bytes	
WorkingStoragePercentUsed	Porcentaje de uso del búfer de carga de la gateway. La muestra se obtiene al final del período de notificación. Unidad: porcentaje	
WorkingStorageUsed	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. Unidad: bytes	

Métrica	Descripción	
`WriteBytes`	El número total de bytes escritos en las aplicaciones on-premises en el período de notificación para todos los volúmenes de la gateway. Utilice esta métrica con la estadística `Sum` para medir la velocidad y con la estadísti ca `Samples` para medir las operaciones de entrada/salida por segundo (IOPS). Unidad: bytes	
`WriteTime`	El número total de milisegun dos empleados en operacion es de escritura desde las aplicaciones on-premises en el período de notificación para todos los volúmenes de la gateway. Use esta métrica con la estadística `Average` para medir la latencia. Unidad: milisegundos	

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`	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` . Los datos de velocidad y latencia de una gateway se basan en todos los volúmenes de esa gateway. Para obtener información acerca del uso de métricas de puerta de enlace, consulte Medición del rendimiento entre la puerta de enlace y AWS.
`VolumeId`	Esta dimensión filtra los datos solicitados a las métricas específicas del volumen. Identifique un volumen de almacenamiento para trabajar mediante el valor `VolumeId`. Para obtener información acerca del uso de métricas de volumen, consulte Medición del rendimiento entre la aplicación y la gateway.

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 volumen.

> **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 `UploadBufferPercentUsed` , `UploadBufferUsed` y `UploadBufferFree` con la estadística `Average`. Por ejemplo, utilice `UploadBufferUsed` con la estadística `Average` 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 tema de Amazon SNS. Para obtener más información sobre Amazon SNS, consulte Configuración de Amazon SNS en la Guía del usuario de Amazon CloudWatch .

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 correo electrónico de Amazon SNS que se envío a la dirección de correo electrónico que especificó al crear el tema.

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.

Monitorice el almacenamiento en caché solamente en la arquitectura de volúmenes almacenados en caché. Para obtener más información, consulte Funcionamiento de puerta de enlace de volumen.

Elemento de Interés	Cómo medirlo
Uso total de caché	Utilice las métricas `CachePercentUsed` y `TotalCacheSize` con la estadística `Average`. Por ejemplo, utilice `CachePercentUsed` con la estadística `Average` para analizar el uso de la memoria caché durante un periodo de tiempo. La métrica `TotalCacheSize` solo cambia cuando se agrega caché a la gateway.
Porcentaje de solicitudes de lectura que se sirven desde la caché	Utilice la métrica `CacheHitPercent` con la estadística `Average`. Normalmente, es deseable que el valor `CacheHitPercent` se mantenga alto.
Porcentaje de la caché que está sucia, es decir, contiene contenido que no se ha cargado en AWS	Utilice la métrica `CachePercentDirty` con la estadística `Average`. Normalmente, es deseable que el valor `CachePercentDirty` se mantenga bajo.

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.

Comprensión de 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 volumen, consulte Descripción de las métricas de cintas virtuales y Información acerca de las métricas de volúmenes. Para cada alarma, especifique las

condiciones que iniciarán su estado de ALARMA. Los indicadores de estado de alarma de la consola de Storage Gateway se iluminan en rojo cuando están en estado de ALARMA, lo que facilita la supervisión del estado de forma proactiva. Puede configurar las alarmas para que invoquen acciones automáticamente en función de los cambios sostenidos de estado. Para obtener más información sobre CloudWatch las alarmas, consulta Uso de CloudWatch las alarmas de Amazon en la Guía del CloudWatch usuario de Amazon.

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

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

- Espera de E/S de alto desempeño: `IoWaitpercent` >= 20 para 3 puntos de datos en 15 minutos
- Porcentaje de caché sucia: `CachePercentDirty` > 80 para 4 puntos de datos en 20 minutos
- Notificaciones de estado: `HealthNotifications` >= 1 para 1 punto de datos en 5 minutos. Al configurar esta alarma, defina Tratamiento de datos faltantes como notBreaching.

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

Para las puertas de enlace en plataformas VMware host 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 como 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.

Estado	Descripción
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 Creación de una CloudWatch alarma personalizada para su puerta de enlace.
No disponible	Se desconoce el estado de la alarma. Elija Unavailable (No disponible) para ver la información de error en la pestaña Monitoring (Monitorización) .

Creación de CloudWatch 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 volumen. 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.

Creación de una CloudWatch alarma personalizada para su puerta de enlace

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

Para crear una CloudWatch alarma en la consola Storage Gateway

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

3. En la página de detalles de la puerta de enlace, elija la pestaña Supervisión.
4. En Alarmas, seleccione Crear alarma para abrir la CloudWatch consola.
5. Usa la CloudWatch consola para crear el tipo de alarma que desees. Puede crear los siguientes tipos de alarma:

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

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

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

     Para crear una alarma de expresión matemática métrica, consulte Creación de una CloudWatch alarma basada en una expresión matemática métrica en la Guía del CloudWatch usuario de Amazon.
   - Alarma compuesta: alarma que determina su estado observando los estados de otras alarmas. Una alarma compuesta puede ayudarle a reducir el ruido de las alarmas.

     Para crear una alarma compuesta, consulta Cómo crear una alarma compuesta en la Guía del CloudWatch usuario de Amazon.
6. Tras crear la alarma en la CloudWatch consola, vuelva a la consola de Storage Gateway. Para ver la alarma, realice una de las siguientes acciones:

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

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

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

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

Supervisión de la puerta de enlace de volumen

Los temas de esta sección describen cómo supervisar una puerta de enlace de volumen en una configuración de volúmenes en caché o volúmenes almacenados, incluida la supervisión de los volúmenes asociados a la puerta de enlace y la supervisión del búfer de carga. Se usa AWS Management Console para ver las métricas de su 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 la nube de Amazon Web Services. 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. Para obtener información detallada al respecto CloudWatch, consulta la Guía del CloudWatch usuario de Amazon.

Temas

- Obtener los registros de estado de Volume Gateway con Amazon CloudWatch Logs- Aprenda a usar Amazon CloudWatch Logs para obtener información sobre el estado de su Volume Gateway y los recursos relacionados.
- Uso de Amazon CloudWatch Metrics- Aprenda a obtener datos de monitoreo para su pasarela mediante la API AWS Management Console o la CloudWatch API.
- Medición del rendimiento entre la aplicación y la gateway: obtenga información sobre cómo medir el rendimiento de datos, la latencia de datos y las operaciones por segundo para entender el rendimiento entre las aplicaciones y la puerta de enlace.
- Medición del rendimiento entre la puerta de enlace y AWS- Aprenda a medir el rendimiento de los datos, la latencia de los datos y las operaciones por segundo para comprender el rendimiento entre su puerta de enlace y la AWS nube.
- Información acerca de las métricas de volúmenes: obtenga información sobre cómo medir las métricas que proporcionan datos sobre los volúmenes asociados a una puerta de enlace.

Obtener los registros de estado de Volume Gateway con Amazon CloudWatch Logs

Puede utilizar Amazon CloudWatch Logs para obtener información sobre el estado de su Volume Gateway y los recursos relacionados. Puede utilizar estos 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 (HA) y necesita saber si hay algún 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, consulteConfiguración de la puerta de enlace de volumen. 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 volúmenes.

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

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 izquierdo, elija Gateways y, a continuación, elija la puerta de enlace para la que desea configurar el grupo de CloudWatch registros.
3. En Acciones, elija Editar la información de la puerta de enlace o, en la pestaña Detalles, en Registros de estado y No activado, elija Configurar grupo de registros para abrir el cuadro de *CustomerGatewayName* diálogo 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 izquierdo, 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 de Amazon.

Uso de Amazon CloudWatch Metrics

Puede obtener los datos de supervisión de su puerta de enlace mediante la API AWS Management Console o la CloudWatch API. La consola muestra una serie de gráficos basados en los datos sin

procesar de la CloudWatch API. También puede utilizar la CloudWatch API a través de uno de los kits de desarrollo de AWS software (SDKs) o las herramientas de la CloudWatch API de Amazon. En función de sus necesidades, es posible que prefiera utilizar los gráficos que se muestran en la consola o que se recuperan de la API.

Independientemente del método que 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`, `GatewayName` y `VolumeId`. En la CloudWatch consola, puede utilizar las `Volume Metrics` vistas `Gateway Metrics` y para seleccionar fácilmente las dimensiones específicas de la pasarela y del volumen. 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 puede utilizar.

CloudWatch Espacio de nombres	Dimensión	Descripción
`AWS/StorageGateway`	`GatewayId` , `GatewayName`	Estas dimensiones filtran datos de métricas que describen aspectos de la gateway. Puede identificar una gateway con la que trabajar especificando las dimensiones `GatewayId` y `GatewayName` . Los datos de rendimiento y latencia de una puerta de enlace se basan en todos los volúmenes de la puerta de enlace. Los datos se encuentran disponibles automáticamente en periodos de 5 minutos sin costo alguno.
	`VolumeId`	Esta dimensión filtra datos de métricas específicos de un volumen. Puede identificar un volumen con el que trabajar por su dimensión `VolumeId`.

CloudWatch Espacio de nombres	Dimensión	Descripción
		Los datos se encuentran disponibles automáticamente en periodos de 5 minutos sin costo alguno.

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

- Visualización de métricas disponibles
- Obtención de estadísticas de una métrica
- Creación de alarmas de CloudWatch

Medición del rendimiento entre la aplicación y la gateway

El rendimiento de datos, la latencia de datos y las operaciones por segundo son tres medidas que puede utilizar para conocer el rendimiento del almacenamiento de aplicación que está utilizando la gateway. Cuando utilice la estadística de agregación correcta, puede utilizar métricas de Storage Gateway para medir estos valores.

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), utilice la `Sum` estadística para el rendimiento de los datos (bytes por segundo) 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 tabla siguiente se indican las métricas y las correspondientes estadísticas que puede utilizar para medir el rendimiento, la latencia y las IOPS entre las aplicaciones y las gateways.

Elemento de Interés	Cómo medirlo
Rendimiento	Utilice las métricas `ReadBytes` y `WriteBytes` con la estadística `Sum` CloudWatch . Por ejemplo, el valor `Sum` de la métrica `ReadBytes` durante un periodo de muestra de 5 minutos dividido entre 300 segundos devuelve el rendimiento como un índice de bytes por segundo.

Elemento de Interés	Cómo medirlo
Latencia	Utilice las métricas `ReadTime` y `WriteTime` 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.
IOPS	Utilice las métricas `ReadBytes` y `WriteBytes` con la estadística `Samples` CloudWatch . Por ejemplo, el valor `Samples` de la métrica `ReadBytes` durante un periodo de muestra de 5 minutos dividido entre 300 segundos proporciona las IOPS.

Para los gráficos de latencia media y los gráficos de tamaño medio, la media se calcula para el número total de operaciones (lectura o escritura, lo que corresponda al gráfico) completadas durante el periodo.

Para medir el rendimiento de datos desde una aplicación hasta un volumen

1. Abre la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. Elija Metrics (Métricas) y, a continuación, elija la pestaña All metrics (Todas las métricas) y elija Storage Gateway.
3. Elija la dimensión Volume metrics (Métricas de volumen) y busque el volumen con el que desee trabajar.
4. Elija las métricas `ReadBytes` y `WriteBytes`.
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 los conjuntos de puntos de datos resultantes ordenados temporalmente (uno para `ReadBytes` y otro para `WriteBytes`), divida cada punto de datos por el periodo (en segundos) para obtener el rendimiento en el punto de muestra. El rendimiento total es la suma de los rendimientos.

Por ejemplo, si el rendimiento de lectura es de 2 384 199 680 bytes durante un periodo de 300 segundos, la tasa de rendimiento aproximado para ese punto de datos es de 7,9 megabytes por segundo.

Para medir las operaciones de entrada/salida de datos por segundo desde una aplicación hasta un volumen

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. Elija Metrics (Métricas) y, a continuación, elija la pestaña All metrics (Todas las métricas) y elija Storage Gateway.
3. Elija la dimensión Volume metrics (Métricas de volumen) y busque el volumen con el que desee trabajar.
4. Elija las métricas `ReadBytes` y `WriteBytes`.
5. Para Time Range (Intervalo de tiempo), elija un valor.
6. Elija la estadística `Samples`.
7. Para Period (Periodo), elija un valor de 5 minutos o mayor.
8. En los conjuntos de puntos de datos resultantes ordenados temporalmente (uno para `ReadBytes` y otro para `WriteBytes`), divida cada punto de datos por el periodo (en segundos) para obtener IOPS.

Por ejemplo, si el número de operaciones de escritura es de 24 373 durante un periodo de 300 segundos, la IOPS de ese punto de datos es de 81 operaciones de escritura por segundo.

Medición del rendimiento entre la puerta de enlace y AWS

El rendimiento de datos, la latencia de datos y las operaciones por segundo son tres medidas que puede utilizar para conocer el rendimiento del almacenamiento de aplicación que está utilizando Storage Gateway. Estos tres valores pueden medirse utilizando las métricas de Storage Gateway que se le proporcionan cuando utiliza la estadística de agregación correcta. En la tabla siguiente se indican las métricas y las correspondientes estadísticas que puede utilizar para medir el rendimiento, la latencia y las operaciones de entrada/salida por segundo (IOPS) entre la puertas de enlace y AWS.

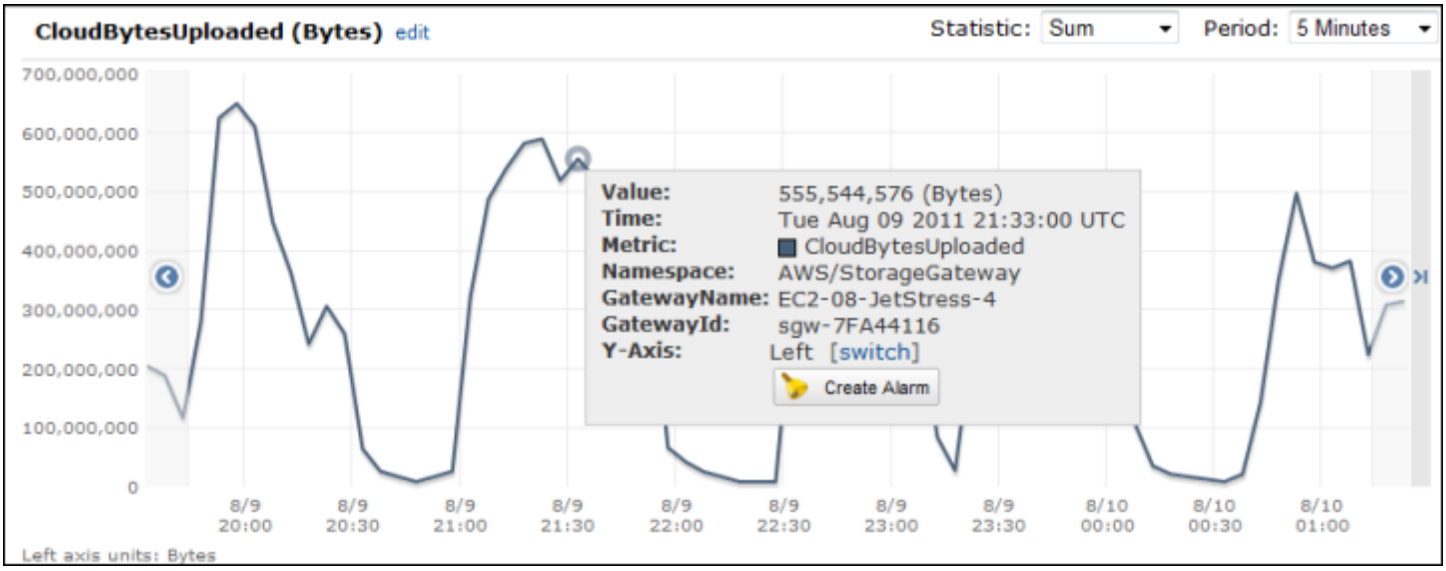
Elemento de Interés	Cómo medirlo
Rendimiento	Utilice las métricas `ReadBytes` y `WriteBytes` con la estadística `Sum` CloudWatch . Por ejemplo, el valor `Sum` de la métrica `ReadBytes` durante un periodo de muestra de 5 minutos dividido entre 300 segundos devuelve el rendimiento como un índice de bytes por segundo.

Elemento de Interés	Cómo medirlo
Latencia	Utilice las métricas `ReadTime` y `WriteTime` 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.
IOPS	Utilice las métricas `ReadBytes` y `WriteBytes` con la estadística `Samples` CloudWatch . Por ejemplo, el valor `Samples` de la métrica `ReadBytes` durante un periodo de muestra de 5 minutos dividido entre 300 segundos proporciona las IOPS.
Rendimiento hasta 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 minutos dividido entre 300 segundos indica el rendimiento desde AWS la puerta de enlace en bytes por segundo.
Latencia de los datos hasta AWS	Utilice la métrica `CloudDownloadLatency` con la estadística `Average`. Por ejemplo, la estadística `Average` de la métrica `CloudDownloadLatency` proporciona la latencia por operación.

Para medir el rendimiento de los datos de carga desde una puerta de enlace a AWS

1. Abre la CloudWatch consola en. https://console.aws.amazon.com/cloudwatch/
2. Elija Metrics (Métricas) y, a continuación, elija la pestaña All metrics (Todas las métricas) y elija Storage Gateway.
3. Elija la dimensión Gateway metrics (Métricas de gateway) y busque el volumen con el 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.

Al mover el cursor sobre un punto de datos se muestra información sobre el punto de datos, incluidos su valor y los bytes cargados. Divida este valor de bytes entre el valor de Period (Periodo) (5 minutos) para obtener el rendimiento en ese punto de muestra. Por ejemplo, si el rendimiento desde la puerta de enlace AWS es de 555.544.576 bytes durante un período de 300 segundos, el rendimiento aproximado por segundo es de 1,85 megabytes por segundo.



Para medir la latencia por operación de una gateway

1. Abra la consola en. CloudWatch https://console.aws.amazon.com/cloudwatch/
2. Elija Metrics (Métricas) y, a continuación, elija la pestaña All metrics (Todas las métricas) y elija Storage Gateway.
3. Elija la dimensión Gateway metrics (Métricas de gateway) y busque el volumen con el que desee trabajar.
4. Elija las métricas `ReadTime` y `WriteTime`.
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.
8. En el conjunto resultante de puntos ordenados temporalmente (uno para `ReadTime` y otro para `WriteTime`), agregue puntos de datos a la misma muestra temporal para obtener la latencia total en milisegundos.

Para medir la latencia de los datos desde una puerta de enlace a AWS

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. Elija Metrics (Métricas) y, a continuación, elija la pestaña All metrics (Todas las métricas) y elija Storage Gateway.
3. Elija la dimensión Gateway metrics (Métricas de gateway) y busque el volumen con el 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 en AWS

1. Abra la CloudWatch consola en. https://console.aws.amazon.com/cloudwatch/
2. Elija Alarms (Alarmas).
3. Seleccione Create Alarm (Crear alarma) para iniciar el asistente Crear alarma.
4. Elija la dimensión Storage Gateway y busque la gateway con la que desee trabajar.
5. Elija la métrica `CloudBytesUploaded`.
6. 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 MB durante 60 minutos.
7. 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.
8. Seleccione Crear alarma.

Para configurar una alarma de umbral superior para leer 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 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.

Información acerca de las métricas de volúmenes

A continuación puede encontrar información sobre las métricas de Storage Gateway que cubren un volumen de una puerta de enlace. Cada volumen de una gateway tiene un conjunto de métricas asociado.

Algunas de las métricas específicas de volumen tienen el mismo nombre que determinadas métricas específicas de gateway. Estas métricas representan el mismo tipo de medidas, pero se asignan al volumen en lugar de a la gateway. Antes de comenzar a trabajar, especifique si desea trabajar con una métrica de gateway o una métrica de volumen. A la hora de trabajar con métricas de volumen, especifique el ID de volumen del volumen de almacenamiento del 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 tabla siguiente se describen las métricas de Storage Gateway que puede utilizar para obtener información sobre los volúmenes de almacenamiento.

Métrica	Descripción	Volúmenes almacenados en caché	Volúmenes almacenados
`AvailabilityNotification`	Número de notificaciones de disponibilidad que ha enviado el volumen. Unidades: recuento	Sí	Sí
`CacheHitPercent`	Porcentaje de operaciones de lectura de la aplicación desde el volumen que se sirven desde la caché. La muestra se obtiene al final del período de notificación. Cuando no hay operaciones de lectura de la aplicación desde el volumen, esta métrica registra un valor del 100%. Unidad: porcentaje	Sí	No
`CachePercentDirty`	La contribución del volumen al porcentaje total de memoria caché de la gateway que no se ha almacenado de forma persistente en AWS. La muestra se obtiene	Sí	Sí

Métrica	Descripción	Volúmenes almacenados en caché	Volúmenes almacenados
	al final del período de notificación. 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. Unidad: porcentaje		

Métrica	Descripción	Volúmenes almacenados en caché	Volúmenes almacenados
`CachePercentUsed`	La contribución del volumen al porcentaje de uso total de almacenamiento en memoria caché de la gateway. La muestra se obtiene al final del período de notificación. Use la métrica `CachePercentUsed` de la gateway para ver el porcentaje de uso total de almacenamiento en memoria caché de la gateway. Para obtener más información, consulte Información acerca de las métricas de gateway. Unidad: porcentaje	Sí	No
`CloudBytesDownloaded`	Número de bytes descargados desde la nube al volumen. Unidades: bytes	Sí	Sí

Métrica	Descripción	Volúmenes almacenados en caché	Volúmenes almacenados
`CloudBytesUploaded`	Número de bytes cargados desde la nube al volumen. Unidades: bytes	Sí	Sí
`HealthNotification`	Número de notificaciones de estado que ha enviado el volumen. Unidades: recuento	Sí	Sí
`IoWaitPercent`	El porcentaje de IoWaitPercent unidades que el volumen utiliza actualmente. Unidad: porcentaje	Sí	Sí
`MemTotalBytes`	Porcentaje de memoria total que utiliza actualmente el volumen. Unidad: porcentaje	Sí	No
`MemoryUsage`	Porcentaje de memoria que utiliza actualmente el volumen. Unidad: porcentaje	Sí	No

Métrica	Descripción	Volúmenes almacenados en caché	Volúmenes almacenados
`ReadBytes`	El número total de bytes leídos desde las aplicaciones on-premises en el período de notificación. Utilice esta métrica con la estadística `Sum` para medir la velocidad y con la estadística `Samples` para medir las operaciones de entrada/salida por segundo (IOPS). Unidades: bytes	Sí	Sí

Métrica	Descripción	Volúmenes almacenados en caché	Volúmenes almacenados
`ReadTime`	El número total de milisegundos empleados en operaciones de lectura desde las aplicaciones en las instalaciones en el periodo de notificación. Use esta métrica con la estadística `Average` para medir la latencia. Unidades: milisegundos	Sí	Sí
`UserCpuPercent`	Porcentaje de unidades informáticas CPU asignadas que se utilizan actualmente en el volumen. Unidad: porcentaje	Sí	Sí

Métrica	Descripción	Volúmenes almacenados en caché	Volúmenes almacenados
`WriteBytes`	El número total de bytes escritos en las aplicaciones on-premises en el período de notificación. Utilice esta métrica con la estadística `Sum` para medir la velocidad y con la estadística `Samples` para medir las operaciones de entrada/salida por segundo (IOPS). Unidades: bytes	Sí	Sí

Métrica	Descripción	Volúmenes almacenados en caché	Volúmenes almacenados
`WriteTime`	El número total de milisegundos empleados en operaciones de escritura desde las aplicaciones en las instalaciones en el periodo de notificación. Use esta métrica con la estadística `Average` para medir la latencia. Unidades: milisegundos	Sí	Sí
`QueuedWrites`	El número de bytes en espera de ser escritos AWS, muestreado al final del período del informe. Unidades: bytes	Sí	Sí

Mantenimiento de la gateway

El mantenimiento de la Puerta de enlace de volumen incluye tareas como la modificación del tamaño y la configuración de los discos locales para el almacenamiento en caché y el espacio en el búfer de carga, la administración de las actualizaciones y el establecimiento de un programa de actualizaciones, la administración del uso del ancho de banda y el cierre o eliminación de la puerta de enlace y los recursos asociados, si es necesario. Estas tareas son comunes para todos los tipos de gateways. Si no ha creado una gateway, consulte Creación de la puerta de enlace.

Temas

- Administración de discos locales para Storage Gateway: obtenga información sobre cómo evaluar los requisitos de tamaño de disco, agregar capacidad de caché y administrar los discos locales que asigna a la Puerta de enlace de volumen para el almacenamiento y el almacenamiento en búfer.
- Administración del ancho de banda de la puerta de enlace de volumen- Aprenda a limitar el rendimiento de carga desde su puerta de enlace AWS para controlar la cantidad de ancho de banda de red que utiliza la puerta de enlace.
- Administración de actualizaciones de puertas de enlace: obtenga información sobre cómo activar o desactivar las actualizaciones de mantenimiento y modificar la programación de los periodos de mantenimiento de la Puerta de enlace de volumen.
- Como apagar la MV de la gateway: obtenga información sobre qué hacer si necesita apagar o reiniciar la máquina virtual de puerta de enlace para realizar tareas de mantenimiento, por ejemplo, al aplicar un parche al hipervisor.
- Eliminación de la puerta de enlace y eliminación de los recursos asociados- Aprenda a eliminar su puerta de enlace mediante la AWS Storage Gateway consola y a limpiar los recursos asociados para evitar que se les cobre por su uso continuo.

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 las EC2 instancias de Amazon utilizan los volúmenes de Amazon EBS como discos locales.

Temas

- Cálculo de la cantidad de almacenamiento en disco local

- 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. En función de la solución de almacenamiento que vaya a implementar, la puerta de enlace requiere el siguiente almacenamiento adicional:

- Puertas de enlace de volumen:
  - Las gateways almacenados requieren al menos un disco para utilizar como búfer de carga.
  - Las gateways en caché 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 de enlace los cargue a Amazon S3. La gateway carga estos datos del búfer a través de una conexión de Capa de conexión segura (SSL) en 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 aplicació n efectúa entradas y salidas en un volumen o cinta, la gateway	

Almacenamiento local	Descripción	
	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 aprovisione discos, recomendamos encarecidamente que no aprovisione 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 de caché y del búfer de carga. Esto también es cierto si la copia de seguridad es una configuración RAID 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.

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 volumen, cuando el búfer de carga alcanza su capacidad, el volumen cambia al estado ACCESO DIRECTO. En este estado, los datos nuevos que escribe la aplicación se conservan localmente, pero no se cargan de inmediato en AWS . Por lo tanto, no se pueden tomar nuevas instantáneas. Cuando se libera capacidad en el búfer de carga, el volumen pasa por el estado BOOTSTRAPPING. En este estado, se cargan todos los datos nuevos que se hayan conservado localmente. AWS Por último, el volumen vuelve al estado ACTIVO. A continuación, Storage Gateway reanuda la sincronización normal de los datos almacenados localmente con la copia almacenada y puede empezar a tomar nuevas instantáneas. AWS Para obtener más información sobre el estado de los volúmenes, consulte Funcionamiento de los estados de volúmenes y las transiciones.

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.

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. Aprovisione uno o más discos nuevos en el hipervisor del host de la puerta de enlace o en la EC2 instancia de Amazon. Para obtener información sobre cómo aprovisionar un disco en un hipervisor, consulte el manual de usuario del hipervisor. Para obtener información sobre el aprovisionamiento de volúmenes de Amazon EBS para una EC2 instancia de Amazon, consulte los volúmenes de Amazon EBS en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux. En los siguientes pasos, configurará este disco como 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 BÚFER DE CARGA o ALMACENAMIENTO EN CACHÉ en el menú desplegable Asignado a.

> **Note**
>
> BÚFER DE CARGA es la única opción disponible para asignar discos en las puertas de enlace de volumen almacenado.

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

Administración del ancho de banda de la puerta de enlace de volumen

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 la AWS Management Console API Storage Gateway (consulte UpdateBandwidthRateLimit) o un kit de desarrollo de AWS software (SDK), o mediante programación. 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

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

6. Tras introducir todos los bandwidth-rate-limit intervalos, seleccione 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 para 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 para Java. Para utilizar el código del ejemplo,

debe haberse familiarizado con la ejecución de aplicaciones de la consola de Java. Para obtener más información, consulte Introducción en la Guía para desarrolladores de AWS SDK para Java .

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

El siguiente ejemplo de código Java actualiza los límites de velocidad del ancho de banda de una puerta de enlace. Debe actualizar el código y proporcionar el punto de conexión de servicio, el Nombre de recurso de Amazon (ARN) de la 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 bandwith.\n" + ex.toString());
        }
    }
}
```

Actualización de los límites de ancho de banda de Gateway mediante AWS SDK para .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 para .NET. Para utilizar el código del ejemplo, debe haberse familiarizado con la ejecución de aplicaciones de la consola de .NET. Para obtener más información, consulte Introducción en la Guía para desarrolladores de AWS SDK para .NET .

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

El siguiente ejemplo de código C# actualiza los límites de velocidad del ancho de banda de una puerta de enlace. Debe actualizar el código y proporcionar el punto de conexión de servicio, el Nombre de recurso de Amazon (ARN) de la 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 bandwith.\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 Herramientas de AWS para PowerShell .

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

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

Administración de actualizaciones de puertas de enlace

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

> **Important**
>
> Debe tratar el dispositivo de Storage Gateway como una máquina virtual administrada y no debe intentar acceder a su instalación ni modificarla de forma alguna. Si intenta instalar o actualizar cualquier paquete de software mediante métodos distintos al mecanismo de actualización habitual de la AWS puerta de enlace (por ejemplo, el SSM o las herramientas de hipervisor), es posible que la puerta de enlace no funcione correctamente.

Frecuencia de actualización y comportamiento esperado

AWS actualiza el componente de servicios en la nube según sea necesario sin interrumpir las pasarelas implementadas. Los dispositivos de puerta de enlace implementados reciben 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 acceso a nuevas características. Todas las actualizaciones son acumulativas y actualizan las puertas de enlace a la versión actual cuando se aplican. Para obtener información sobre los cambios específicos incluidos en cada actualización, consulte las notas de la versión del software del dispositivo de puerta de enlace de volumen.

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 periodo de tiempo mientras el dispositivo de puerta de enlace se actualiza y se reinicia. Puede reducir la probabilidad de interrupción de las aplicaciones a causa del reinicio de la gateway aumentando los tiempos de espera del iniciador iSCSI. Para obtener más información sobre el aumento de los tiempos de espera de los iniciadores iSCSI para Windows y Linux, consulte Personalización de la configuración iSCSI de Windows y Personalización de la configuración de iSCSI de Linux.

Cuando implemente y active la puerta de enlace, se establecerá un calendario de periodos de mantenimiento semanal predeterminado. Puede modificar el calendario de periodos 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 periodos de mantenimiento, incluso si las actualizaciones de mantenimiento periódicas están desactivadas.

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

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

Activación o desactivación de las actualizaciones de mantenimiento

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

Si las actualizaciones de mantenimiento están desactivadas, la puerta de enlace no las aplicará automáticamente, pero siempre podrá aplicarlas manualmente mediante la consola, la API o la CLI de Storage Gateway. En ocasiones, las actualizaciones urgentes se aplicarán durante el periodo de mantenimiento configurado, independientemente de esta configuración.

> **Note**
>
> En el siguiente procedimiento se describe cómo activar o desactivar las actualizaciones de puerta de enlace mediante la consola de Storage Gateway. Para cambiar esta

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

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

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

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

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

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

> **Note**
>
> El siguiente procedimiento describe cómo modificar la programación del período de mantenimiento mediante la consola de Storage Gateway. Para cambiar esta configuración mediante programación mediante la API, consulte la referencia de la API UpdateMaintenanceStartTimede Storage Gateway.

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

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

2. En el panel de navegación, elija Puertas de enlace y, a continuación elija la puerta de enlace para la que desee configurar actualizaciones de mantenimiento.
3. Elija Acciones y, a continuación, elija Editar la configuración de mantenimiento.
4. En Hora de inicio del periodo de mantenimiento, haga lo siguiente:

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

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

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

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

5. Cuando haya finalizado, elija Guardar cambios.

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

Aplicación de una actualización manualmente

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

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

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

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

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

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

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

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. Aunque esta sección se centra en iniciar y detener la puerta de enlace desde la consola de administración de Storage Gateway, tenga en cuenta que también puede hacerlo desde la consola

local de la máquina virtual o con la API de Storage Gateway. 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 nueva EC2 .

> **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 de Puerta de enlace de volumen.
- API Storage Gateway: consulte ShutdownGateway

Inicio y detención de una puerta de enlace de volumen

Para detener una puerta de enlace de volumen

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 volumen

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).

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

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

Al eliminar una puerta de enlace, deja de aparecer en la consola de AWS Storage Gateway administración y su conexión iSCSI 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.

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

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 planee utilizar.

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

Para eliminar una puerta de enlace

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

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

puede producirse pérdida de datos. Cuando se elimina una gateway, no se puede recuperar.

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

Important

Ya no pagas cargos de software después de eliminar una puerta de enlace, pero recursos como las cintas virtuales, las instantáneas de Amazon Elastic Block Store (Amazon EBS) y EC2 las instancias de Amazon persisten. Estos recursos se le seguirán facturando. Puede optar por eliminar las EC2 instancias de Amazon y las instantáneas de Amazon EBS cancelando su suscripción a Amazon. EC2 Si quieres conservar tu EC2 suscripción a Amazon, puedes eliminar las instantáneas de Amazon EBS mediante la consola de Amazon EC2.

Eliminación de recursos de una gateway implementada on-premises

Puede utilizar las instrucciones siguientes para eliminar recursos de una gateway implementada on-premises.

Eliminación de recursos de una gateway de volúmenes implementada en una MV

Si la puerta de enlace que desea eliminar está implementada en una máquina virtual (VM), le sugerimos que realice las acciones siguientes para limpiar los recursos:

- Elimine la puerta de enlace. Para obtener instrucciones, consulte Eliminación de la puerta de enlace mediante la consola de Storage Gateway.
- Elimine todas las instantáneas de Amazon EBS que no necesite. Para obtener instrucciones, consulte Eliminar una instantánea de Amazon EBS en la Guía del EC2 usuario de Amazon.

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 volumen de Amazon EBS y también las cintas si implementó una puerta de enlace de cinta. Así contribuirá a evitar cargos por uso no deseados.

Eliminar recursos de los volúmenes en caché implementados en Amazon EC2

Si implementó una puerta de enlace con los volúmenes en caché activados EC2, le sugerimos que tome las siguientes medidas para eliminar la puerta de enlace y limpiar sus recursos:

1. En la consola de Storage Gateway, elimine la puerta de enlace como se muestra en Eliminación de la puerta de enlace mediante la consola de Storage Gateway.
2. En la EC2 consola de Amazon, detiene la EC2 instancia si piensas volver a usarla. De lo contrario, finalice la instancia. Si piensa eliminar volúmenes, anote los dispositivos de bloques asociados a la instancia y los identificadores de los dispositivos antes de finalizar la instancia. Los necesitará para identificar los volúmenes que desee eliminar.
3. En la EC2 consola de Amazon, elimina todos los volúmenes de Amazon EBS que estén adjuntos a la instancia si no piensas volver a usarlos. Para obtener más información, consulta Limpiar tu instancia y volumen en la Guía del EC2 usuario de Amazon.

Realización de tareas de mantenimiento con la consola local

Esta sección contiene los siguientes temas, que proporcionan información sobre cómo realizar tareas de mantenimiento mediante la consola local del dispositivo de puerta de enlace. La consola local se ejecuta directamente en la plataforma de host de virtualización que aloja el dispositivo de puerta de enlace. En el caso de las puertas de enlace locales, puede acceder a la consola local a través de su host de VMware virtualización KVM de Hyper-V o Linux. En el caso de EC2 las pasarelas de Amazon, se accede a la consola conectándose a la EC2 instancia de Amazon mediante SSH. La mayoría de las tareas son comunes entre las distintas plataformas de hosts, pero también hay algunas diferencias.

Temas

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

Acceso a la consola local de la 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 de la máquina virtual basada en el núcleo de Linux (KVM) VMware ESXi y Microsoft Hyper-V Manager.

Temas

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

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

Acceso a la consola local de la gateway con Linux KVM

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

Para obtener acceso a la consola local de la gateway con KVM

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

   ```
   # virsh list
   ```

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

   ```
   # virsh console Id
   ```

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

   La consola local de AWS Appliance Gateway le pide que inicie sesión para cambiar la configuración de la red y otros ajustes.
3. Ingrese el nombre de usuario y la contraseña para iniciar sesión en la consola local de la puerta de enlace. Para obtener más información, consulte Inicio de sesión en la consola local de la puerta de enlace de volumen.

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

Acceder a la consola local de Gateway con VMware ESXi

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

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

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

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

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

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

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

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

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

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

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

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

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

3. Elija Conectar en el panel Acciones.

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

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

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

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

Realización de tareas en la consola local de la MV de

Para Puerta de enlace de volumen que se implemente en las instalaciones, puede realizar las siguientes tareas de mantenimiento mediante la consola local de la puerta de enlace a la que accede desde la plataforma de host de la máquina virtual. Estas tareas son comunes a los VMware hipervisores de máquinas virtuales basadas en el núcleo (KVM) de Microsoft Hyper-V y Linux.

Temas

- Inicio de sesión en la consola local de Puerta de enlace de volumen: obtenga información sobre cómo iniciar sesión en la consola local de la puerta de enlace, donde puede configurar los ajustes de red de la puerta de enlace y cambiar la contraseña predeterminada.
- Configuración de un SOCKS5 proxy para su puerta de enlace local- Obtenga información sobre cómo configurar Storage Gateway para enrutar todo el tráfico AWS de puntos finales a través de un servidor proxy Socket Secure versión 5 (SOCKS5).
- Configuración de red de la gateway: obtenga información sobre cómo puede configurar la puerta de enlace para utilizar DHCP o asignar una dirección IP estática.
- Prueba de la conexión de la puerta de enlace a Internet: obtenga información sobre cómo puede utilizar la consola local de la puerta de enlace para probar la conexión entre la puerta de enlace e Internet.
- Ejecución de comandos de puerta de enlace de almacenamiento en la consola local para una puerta de enlace en las instalaciones- Obtenga información sobre cómo ejecutar los comandos de la consola local que le permiten realizar tareas adicionales, como guardar tablas de enrutamiento, conectarse a Soporte ellas y mucho más.
- Visualización del estado de los recursos de sistema de la puerta de enlace: obtenga información sobre cómo comprobar los núcleos de la CPU virtuales, el tamaño del volumen raíz y la RAM disponibles en el dispositivo de puerta de enlace.

Inicio de sesión en la consola local de Puerta de enlace de volumen

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

- 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 puerta de enlace de almacenamiento en la consola local para una puerta de enlace en las instalaciones. 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.

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

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. En el panel de navegación, elija Gateways y, a continuación, elija la gateway para la que 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.

Configuración de un SOCKS5 proxy para su puerta de enlace local

Las pasarelas de volumen y las pasarelas de cinta admiten la configuración de un proxy de Socket Secure versión 5 (SOCKS5) entre la puerta de enlace local y. AWS

> **Note**
>
> La única configuración de proxy compatible es. SOCKS5

Si la gateway debe utilizar un servidor proxy para comunicarse con Internet, debe configurar los ajustes del proxy SOCKS para la gateway. Para ello, especifique una dirección IP y un número de puerto para el host en el que se ejecuta el proxy. Después de hacerlo, Storage Gateway 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 proxy SOCKS para una puerta de enlace de volumen y una puerta de enlace de cinta.

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, consulteAcceder a la consola local de Gateway con VMware ESXi.

- Microsoft Hyper-V: para obtener más información, consulte Acceso a la consola local de la gateway con Microsoft Hyper-V.
- KVM: para obtener más información, consulte Acceso a la consola local de la gateway con Linux KVM.

2. En el menú principal AWS Storage Gateway - Configuración, introduzca el número correspondiente para seleccionar Configurar el proxy SOCKS.
3. En el menú Configuración de proxy SOCKS de AWS Storage Gateway, introduzca el número correspondiente para realizar una de las siguientes tareas:

Para llevar a cabo esta tarea	Haga lo siguiente
Configurar un proxy SOCKS	Introduzca el número correspondiente para seleccionar Configurar el proxy SOCKS. Deberá proporcionar un nombre de host y un puerto para completar la configuración.
Ver la configuración del proxy SOCKS actual	Introduzca el número correspondiente para seleccionar Ver la configuración actual del proxy SOCKS. Si no está configurado un proxy SOCKS, se muestra el mensaje `SOCKS Proxy not configured` . Si está configurado un proxy SOCKS, se muestran el nombre de host y el puerto del proxy.
Eliminar la configuración de un proxy SOCKS	Introduzca el número correspondiente para seleccionar Eliminar la configuración del proxy SOCKS. Se muestra el mensaje `SOCKS Proxy Configuration Removed` .

4. Reinicie la MV para aplicar la configuración de HTTP.

Configuración de red de la gateway

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

Para configurar la gateway para que utilice direcciones IP estáticas

1. Inicie sesión en la consola local de la gateway.
   - VMware ESXi — para obtener más información, consulteAcceder a la consola local de Gateway con VMware ESXi.
   - Microsoft Hyper-V: para obtener más información, consulte Acceso a la consola local de la gateway con Microsoft Hyper-V.
   - KVM: para obtener más información, consulte Acceso a la consola local de la 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	Introduzca el número correspondiente para seleccionar Describir el adaptador. 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: • Dirección MAC (Media Access Control) • Dirección IP

Para llevar a cabo esta tarea	Haga lo siguiente
	• Máscara de red • Dirección IP de la gateway • Estado de DHCP activado 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.
Configuración de DHCP	Introduzca el número correspondiente para seleccionar Configurar DHCP. Se le pedirá que configure la interfaz de red para utilizar DHCP.

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

Para llevar a cabo esta tarea	Haga lo siguiente
	interfaces activadas para que utilicen DHCP o direcciones IP estáticas. Por ejemplo, suponga que la MV de la gateway 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 establece rla en una IP estática. Si ambas interfaces se establecen inicialme nte para que utilicen direcciones IP estáticas y, a continuación, configura la gateway para que utilice DHCP, ambas interfaces utilizarán DHCP.

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

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

Para llevar a cabo esta tarea	Haga lo siguiente
Ver tablas de ruteo	Introduzca el número correspondiente para seleccionar Ver rutas. Se muestra la ruta predeterminada de la gateway.

Prueba de la conexión de la puerta de enlace 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.
   - VMware ESXi — para obtener más información, consulteAcceder a la consola local de Gateway con VMware ESXi.
   - Microsoft Hyper-V: para obtener más información, consulte Acceso a la consola local de la gateway con Microsoft Hyper-V.
   - KVM: para obtener más información, consulte Acceso a la consola local de la 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 obtener una lista de puntos de enlace de AWS servicio compatibles Regiones de AWS y de los que puede usar con Storage Gateway, consulte AWS Storage Gateway puntos de enlace y cuotas en. Referencia general de AWS

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

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

Ejecución de comandos de puerta de enlace de almacenamiento en la consola local para una puerta de enlace en las instalaciones

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

Para ejecutar un comando de configuración o diagnóstico

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

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

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

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

Comando	Función
ncport	Probar la conexión a un puerto TCP específico en una red.
nping	Recopilar los resultados de nping para la solución de problemas de red.
open-support-channel	Connect to AWS Support.
passwd	Actualizar tokens de autenticación.
save-iptables	Mantener tablas de IP.
save-routing-table	Guardar una entrada de la tabla de enrutamie nto recién agregada.
sslcheck	Devuelve el resultado con el emisor del certificado **Note** Storage Gateway utiliza la verificación del emisor del certificado y no admite la inspección de SSL. Si este comando devuelve un emisor distinto de aws-appliance@amazon.com, es probable que se trate de una aplicación que esté realizando una inspección de SSL. En ese caso, recomendamos omitir la inspección de SSL para el dispositivo de Storage Gateway.
tcptraceroute	Recopilar la salida de traceroute del tráfico TCP a un destino.

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

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

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

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

Para ver el estado de un recurso del sistema, consulte

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

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

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

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

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

Mensaje	Descripción
[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.

Realización de tareas en la consola EC2 local de Amazon

Algunas tareas de mantenimiento de Storage Gateway requieren que inicie sesión en la consola local de la puerta de enlace de una puerta de enlace que haya implementado en una EC2 instancia de Amazon. Puedes acceder a la consola local de la puerta de enlace de tu EC2 instancia de Amazon mediante un cliente Secure Shell (SSH). Los temas de esta sección describen cómo iniciar sesión en la consola local de puerta de enlace y realizar tareas de mantenimiento.

Temas

- Inicio de sesión en la consola local de Amazon EC2 Gateway- Obtén información sobre cómo conectarte a la consola local de la puerta de enlace de tu EC2 instancia de Amazon e iniciar sesión en ella mediante un cliente Secure Shell (SSH).
- Enrutamiento de su puerta de enlace implementada EC2 a través de un proxy HTTP- Obtenga información sobre cómo configurar Storage Gateway para AWS enrutar todo el tráfico de puntos finales a través de un servidor proxy Socket Secure versión 5 (SOCKS5) a su instancia de Amazon EC2 Gateway.
- Prueba de la conectividad de red de la puerta de enlace: obtenga información sobre cómo utilizar la consola local de la puerta de enlace para probar la conectividad de red entre la puerta de enlace y varios recursos de la red.
- Visualización del estado de los recursos de sistema de la puerta de enlace: obtenga información sobre cómo puede utilizar la consola local de puerta de enlace para comprobar los núcleos de la CPU virtual, el tamaño del volumen raíz y la RAM disponibles en el dispositivo de puerta de enlace.

- Ejecución de comandos de Storage Gateway en la consola local- Obtenga información sobre cómo ejecutar comandos de consola local que le permiten realizar tareas adicionales, como guardar tablas de enrutamiento, conectarse a Soporte ellas y mucho más.

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 conectarse de esta manera, necesitará el par de claves SSH que haya especificado al iniciar 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
Configurar un proxy SOCKS para la gateway	Enrutamiento de su puerta de enlace implementada EC2 a través de un proxy HTTP
Probar la conectividad de red	Prueba de la conectividad 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**.

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

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

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

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

1. Inicie sesión en la consola local de la gateway. Para obtener instrucciones, consulte Inicio de sesión en la consola local de Amazon EC2 Gateway.
2. En el menú principal Activación de dispositivo de AWS - Configuración, introduzca el número correspondiente para seleccionar Configurar proxy HTTP.
3. En el menú Configuración de proxy HTTP de activación de dispositivo de AWS , introduzca el número correspondiente a la tarea que desee realizar:
   - Configurar proxi HTTP: deberá proporcionar un nombre de host y un puerto para completar la configuración.
   - Ver la configuración de proxy HTTP actual: si no está configurado un proxy HTTP, se muestra el mensaje `HTTP Proxy not configured`. Si se ha configurado un proxy HTTP, se muestran el nombre de host y el puerto del proxy.
   - Eliminar la configuración de un proxy HTTP: se muestra el mensaje `HTTP Proxy Configuration Removed`.

Prueba de la conectividad de red de la puerta de enlace

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

Para probar la conexión de red de la puerta de enlace

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

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

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

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

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

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

Para ver el estado de un recurso del sistema, consulte

1. Inicie sesión en la consola local de la gateway. Para obtener instrucciones, consulte Inicio de sesión en la consola local de 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 [CORRECTO], [ADVERTENCIA] o [ERROR], lo que indica el estado del recurso de la siguiente manera:

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

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

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 Soporte ellas.

Para ejecutar un comando de configuración o diagnóstico

1. Inicie sesión en la consola local de la gateway. Para obtener instrucciones, consulte Inicio de sesión en la consola local de Amazon EC2 Gateway.

2. En el menú principal Activación de dispositivo de AWS - Configuración, introduzca el número correspondiente para seleccionar Consola de puerta de enlace.
3. En la línea de comandos de la consola de la puerta de enlace, introduzca h.

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

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

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

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

Para obtener información sobre un comando, introduzca el nombre del comando seguido de la opción `-h` (por ejemplo, `sslcheck -h`).

Rendimiento y optimización para puerta de enlace de volumen

En esta sección se describe el rendimiento de Storage Gateway.

Temas

Optimizing Gateway Performance

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 24 núcleos de CPU físicos dedicados
- En el caso de la puerta de enlace de volumen, el hardware debe dedicar las siguientes cantidades de RAM:
  - Al menos 16 GiB de RAM reservados para puertas de enlace con un tamaño de caché de hasta 16 TiB
  - Al menos 32 GiB de RAM reservados para puertas de enlace con un tamaño de caché de 16 TiB a 32 TiB
  - Al menos 48 GiB de RAM reservados para puertas de enlace con un tamaño de caché de 32 TiB a 64 TiB
- Disco 1, que se utilizará como caché de puerta de enlace de la siguiente manera:
  - SSD mediante un NVMe controlador.
- Disco 2, que se utilizará como búfer de carga de la puerta de enlace de la siguiente manera:
  - SSD que utiliza un controlador NVMe .
- Disco 3, que se utilizará como búfer de carga de la puerta de enlace de la siguiente manera:
  - SSD con un NVMe controlador.
- Adaptador de red 1 configurado en red de MV 1:
  - Utilice la red VM 1 y añada VMXnet3 (10 Gbps) para utilizarla en la ingestión.

- Adaptador de red 2 configurado en red de MV 2:
  - Utilice la red VM 2 y añada una VMXnet3 (10 Gbps) para conectarla. AWS

Añada recursos a la gateway

Los siguientes obstáculos pueden reducir el rendimiento de su por debajo del rendimiento máximo sostenido teórico (su ancho de banda a la nube): AWS

- Recuento de núcleos de CPU
- Rendimiento del disco de búfer de carga/caché
- Cantidad total de RAM
- 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:

- Utilice un RAID seccionado, como RAID 10, para mejorar el rendimiento del disco, a ser posible con un controlador de RAID de hardware.

> **Note**
>
> El RAID (matriz redundante de discos independientes) o, específicamente, las configuraciones de RAID seccionado en discos, como RAID 10, es el proceso de dividir un conjunto de datos en bloques y distribuirlos entre varios dispositivos de almacenamiento. El nivel de RAID que utilice afectará a la velocidad exacta y a la tolerancia a errores que pueda alcanzar. Al seccionar las cargas de trabajo de E/S en

varios discos, el rendimiento general del dispositivo RAID 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 NVMe controladora. También puede asociar discos virtuales a la MV directamente desde una red de área de almacenamiento (SAN) en lugar de Microsoft Hyper-V NTFS. La mejora del rendimiento del disco suele producir un mejor rendimiento y más operaciones de entrada/salida por segundo (IOPS).

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

  > **Note**
  >
  > CloudWatch las métricas no están disponibles para todas las 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, añada 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 aprovisione discos para una puerta de enlace, le recomendamos encarecidamente que no aprovisione 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 aprovisione un disco virtual (por ejemplo, como búfer de carga), puede almacenar el disco virtual en el mismo almacén de datos que la máquina virtual o en un almacén de datos diferente.

Si tiene más de un almacén de datos, le recomendamos encarecidamente que elija un almacén de datos para cada tipo de almacenamiento local que esté creando. Un almacén de datos respaldado por un único disco físico subyacente puede dar lugar a un bajo rendimiento. Por ejemplo, cuando se utiliza el mismo disco para respaldar tanto el almacenamiento en caché como para el búfer de carga en una configuración de gateway. Del mismo modo, un almacén de datos respaldado por una configuración RAID que no sea de alto rendimiento, como RAID 1 o RAID 6, puede dar lugar a un bajo rendimiento.

Añada recursos de CPU al host de la gateway

El requisito mínimo para un servidor de alojamiento de gateway son cuatro procesadores virtuales. Para optimizar el rendimiento de la puerta de enlace, compruebe que cada procesador virtual asignado a la máquina virtual de la puerta de enlace está respaldado por un núcleo de CPU 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. CPUs Además, ayudan a garantizar que su puerta de enlace reciba suficientes recursos de CPU cuando el host se comparte con otros VMs. Proporcionar suficientes recursos de CPU tiene el efecto general de mejorar el rendimiento.

Aumente el ancho de banda entre la puerta de enlace y la nube de AWS

Si aumentas el ancho de banda hacia y desde, AWS aumentarás la velocidad máxima de entrada de datos a tu puerta de enlace y de salida a AWS 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.

> **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 de búfer de carga y caché, el número de núcleos de CPU, la

cantidad total de RAM 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.

Cambie la configuración de los volúmenes

Para puertas de enlace de volumen, si comprueba que la adición de más volúmenes a una puerta de enlace reduce el rendimiento de la puerta de enlace, considere la posibilidad de agregar los volúmenes a una puerta de enlace independiente. En particular, si se utiliza un volumen para una aplicación de alto rendimiento, considere la posibilidad de crear una gateway independiente para la aplicación de alto rendimiento. Sin embargo, como norma general, no debe utilizar una gateway para todas las aplicaciones de alto rendimiento y otra gateway para todas las aplicaciones de bajo rendimiento. Para medir el rendimiento del volumen, utilice las métricas `ReadBytes` y `WriteBytes`.

Para obtener más información sobre estas métricas, consulte Medición del rendimiento entre la aplicación y la gateway.

Optimizar la configuración iSCSI

Puede optimizar la configuración iSCSI en su iniciador iSCSI 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 acerca de la configuración de iSCSI, consulte Personalización de la configuración de iSCSI.

> **Note**
>
> Estos ajustes recomendados pueden facilitar un mejor rendimiento general. Sin embargo, la configuración iSCSI específica que se necesita para optimizar el rendimiento varía en función del software de copia de seguridad que utilice. Para obtener más información, consulte la documentación del software de copia de seguridad.

Añada recursos al entorno de aplicaciones

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

La conexión entre el iniciador iSCSI y la puerta de enlace puede limitar el rendimiento de carga y descarga. Si el rendimiento de la puerta de enlace es considerablemente inferior al esperado y ya ha mejorado el número de núcleos de CPU 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.

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

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

Añada recursos de CPU al entorno de aplicaciones

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

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. También eres responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo puede aplicar el modelo de responsabilidad compartida cuando se utiliza Storage Gateway. En los siguientes temas, se le mostrará cómo configurar Storage Gateway para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a usar otros AWS servicios que le ayudan a monitorear y proteger los recursos de Storage Gateway.

Temas

Protección de datos en AWS Storage Gateway

El modelo de se aplica a protección de datos en AWS Storage Gateway. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulta las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulta Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con Storage Gateway u otro Servicios de AWS dispositivo mediante la consola AWS CLI, la API o AWS SDKs. Cualquier dato que ingrese

en etiquetas o campos de texto de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Cifrado de datos mediante AWS KMS

Storage Gateway utiliza SSL/TLS (Secure Socket Layers/Transport Layer Security (seguridad de capa) para cifrar los datos que se transfieren entre el dispositivo de puerta de enlace y el AWS almacenamiento. De forma predeterminada, Storage Gateway utiliza claves de cifrado administradas por Amazon S3 (SSE-S3) para cifrar en el lado del servidor todos los datos que almacena en Amazon S3. Tiene la opción de usar la API Storage Gateway 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 la puerta de enlace para cifrar los objetos con claves administradas por AWS KMS mediante SSE-KMS. Para obtener información sobre el uso de la API Storage Gateway para cifrar los datos escritos en un recurso compartido de archivos, consulte Crear NFSFile recurso compartido en la referencia de la AWS Storage Gateway API.

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 la API Storage Gateway. Puede especificar una de las claves administradas como clave de KMS. No se puede cambiar la clave que se utiliza para cifrar el volumen después de crearlo. Para obtener información sobre el uso de la API Storage Gateway para cifrar los datos escritos en un volumen almacenado o en caché, consulte CreateCachediSCSIVolumeo CreateStorediSCSIVolumeen la Referencia de la AWS Storage Gateway API.

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 claves AWS KMS administradas mediante la API Storage Gateway. Puede especificar una de las claves administradas como clave de 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 la API Storage Gateway para cifrar los datos escritos CreateTapesen una cinta virtual, consulte la referencia de la AWS Storage Gateway API.

Cuando AWS KMS la 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.
- Los usuarios de IAM deben tener los permisos necesarios para llamar a las operaciones de la AWS KMS API. Para obtener más información, consulte Uso de políticas de IAM con AWS KMS en la Guía para desarrolladores de AWS Key Management Service .
- Si eliminas o desactivas tu AWS AWS KMS clave o revocas el token de concesión, no podrás acceder a los datos del volumen o la cinta. Para obtener más información, consulte Eliminación de claves de KMS en la Guía para desarrolladores de AWS Key Management Service .
- Si crea una instantánea de un volumen cifrado con KMS, la instantánea está cifrada. La instantánea hereda la clave de KMS del volumen.
- Si crea un volumen a partir de una instantánea cifrada con KMS, el volumen está cifrado. Para especificar otra clave de KMS para el volumen nuevo.

> **Note**
>
> Storage Gateway no admite la creación de un volumen sin cifrar a partir de un punto de recuperación de un volumen cifrado con KMS o de una instantánea cifrada con KMS.

Para obtener más información al respecto AWS KMS, consulta ¿Qué es? AWS Key Management Service

Configuración de la autenticación CHAP para los volúmenes

En Storage Gateway, los iniciadores de iSCSI se conectan a sus volúmenes como destinos de iSCSI. Storage Gateway utiliza el protocolo CHAP (Challenge-Handshake Authentication Protocol) para autenticar iSCSI y las conexiones de iniciadores. El protocolo CHAP ofrece protección

contra ataques que requieren autenticación para el acceso a los destinos de los volúmenes de almacenamiento. Para cada volumen de destino, puede definir una o varias credenciales del protocolo CHAP. Puede ver y editar estas credenciales para los diferentes iniciadores en el cuadro de diálogo Configure CHAP credentials.

Para configurar credenciales de CHAP

1. En la consola de Storage Gateway, elija Volúmenes y seleccione el volumen para el que desea configurar las credenciales de CHAP.
2. En Actions, elija Configure CHAP authentication.
3. En Initiator name, escriba el nombre del iniciador. El nombre debe tener 1 carácter como mínimo y 255 caracteres como máximo.
4. En Secreto del iniciador, proporcione la frase secreta que desea utilizar para autenticar el iniciador de iSCSI. La frase secreta del iniciador debe tener 12 caracteres como mínimo y 16 caracteres como máximo.
5. Para Target secret, escriba la frase secreta que desea utilizar para autenticar el destino para el protocolo CHAP mutuo. La frase secreta del destino debe tener 12 caracteres como mínimo y 16 caracteres como máximo.
6. Elija Save para guardar las entradas.

Para ver o actualizar las credenciales de CHAP, debe contar con los permisos del rol de IAM necesarios que le permitan realizar esa operación.

Visualización y edición de credenciales de CHAP

Puede añadir, eliminar o actualizar las credenciales de CHAP para cada usuario. Debe contar con los permisos del rol de IAM necesarios para ver o editar las credenciales de CHAP y el destino del iniciador debe estar asociado a una puerta de enlace en funcionamiento.

Para añadir credenciales de CHAP

1. En la consola de Storage Gateway, elija Volúmenes y seleccione el volumen para el que desea agregar las credenciales de CHAP.
2. En Actions, elija Configure CHAP authentication.
3. En la página Configure CHAPS, rellene los campos Initiator name, Initiator secret y Target secret en las respectivas casillas y seleccione Save.

Para eliminar credenciales de CHAP

1. En la consola de Storage Gateway, elija Volúmenes y seleccione el volumen para el que desea eliminar las credenciales de CHAP.
2. En Actions, elija Configure CHAP authentication.
3. Haga clic en la X junto a las credenciales que desea eliminar y seleccione Save.

Para actualizar las credenciales de CHAP

1. En la consola de Storage Gateway, elija Volúmenes y seleccione el volumen para el que desea actualizar CHAP.
2. En Actions, elija Configure CHAP authentication.
3. En la página Configure CHAP credentials, cambie las entradas de las credenciales que desea actualizar.
4. Seleccione Guardar.

Identity and Access Management para AWS Storage Gateway

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los recursos. AWS Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar AWS los recursos de SGW. El IAM es un servicio Servicio de AWS que puede utilizar sin coste adicional.

Temas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que se realice en AWS SGW.

Usuario del servicio: si utiliza el servicio AWS SGW para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más funciones de AWS SGW para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarle a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en SGW AWS , consulte Solución de problemas AWS de identidad y acceso a Storage Gateway.

Administrador de servicios: si está a cargo de los recursos de AWS SGW en su empresa, probablemente tenga acceso completo a AWS SGW. Su trabajo consiste en determinar a qué funciones y recursos de AWS SGW deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su gestionador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar la IAM con AWS SGW, consulte. Cómo funciona AWS Storage Gateway con IAM

Administrador de IAM: si es administrador de IAM, puede que desee obtener más información sobre cómo redactar políticas para administrar el acceso a SGW. AWS Para ver ejemplos de políticas de AWS SGW basadas en la identidad que puede utilizar en IAM, consulte. Ejemplos de políticas basadas en identidad para Storage Gateway

Autenticación con identidades

La autenticación es la forma de iniciar sesión con sus AWS credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su gestionador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre la firma de solicitudes, consulte AWS Signature Versión 4 para solicitudes API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Autenticación multifactor AWS en IAM en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utiliza el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulta Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios empresarial, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utiliza AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulta ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulta Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puedes iniciar sesión como grupo. Puedes usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una persona determinada. Para asumir temporalmente un rol de IAM en el AWS Management Console, puede cambiar de un rol de usuario a uno de IAM (consola). Puedes asumir un rol llamando a una operación de AWS API AWS CLI o usando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulta Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puedes crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles de federación, consulte Crear un rol para un proveedor de identidad de terceros (federación) en la Guía de usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué puedes acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulta Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puedes asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puedes utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulta Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en AWS ellas, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulta Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio

desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

- Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puedes asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puedes ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y realizan AWS CLI solicitudes a la AWS API. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte Usar un rol de IAM para conceder permisos a las aplicaciones que se ejecutan en EC2 instancias de Amazon en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulta Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puedes crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utiliza para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción

`iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puedes asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades puedes clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para obtener más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios puedes utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puedes realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso () ACLs

Las listas de control de acceso (ACLs) controlan qué responsables (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios compatibles. AWS WAF ACLs Para obtener más información ACLs, consulte la descripción general de la lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas puedes establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puedes conceder a una entidad de IAM (usuario o rol de IAM). Puedes establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulta Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): SCPs son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una Usuario raíz de la cuenta de AWS. Para obtener más información sobre Organizations SCPs, consulte las políticas de control de servicios en la Guía del AWS Organizations usuario.
- Políticas de control de recursos (RCPs): RCPs son políticas de JSON que puedes usar para establecer los permisos máximos disponibles para los recursos de tus cuentas sin actualizar las políticas de IAM asociadas a cada recurso que poseas. El RCP limita los permisos de los recursos en las cuentas de los miembros y puede afectar a los permisos efectivos de las identidades, incluidos los permisos Usuario raíz de la cuenta de AWS, independientemente de si pertenecen a su organización. Para obtener más información sobre Organizations e RCPs incluir una lista de Servicios de AWS ese apoyo RCPs, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades

del rol y las políticas de la sesión. Los permisos también puedes proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulta Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona AWS Storage Gateway con IAM

Antes de usar IAM para administrar el acceso a AWS SGW, infórmese sobre las funciones de IAM disponibles para su uso con SGW. AWS

Funciones de IAM que puede usar con AWS Storage Gateway

Característica de IAM	AWS Soporte para SGW
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
ACLs	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Sesiones de acceso directo (FAS)	Sí

Característica de IAM	AWS Soporte para SGW
Roles de servicio	Sí
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo funcionan AWS SGW y otros AWS servicios con la mayoría de las funciones de IAM, consulte los AWS servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas de SGW basadas en la identidad AWS

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está asociada. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en la identidad para SGW AWS

Para ver ejemplos de políticas de AWS SGW basadas en la identidad, consulte. Ejemplos de políticas basadas en identidad para Storage Gateway

Políticas basadas en recursos dentro de SGW AWS

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los

administradores de servicios puedes utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puedes realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política basada en recursos concede acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Cross account resource access in IAM en la Guía del usuario de IAM.

Acciones políticas para SGW AWS

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puedes utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de AWS SGW, consulte Acciones definidas por AWS Storage Gateway en la Referencia de autorización de servicios.

Las acciones políticas en AWS SGW utilizan el siguiente prefijo antes de la acción:

```
sgw
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "sgw:action1",
      "sgw:action2"
         ]
```

Para ver ejemplos de políticas de AWS SGW basadas en la identidad, consulte. Ejemplos de políticas basadas en identidad para Storage Gateway

Recursos de políticas para SGW AWS

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puedes hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utiliza un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de los tipos de recursos de AWS SGW y sus tipos ARNs, consulte Recursos definidos por AWS Storage Gateway en la Referencia de autorización de servicios. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte Actions Defined by AWS Storage Gateway.

Para ver ejemplos de políticas de AWS SGW basadas en la identidad, consulte. Ejemplos de políticas basadas en identidad para Storage Gateway

Claves de condición de la política para SGW AWS

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puedes crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puedes conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulta Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de claves de condición de AWS SGW, consulte Claves de condición de AWS Storage Gateway en la Referencia de autorización de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Actions Defined by AWS Storage Gateway.

Para ver ejemplos de políticas de AWS SGW basadas en la identidad, consulte. Ejemplos de políticas basadas en identidad para Storage Gateway

ACLs AWS en SGW

Soportes ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con SGW AWS

Compatibilidad con ABAC (etiquetas en las políticas): parcial

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulta Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con SGW AWS

Compatibilidad con credenciales temporales: sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más

información sobre el cambio de roles, consulte Cambio de un usuario a un rol de IAM (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Sesiones de acceso directo para AWS SGW

Admite sesiones de acceso directo (FAS): sí

Cuando utiliza un usuario o un rol de IAM para realizar acciones en él AWS, se le considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulta Reenviar sesiones de acceso.

Roles de servicio de AWS SGW

Compatibilidad con roles de servicio: sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Si se cambian los permisos de un rol de servicio, es posible que se interrumpa la funcionalidad de la AWS SGW. Edite las funciones de servicio solo cuando AWS SGW le dé instrucciones para hacerlo.

Funciones vinculadas al servicio para SGW AWS

Admite roles vinculados a servicios: sí

Un rol vinculado al servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puedes asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puedes ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulta Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en identidad para Storage Gateway

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de AWS SGW. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o la AWS API. Un administrador de IAM puedes crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por AWS SGW, incluido el formato de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de AWS Storage Gateway en la Referencia de autorización del servicio. ARNs

Temas

- Prácticas recomendadas sobre las políticas
- Uso de la consola SGW AWS
- Cómo permitir a los usuarios consultar sus propios permisos

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear, acceder o eliminar los recursos de AWS SGW de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulta las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se puedes llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utiliza condiciones en las políticas de IAM para restringir aún más el acceso: puedes agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puedes escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de la consola SGW AWS

Para acceder a la consola AWS Storage Gateway, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de AWS SGW que tiene. Cuenta de AWS Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS API. En su lugar, permite el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la consola de AWS SGW, adjunte también la AWS SGW *ConsoleAccess* o la política *ReadOnly* AWS gestionada a las entidades. Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas gestionadas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API o. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
```

```
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Solución de problemas AWS de identidad y acceso a Storage Gateway

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas habituales que pueden surgir al trabajar con AWS SGW e IAM.

Temas

- No estoy autorizado a realizar ninguna acción en SGW AWS
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de AWS SGW

No estoy autorizado a realizar ninguna acción en SGW AWS

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `sgw:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 sgw:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `sgw:GetWidget`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibes un mensaje de error que indica que no estás autorizado a realizar la `iam:PassRole` acción, debes actualizar tus políticas para que puedas transferir una función a AWS SGW.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en AWS SGW. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de AWS SGW

Puedes crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puedes especificar una persona de confianza para que asuma el rol. En el caso de los servicios que respaldan políticas basadas en recursos o listas de control de acceso (ACLs), puede usar esas políticas para permitir que las personas accedan a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si AWS SGW admite estas funciones, consulte. Cómo funciona AWS Storage Gateway con IAM
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulta Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Validación de conformidad para AWS Storage Gateway

Los auditores externos evalúan la seguridad y el cumplimiento de AWS Storage Gateway como parte de varios programas de AWS cumplimiento. Estos incluyen SOC, PCI, ISO, FedRAMP, HIPAA, MTSC, C5, K-ISMS, ENS High, OSPAR y HITRUST CSF.

Para obtener una lista de AWS los servicios incluidos en el ámbito de los programas de conformidad específicos, consulte AWS Servicios incluidos en el ámbito de aplicación por programa de conformidad y . Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad en el ámbito de la conformidad al usar Storage Gateway viene determinada por la confidencialidad de los datos, los objetivos de conformidad de la empresa y las leyes y regulaciones aplicables. AWS proporciona los siguientes recursos para ayudarlo con los requisitos de conformidad:

- Guías de inicio rápido sobre : estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en la seguridad y el cumplimiento. AWS

- Documento técnico sobre cómo diseñar una arquitectura basada en la seguridad y el cumplimiento de la HIPAA: este documento técnico describe cómo pueden utilizar las empresas para crear aplicaciones que cumplan con la HIPAA. AWS
- AWS Recursos de cumplimiento Recursos de de trabajo y guías puede aplicarse a su sector y ubicación.
- Evaluación de los recursos con las reglas de la Guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Este AWS servicio proporciona una visión integral del estado de su seguridad AWS que le ayuda a comprobar su conformidad con los estándares y las mejores prácticas del sector de la seguridad.

Resiliencia en AWS Storage Gateway

La infraestructura AWS global se basa en distintas zonas Regiones de AWS de disponibilidad.

Una Región de AWS es una ubicación física en todo el mundo donde los centros de datos están agrupados. Cada grupo de centros de datos lógicos se denomina zona de disponibilidad (AZ). Cada uno Región de AWS consta de un mínimo de tres aislados y separados físicamente AZs dentro de un área geográfica. A diferencia de otros proveedores de servicios en la nube, que suelen definir una región como un único centro de datos, el diseño de múltiples zonas de disponibilidad de cada uno de Región de AWS ellos ofrece claras ventajas. Cada zona de disponibilidad tiene alimentación, refrigeración y seguridad física independientes y está conectada a través de ultra-low-latency redes redundantes. Si su implementación requiere centrarse en la alta disponibilidad, puede configurar los servicios y los recursos en varios para lograr una mayor AZs tolerancia a los errores.

Regiones de AWS cumplen con los niveles más altos de seguridad de infraestructura, cumplimiento y protección de datos. Todo el tráfico intermedio AZs está cifrado. El rendimiento de la red es suficiente para realizar una replicación sincrónica entre AZs ellas. AZs facilitan la partición de servicios y recursos para lograr una alta disponibilidad. Si su implementación está dividida AZs, sus recursos estarán mejor aislados y protegidos de problemas como cortes de energía, rayos, tornados, terremotos y más. AZs están separados físicamente por una distancia significativa de cualquier otra zona de disponibilidad, aunque todas se encuentran a menos de 100 km (60 millas) una de la otra.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura AWS global.

Además de la infraestructura AWS global, Storage Gateway ofrece varias funciones para respaldar sus necesidades de respaldo y resiliencia de datos:

- Use VMware vSphere High Availability (VMware HA) para proteger las cargas de trabajo de almacenamiento contra errores de hardware, hipervisor o red. Para obtener más información, consulte Uso de VMware vSphere High Availability con Storage Gateway.
- Úselo AWS Backup para hacer copias de seguridad de sus volúmenes. Para obtener más información, consulte Realización de la copia de seguridad de los volúmenes.
- Clone el volumen desde un punto de recuperación. Para obtener más información, consulte Clonación de un volumen en caché desde un punto de recuperación.

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.

Las llamadas a la API AWS publicadas se utilizan para acceder a Storage Gateway a través de la red. Los clientes deben admitir el protocolo de seguridad de la capa de transporte (TLS) 1.2. Los clientes también deben ser compatibles con conjuntos de cifrado con confidencialidad directa total (PFS) tales como Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puedes utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

> **Note**
>
> Debe tratar el dispositivo AWS Storage Gateway como una máquina virtual administrada y no debe intentar acceder a su instalación ni modificarla de ninguna manera. El intento de instalar un software de escaneo o actualizar cualquier paquete de software mediante métodos distintos al mecanismo de actualización de la puerta de enlace normal puede provocar un mal funcionamiento de la puerta de enlace y afectar a nuestra capacidad de admitir o reparar la puerta de enlace.

AWS revisa, analiza y CVEs corrige periódicamente. Incorporamos correcciones para estos problemas en Storage Gateway como parte de nuestro ciclo de lanzamiento de software normal. Por lo general, estos ajustes se aplican como parte del proceso normal de actualización de la puerta de enlace durante los periodos de mantenimiento programados. Para obtener más información sobre las actualizaciones de la puerta de enlace, consulte .

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 .

Inicio de sesión y supervisión AWS Storage Gateway

Storage Gateway está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Storage Gateway. CloudTrail captura todas las llamadas a la API de Storage Gateway como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de Storage Gateway y las llamadas de código a las operaciones de la API de Storage Gateway. Si crea una ruta, puede activar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Storage Gateway. Si no configura 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 archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando crea una ruta en la consola, la ruta se aplica a todas AWS las regiones. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail Integraciones y servicios compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas las acciones de Storage Gateway están registradas y documentadas en el tema Acciones. Por ejemplo, las llamadas a las `ActivateGateway` `ShutdownGateway` acciones y las llamadas generan entradas en los archivos de CloudTrail registro. `ListGateways`

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el Elemento userIdentity de CloudTrail .

Descripción de las entradas de archivos de registro de Storage Gateway

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud,

etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la acción.


```
{ "Records": [{
                "eventVersion": "1.02",
                "userIdentity": {
                "type": "IAMUser",
                "principalId": "AIDAII5AUEPBH2M7JTNVC",
                "arn": "arn:aws:iam::111122223333:user/StorageGateway-team/JohnDoe",
                "accountId": "111122223333",
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                 "userName": "JohnDoe"
               },
                   "eventTime": "2014-12-04T16:19:00Z",
                   "eventSource": "storagegateway.amazonaws.com",
                   "eventName": "ActivateGateway",
                   "awsRegion": "us-east-2",
                   "sourceIPAddress": "192.0.2.0",
                   "userAgent": "aws-cli/1.6.2 Python/2.7.6 Linux/2.6.18-164.el5",
                    "requestParameters": {
                                          "gatewayTimezone": "GMT-5:00",
                                          "gatewayName": "cloudtrailgatewayvtl",
                                          "gatewayRegion": "us-east-2",
                                          "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
                                          "gatewayType": "VTL"
                                               },
                                               "responseElements": {
                                                                     "gatewayARN":
 "arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayvtl"
                                               },
                                               "requestID":
 "54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
                                               "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
                                               "eventType": "AwsApiCall",
                                               "apiVersion": "20130630",
                                               "recipientAccountId": "444455556666"
             }]
}
```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la ListGateways acción.

```
{
 "Records": [{
               "eventVersion": "1.02",
               "userIdentity": {
                                 "type": "IAMUser",
                                 "principalId": "AIDAII5AUEPBH2M7JTNVC",
                                 "arn": "arn:aws:iam::111122223333:user/StorageGateway-
team/JohnDoe",
                                 "accountId:" 111122223333", " accessKeyId ":"
 AKIAIOSFODNN7EXAMPLE",
                                 " userName ":" JohnDoe "
                                 },

                                 " eventTime ":" 2014 - 12 - 03T19: 41: 53Z ",
                                 " eventSource ":" storagegateway.amazonaws.com ",
                                 " eventName ":" ListGateways ",
                                 " awsRegion ":" us-east-2 ",
                                 " sourceIPAddress ":" 192.0.2.0 ",
                                 " userAgent ":" aws - cli / 1.6.2 Python / 2.7.6
 Linux / 2.6.18 - 164.el5 ",
                                 " requestParameters ":null,
                                 " responseElements ":null,
                                 "requestID ":"
 6U2N42CU37KAO8BG6V1I23FRSJ1Q8GLLE1QEU3KPGG6F0KSTAUU0 ",
                                 " eventID ":" f76e5919 - 9362 - 48ff - a7c4 -
 d203a189ec8d ",
                                 " eventType ":" AwsApiCall ",
                                 " apiVersion ":" 20130630 ",
                                 " recipientAccountId ":" 444455556666"
             }]
}
```

Solución de problemas de la gateway

A continuación, puede encontrar información sobre las prácticas recomendadas y la solución de problemas relacionados con las puertas de enlace, las plataformas de host, los volúmenes, la alta disponibilidad, la recuperación de datos y las instantáneas. La información sobre la solución de problemas de las puertas de enlace en las instalaciones cubre las puertas de enlace implementadas en las plataformas de virtualización compatibles. La información de solución de problemas de alta disponibilidad abarca las puertas de enlace que se ejecutan en la plataforma VMware vSphere High Availability (HA).

Temas

- Solución de problemas: problemas sin conexión de puerta de enlace: obtenga información sobre cómo diagnosticar los problemas que pueden provocar que la puerta de enlace aparezca sin conexión en la consola de Storage Gateway.
- Solución de problemas: error interno durante la activación de la puerta de enlace: obtenga información sobre qué hacer si recibe un mensaje de error interno al intentar activar la Storage Gateway.
- Solución de problemas de puerta de enlace en las instalaciones- Obtenga información sobre los problemas habituales que se pueden producir al trabajar con las puertas de enlace locales y cómo permitir la conexión Soporte a ellas para facilitar la solución de problemas.
- Solución de problemas de configuración de Microsoft Hyper-V: obtenga información sobre los problemas habituales que podrían surgir al implementar Storage Gateway en la plataforma de Microsoft Hyper-V.
- Solución de problemas de Amazon EC2 Gateway- Obtenga información sobre los problemas típicos que puede encontrar al trabajar con pasarelas implementadas en Amazon EC2.
- Solución de problemas del dispositivo de hardware: obtenga información sobre cómo resolver los problemas que pueda encontrar con el dispositivo de hardware de Storage Gateway.
- Solución de problemas con volúmenes: encuentre información sobre los problemas más habituales que podría encontrar al trabajar con volúmenes y las acciones que le sugerimos para corregirlos.
- Solución de problemas de alta disponibilidad- Obtenga información sobre qué hacer si tiene problemas con las puertas de enlace que se implementan en un VMware entorno de alta disponibilidad.

Solución de problemas: problemas sin conexión de puerta de enlace

Utilice la siguiente información de solución de problemas para determinar qué hacer si la consola de AWS Storage Gateway muestra que la puerta de enlace está desconectada.

La puerta de enlace puede mostrarse como desconectada por uno o varios de los motivos siguientes:

- La puerta de enlace no puede llegar a los puntos de conexión del servicio de Storage Gateway.
- La puerta de enlace se cerró inesperadamente.
- Se desconectó o modificó un disco caché asociado a la puerta de enlace, o se produjo un error.

Para volver a conectar la puerta de enlace, identifique y resuelva el problema que provocó que la puerta de enlace se desconectara.

Comprobación del firewall o el proxy asociados

Si configuró la puerta de enlace para usar un proxy o la colocó detrás de un firewall, revise las reglas de acceso del proxy o el firewall. El proxy o el firewall deben permitir el tráfico hacia y desde los puertos de red y los puntos de conexión de servicio requeridos por Storage Gateway. Para obtener más información, consulte Requisitos de red y firewall.

Comprobación para una inspección continua de SSL o de paquetes exhaustiva del tráfico de la puerta de enlace

Si actualmente se está realizando una inspección profunda de paquetes o SSL en el tráfico de red entre la puerta de enlace y la puerta de enlace AWS, es posible que la puerta de enlace no pueda comunicarse con los puntos finales de servicio necesarios. Para que la puerta de enlace vuelva a estar en línea, debe desactivar la inspección.

Comprobación de si hay un corte de energía o un error de hardware en el host del hipervisor

Un corte de energía o un error de hardware en el host del hipervisor de la puerta de enlace pueden provocar que la puerta de enlace se cierre inesperadamente y no se pueda acceder a ella. Tras

restablecer la alimentación y la conectividad de red, se volverá a poder acceder a la puerta de enlace.

Cuando la puerta de enlace vuelva a estar en línea, asegúrese de tomar las medidas necesarias para recuperar los datos. Para obtener más información, consulte Prácticas recomendadas para recuperar datos.

Comprobación de si hay problemas con un disco de caché asociado

La puerta de enlace se puede desconectar si al menos uno de los discos de caché asociados a la puerta de enlace se ha eliminado, modificado, redimensionado o está dañado.

Si se ha eliminado un disco de caché en funcionamiento del host del hipervisor:

1. Apague la gateway.
2. Vuelva a agregar el disco.

   > **Note**
   >
   > Asegúrese de agregar el disco al mismo nodo de disco.

3. Reinicie la gateway.

Si un disco de caché está dañado, se reemplazó o se cambió su tamaño:

1. Apague la gateway.
2. Restablezca el disco de la caché.
3. Vuelva a configurar el disco para el almacenamiento en caché.
4. Reinicie la gateway.

Solución de problemas: error interno durante la activación de la puerta de enlace

Las solicitudes de activación de Storage Gateway atraviesan dos rutas de red. Las solicitudes de activación entrantes enviadas por un cliente se conectan a la máquina virtual (VM) de la puerta de enlace o a la instancia de Amazon Elastic Compute Cloud (Amazon EC2) a través del puerto 80. Si

la puerta de enlace recibe correctamente la solicitud de activación, la puerta de enlace se comunica con los puntos de conexión de Storage Gateway para recibir una clave de activación. Si la puerta de enlace no puede llegar a los puntos de conexión de Storage Gateway, la puerta de enlace responde al cliente con un mensaje de error interno.

Utilice la siguiente información de solución de problemas para determinar qué hacer si recibe un mensaje de error interno al intentar activar AWS Storage Gateway.

> **Note**
>
> - Asegúrese de implementar nuevas puertas de enlace con la versión del archivo de imagen de máquina virtual más reciente o de Imagen de máquina de Amazon (AMI). Recibirá un error interno si intenta activar una puerta de enlace que utiliza una AMI desactualizada.
> - Asegúrese de seleccionar el tipo de puerta de enlace correcto que pretende implementar antes de descargar la AMI. Los archivos.ova y AMIs para cada tipo de puerta de enlace son diferentes y no son intercambiables.

Resolución de errores al activar la puerta de enlace mediante un punto de conexión público

Para resolver los errores de activación al activar la puerta de enlace mediante un punto de conexión público, realice las siguientes comprobaciones y configuraciones.

Comprobación de los puertos necesarios

Para las puertas de enlace implementadas en las instalaciones, compruebe que los puertos estén abiertos en el firewall local. En el caso de las puertas de enlace implementadas en una EC2 instancia de Amazon, comprueba que los puertos estén abiertos en el grupo de seguridad de la instancia. Para confirmar que los puertos están abiertos, ejecute un comando telnet en el punto de conexión público desde un servidor. Este servidor debe estar en la misma subred que la puerta de enlace. Por ejemplo, los siguientes comandos telnet prueban la conexión al puerto 443:

```
telnet d4kdq0yaxexbo.cloudfront.net 443
telnet storagegateway.region.amazonaws.com 443
telnet dp-1.storagegateway.region.amazonaws.com 443
telnet proxy-app.storagegateway.region.amazonaws.com 443
```

```
telnet client-cp.storagegateway.region.amazonaws.com 443
telnet anon-cp.storagegateway.region.amazonaws.com 443
```

Para confirmar que la propia puerta de enlace puede llegar al punto de conexión, acceda a la consola de máquina virtual local de la puerta de enlace (para las puertas de enlace implementadas en las instalaciones). O bien, puedes usar SSH a la instancia de la puerta de enlace (para las puertas de enlace implementadas en Amazon EC2). A continuación, ejecute una prueba de conectividad de red. Confirme que la prueba devuelve `[PASSED]`. Para obtener más información, consulte Testing your gateway's network connectivity.

> **Note**
>
> El nombre de usuario de inicio de sesión predeterminado para la consola de la puerta de enlace es `admin` y la contraseña predeterminada es `password`.

Asegúrese de que la seguridad del firewall no modifique los paquetes enviados desde la puerta de enlace a los puntos de conexión públicos

Las inspecciones de SSL, las inspecciones exhaustivas de paquetes u otras formas de seguridad mediante firewall pueden interferir con los paquetes enviados desde la puerta de enlace. El protocolo de enlace SSL produce un error si el certificado SSL se modifica con respecto a lo esperado del punto de conexión de activación. Para confirmar que no hay ninguna inspección de SSL en curso, ejecute un comando de OpenSSL en el punto de conexión de activación principal (`anon-cp.storagegateway.region.amazonaws.com`) del puerto 443. Debe ejecutar este comando desde una máquina que se encuentre en la misma subred que la puerta de enlace:

```
$ openssl s_client -connect  anon-cp.storagegateway.region.amazonaws.com:443 -
servername anon-cp.storagegateway.region.amazonaws.com
```

> **Note**
>
> Sustitúyala por *`region`* la tuya. Región de AWS

Si no hay ninguna inspección de SSL en curso, el comando devuelve una respuesta similar a la siguiente:

```
$ openssl s_client -connect anon-cp.storagegateway.us-east-2.amazonaws.com:443 -
servername anon-cp.storagegateway.us-east-2.amazonaws.com
CONNECTED(00000003)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-2.amazonaws.com
verify return:1
---
Certificate chain
 0 s:/CN=anon-cp.storagegateway.us-east-2.amazonaws.com
   i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
 1 s:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
   i:/C=US/O=Amazon/CN=Amazon Root CA 1
 2 s:/C=US/O=Amazon/CN=Amazon Root CA 1
   i:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
 3 s:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
   i:/C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification Authority
---
```

Si hay una inspección de SSL en curso, la respuesta muestra una cadena de certificados alterada, similar a la siguiente:

```
$ openssl s_client -connect  anon-cp.storagegateway.ap-southeast-1.amazonaws.com:443 -
servername anon-cp.storagegateway.ap-southeast-1.amazonaws.com
CONNECTED(00000003)
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.ap-southeast-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

El punto de conexión de activación solo acepta los protocolos de enlace de SSL si reconoce el certificado SSL. Esto significa que el tráfico saliente de la puerta de enlace hacia los puntos de conexión debe estar exento de las inspecciones realizadas por los firewalls de la red. Es posible que estas inspecciones sean una inspección de SSL o una inspección profunda de paquetes.

Comprobación de la sincronización horaria de la puerta de enlace

Los sesgos horarios excesivos pueden provocar errores en el protocolo de enlace de SSL. En el caso de las puertas de enlace en las instalaciones, puede utilizar la consola de máquina virtual local de la puerta de enlace para comprobar la sincronización horaria de la puerta de enlace. El sesgo horario no debe ser superior a 60 segundos. Para obtener más información, consulte Sincronización de la hora de la MV de la gateway.

La opción de administración del tiempo del sistema no está disponible en las pasarelas alojadas en EC2 instancias de Amazon. Para asegurarte de que EC2 las pasarelas de Amazon pueden sincronizar la hora correctamente, confirma que la EC2 instancia de Amazon se puede conectar a la siguiente lista de servidores NTP a través de los puertos UDP y TCP 123:

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

Resolución de errores al activar la puerta de enlace mediante un punto de conexión de VPC de Amazon

Para resolver los errores de activación al activar la puerta de enlace mediante un punto de conexión de Amazon Virtual Private Cloud (Amazon VPC), realice las siguientes comprobaciones y configuraciones.

Comprobación de los puertos necesarios

Asegúrese de que los puertos necesarios del firewall local (para las puertas de enlace implementadas en las instalaciones) o del grupo de seguridad (para las puertas de enlace implementadas en Amazon EC2) estén abiertos. Los puertos necesarios para conectar una puerta de enlace a un punto de conexión de VPC de Storage Gateway difieren de los necesarios al conectar una puerta de enlace a puntos de conexión públicos. Se requieren los siguientes puertos para conectarse a un punto de conexión de VPC de Storage Gateway:

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

Para obtener más información, consulte Creating a VPC endpoint for Storage Gateway.

Además, compruebe el grupo de seguridad que está conectado al punto de conexión de VPC de Storage Gateway. Es posible que el grupo de seguridad predeterminado asociado al punto de conexión no permita los puertos necesarios. Cree un nuevo grupo de seguridad que permita el tráfico desde el rango de direcciones IP de la puerta de enlace a través de los puertos necesarios. A continuación, asocie ese grupo de seguridad al punto de conexión de VPC.

> **Note**
>
> Utilice la consola de Amazon VPC para verificar el grupo de seguridad que está conectado al punto de conexión de VPC. Consulte el punto de conexión de VPC de Storage Gateway desde la consola y, a continuación, elija la pestaña Grupos de seguridad.

Para confirmar que los puertos necesarios están abiertos, puede ejecutar comandos telnet en el punto de conexión de VPC de Storage Gateway. Debe ejecutar estos comandos desde un servidor que esté en la misma subred que la puerta de enlace. Puede ejecutar las pruebas en el primer nombre de DNS que no especifique una zona de disponibilidad. Por ejemplo, los siguientes comandos telnet prueban las conexiones de puerto necesarias con el nombre de DNS vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 443
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1026
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1027
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1028
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1031
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 2222
```

Asegúrese de que la seguridad del firewall no modifique los paquetes enviados desde la puerta de enlace al punto de conexión de VPC de Amazon de Storage Gateway

Las inspecciones de SSL, las inspecciones exhaustivas de paquetes u otras formas de seguridad mediante firewall pueden interferir con los paquetes enviados desde la puerta de enlace. El protocolo de enlace SSL produce un error si el certificado SSL se modifica con respecto a lo esperado del punto de conexión de activación. Para confirmar que no hay ninguna inspección de SSL en curso, ejecute un comando de OpenSSL en el punto de conexión de VPC de Storage Gateway. Debe ejecutar este comando desde una máquina que se encuentre en la misma subred que la puerta de enlace. Ejecute el comando para cada puerto requerido:

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:443 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1026 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1028 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1031 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:2222 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

Si no hay ninguna inspección de SSL en curso, el comando devuelve una respuesta similar a la siguiente:

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

```
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-1.amazonaws.com
verify return:1
---
Certificate chain
 0 s:CN = anon-cp.storagegateway.us-east-1.amazonaws.com
   i:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
 1 s:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
   i:C = US, O = Amazon, CN = Amazon Root CA 1
 2 s:C = US, O = Amazon, CN = Amazon Root CA 1
   i:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
 3 s:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
   i:C = US, O = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification
 Authority
---
```

Si hay una inspección de SSL en curso, la respuesta muestra una cadena de certificados alterada, similar a la siguiente:

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.us-
east-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.us-east-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

El punto de conexión de activación solo acepta los protocolos de enlace de SSL si reconoce el certificado SSL. Esto significa que el tráfico saliente de la puerta de enlace hacia el punto de conexión de VPC debe estar exento de las inspecciones realizadas por los firewalls de la red. Es posible que estas inspecciones sean inspecciones de SSL o inspecciones profundas de paquetes.

Comprobación de la sincronización horaria de la puerta de enlace

Los sesgos horarios excesivos pueden provocar errores en el protocolo de enlace de SSL. En el caso de las puertas de enlace en las instalaciones, puede utilizar la consola de máquina virtual local de la puerta de enlace para comprobar la sincronización horaria de la puerta de enlace. El sesgo horario no debe ser superior a 60 segundos. Para obtener más información, consulte Sincronización de la hora de la MV de la gateway.

La opción de administración del tiempo del sistema no está disponible en las pasarelas alojadas en EC2 instancias de Amazon. Para asegurarte de que EC2 las pasarelas de Amazon pueden sincronizar la hora correctamente, confirma que la EC2 instancia de Amazon se puede conectar a la siguiente lista de servidores NTP a través de los puertos UDP y TCP 123:

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

Comprobación de un proxy HTTP y confirmación de la configuración del grupo de seguridad asociado

Antes de la activación, compruebe si tiene un proxy HTTP en Amazon EC2 configurado en la máquina virtual de puerta de enlace local como un proxy Squid en el puerto 3128. En este caso, confirme lo siguiente:

- El grupo de seguridad adjunto al proxy HTTP de Amazon EC2 debe tener una regla de entrada. Esta regla de entrada debe permitir el tráfico del proxy Squid en el puerto 3128 desde la dirección IP de la máquina virtual de la puerta de enlace.
- El grupo de seguridad adjunto al punto de conexión de Amazon EC2 VPC debe tener reglas de entrada. Estas reglas de entrada deben permitir el tráfico en los puertos 1026-1028, 1031, 2222 y 443 desde la dirección IP del proxy HTTP de Amazon. EC2

Resuelva los errores al activar la puerta de enlace mediante un punto de conexión público y hay un punto de conexión de VPC de Storage Gateway en la misma VPC

Para resolver los errores al activar la puerta de enlace mediante un punto de conexión público cuando hay un punto de conexión de Amazon Virtual Private Cloud (Amazon VPC) en la misma VPC, realice las siguientes comprobaciones y configuraciones.

Confirmar que la configuración Habilitar nombre de DNS privado no esté habilitada en el punto de conexión de VPC de Storage Gateway

Si la opción Habilitación de nombre de DNS privado está habilitada, no podrá activar ninguna puerta de enlace desde esa VPC al punto de conexión público.

Para desactivar la opción de nombre de DNS privado:

1. Abra la Consola de Amazon VPC.
2. En el panel de navegación, elija Puntos de conexión.
3. Elija el punto de conexión de VPC de Storage Gateway.
4. Elija Acciones.
5. Elija Administrar nombres de DNS privados.
6. Para Habilitar nombre de DNS privado, borre Habilitar para este punto de conexión.
7. Elija Modificar nombres de DNS privados para guardar la configuración.

Solución de problemas de puerta de enlace en las instalaciones

A continuación, encontrará información sobre los problemas típicos que puede encontrar al trabajar con las puertas de enlace locales y sobre cómo activarlos para ayudar Soporte a solucionar los problemas de la puerta 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. • Para VMware ESXi, la dirección IP de la máquina virtual se encuentra en el cliente de vSphere, en la pestaña Resumen. • Para Microsoft Hyper-V, la dirección IP de la MV puede encontrar se al iniciar sesión en la consola local. Si continúa teniendo problemas para encontrar la dirección IP de la gateway: • Compruebe que la MV esté activada. Solo cuando está activada la MV se asigna una dirección IP a la gateway. • Espere a que la MV termine de configurarse. Si acaba de activar la MV, la gateway puede tardar varios minutos en finalizar la secuencia de arranque.
Tiene problemas de red o de firewall.	• Asigne permisos a los puertos adecuados para la gateway. • Certificado SSL: validation/inspection should not be activated. Storage Gateway utilizes mutual TLS authentication which would fail if any 3rd party application tries to intercept/sign cualquiera de los dos 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.
La activación de la puerta de enlace produce un error al hacer clic en el botón Proceder a la activación de la consola de administr ación de Storage Gateway.	• Compruebe que la MV de la gateway permita el acceso haciendo ping a la MV desde el cliente. • Compruebe que la MV tenga conectividad de red a Internet. De lo contrario, deberá configurar un proxy SOCKS. Para obtener más información sobre cómo hacerlo, consulte Configuración de un SOCKS5 proxy para su puerta de enlace local.

Problema	Acción que ejecutar
	• Compruebe que el host tenga la hora correcta, que el host esté configurado para sincronizar la hora de forma automática con un servidor NTP (Network Time Protocol) y que la MV de la gateway tenga la hora correcta. Para obtener información sobre la sincronización de la hora de los hosts de los hipervisores y VMs, consulte. Sincronización de la hora de la máquina virtual con la hora del host KVM de Hyper-V o Linux • 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. • Certificado SSL para cualquiera de los dos certificados. validatio n/inspection should not be activated. Storage Gateway utilizes mutual TLS authentication which would fail if any 3rd party application tries to intercept/sign • Compruebe que la MV tenga al menos 7,5 GB de RAM. La asignación de la gateway produce un error si hay menos de 7,5 GB de RAM. Para obtener más información, consulte Requisitos para configurar puerta de enlace de volumen.
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.	Para obtener instrucciones sobre cómo eliminar un disco asignado como espacio de búfer de carga, consulte Retirada de discos de la gateway.

Problema	Acción que ejecutar
Debe mejorar el ancho de banda entre la puerta de enlace y AWS.	Puede mejorar el ancho de banda de la puerta de enlace AWS configurando la conexión a Internet AWS en un adaptador de red (NIC) independiente del que conecta las aplicaciones y la máquina virtual de la puerta de enlace. Este enfoque resulta útil si tiene una conexión con un ancho de banda elevado AWS y quiere evitar la contención del ancho de banda, especialmente durante una restauración instantánea. Para necesidades de carga de trabajo de alto rendimiento, puede usar AWS Direct Connect para establecer una conexión de red dedicada entre la puerta de enlace en las instalaciones y AWS. Para medir el ancho de banda de la conexión desde la puerta de enlace AWS, utilice las `CloudBytesUploaded` métricas `CloudBytesDownloaded` y de la puerta de enlace. Para obtener más información sobre este tema, consulte Medición del rendimiento entre la puerta de enlace y AWS. Mejorar la conectividad a Internet ayuda a garantizar que el búfer de carga no se llene.

Problema	Acción que ejecutar

El rendimiento hacia o desde la gateway disminuye a cero.	• En la pestaña Gateway de la consola Storage Gateway, compruebe que las direcciones IP de la máquina virtual de puerta de enlace son las mismas que las que ve al utilizar el software cliente del hipervisor (es decir, el cliente VMware vSphere o Microsoft Hyper-V Manager). Si encuentra una discrepancia, reinicie la puerta de enlace desde la consola de Storage Gateway, como se muestra en Como apagar la MV de la gateway. Tras el reinicio, las direcciones de la lista Direccion es IP de la pestaña Puerta de enlace de la consola de Storage Gateway deberían coincidir con las direcciones IP de la puerta de enlace, las cuales determina desde el cliente del hipervisor.
	  • Para VMware ESXi, la dirección IP de la máquina virtual se encuentra en el cliente de vSphere, en la pestaña Resumen.
	  • Para Microsoft Hyper-V, la dirección IP de la MV puede encontrarse al iniciar sesión en la consola local.
	• Compruebe la conectividad de la puerta de enlace AWS tal y como se describe enPrueba de la conexión de la puerta de enlace 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 configura ción 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.
	
	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 la puerta de enlace y AWS

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 Soporte.

Permiten ayudar Soporte 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 Soporte para acceder a su puerta de enlace para ayudarlo a solucionar problemas de la puerta de enlace. De forma predeterminada, el Soporte acceso a la puerta de enlace está desactivado. Proporcione este acceso mediante la consola local del host. Para Soporte acceder a su puerta de enlace, primero debe iniciar sesión en la consola local del host, ir a la consola de Storage Gateway y, a continuación, conectarse al servidor de soporte.

Para permitir el Soporte acceso a su puerta de enlace

1. Inicie sesión en la consola local del host.
   - VMware ESXi — para obtener más información, consulteAcceder a la consola local de Gateway con VMware ESXi.
   - Microsoft Hyper-V: para obtener más información, consulte Acceso a la consola local de la gateway con Microsoft Hyper-V.
2. Cuando se le solicite, introduzca el número correspondiente para seleccionar Consola de puerta de enlace.
3. Introduzca **h** para abrir la lista de comandos disponibles.
4. Realice una de las siguientes acciones:

- Si la puerta de enlace está utilizando un punto de conexión público, en la ventana COMANDOS DISPONIBLES introduzca **`open-support-channel`** para conectar con el servicio de atención al cliente de Storage Gateway. Permitir el puerto TCP 22 para poder abrir un canal de soporte en AWS. Cuanto conecte con el servicio de atención al cliente, Storage Gateway le asignará un número de soporte. Apunte el número de soporte.
- Si la gateway está utilizando un punto de enlace de la VPC, en la ventana AVAILABLE COMMANDS (COMANDOS DISPONIBLES), introduzca **`open-support-channel`**. Si la puerta de enlace no está activada, proporcione el punto de conexión de VPC o la dirección IP para conectar con el servicio de atención al cliente de Storage Gateway. Permitir el puerto TCP 22 para poder abrir un canal de soporte en AWS. Cuanto conecte con el servicio de atención al cliente, Storage Gateway le asignará un número de soporte. Apunte el número de soporte.

> **Note**
>
> El número de canal no es un número de puerto Protocol/User Datagram Protocol (TCP/UDP (Control de transmisión). En lugar de ello, la puerta de enlace realiza una conexión Secure Shell (SSH) (TCP 22) a los servidores de Storage Gateway y proporciona el canal de soporte para la conexión.

5. Una vez establecido el canal de soporte, proporcione su número de servicio de soporte para Soporte que Soporte pueda ayudarlo a solucionar problemas.
6. Cuando se complete la sesión de soporte, introduzca **`q`** para finalizarla. No cierre la sesión hasta que el servicio de soporte de Amazon Web Services le notifique que la sesión de soporte se ha completado.
7. Introduzca **`exit`** para cerrar sesión en la consola de 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
Se intenta importar una puerta de enlace y se recibe el mensaje de error siguiente: “Se ha producido un error al intentar importar la máquina virtual. Se ha producido un error al importar. Imposible encontrar los archivos de importación de la máquina virtual en la ubicación […]. Solo puede importar una máquina virtual si utilizó Hyper-V para crearla y exportarla”.	Este error puede producirse por las razones siguientes: • Si no apunta a la raíz de los archivos de origen de la gateway sin comprimir. La última parte de la ubicación que especifique en el cuadro de diálogo Importar máquina virtual debe ser `AWS-Storage-Gateway` . Por ejemplo: `C:\prod-gateway\unzippedSourceVM\AWS-Storage-Gateway\` . • Si ya ha implementado una gateway, pero no seleccionó la opción Copy the virtual machine (Copia la máquina virtual) ni activó la opción Duplicate all files (Duplicar todos los archivos) en el cuadro de diálogo Import Virtual Machine (Importar máquina virtual), la máquina virtual se creó en la ubicación donde tiene los archivos de la gateway sin comprimir y no puede volver a importarla desde esta ubicación. Para solucionar este problema, obtenga una copia nueva de los archivos de origen de la gateway sin comprimir y cópiela en una nueva ubicación. Utilice la nueva ubicación como origen de la importación. Si planea crear varias puertas de enlace desde una ubicación de archivos de origen descomprimida, debe seleccionar Copiar la máquina virtual y marcar la casilla Duplicar todos los archivos en el cuadro de diálogo Importar máquina virtual.
Se intenta importar una puerta de enlace y se recibe el mensaje de error siguiente: “Se ha producido un error al intentar importar la máquina virtual. Se ha producido un error al importar. La tarea de importación no pudo copiar	Si ya ha implementado una gateway e intenta reutilizar las carpetas predeterminadas donde se almacenan los archivos del disco duro virtual y los archivos de configuración de máquinas virtuales, se producirá este error. Para solucionar este problema, especifique las nuevas ubicaciones en Servidor, en el panel situado a la izquierda del cuadro de diálogo de configuración de Hyper-V.

Problema	Acción que ejecutar
el archivo de [...]: el archivo existe. (0x80070050)”	
Se intenta importar una puerta de enlace y se recibe el mensaje de error siguiente: “Se ha producido un error al intentar importar la máquina virtual. Se ha producido un error al importar. Import failed because the virtual machine must have a new identifier. Select a new identifier and try the import again."	Al importar la puerta de enlace, asegúrese de que selecciona la opción Copiar la máquina virtual y de que marca la casilla Duplicar todos los archivos en el cuadro de diálogo Importar máquina virtual para crear un nuevo ID único para la máquina virtual.
Se intenta iniciar una máquina virtual de puerta de enlace y se recibe el mensaje de error siguiente: “Se ha producido un error al intentar iniciar las máquinas virtuales seleccionadas. La configuración del procesador de particiones secundario no es compatible con la partición principal . No se pudo inicializar “AWS-Storage-Gateway”. (ID de máquina virtual [...])”	Es probable que este error se deba a una discrepancia de CPU entre lo necesario CPUs para la puerta de enlace y lo disponible CPUs en el host. Asegúrese de que el número de CPU de MV sea compatible con el hipervisor subyacente. Para obtener más información sobre los requisitos de Storage Gateway, consulte Requisitos para configurar puerta de enlace de volumen.

Problema	Acción que ejecutar
Se intenta iniciar una máquina virtual de puerta de enlace y se recibe el mensaje de error siguiente: “Se ha producido un error al intentar iniciar las máquinas virtuales seleccionadas. No se pudo inicializar “AWS-Storage-Gateway”. (ID de máquina virtual [...]) No se pudo crear la partición : los recursos del sistema son insuficientes para completar el servicio solicitado. (0x800705AA)”	Es probable que este error se deba a una discrepancia de RAM entre la RAM requerida para la gateway y la RAM disponible en el host. Para obtener más información sobre los requisitos de Storage Gateway, consulte Requisitos para configurar puerta de enlace de volumen.
Las actualizaciones del software de la gateway y de las instantáneas se producen a horas ligeramente diferentes de lo esperado.	El reloj de la MV de la gateway puede desviarse de la hora real, lo que se conoce como deriva del reloj. Compruebe y corrija la hora de la MV mediante la opción de sincronización de hora de la consola de la gateway local. Para obtener más información, consulte Sincronización de la hora de la máquina virtual con la hora del host KVM de Hyper-V o Linux.
Debe colocar los archivos de Microsoft Hyper-V Storage Gateway sin comprimir en el sistema de archivos del host.	Acceda al host como lo hace en un servidor de Microsoft Windows típico. Por ejemplo, si el host del hipervisor se llama `hyperv-server` , puede utilizar la siguiente ruta UNC `\\hyperv-server\c$` , en la que se asume que el nombre `hyperv-server` se puede resolver o está definido en el archivo del host local.
Se le solicitan credenciales al conectarse al hipervisor.	Agregue sus credenciales de usuario como administrador local para el host del hipervisor a través de la herramienta Sconfig.cmd.

Problema	Acción que ejecutar
Es posible que observe un rendimiento de red deficiente si activa la cola de máquinas virtuales (VMQ) para un host Hyper-V que utilice un adaptador de red Broadcom.	Para obtener información sobre una solución alternativa, consulte la documentación de Microsoft y consulte Rendimiento de red deficiente en máquinas virtuales en el host Hyper-V de Windows Server 2012 si VMQ se ha activado.

Solución de problemas 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 Amazon EC2. Para obtener más información sobre la diferencia entre una puerta de enlace local y una puerta de enlace implementada en Amazon EC2, consulteImplemente una EC2 instancia de Amazon personalizada para Volume Gateway.

Temas

- La puerta de enlace no se ha activado poco tiempo después
- No puede encontrar su instancia de EC2 gateway en la lista de instancias
- Creó un volumen de Amazon EBS pero no puede adjuntarlo a su instancia de EC2 puerta de enlace
- No puede adjuntar un iniciador a un destino de volumen de su puerta de enlace EC2
- 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 Soporte 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 State de la instancia debe ser RUNNING.
- Asegúrese de que el tipo de EC2 instancia de Amazon cumpla los requisitos mínimos, tal y como se describe enRequisitos de almacenamiento.

Después de corregir el problema, intente activar la gateway de nuevo. Para ello, abra la consola de Storage Gateway, elija Deploy a new Gateway on Amazon EC2 y vuelva a introducir la dirección IP de la instancia.

No puede encontrar su instancia de EC2 gateway en la lista de instancias

Si no asignó a la instancia una etiqueta de recurso y tiene muchas instancias en funcionamiento, puede ser difícil saber qué instancia lanzó. En este caso, puede realizar las siguientes acciones para encontrar la instancia de la gateway:

- Compruebe el nombre la Imagen de máquina de Amazon (AMI) en la pestaña Description (Descripción) de la instancia. Una instancia basada en la AMI de Storage Gateway debe empezar con el texto **`aws-storage-gateway-ami`**.
- Si tiene varias instancias basadas en la AMI de Storage Gateway, compruebe el momento de lanzar la instancia para encontrar la instancia correcta.

Creó un volumen de Amazon EBS pero no puede adjuntarlo a su instancia de EC2 puerta de enlace

Compruebe que el volumen de Amazon EBS en cuestión esté en la misma zona de disponibilidad que la instancia de la puerta de enlace. Si existe una discrepancia en las zonas de disponibilidad, cree un nuevo volumen de Amazon EBS en la misma zona de disponibilidad que la instancia.

No puede adjuntar un iniciador a un destino de volumen de su puerta de enlace EC2

Compruebe que el grupo de seguridad con el que ha lanzado la instancia incluya una regla que admita el puerto que está utilizando para el acceso iSCSI. El puerto suele estar configurado como

3260. Para obtener más información sobre la conexión a volúmenes, consulte Conexión a los volúmenes de un cliente de Windows.

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 Amazon EC2, los discos locales son volúmenes de Amazon EBS adjuntos a la instancia. Este mensaje de error se produce probablemente porque no hay volúmenes de Amazon EBS definidos para la instancia.

Consulte los dispositivos de bloques definidos para la instancia que está ejecutando la gateway. Si solo hay dos dispositivos de bloques (los dispositivos predeterminados que acompañan a la AMI), debe agregar almacenamiento. Para obtener más información sobre cómo hacerlo, consulte Implemente una EC2 instancia de Amazon personalizada para Volume Gateway. Después de conectar dos o más volúmenes de Amazon EBS, pruebe a crear almacenamiento de volumen 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 puerta de enlace AWS, consulta. Medición del rendimiento entre la puerta de enlace y AWS

¿Desea ayudar Soporte 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 Soporte para acceder a su puerta de enlace para ayudarlo a solucionar problemas de la puerta de enlace. De forma predeterminada, el Soporte acceso a la puerta de enlace está desactivado. Usted proporciona este acceso a través de la consola EC2 local de Amazon. Inicia sesión en la consola EC2 local de Amazon a través de un Secure Shell (SSH). Para iniciar sesión correctamente mediante SSH, el grupo de seguridad de la instancia debe tener una regla que abra el puerto TCP 22.

> **Note**
>
> Si agrega una nueva regla a un grupo de seguridad existente, la nueva regla se aplicará a todas las instancias que utilicen ese grupo de seguridad. Para obtener más información sobre los grupos de seguridad y cómo añadir una regla de grupo de seguridad, consulte los grupos de EC2 seguridad de Amazon en la Guía del EC2 usuario de Amazon.

Para permitir la Soporte conexión a su puerta de enlace, primero debe iniciar sesión en la consola local de la EC2 instancia de Amazon, navegar hasta la consola de Storage Gateway y, a continuación, proporcionar el acceso.

Para activar el Soporte acceso a una puerta de enlace implementada en una EC2 instancia de Amazon

1. Inicia sesión en la consola local de tu EC2 instancia de Amazon. Para obtener instrucciones, consulta Connect to your instance en la Guía del EC2 usuario de Amazon.

   Puedes usar el siguiente comando para iniciar sesión en la consola local de la EC2 instancia.

   ```
   ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
   ```

   > **Note**
   >
   > *PRIVATE-KEY*Es el `.pem` archivo que contiene el certificado privado del EC2 key pair que utilizaste para lanzar la EC2 instancia de Amazon. Para obtener más información,

consulta Cómo recuperar la clave pública de tu par de claves en la Guía del EC2 usuario de Amazon.

*INSTANCE-PUBLIC-DNS-NAME*Es el nombre del Sistema de nombres de dominio (DNS) público de la EC2 instancia de Amazon en la que se ejecuta la puerta de enlace. Para obtener este nombre de DNS público, seleccione la EC2 instancia de Amazon en la EC2 consola y haga clic en la pestaña Descripción.

2. En el símbolo del sistema, introduzca **`6 - Command Prompt`** para abrir la consola del canal de Soporte .
3. Introduzca **h** para abrir la ventana AVAILABLE COMMANDS (COMANDOS DISPONIBLES).
4. Realice una de las siguientes acciones:

   - Si la puerta de enlace está utilizando un punto de conexión público, en la ventana COMANDOS DISPONIBLES introduzca **`open-support-channel`** para conectar con el servicio de atención al cliente de Storage Gateway. Permitir el puerto TCP 22 para poder abrir un canal de soporte en AWS. Cuanto conecte con el servicio de atención al cliente, Storage Gateway le asignará un número de soporte. Apunte el número de soporte.
   - Si la gateway está utilizando un punto de enlace de la VPC, en la ventana AVAILABLE COMMANDS (COMANDOS DISPONIBLES), introduzca **`open-support-channel`**. Si la puerta de enlace no está activada, proporcione el punto de conexión de VPC o la dirección IP para conectar con el servicio de atención al cliente de Storage Gateway. Permitir el puerto TCP 22 para poder abrir un canal de soporte en AWS. Cuanto conecte con el servicio de atención al cliente, Storage Gateway le asignará un número de soporte. Apunte el número de soporte.

   > **Note**
   >
   > El número de canal no es un número de puerto Protocol/User Datagram Protocol (TCP/UDP (Transmission Control). En lugar de ello, la puerta de enlace realiza una conexión Secure Shell (SSH) (TCP 22) a los servidores de Storage Gateway y proporciona el canal de soporte para la conexión.

5. Una vez establecido el canal de soporte, proporcione su número de servicio de soporte para Soporte que Soporte pueda ayudarlo a solucionar problemas.
6. Cuando se complete la sesión de soporte, introduzca **q** para finalizarla. No cierre la sesión hasta que se le Soporte 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 administración iDRAC de Dell. Para obtener más información, consulte i Ciclo de alimentación DRAC9 virtual: ciclo de alimentación remoto de PowerEdge los servidores Dell EMC en el InfoHub sitio web de Dell Technologies.

¿Cómo se obtiene soporte de iDRAC de Dell?

El PowerEdge servidor Dell incluye la interfaz de administración iDRAC de Dell. Le recomendamos lo siguiente:

- Si utiliza la interfaz de administración iDRAC, debe cambiar la contraseña predeterminada. Para obtener más información sobre las credenciales de iDRAC, consulte Dell PowerEdge : ¿Cuáles son las credenciales de inicio de sesión predeterminadas para iDRAC? .
- Asegúrese de que el firmware sea up-to-date para evitar violaciones de seguridad.
- Mover la interfaz de red del iDRAC a un puerto normal (`em`) puede provocar problemas de rendimiento o impedir el funcionamiento normal del dispositivo.

No puede encontrar el número de serie del dispositivo hardware

Puede encontrar el número de serie del dispositivo de hardware de Storage Gateway con la consola de Storage Gateway.

Para encontrar el número de serie del dispositivo de hardware:

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Elija Hardware en el menú de navegación del lado izquierdo de la página.
3. Seleccione el dispositivo de hardware de la lista.
4. Localice el campo del número de serie en la pestaña Detalles del dispositivo.

Dónde obtener soporte para el dispositivo de hardware

Para ponerse en contacto con AWS el soporte técnico de su dispositivo de hardware, consulte Soporte.

Es posible que el Soporte equipo le pida que active el canal de soporte para solucionar los problemas de la puerta de enlace de forma remota. No necesita que este puerto esté abierto para el funcionamiento normal de la gateway, pero es necesario para la solución de problemas. Puede activar el canal de soporte desde la consola del hardware, como se muestra en el siguiente procedimiento.

Para abrir un canal de soporte para AWS

1. Abra la consola del hardware.
2. Elija Abrir canal de soporte en la parte inferior de la página principal de la consola de hardware y, a continuación, pulse `Enter`.

   El número de puerto asignado debe aparecer en 30 segundos si no hay problemas de firewall o de conectividad de red. Por ejemplo:

   Estado: Abierto en el puerto 19599
3. Anote el número de puerto e indíquelo en Soporte.

Solución de problemas con volúmenes

Puede encontrar más información sobre los problemas más habituales que podría encontrar al trabajar con volúmenes y las acciones que le sugerimos para corregirlos.

Temas

La consola dice que el volumen no está configurado

Si la consola de Storage Gateway indica que el volumen tiene el estado BÚFER DE CARGA NO CONFIGURADO, incremente la capacidad de búfer de carga a la puerta de enlace. No puede utilizar una gateway para almacenar datos de la aplicación si el búfer de carga de la gateway no está configurado. Para obtener más información, consulte Para configurar búfer de carga o el almacenamiento en caché adicional a la puerta de enlace.

La consola dice que el volumen es irrecuperable

En el caso de volúmenes almacenados, si la consola de Storage Gateway indica que el volumen tiene el estado IRRECUPERABLE, ya no podrá utilizar este volumen. Puede intentar eliminar el volumen en la consola de Storage Gateway. Si hay datos en el volumen, puede recuperar los datos al crear un nuevo volumen basado en el disco local de la MV utilizada inicialmente para crear el volumen. Cuando cree el volumen nuevo, seleccione Preserve existing data (Conservar los datos existentes). Elimine las instantáneas pendientes del volumen antes de eliminar el volumen. Para obtener más información, consulte Eliminación de instantáneas de los volúmenes de almacenamiento. Si la eliminación del volumen en la consola de Storage Gateway no funciona, es posible que el disco asignado para el volumen se haya retirado de la VM de manera incorrecta y no pueda retirarse del dispositivo.

Para volúmenes en caché, si la consola de Storage Gateway indica que el volumen tiene el estado IRRECUPERABLE, ya no podrá utilizar este volumen. Si hay datos en el volumen, puede crear una instantánea del volumen y, a continuación, recuperar los datos de la instantánea o clonar el volumen desde el último punto de recuperación. Puede eliminar el volumen después de recuperar los datos. Para obtener más información, consulte La gateway almacenada en la caché es inaccesible y desea recuperar los datos.

Para volúmenes almacenados, puede crear un nuevo volumen desde el disco que se usó para crear el volumen irrecuperable. Para obtener más información, consulte Creación de un volumen de almacenamiento. Para obtener información sobre el estado de los volúmenes, consulte Funcionamiento de los estados de volúmenes y las transiciones.

La gateway almacenada en la caché es inaccesible y desea recuperar los datos

Cuando la gateway no permite el acceso (como cuando se apaga), tiene la opción de crear una instantánea de un punto de recuperación de volumen y utilizar esa instantánea o clonar un nuevo

volumen desde el último punto de recuperación para un volumen existente. La clonación a partir de un punto de recuperación de volumen es más rápida y más rentable que la creación de una instantánea. Para obtener más información acerca de cómo clonar volúmenes, consulte Clonación de un volumen en caché desde un punto de recuperación.

Storage Gateway proporciona puntos de recuperación para cada volumen en una arquitectura de puerta de enlace de volumen en caché. Un punto de recuperación de volumen es un momento en el que todos los datos del volumen son coherentes y desde el que se puede crear una instantánea o clonar un volumen.

La consola dice que el estado del volumen es PASS THROUGH

En algunos casos, la consola de Storage Gateway podría indicar que el estado del volumen es ACCESO DIRECTO. Un volumen puede tener el estado PASSTHROUGH por varios motivos. Algunos motivos requieren una acción y otros no.

Un ejemplo de cuando se debe actuar si el estado del volumen es PASS THROUGH es cuando la gateway se queda sin espacio de búfer de carga. Para comprobar si se ha superado tu búfer de carga en el pasado, puedes ver la `UploadBufferPercentUsed` métrica en la CloudWatch consola de Amazon; para obtener más información, consultaSupervisión del búfer de carga. Si la puerta de enlace tiene el estado ACCESO DIRECTO porque se ha quedado sin espacio en el búfer de carga, debe asignar más espacio en el búfer de carga a la puerta de enlace. Al agregar más espacio en el búfer, el volumen pasará de ACCESO DIRECTO a ARRANCANDO y pasará a estar DISPONIBLE automáticamente. Aunque el estado del volumen sea ARRANCANDO, la puerta de enlace lee los datos del disco del volumen, carga estos datos en Amazon S3 y se pone al día según sea necesario. Cuando la puerta de enlace se pone al día y guarda los datos del volumen en Amazon S3, el estado del volumen pasa a ser DISPONIBLE y las instantáneas pueden iniciarse de nuevo. Tenga en cuenta que cuando el estado del volumen es PASS THROUGH o BOOTSTRAPPING, puede continuar leyendo y escribiendo datos en el disco del volumen. Para obtener más información sobre la adición de más espacio de búfer de carga, consulte Determinación del tamaño que se va a asignar al búfer de carga.

Para actuar antes de que se supere el búfer de carga, puede definir un umbral de alarma en el búfer de carga de la gateway. Para obtener más información, consulte Para establecer una alarma de umbral superior para el búfer de carga de una gateway.

En cambio, un ejemplo en el que no es necesario actuar cuando el estado de un volumen es PASS THROUGH es cuando el volumen está a la espera de arrancar porque hay otro volumen que está arrancando. La gateway inicia los volúmenes de uno en uno.

De manera infrecuente, el estado PASS THROUGH puede indicar que un disco asignado a un búfer de carga ha producido un error. En este caso, debe retirar el disco. Para obtener más información, consulte Uso de los recursos de almacenamiento de puerta de enlace de volumen. Para obtener información sobre el estado de los volúmenes, consulte Funcionamiento de los estados de volúmenes y las transiciones.

Desea verificar la integridad del volumen y solucionar posibles errores

Si desea comprobar la integridad del volumen y solucionar posibles errores, y la gateway utiliza iniciadores de Microsoft Windows para conectarse a sus volúmenes, puede utilizar la utilidad CHKDSK de Windows para verificar la integridad de los volúmenes y solucionar los errores de los volúmenes. Windows puede ejecutar automáticamente la herramienta CHKDSK automáticamente cuando se detecta algún daño en el volumen, o bien puede ejecutarla usted mismo.

El destino iSCSI del volumen no aparece en la consola de administración de discos de Windows

Si el destino iSCSI del volumen no aparece en la consola de administración de discos de Windows, compruebe que haya configurado el búfer de carga de la gateway. Para obtener más información, consulte Para configurar búfer de carga o el almacenamiento en caché adicional a la puerta de enlace.

Desea cambiar el nombre del destino iSCSI del volumen

Si desea cambiar el nombre de del destino iSCSI del volumen, debe eliminar el volumen y agregarlo de nuevo con un nuevo nombre de destino. Si lo hace, puede conservar los datos del volumen.

La instantánea de volumen programada no se produjo

Si no se realizó la snapshot programada de un volumen, compruebe si el estado del volumen es PASSTHROUGH o si el búfer de carga de la gateway se ha llenado inmediatamente antes de la hora de la snapshot programada. Puedes comprobar la `UploadBufferPercentUsed` métrica de la puerta de enlace en la CloudWatch consola de Amazon y crear una alarma para esta métrica. Para obtener más información, consulte Supervisión del búfer de carga y Para establecer una alarma de umbral superior para el búfer de carga de una gateway.

Necesita extraer o sustituir un disco en el que ha fallado

Si necesita sustituir un disco de volumen que ha fallado o retirarlo porque ya no es necesario, primero debe retirar el volumen mediante la consola de Storage Gateway. Para obtener más información, consulte Para eliminar un volumen. A continuación, utilice el cliente del hipervisor para retirar el almacenamiento de respaldo:

- VMware ESXiEn caso contrario, retire el almacenamiento posterior tal y como se describe enEliminación de volúmenes de almacenamiento.
- Para Microsoft Hyper-V, retire el almacenamiento de respaldo.

El rendimiento desde la aplicación hasta un volumen ha disminuido a cero

Si el rendimiento desde la aplicación hasta un volumen ha disminuido a cero, intente lo siguiente:

- Si utiliza el cliente VMware vSphere, compruebe que la dirección IP del host del volumen coincida con una de las direcciones que aparecen en el cliente de vSphere en la pestaña Resumen. Puede encontrar la dirección IP del host de un volumen de almacenamiento en la consola de Storage Gateway, en la pestaña Detalles para dicho volumen. Una discrepancia en la dirección IP puede producirse, por ejemplo, cuando se asigna una nueva dirección IP estática para la gateway. Si hay una discrepancia, reinicie la puerta de enlace desde la consola de Storage Gateway, como se muestra en Como apagar la MV de la gateway. Después de reiniciar, la dirección Host IP (IP del host) de la pestaña ISCSI Target Info (Información de destinos iSCSI) para un volumen de almacenamiento debe coincidir con la dirección IP que se muestra en el cliente vSphere en la pestaña Summary (Resumen) para la gateway.
- Si no hay ninguna dirección IP en el cuadro Host IP (IP del host) para el volumen y la gateway está online. Por ejemplo, esto podría ocurrir si crea un volumen asociado con una dirección IP de un adaptador de red de una gateway que tenga dos o más adaptadores de red. Al eliminar o desactivar el adaptador de red al que está asociado el volumen, es posible que la dirección IP no aparezca en el cuadro IP del host. Para solucionar este problema, elimine el volumen y, a continuación, vuelva a crearlo conservando sus datos existentes.
- Compruebe que el iniciador iSCSI que utiliza la aplicación está asignado correctamente al destino iSCSI para el volumen de almacenamiento. Para obtener más información sobre la conexión a volúmenes de almacenamiento, consulte Conexión a los volúmenes de un cliente de Windows.

Puede ver el rendimiento de los volúmenes y crear alarmas desde la CloudWatch consola de Amazon. Para ver más información sobre la medición del rendimiento desde la aplicación hasta un volumen, consulte Medición del rendimiento entre la aplicación y la gateway.

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 estado DISPONIBLE. Las demás cintas y volúmenes tendrán el estado IRRECUPERABLE.
>
> 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.

El estado de una instantánea de volumen es PENDING durante más tiempo del esperado

Si una snapshot de volumen permanece en estado PENDING más de lo esperado, es posible que la MV de la gateway se haya bloqueado inesperadamente o que el estado de un volumen haya cambiado a PASS THROUGH o IRRECOVERABLE. Si se da cualquiera de estos casos, la instantánea permanece en estado PENDING y la instantánea no se completa correctamente. En

estos casos, le recomendamos que elimine la snapshot. Para obtener más información, consulte Eliminación de instantáneas de los volúmenes de almacenamiento.

Cuando el volumen vuelva al estado AVAILABLE, cree una nueva snapshot del volumen. Para obtener información sobre el estado de los volúmenes, consulte Funcionamiento de los estados de volúmenes y las transiciones.

Notificaciones de estado de alta disponibilidad

Al ejecutar la puerta de enlace en la plataforma VMware vSphere High Availability (HA), es posible que reciba notificaciones de estado. Para obtener más información sobre las notificaciones de estado, consulte Solución de problemas 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 el VMware caso de las puertas de enlace, un restablecimiento realizado por vSphere High Availability Application Monitoring puede provocar este evento.

Acción necesaria

Cuando la puerta de enlace se ejecute en un entorno de este tipo, compruebe la presencia de la `HealthCheckFailure` notificación y consulte el registro de VMware eventos de la máquina virtual.

Notificación: HealthCheckFailure

En el caso de una puerta de enlace en VMware vSphere HA, puede recibir una `HealthCheckFailure` notificación cuando se produzca un error en una comprobación de estado y se solicite el reinicio de la máquina virtual. Este evento también se produce durante una prueba para monitorizar la disponibilidad y se indica mediante una notificación `AvailabilityMonitorTest`. En este caso, la notificación `HealthCheckFailure` es normal.

> **Note**
>
> Esta notificación es solo para VMware las puertas de enlace.

Acción necesaria

Si este evento se produce de forma repetida sin una notificación `AvailabilityMonitorTest`, compruebe si la infraestructura de la MV presenta algún problema (almacenamiento, memoria, etc.). Si necesita ayuda adicional, póngase en contacto con Soporte.

Notificación: AvailabilityMonitorTest

En el caso de una puerta de enlace en VMware vSphere HA, puede recibir una `AvailabilityMonitorTest` notificación cuando ejecute una prueba del sistema de supervisión de disponibilidad y aplicaciones en. VMware

Métricas

La métrica `AvailabilityNotifications` está disponible en todas las gateways. Esta métrica es un recuento del número de notificaciones de estado relacionadas con la disponibilidad que ha generado la gateway. Utilice la estadística `Sum` para comprobar si se está produciendo algún evento relacionado con la disponibilidad en la gateway. Consulte con el grupo de CloudWatch registros configurado para obtener detalles sobre los eventos.

Prácticas recomendadas para puerta de enlace de volumen

Esta sección contiene los siguientes temas, que proporcionan información sobre las prácticas recomendadas para trabajar con puertas de enlace, discos locales, instantáneas y datos. Le recomendamos que se familiarice con la información que se describe en esta sección e intente seguir estas directrices para evitar problemas con AWS Storage Gateway. Para obtener orientación adicional sobre diagnóstico y solución de problemas comunes que pueden surgir con la implementación, consulte Solución de problemas de la gateway.

Temas

Prácticas recomendadas: recuperación de los datos

Aunque es infrecuente, es posible que su gateway se enfrente a un error irrecuperable. Este error puede producir en la máquina virtual (VM), en la propia gateway, en el almacenamiento local o en otro lugar. Si se produce un error, le recomendamos que siga las instrucciones de la sección adecuada, a continuación, para recuperar los datos.

> **Important**
>
> Storage Gateway no admite la recuperación de una máquina virtual de puerta de enlace a partir de una instantánea creada por el hipervisor o desde la EC2 Amazon Machine Image (AMI) de Amazon. Si la MV de la gateway no funciona correctamente, active una nueva gateway y recupere los datos para esa gateway utilizando las instrucciones siguientes.

Temas

- Recuperación de los datos a partir de un sistema de archivos dañado
- 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 la conexión de la puerta de enlace a Internet.
- En el caso de las configuraciones de volúmenes en caché, cuando sea posible el acceso a la puerta de enlace, los volúmenes pasarán al estado ARRANCADO. Esta funcionalidad garantiza que los datos almacenados localmente continúen sincronizados con ellos. AWS Para obtener más información sobre este estado, consulte Funcionamiento de los estados de volúmenes y las transiciones.
- 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 o la máquina virtual no funcionan correctamente, puede recuperar los datos que se hayan cargado AWS y almacenado en un volumen de Amazon S3. En el caso de puertas de enlace de volúmenes en caché, puede recuperar los datos a partir de una instantánea de recuperación. Para puertas de enlace de volumen en caché, puede recuperar los datos a partir de la instantánea EBS más reciente del volumen. Para puerta de enlace de cinta, recupere una más cintas desde un punto de recuperación hasta una nueva puerta de enlace de cinta.

Si el acceso a la puerta de enlace de los volúmenes en caché deja de ser posible, puede hacer lo siguiente para recuperar los datos desde una instantánea de recuperación:

1. En el AWS Management Console, elija la puerta de enlace que no funciona correctamente, elija el volumen que desea recuperar y, a continuación, cree una instantánea de recuperación a partir de ella.
2. Implemente y active una nueva puerta de enlace de volúmenes. O bien, si dispone de una puerta de enlace de volúmenes en funcionamiento, puede utilizar esa puerta de enlace para recuperar los datos del volumen.
3. Busque la instantánea que ha creado y restáurela en un nuevo volumen en la gateway en funcionamiento.
4. Monte el nuevo volumen como un dispositivo iSCSI en el servidor de aplicaciones presente en sus instalaciones.

Para obtener información detallada sobre cómo recuperar datos de volúmenes almacenados en caché a partir de una instantánea de recuperación, consulte La gateway almacenada en la caché es inaccesible y desea recuperar los datos.

Recuperación de los datos desde un volumen irrecuperable

Si el estado del volumen es IRRECOVERABLE, ya no podrá utilizar este volumen.

EN el caso de volúmenes almacenados, puede hacer lo siguiente para recuperar los datos del volumen irrecuperable en un nuevo volumen:

1. Cree un nuevo volumen desde el disco que se usó para crear el volumen irrecuperable.
2. Conserve los datos existentes cuando cree el nuevo volumen.
3. Elimine todos los trabajos de instantánea pendientes para el volumen irrecuperable.
4. Elimine de la gateway el volumen irrecuperable.

En el caso de volúmenes almacenados en caché, recomendamos utilizar el último punto de recuperación para clonar un nuevo volumen.

Para obtener información detallada acerca de cómo recuperar los datos de un volumen irrecuperable a un nuevo volumen, consulte La consola dice que el volumen es irrecuperable.

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.

Recuperación de los datos a partir de un sistema de archivos dañado

Si el sistema de archivos se daña, puede utilizar el comando **`fsck`** para comprobar si hay errores en el sistema de archivos y repararlos. Si puede reparar el sistema de archivos, puede recuperar los datos de los volúmenes del sistema de archivos como se describe a continuación:

1. Apague la máquina virtual y utilice la consola de administración de Storage Gateway para crear una instantánea de recuperación. Esta instantánea representa los datos más recientes almacenados en AWS.

   > **Note**
   >
   > Puede utilizar esta instantánea como segunda opción si no se puede reparar el sistema de archivos o no se puede completar correctamente el proceso de creación de instantáneas.

   Para obtener más información sobre cómo crear una instantánea de recuperación, consulte La gateway almacenada en la caché es inaccesible y desea recuperar los datos.
2. Utilice el comando **`fsck`** para comprobar si hay errores en el sistema de archivos e intentar repararlos.
3. Reinicie la MV de la gateway.
4. Cuando el host del hipervisor comience a arrancar, pulse y mantenga pulsada la tecla mayúsculas para entrar en el menú de inicio de grub.
5. Desde el menú, pulse **e** para editar.
6. Elija la línea del kernel (la segunda) y, a continuación, pulse **e** para editar.

7. Agregue la siguiente opción a la línea de comandos del kernel: **`init=/bin/bash`**. Separe la opción que acaba de agregar de la opción anterior con un espacio.
8. Elimine ambas líneas de la `console=`, asegurándose de eliminar todos los valores que siguen al símbolo =, incluidos los separados por comas.
9. Pulse **`Return`** (Intro) para guardar los cambios.
10. Pulse **`b`** para arrancar el equipo con la opción del kernel modificada. El equipo arrancará con un símbolo `bash#`.
11. Introduzca **`/sbin/fsck -f /dev/sda1`** para ejecutar este comando manualmente desde el símbolo para comprobar y reparar el sistema de archivos. Si el comando no funciona con la ruta de `/dev/sda1`, puede utilizar **`lsblk`** para determinar el dispositivo raíz del sistema de archivos para `/` y utilizar esa ruta en su lugar.
12. Cuando la comprobación y la reparación del sistema de archivos, reinicie la instancia. Los ajustes de grub recuperarán sus valores originales y la gateway se iniciará normalmente.
13. Espere a que se completen las instantáneas en curso de la gateway original y, a continuación, valide los datos de la instantánea.

Puede seguir utilizando el volumen original tal y como está o puede crear una nueva gateway con un volumen nuevo basado en la instantánea de recuperación o la instantánea completa. También puede crear un nuevo volumen a partir de cualquiera de las instantáneas completadas de este volumen.

Recuperación de los datos de un centro de datos inaccesible

Si su puerta de enlace o centro de datos se vuelve inaccesible por algún motivo, puede recuperar los datos en otra puerta de enlace de un centro de datos diferente o recuperarlos en una puerta de enlace alojada en una EC2 instancia de Amazon. Si no tienes acceso a otro centro de datos, te recomendamos crear la puerta de enlace en una EC2 instancia de Amazon. Los pasos que siga dependerán del tipo de gateway cuyos datos intenta recuperar.

Para recuperar datos de una puerta de enlace de volumen en un centro de datos inaccesible

1. Crea y activa un nuevo Volume Gateway en un EC2 host de Amazon. Para obtener más información, consulte Implemente una EC2 instancia de Amazon personalizada para Volume Gateway.

> **Note**
>
> Los volúmenes almacenados en Gateway no se pueden alojar en la EC2 instancia de Amazon.

2. Cree un volumen nuevo y elija la EC2 puerta de enlace como puerta de enlace de destino. Para obtener más información, consulte Creación de un volumen de almacenamiento.

   Cree el nuevo volumen basado en una instantánea o un clon de Amazon EBS a partir del último punto de recuperación del volumen que desea recuperar.

   Si el volumen se basa en una instantánea, proporcione el ID de instantánea.

   Si va a clonar un volumen a partir de un punto de recuperación, elija el volumen de origen.

Limpieza 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.

Para eliminar los recursos innecesarios

1. Elimine las instantáneas. Para obtener instrucciones, consulte Eliminación de instantáneas de los volúmenes de almacenamiento.
2. A menos que planee seguir utilizando la gateway, elimínela. Para obtener más información, consulte Eliminación de la puerta de enlace y eliminación de 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.

Cómo reducir la cantidad de almacenamiento facturado en un volumen

La eliminación de archivos del sistema de archivos no elimina necesariamente datos del dispositivo de bloques subyacente ni reduce la cantidad de datos almacenados en el volumen. Si desea reducir la cantidad de almacenamiento facturado en el volumen, recomendamos que sobrescriba los archivos con ceros para comprimir el almacenamiento a una cantidad insignificante de

almacenamiento real. Storage Gateway cobra por el uso del volumen en función del almacenamiento comprimido.

> **Note**
>
> Si utiliza una herramienta de borrado que sobrescribe los datos en el volumen con datos aleatorios, el uso no se reducirá. Esto se debe a que los datos aleatorios no se pueden comprimir.

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 la máquina virtual de la puerta de enlace: obtenga información sobre cómo implementar y configurar un host de máquina virtual para la puerta de enlace.
- Uso de los recursos de almacenamiento de puerta de enlace de volumen- Obtenga información sobre los procedimientos relacionados con los recursos de almacenamiento de Volume Gateway, como la eliminación de discos locales y la administración de los volúmenes de Amazon EBS en las EC2 instancias de Amazon Gateway.
- Obtención de una clave de activación para la puerta de enlace: obtenga información sobre dónde encontrar la clave de activación que debe proporcionar al implementar una nueva puerta de enlace.
- Conexión de iniciadores iSCSI: obtenga información sobre cómo trabajar con volúmenes o dispositivos de biblioteca de cintas virtual (VTL) expuestos como destinos de interfaz de sistemas informáticos pequeños de Internet (iSCSI).
- Uso AWS Direct Connect con Storage Gateway: obtenga información sobre cómo crear una conexión de red dedicada entre la puerta de enlace en las instalaciones y la nube de AWS .
- Obtención de la dirección IP para el dispositivo de puerta de enlace: obtenga información sobre dónde encontrar la dirección IP del host de la máquina virtual de la puerta de enlace, que debe proporcionar al implementar una nueva puerta de enlace.
- Descripción de los recursos y recursos de Storage Gateway IDs- Aprenda a AWS identificar los recursos y subrecursos que crea Storage Gateway.
- Etiquetado de recursos de Storage Gateway: obtenga información sobre cómo usar las etiquetas de metadatos para clasificar los recursos y facilitar su administración.
- Uso de componentes de código abierto para Storage Gateway: obtenga información sobre las herramientas y licencias de terceros que se utilizan para ofrecer la funcionalidad de Storage Gateway.

- AWS Storage Gateway cuotas: obtenga información sobre los límites y las cuotas de la puerta de enlace de volumen, incluidas las limitaciones máximas de tamaño y cantidad del volumen y las recomendaciones sobre el tamaño del disco local.

Implementación y configuración del host de la máquina virtual de la puerta de enlace

En los temas de esta sección se describe cómo configurar y administrar el host de la máquina virtual del dispositivo Storage Gateway, incluidos los dispositivos locales que se ejecutan en VMware KVM de Hyper-V o Linux y los dispositivos que se ejecutan en EC2 instancias de Amazon en la nube. AWS

Temas

- Implemente un EC2 host de Amazon predeterminado para Volume Gateway- Obtenga información sobre cómo implementar y activar una puerta de enlace por volumen de en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) utilizando las especificaciones predeterminadas.
- Implemente una EC2 instancia de Amazon personalizada para Volume Gateway- Obtenga información sobre cómo implementar y activar una puerta de enlace por volumen de en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) mediante una configuración personalizada.
- Modificar las opciones de metadatos de las EC2 instancias de Amazon- Obtenga información sobre cómo configurar su instancia de Amazon EC2 Gateway para que acepte las solicitudes de metadatos entrantes que usen la versión 1 (IMDSv1) del IMDS o exijan que todas las solicitudes de metadatos usen la versión 2 (IMDSv2) del IMDS.
- Sincronización de la hora de la máquina virtual con la hora del host KVM de Hyper-V o Linux: obtenga información sobre cómo ver y sincronizar la hora de una máquina virtual de puerta de enlace KVM Hyper-V o Linux en las instalaciones con un servidor de protocolo de tiempo de red (NTP).
- Sincronice la hora de la máquina virtual con la hora VMware del host- Obtenga información sobre cómo comprobar la hora del host de una máquina virtual de VMware puerta de enlace y, si es necesario, configurar la hora y configurar el host para que sincronice su hora automáticamente con un servidor de protocolo de tiempo de red (NTP).

- Configuración de la paravirtualización en un host VMware - Obtenga información sobre cómo configurar la plataforma VMware host para que su dispositivo Storage Gateway utilice controladores paravirtuales de Internet Small Computer System Interface Protocol (iSCSI).
- Configuración de adaptadores de red para la puerta de enlace- Obtenga información sobre cómo puede reconfigurar su puerta de enlace para usar el adaptador de red VMXNET3 (10 GbE) o para usar más de un adaptador de red para poder acceder a él desde varias direcciones IP.
- Uso de VMware vSphere High Availability con Storage Gateway- Obtenga información sobre cómo proteger sus cargas de trabajo de almacenamiento contra errores de hardware, hipervisor o red configurando Storage Gateway para que funcione con VMware vSphere High Availability.

Implemente un EC2 host de Amazon predeterminado para Volume Gateway

En este tema se enumeran los pasos para implementar un EC2 host de Amazon con las especificaciones predeterminadas.

Puede implementar y activar una puerta de enlace por volumen de 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**
>
> La comunidad Storage Gateway AMIs está publicada y cuenta con el apoyo total de AWS. Puede ver que el editor es AWS un proveedor verificado.

1. Para configurar Amazon EC2instance, elige Amazon EC2 como plataforma de alojamiento en la sección de opciones de plataforma del flujo de trabajo. Para obtener instrucciones sobre la configuración de la EC2 instancia de Amazon, consulte Implementación de una EC2 instancia de Amazon para alojar su Volume Gateway.
2. Seleccione Launch instance para abrir la plantilla AMI de AWS Storage Gateway en la EC2 consola de Amazon y personalizar ajustes adicionales, como los tipos de instancia, los ajustes de red y configurar el almacenamiento.
3. Si lo desea, puede seleccionar Usar la configuración predeterminada en la consola de Storage Gateway para implementar una EC2 instancia de Amazon con la configuración predeterminada.

La EC2 instancia de Amazon que crea Use default settings tiene las siguientes especificaciones predeterminadas:

- Tipo de instancia: m5.xlarge
- Configuración de red
  - Para la VPC, selecciona la VPC en la que quieres que se ejecute la EC2 instancia.
  - En Subnet, especifica la subred en la que se debe lanzar la EC2 instancia.

    > **Note**
    >
    > Las subredes de VPC aparecerán en el menú desplegable solo si tienen activada la configuración de asignación automática de IPv4 direcciones públicas desde la consola de administración de VPC.

  - Asignar una IP pública de forma automática: Activada

Se crea un grupo EC2 de seguridad y se asocia a la instancia. EC2 El grupo de seguridad tiene las siguientes reglas de puerto de entrada:

> **Note**
>
> Necesitará que el puerto 80 esté abierto durante la activación de la puerta de enlace. El puerto se cierra inmediatamente después de la activación. A partir de entonces, solo se podrá acceder a la EC2 instancia a través de los demás puertos de la VPC seleccionada.
> Solo se puede acceder a los 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 EC2 instancia de Amazon, seleccione Seguridad, vaya a Detalles del grupo de seguridad y elija el ID del grupo de seguridad.

Puerto	Protocolo	Protocolo del sistema de archivos				
80	TCP	Acceso HTTP para la activación				
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 finalizar	Sí	Sí	Sí			
Encriptado	No	No	No			

Configuración predeterminada	Volumen raíz de AMI	Caché de volumen 2	Caché de volumen 3			
Rendimiento	125	125	125			

Implemente una EC2 instancia de Amazon personalizada para Volume Gateway

Puede implementar y activar una puerta de enlace por volumen de en una instancia de Amazon Elastic Compute Cloud (Amazon EC2). La imagen de máquina de Amazon (AMI) de AWS Storage Gateway se encuentra disponible como AMI de la comunidad.

> **Note**
>
> La comunidad Storage Gateway AMIs está publicada y cuenta con el apoyo total de AWS. Puede ver que el editor es AWS un proveedor verificado.
> Volume Gateway AMIs utiliza la siguiente convención de nomenclatura. El número de versión adjunto al nombre de la AMI cambia con cada versión publicada.
> `aws-storage-gateway-CLASSIC-2.9.0`

Para implementar una EC2 instancia de Amazon para alojar su Volume 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 volumen. Cuando llegue a la sección de 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 Volume Gateway.

   > **Note**
   >
   > La plataforma de EC2 alojamiento de Amazon solo admite volúmenes en caché. Las pasarelas de volumen almacenadas no se pueden implementar en las EC2 instancias.

2. Elija Launch instance para abrir la plantilla de AWS Storage Gateway AMI en la EC2 consola de Amazon, donde podrá configurar ajustes adicionales.

   Usa Quicklaunch para lanzar la EC2 instancia de Amazon con la configuración predeterminada. Para obtener más información sobre las especificaciones predeterminadas de Amazon EC2 Quicklaunch, consulte Amazon. EC2 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 i3 EC2, utilizan discos NVMe SSD. Estos pueden causar problemas al iniciar o detener una puerta de enlace de volumen; 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 la VPC (obligatorio), elige la VPC en la que quieres lanzar tu instancia de Amazon. EC2 Para obtener más información, consulte Cómo funciona Amazon VPC en la Guía del usuario de Amazon Virtual Private Cloud.

b. (Opcional) En Subnet, elige la subred en la que quieres lanzar tu instancia de Amazon EC2 .

c. En Auto-assign Public IP (Autoasignar IP pública), elija Enable (Habilitar).

7. En la subsección Firewall (grupos de seguridad), revise los ajustes preconfigurados. Si lo deseas, puedes cambiar el nombre y la descripción predeterminados del nuevo grupo de seguridad que se va a crear para tu EC2 instancia de Amazon, o bien optar por aplicar reglas de firewall desde un grupo de seguridad existente.

8. En la subsección Reglas de grupos de seguridad de entrada, agregue reglas de firewall para abrir los puertos que los clientes utilizarán para conectarse a su instancia. Para obtener más información sobre los puertos necesarios para puerta de enlacepuerta de enlace de volumen, 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**
>
> La puerta de enlace de volumen requiere que el puerto TCP 80 esté abierto para el tráfico entrante y para el acceso HTTP único durante la activación de la puerta de enlace. Tras la activación, puede cerrar este puerto.
> Además, debe abrir el puerto TCP 3260 para el acceso 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 agregar al menos un volumen de Amazon EBS con una capacidad mínima de 165 GiB para el almacenamiento en caché y al menos un volumen de Amazon EBS con una capacidad mínima de 150 GiB para el búfer de carga, además del volumen raíz preconfigurado. Para aumentar el rendimiento, recomendamos asignar varios volúmenes de EBS para el almacenamiento en caché de al menos 150 GiB cada uno.

11. En la subsección Detalles avanzados, revise los ajustes preconfigurados y realice los cambios necesarios.
12. Elija Launch instance para lanzar su nueva instancia de Amazon EC2 Gateway con los ajustes configurados.
13. Para comprobar que la nueva instancia se lanzó correctamente, vaya a la página de instancias de la EC2 consola de Amazon y busque la nueva instancia por su nombre. Asegúrese de que el Estado de la instancia se muestre En ejecución con una marca de verificación verde y de que la Comprobación de estado se haya completado y muestre una marca de verificación verde.
14. Seleccione la instancia de la página de detalles. Copie la IPv4dirección pública de la sección de resumen de la instancia y, a continuación, vuelva a la página Configurar puerta de enlace de la consola Storage Gateway para reanudar la configuración de la puerta de enlace por volumen de .

Puede determinar el ID de AMI que se utilizará para lanzar una puerta de enlace por volumen de mediante la consola Storage Gateway o consultando el almacén de AWS Systems Manager parámetros.

Para determinar la ID de AMI, lleve a cabo alguna de las siguientes operaciones:

- Empiece configurando una nueva puerta de enlace mediante la consola de Storage Gateway. Para obtener instrucciones, consulte Configuración de una puerta de enlace de volumen. Cuando llegue a la sección de opciones de plataforma, elija Amazon EC2 como plataforma host y, a continuación, elija Launch instance para abrir la plantilla de AWS Storage Gateway AMI en la EC2 consola de Amazon.

  Se le redirigirá a la página de AMI de la EC2 comunidad, donde podrá ver el ID de la AMI de su AWS región en la URL.
- Consulta del almacén de parámetros de Systems Manager. Puede utilizar la API Storage Gateway AWS CLI o Storage Gateway para consultar el parámetro público de Systems Manager en el espacio de nombres `/aws/service/storagegateway/ami/CACHED/latest` de las puertas de enlace de volumen en caché o `/aws/service/storagegateway/ami/STORED/latest` de las puertas de enlace de volumen almacenado. Por ejemplo, si utiliza el siguiente comando de CLI, se devuelve el ID de la AMI actual Región de AWS que especifique.

```
aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/
STORED/latest
```

El comando de la CLI devuelve un resultado similar al siguiente.

```
{
    "Parameter": {
        "Type": "String",
        "LastModifiedDate": 1561054105.083,
        "Version": 4,
        "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/
STORED/latest",
        "Name": "/aws/service/storagegateway/ami/STORED/latest",
        "Value": "ami-123c45dd67d891000"
    }
}
```

Modificar las opciones de metadatos de las EC2 instancias de Amazon

El servicio de metadatos de instancias (IMDS) es un componente de la instancia que proporciona acceso seguro a los metadatos de las EC2 instancias de Amazon. Se puede configurar una instancia para que acepte las solicitudes de metadatos entrantes que usen la versión 1 (IMDSv1) del IMDS o para que todas las solicitudes de metadatos usen la versión 2 () del IMDS. IMDSv2 IMDSv2 utiliza solicitudes orientadas a la sesión y mitiga varios tipos de vulnerabilidades que podrían utilizarse para intentar acceder al IMDS. Para obtener más información IMDSv2, consulte Cómo funciona Instance Metadata Service versión 2 en la Guía del usuario de Amazon Elastic Compute Cloud.

Le recomendamos que lo requiera IMDSv2 para todas las EC2 instancias de Amazon que alojen Storage Gateway. IMDSv2 es obligatorio de forma predeterminada en todas las instancias de gateway recién lanzadas. Si tiene instancias existentes que aún están configuradas para aceptar solicitudes de IMDSv1 metadatos, consulte Requerir el uso de IMDSv2 en la Guía del usuario de Amazon Elastic Compute Cloud para obtener instrucciones sobre cómo modificar las opciones de metadatos de la instancia para requerir el uso de IMDSv2. La aplicación de este cambio no requiere un reinicio de la instancia.

Sincronización de la hora de la máquina virtual con la hora del host KVM de Hyper-V o Linux

Para una puerta de enlace implementada en VMware ESXi, basta con configurar la hora del host del hipervisor y sincronizar la hora de la máquina virtual con el host para evitar la pérdida de tiempo. Para obtener más información, consulte Sincronice la hora de la máquina virtual con la

hora VMware del host. Para una puerta de enlace implementada en Microsoft Hyper-V o Linux KVM, le recomendamos que compruebe periódicamente la hora de la máquina virtual mediante el procedimiento que se describe a continuación.

Visualización y sincronización de la hora de la máquina virtual de una puerta de enlace de hipervisor con un servidor de Network Time Protocol (NTP)

1. Inicie sesión en la consola local de la gateway:
   - Para obtener más información sobre el inicio de sesión en la consola local de Microsoft Hyper-V, consulte Acceso a la consola local de la gateway con Microsoft Hyper-V.
   - Para obtener más información sobre cómo iniciar sesión en la consola local de la máquina virtual basada en el kernel (KVM) de Linux, consulte Acceso a la consola local de la gateway con Linux KVM.
2. En la pantalla del menú principal de Configuración de Storage Gateway, ingrese el número correspondiente para seleccionar Administración de la hora del sistema.
3. En la pantalla del menú Administración de la hora del sistema, ingrese el número correspondiente para seleccionar Ver y sincronizar la hora del sistema.

   La consola local de la puerta de enlace muestra la hora actual del sistema y la compara con la hora indicada por el servidor NTP. A continuación, indica la discrepancia exacta entre ambas horas en segundos.
4. Si la discrepancia horaria es superior a 60 segundos, ingrese **y** para sincronizar la hora del sistema con la hora de NTP. De lo contrario, escriba **n**.

   La sincronización de la hora puede tardar unos instantes.

Sincronice la hora de la máquina virtual con la hora VMware del host

Para activar la gateway correctamente, debe asegurarse de que la hora de la máquina virtual esté sincronizada con la hora del host y de que esta última esté configurada de forma correcta. En esta sección, primero se sincroniza la hora de la máquina virtual con la hora del host. A continuación, se comprueba la hora del host. Después, si es preciso, se establece la hora del host y se configura este último para que sincronice la hora automáticamente con un servidor NTP (Network Time Protocol).

> **Important**
>
> Sincronizar la hora de la máquina virtual con la hora del host es imprescindible para que la gateway se active correctamente.

Para sincronizar la hora de la máquina virtual con la hora del host

1. Configure la hora de la máquina virtual.

   a. En el cliente de vSphere, haga clic con el botón derecho en el nombre de la máquina virtual de puerta de enlace en el panel de la izquierda de la ventana de la aplicación para abrir el menú contextual para la máquina virtual y, a continuación, elija Editar configuración.

      Se abrirá el cuadro de diálogo Virtual Machine Properties (Propiedades de la máquina virtual).

   b. Seleccione la pestaña Opciones y, a continuación, seleccione VMware Herramientas en la lista de opciones.

   c. Marque la opción Sincronizar tiempo del invitado con el host en la sección Avanzadas situada a la derecha del cuadro de diálogo de propiedades de la máquina virtual, y, a continuación, elija Aceptar.

      La máquina virtual sincronizará su hora con la del host.

2. Configurar la hora del host.

   Es importante asegurarse de que el reloj del host esté establecido en la hora correcta. Si no ha configurado el reloj del host, siga estos pasos para configurarlo y sincronizarlo con un servidor NTP.

   a. En el cliente de VMware vSphere, seleccione el nodo host de vSphere en el panel izquierdo y, a continuación, elija la pestaña Configuración.

   b. Seleccione Time Configuration (Configuración de tiempo) en el panel Software y, a continuación, elija el enlace Properties (Propiedades).

      Aparecerá el cuadro de diálogo Time Configuration (Configuración de tiempo).

   c. En Fecha y hora, defina la fecha y la hora del host de vSphere.

   d. Configure el host para que sincronice la hora automáticamente con un servidor de NTP.

i. Elija Opciones en el cuadro de diálogo Configuración de tiempo. A continuación, en el cuadro de diálogo Opciones de NTP Daemon (ntpd), elija Configuración de NTP en el panel de la izquierda.

ii. Elija Add (Añadir) para agregar un nuevo servidor NTP.

iii. En el cuadro de diálogo Add NTP Server (Añadir servidor NTP), escriba la dirección IP o el nombre de dominio completo de un servidor NTP y, a continuación, elija OK (Aceptar).

Puede usar `pool.ntp.org` como nombre de dominio.

iv. En el cuadro de diálogo Opciones de NTP Daemon (ntpd), elija Generales en el panel de la izquierda.

v. En Comandos de servicio, elija Iniciar para iniciar el servicio.

Tenga en cuenta que si cambia esta referencia del servidor NTP o agrega otra más adelante, tendrá que reiniciar el servicio para utilizar el nuevo servidor.

e. Elija OK (Aceptar) para cerrar el cuadro de diálogo NTP Daemon (ntpd) Options (Opciones de NTP Daemon (ntpd)).

f. Elija OK (Aceptar) para cerrar el cuadro de diálogo Time Configuration (Configuración de tiempo).

Configuración de la paravirtualización en un host VMware

El siguiente procedimiento describe cómo configurar la plataforma VMware host para que el dispositivo Storage Gateway utilice controladores paravirtuales de Internet Small Computer System Interface Protocol (iSCSI). Los controladores de iSCSI paravirtuales son de almacenamiento de alto rendimiento que pueden generar un mayor rendimiento y un menor uso de la CPU. Estos controladores son los más adecuados para entornos de almacenamiento de alto rendimiento. Al configurar los controladores de iSCSI de esta manera, la máquina virtual de Storage Gateway funciona con el sistema operativo host para permitir que la consola de la puerta de enlace identifique los discos virtuales que agrega a la máquina virtual.

> **Note**
>
> Tiene que completar este paso para evitar problemas en la identificación de estos discos cuando se configuren en la consola de puerta de enlace.

Para configurar la plataforma de VMware host para que utilice controladores paravirtualizados

1. En el cliente VMware vSphere, haga clic con el botón derecho en el nombre de la máquina virtual de puerta de enlace en el panel de navegación de la parte izquierda de la ventana de la aplicación para abrir el menú contextual y, a continuación, seleccione Editar configuración.
2. En el cuadro de diálogo de Propiedades de la máquina virtual, elija la pestaña Hardware.
3. En la pestaña Hardware, seleccione el controlador SCSI 0 y, a continuación, elija Cambiar tipo.
4. En el cuadro de diálogo Cambiar el tipo de controlador SCSI, seleccione el tipo de controlador SCSI VMware paravirtual y, a continuación, elija Aceptar para guardar la configuración.

Configuración de adaptadores de red para la puerta de enlace

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

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. En VMware, 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 podría provocar problemas de red.

5. Elija Add (Añadir) para abrir el asistente para agregar hardware.
6. Elija Ethernet Adapter (Adaptador Ethernet) y, a continuación, seleccione Next (Siguiente).
7. En el asistente de tipo de red, seleccione **`VMXNET3`** para Adapter Type (Tipo de adaptador) y, a continuación, elija Next (Siguiente).
8. En el asistente de propiedades de 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, introduzca el número correspondiente para seleccionar Restablecer todo a DHCP y, a continuación, introduzca **y** (para Sí) en el símbolo del sistema para establecer todos los adaptadores de modo que utilicen el protocolo de configuración dinámica de host (DHCP). Todos los adaptadores disponibles se establecen para utilizar 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 red: es posible que el entorno de aplicaciones le exija mantener los destinos iSCSI y los iniciadores que se conecten con ellos en una red aislada, diferente de la red mediante la cual la gateway se comunica con AWS.

En un caso de uso típico de varios adaptadores, un adaptador se configura como la ruta por la que se comunica la puerta de enlace AWS (es decir, como la puerta de enlace predeterminada). Excepto para este adaptador, los iniciadores deben estar en la misma subred que el adaptador que contiene los destinos iSCSI a los que se conecte. De lo contrario, puede que la comunicación con los objetivos reales no sea posible. Si un destino está configurado en el mismo adaptador con el que se utiliza para la comunicación AWS, el tráfico iSCSI 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 varios adaptadores de red en un host VMware ESXi
- Configuración de varios adaptadores de red en el host Microsoft Hyper-V

Configuración de varios adaptadores de red en un host VMware ESXi

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 VMwareESXi.

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

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

   La MV puede mantenerse activada para este procedimiento.
3. En el cliente, abra el menú contextual (haga clic con el botón derecho) de la MV de la gateway y elija Edit Settings (Editar configuración).
4. En la pestaña Hardware del cuadro de diálogo Virtual Machine Properties (Propiedades de la MV), elija Add (Agregar) para agregar un dispositivo.
5. Siga el asistente para agregar hardware para agregar un adaptador de red.

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

   b. En el panel Network Type (Tipo de red), asegúrese de que Se haya seleccionado Connect at power on (Conectar al inicio) para Type (Tipo) y, a continuación, elija Next (Siguiente).

Se recomienda utilizar el adaptador de VMXNET3 red con Storage Gateway. Para obtener más información sobre los tipos de adaptadores que pueden aparecer en la lista de adaptadores, consulte Tipos de adaptadores de red en la ESXi documentación de vCenter Server.

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

6. Elija la pestaña Resumen de la VM y elija Ver todo junto al cuadro Dirección IP. En la ventana Direcciones IP de máquina virtual se muestran todas las direcciones IP que se pueden utilizar para obtener acceso a la puerta de enlace. Confirme que aparece una segunda dirección IP para la gateway.

> **Note**
>
> Pueden pasar unos momentos hasta que los cambios del adaptador surtan efecto y el resumen de información de la MV se actualice.

7. En la consola de Storage Gateway, active la puerta de enlace.
8. En el panel Navegación de la consola de Storage Gateway, elija Puertas de enlace y elija la puerta de enlace a la que ha agregado el adaptador. Confirme que la segunda dirección IP aparece en la pestaña Details.

Para obtener información sobre las tareas de la consola local comunes a los VMware hosts de Hyper-V y KVM, consulte Realización de tareas en la consola local de la MV de

Configuración de varios adaptadores de red en el host Microsoft Hyper-V

En el siguiente procedimiento se supone que la MV de la gateway ya tiene un adaptador de red definido y que está agregando un segundo adaptador. Este procedimiento muestra cómo añadir un adaptador para el host Microsoft Hyper-V.

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

1. En la consola de Storage Gateway, desactive la puerta de enlace.
2. En Microsoft Hyper-V Manager, seleccione la máquina virtual de la puerta de enlace del panel Máquinas virtuales.

3. Si la máquina virtual de la puerta de enlace no está ya desactivada, haga clic con el botón derecho en el nombre de la máquina virtual para abrir el menú contextual y, a continuación, elija Desactivar.
4. Haga clic con el botón derecho en el nombre de la máquina virtual de la puerta de enlace para abrir el menú contextual y, a continuación, elija Configuración.
5. En el cuadro de diálogo Configuración, en Hardware, elija Agregar hardware.
6. En el panel Agregar hardware, en la parte derecha del cuadro de diálogo de configuración, elija Adaptador de red y, a continuación, elija Agregar para agregar un dispositivo.
7. Configure el adaptador de red y, a continuación, elija Apply para aplicar la configuración.
8. En el cuadro de diálogo Configuración, en Hardware, confirme que se ha agregado el nuevo adaptador de red a la lista de hardware y, a continuación, elija Aceptar.
9. Active la puerta de enlace mediante la consola de Storage Gateway.
10. En el panel de Navegación de la consola de Storage Gateway, elija Puertas de enlace y elija la puerta de enlace a la que ha agregado el adaptador. Confirme que una segunda dirección IP aparece en la pestaña Detalles.

Para obtener información sobre las tareas de la consola local comunes a los VMware hosts de Hyper-V y KVM, consulte Realización de tareas en la consola local de la MV de

Uso de VMware vSphere High Availability con Storage Gateway

Storage Gateway proporciona alta disponibilidad VMware mediante un conjunto de comprobaciones de estado a nivel de aplicación integradas con VMware vSphere High Availability (HA). VMware Este enfoque protege las cargas de trabajo de almacenamiento de los fallos de hardware, hipervisor o red. También protege de los errores de software, como los tiempos de espera de conexión y los recursos compartidos de archivos o la falta de disponibilidad de volumen.

vSphere HA funciona agrupando las máquinas virtuales y los hosts en los que residen en un clúster para lograr redundancia. Los hosts del clúster se supervisan y, en caso de que se produzca un 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 sobre vSphere HA, consulte Cómo funciona vSphere HA en la documentación. VMware

Note

El tiempo necesario para reiniciar una máquina virtual que ha producido un error y restablecer la conexión iSCSI 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 SAN/almacenamiento. Para minimizar el tiempo de inactividad de la conmutación por error, implemente las recomendaciones descritas en Optimización del rendimiento de la puerta de enlace.

Para usar Storage Gateway con VMware HA, se recomienda hacer lo siguiente:

- Implemente el paquete `.ova` descargable de VMware ESX 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 los ajustes de iSCSI recomendados para el 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 espera de iSCSI recomendados para clientes Windows y Linux son mayores que el tiempo necesario habitualmente para una conmutación por error. Para obtener más información sobre la personalización de ajustes de tiempo de espera de clientes Windows, consulte Personalización de la configuración iSCSI de Windows. Para obtener más información sobre la personalización de ajustes de tiempo de espera de clientes Linux, consulte Personalización de la configuración de iSCSI de Linux.
- Con clústeres, si implementa el paquete `.ova` en el clúster, seleccione un host cuando se le solicite que lo haga. Además, puede implementar directamente en un host de un clúster.

En los siguientes temas se describe cómo implementar Storage Gateway en un clúster VMware de alta disponibilidad:

Temas

- Configure su clúster de vSphere HA VMware
- Descarga de la imagen .ova de la consola de Storage Gateway
- Implementar la gateway
- (Opcional) Agregue opciones de anulación para otras del clúster VMs
- Activar la gateway
- Pruebe su configuración VMware de alta disponibilidad

Configure su clúster de vSphere HA VMware

En primer lugar, si aún no ha creado un VMware clúster, cree uno. Para obtener información sobre cómo crear un VMware clúster, consulte Crear un clúster de vSphere HA en la VMware documentación.

A continuación, configure el VMware clúster para que funcione con Storage Gateway.

Para configurar el VMware clúster

1. En la página Editar la configuración del clúster de VMware vSphere, asegúrese de que la supervisión de máquinas virtuales esté configurada para la supervisión de máquinas virtuales y aplicaciones. Para ello, defina los valores siguientes de cada opción:
   - Respuesta a un error del host: reinicie VMs
   - Respuesta al aislamiento del host: apague y reinicie VMs
   - Datastore with PDL (Almacén de datos con PDL): Disabled (Deshabilitado)
   - Datastore with APD (Almacén de datos con APD): Disabled (Deshabilitado)
   - VM Monitoring (Monitorización de MV): VM and Application Monitoring (Monitorización de aplicaciones y MV)
2. Ajuste la sensibilidad del clúster mediante la configuración de los siguientes valores:
   - Failure interval: después de este intervalo, la máquina virtual se reinicia si no se recibe un latido de la máquina virtual.
   - Minimum uptime: el clúster espera este tiempo después de que una máquina virtual comience a supervisar los latidos de las herramientas de la máquina virtual.
   - Maximum per-VM resets: el clúster reinicia la máquina virtual un máximo de estas veces dentro del intervalo de tiempo máximo de reinicios.

- Maximum resets time window: el intervalo de tiempo en el que se cuentan los reinicios máximos por máquina virtual.

Si no está seguro de los valores que tiene que establecer, utilice esta configuración de ejemplo:

- Failure interval (Intervalo de error): **30** segundos
- Minimum uptime (Tiempo de actividad mínimo): **120** segundos
- Maximum per-VM resets (Reinicios máximos por MV): **3**
- Maximum resets time window (Periodo de tiempo de reinicio máximo): **1** hora

Si tiene otros en VMs ejecución en el clúster, es posible que desee establecer estos valores específicamente para su máquina virtual. No puede hacerlo hasta que implemente la MV desde la imagen .ova. Para obtener más información acerca de la configuración de estos valores, consulte (Opcional) Agregue opciones de anulación para otras del clúster VMs .

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 volumen.

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 SCSI paravirtualizados. 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 cliente VMware vSphere, 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 Virtual Machine Properties (Propiedades de la máquina virtual), elija la pestaña Hardware, seleccione SCSI controller 0 (Controladora SCSI 0) y, a continuación, elija Change Type (Cambiar tipo).
3. En el cuadro de diálogo Cambiar el tipo de controlador SCSI, seleccione el tipo de controlador SCSI VMware paravirtual y, a continuación, elija Aceptar.

(Opcional) Agregue opciones de anulación para otras del clúster VMs

Si tiene otros en VMs ejecución en su clúster, es posible que desee establecer los valores del clúster específicamente para cada máquina virtual. Para obtener instrucciones, consulte Personalización de una máquina virtual individual en la documentación en línea de VMware vSphere.

Para añadir opciones de anulación para otras de VMs su clúster

1. En la página Resumen de VMware vSphere, elija el clúster para abrir la página del clúster y, a continuación, elija Configurar.
2. Seleccione la pestaña Configuration (Configuración) y, a continuación, seleccione VM Overrides (Anulaciones de MV).
3. Adición de una nueva opción de anulación de VM para cambiar cada valor.

   Establezca los siguientes valores para cada opción en vSphere HA: supervisión de máquina virtual:

   - Supervisión de máquina virtual: invalidación habilitada - supervisión de máquina virtual y aplicaciones
   - Confidencialidad de supervisión de máquina virtual: invalidación habilitada - supervisión de máquina virtual y aplicaciones
   - Supervisión de máquina virtual: personalizar
   - Intervalo de error: **30** segundos
   - Tiempo de actividad mínimo: **120** segundos
   - Maximum per-VM resets (Reinicios máximos por MV): **5**

- Periodo máximo de reinicios: en **1** horas

Activar la gateway

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 Volume Gateway a AWS
  b. Revisión de la configuración y activación de la puerta de enlace de volumen
  c. Configuración de la puerta de enlace de volumen

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 disponibilidad VMware .
3. En Acciones, elija Verificar alta disponibilidad VMware.
4. En el cuadro Verificar la configuración de VMware alta disponibilidad que aparece, selecciona Aceptar.

> **Note**
>
> Al probar la configuración de VMware alta disponibilidad, se reinicia la máquina virtual de la puerta de enlace e interrumpe la conectividad con la puerta de enlace. La prueba puede tardar unos minutos en completarse.

Si la prueba se realiza correctamente, el estado de Verified (Verificado) aparece en la pestaña de detalles de la gateway en la consola.

5. Seleccione 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 registros de estado de Volume Gateway con CloudWatch grupos de registros.

Uso de los recursos de almacenamiento de puerta de enlace de volumen

En los temas de esta sección se describe cómo puede administrar los recursos de almacenamiento asociados al dispositivo de puerta de enlace de volumen y a su plataforma de host virtual. Esto incluye recursos como los discos físicos conectados a la plataforma de host de hipervisor de una puerta de enlace, con procedimientos específicos para eliminar discos de los hosts de virtualización de máquinas virtuales basadas en el núcleo (KVM) de VMware ESXi vSphere, Microsoft Hyper-V o Linux. Esto también incluye la administración de los volúmenes de Amazon EBS adjuntos a la EC2 instancia de Amazon de una puerta de enlace para las puertas de enlace alojadas EC2 en Amazon en la AWS nube.

Temas

- Retirada de discos de la gateway- Obtenga información sobre qué hacer si necesita extraer un disco de la plataforma de host de virtualización de máquinas virtuales (KVM) basadas en el núcleo (KVM) VMware vSphere, ESXi Microsoft Hyper-V o Linux de su puerta de enlace, por ejemplo, si se produce un fallo en el disco físico.
- Administración de volúmenes de Amazon EBS en Amazon Gateways EC2- Obtenga información sobre cómo puede aumentar o reducir la cantidad de volúmenes de Amazon EBS que se asignan para su uso como búfer de carga o almacenamiento en caché para una puerta de enlace alojada en una EC2 instancia de Amazon, por ejemplo, si las necesidades de almacenamiento de su aplicación aumentan o disminuyen con el tiempo.

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 cliente de vSphere, abra el menú contextual (haga clic con el botón derecho), elija el nombre de la máquina virtual de la gateway y, a continuación, elija Edit Settings (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 se agregan a una gateway aparecen en la entrada Controladora SCSI en la lista 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.

   La primera controladora SCSI que se muestra en Microsoft Hyper-V Manager es la controladora 0.

3. Elija Aceptar para aplicar el cambio.

Retirada de un disco de una gateway alojada en Linux KVM

Para desasociar un disco de la gateway alojada en el hipervisor de la máquina virtual de Linux basada en kernel (KVM), puede utilizar un comando `virsh` similar al siguiente.

```
$ virsh detach-disk domain_name /device/path
```

Para obtener más detalles sobre la administración de discos de KVM, consulte la documentación de su distribución Linux.

Administración de volúmenes de Amazon EBS en Amazon Gateways EC2

Cuando configuró inicialmente su puerta de enlace para que se ejecutara como una EC2 instancia de Amazon, asignó volúmenes de Amazon EBS para usarlos como búfer de carga y almacenamiento en caché. Con el paso del tiempo, a medida que cambian las necesidades de las aplicaciones, puede asignar volúmenes de Amazon EBS adicionales para este uso. También puede reducir el almacenamiento asignado mediante la eliminación de volúmenes de Amazon EBS asignados previamente. Para obtener más información sobre Amazon EBS, consulte Amazon Elastic Block Store (Amazon EBS) en la Guía del usuario de Amazon. EC2

Antes de agregar más almacenamiento a la gateway, debe revisar cuáles son las necesidades de tamaño del búfer de carga y el almacenamiento de 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. Puede asociar tantos volúmenes de Amazon EBS a la instancia como desee, pero solo puede configurar estos volúmenes como búfer de carga y almacenamiento de caché hasta estas cuotas de almacenamiento. Para obtener más información, consulte AWS Storage Gateway cuotas.

Para agregar un volumen de Amazon EBS y configurarlo para la puerta de enlace

1. Creación de un volumen de Amazon EBS. Para obtener instrucciones, consulte Creación o restauración de un volumen de Amazon EBS en la Guía del EC2 usuario de Amazon.

2. Adjunta el volumen de Amazon EBS a tu EC2 instancia de Amazon. Para obtener instrucciones, consulte Adjuntar un volumen de Amazon EBS a una instancia en la Guía EC2 del usuario de Amazon.
3. Configure el volumen de Amazon EBS que agregó 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 volumen de Amazon EBS

> **Warning**
>
> Estos pasos se aplican únicamente a los volúmenes de Amazon EBS asignados como espacio de búfer de carga, no a los volúmenes asignados como almacenamiento en caché.

1. Para cerrar la gateway, siga el enfoque que se describe en la sección Como apagar la MV de la gateway.
2. Separe el volumen de Amazon EBS de su instancia de Amazon EC2 . Para obtener instrucciones, consulte Separar un volumen de Amazon EBS de una instancia en la Guía del EC2 usuario de Amazon.
3. Eliminación del volumen de Amazon EBS. Para obtener instrucciones, consulte Eliminar un volumen de Amazon EBS 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.

Obtención de una clave de activación para la puerta de enlace

Para recibir una clave de activación para la puerta de enlace, realice una solicitud web a la máquina virtual (VM) de la puerta de enlace. La máquina virtual devuelve un redireccionamiento que contiene la clave de activación, la cual se transfiere como uno de los parámetros de la acción de la API de `ActivateGateway` para especificar la configuración de la puerta de enlace. Para obtener más información, consulte la referencia ActivateGatewayde la API de Storage Gateway.

> **Note**
>
> Las claves de activación de la puerta de enlace caducan en 30 minutos si no se utilizan.

La solicitud que realiza a la máquina virtual de puerta de enlace incluye la AWS región en la que se produce la activación. La URL que devuelve el redireccionamiento en la respuesta contiene un parámetro de cadena de consulta llamado `activationkey`. Este parámetro de cadena de consulta es su clave de activación. El formato de la cadena de consulta tiene el aspecto siguiente: `http://`*`gateway_ip_address`*`/?activationRegion=`*`activation_region`*. El resultado de esta consulta devuelve la región y la clave de activación.

La URL también incluye `vpcEndpoint`, el ID del punto de conexión de VPC para las puertas de enlace que se conectan mediante el tipo de punto de conexión de VPC.

> **Note**
>
> El Storage Gateway Hardware Appliance, las plantillas de imágenes de máquinas virtuales y EC2 Amazon Machine Images (AMI) vienen preconfigurados con los servicios HTTP necesarios para recibir y responder a las solicitudes web que se describen en esta página. No es obligatorio ni recomendable instalar ningún servicio adicional en la puerta de enlace.

Temas

Linux (curl)

En los siguientes ejemplos se muestra cómo obtener una clave de activación con Linux (curl).

> **Note**
>
> Sustituya las variables resaltadas por valores reales de la puerta de enlace. Los valores aceptables son los siguientes:

- *gateway_ip_address*- La IPv4 dirección de su puerta de enlace, por ejemplo `172.31.29.201`
- *gateway_type*- El tipo de puerta de enlace que desea activar`STORED`, como`CACHED`,`VTL`,`FILE_S3`, o`FILE_FSX_SMB`.
- *region_code*- La región en la que quieres activar tu puerta de enlace. Consulte Puntos de conexión regionales en la Guía de referencia general de AWS . Si no se especifica este parámetro o si el valor proporcionado está mal escrito o no coincide con una región válida, el comando utilizará la región `us-east-1` de forma predeterminada.
- *vpc_endpoint*- El nombre del punto de conexión de VPC de su puerta de enlace, por ejemplo. `vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com`

Para obtener la clave de activación de un punto de conexión público:

```
curl "http://gateway_ip_address/?activationRegion=region_code&no_redirect"
```

Para obtener la clave de activación de un punto de conexión de VPC:

```
curl "http://gateway_ip_address/?
activationRegion=region_code&vpcEndpoint=vpc_endpoint&no_redirect"
```

Linux (bash/zsh)

En el siguiente ejemplo se muestra cómo utilizar Linux (bash/zsh) para recuperar la respuesta HTTP, analizar los encabezados HTTP y obtener la clave de activación.

```
function get-activation-key() {
  local ip_address=$1
  local activation_region=$2
  if [[ -z "$ip_address" || -z "$activation_region" || -z "$gateway_type" ]]; then
    echo "Usage: get-activation-key ip_address activation_region gateway_type"
    return 1
  fi
```

```
  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region&gatewayType=$gateway_type"); then
    activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
    echo "$activation_key_param" | cut -f2 -d=
  else
    return 1
  fi
}
```

Microsoft Windows PowerShell

El siguiente ejemplo muestra cómo utilizar Microsoft Windows PowerShell para obtener la respuesta HTTP, analizar los encabezados HTTP y obtener la clave de activación.

```
function Get-ActivationKey {
  [CmdletBinding()]
  Param(
    [parameter(Mandatory=$true)][string]$IpAddress,
    [parameter(Mandatory=$true)][string]$ActivationRegion,
    [parameter(Mandatory=$true)][string]$GatewayType
  )
  PROCESS {
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion&gatewayType=$GatewayType" -MaximumRedirection 0 -
ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

Mediante la consola local

En el siguiente ejemplo se muestra cómo utilizar la consola local para generar y mostrar una clave de activación.

Para obtener una clave de activación para la puerta de enlace desde la consola local

1. Inicie sesión en la consola local. Si te conectas a tu EC2 instancia de Amazon desde un ordenador Windows, inicia sesión como administrador.

2. Tras iniciar sesión y ver el menú principal Activación del dispositivo de AWS - Configuración, seleccione `0` para elegir Obtener clave de activación.
3. Seleccione Storage Gateway como opción de familia de puertas de enlace.
4. Cuando se le solicite, introduzca la AWS región en la que desea activar la puerta de enlace.
5. Introduzca 1 para punto de conexión público o 2 para punto de conexión de VPC como tipo de red.
6. Introduzca 1 para estándar o 2 estándar federal de procesamiento de información (FIPS) como tipo de punto de conexión.

Conexión de iniciadores iSCSI

Al administrar la gateway, se utilizan volúmenes o dispositivos de biblioteca de cintas virtuales (VTL) que se exponen como destinos iSCSI (Internet Small Computer System Interface). Para las puertas de enlace de volumen, los destinos iSCSI son volúmenes. Para las puertas de enlace de cinta, los destinos son dispositivos VTL. El trabajo de administración incluye tareas como conectarse a estos destinos, personalizar la configuración iSCSI, conectarse desde un cliente de Red Hat Linux o configurar el Protocolo de autenticación por desafío mutuo (CHAP, Challenge-Handshake Authentication Protocol).

Temas

El estándar iSCSI es un estándar de red de almacenamiento basado en el Protocolo de Internet (IP, Internet Protocol) para iniciar y administrar las conexiones entre los dispositivos de almacenamiento basados en IP y los clientes. En la siguiente lista se definen algunos de los términos que se utilizan para describir la conexión iSCSI y los componentes que intervienen en ella.

Iniciador iSCSI

> Componente cliente de una red iSCSI. El iniciador envía las solicitudes al destino iSCSI. Los iniciadores pueden implementarse en software o hardware. Storage Gateway solo admite los iniciadores de software.

Destino iSCSI

Componente de servidor de la red iSCSI que recibe las solicitudes de los iniciadores y responde a ellas. Cada uno de los volúmenes se expone como un destino iSCSI. Debe conectarse un solo iniciador iSCSI a cada destino iSCSI.

Iniciador iSCSI de Microsoft

Programa de software de los equipos Microsoft Windows que permite conectar un equipo cliente (es decir, el equipo en el que se ejecuta la aplicación cuyos datos desea grabar en la puerta de enlace) a una matriz externa basada en iSCSI (es decir, la puerta de enlace). La conexión se efectúa a través de la tarjeta adaptadora de red Ethernet del equipo. El iniciador iSCSI de Microsoft se validó con Storage Gateway en Windows Server 2022. El iniciador está integrado en el sistema operativo.

Iniciador iSCSI de Red Hat

El paquete `iscsi-initiator-utils` de Resource Package Manager (RPM) proporciona un iniciador iSCSI implementado en el software para Red Hat Linux. El paquete incluye un demonio de servidor para el protocolo iSCSI.

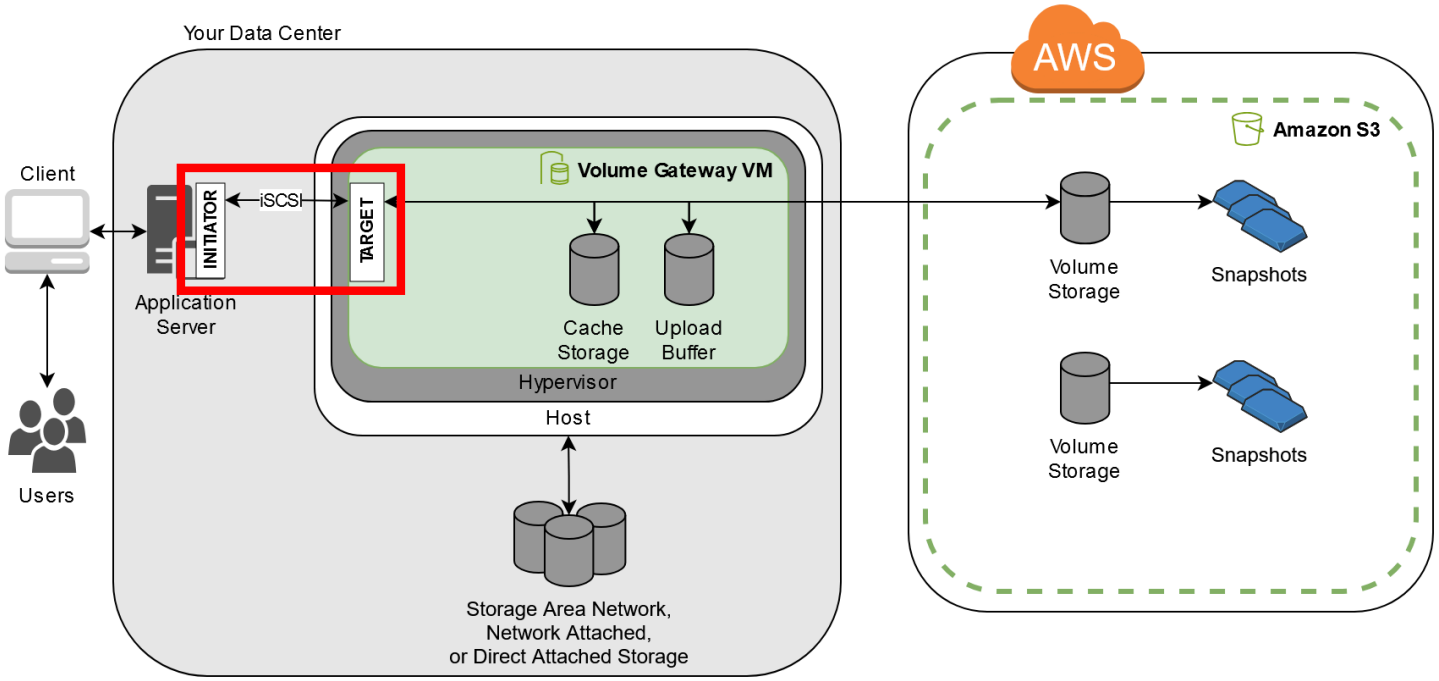
Cada tipo de gateway puede conectarse a dispositivos iSCSI y puede personalizar las conexiones, tal y como se describe a continuación.

Conexión a los volúmenes de un cliente de Windows

Una puerta de enlace de volumen expone los volúmenes que ha creado para la puerta de enlace como destinos iSCSI. Para obtener más información, consulte Conexión de los volúmenes al cliente.

> **Note**
>
> Para conectarse al destino del volumen, la gateway debe tener configurado un búfer de carga. Si no hay un búfer de carga configurado para la gateway, entonces el estado de los volúmenes será UPLOAD BUFFER NOT CONFIGURED. Para configurar un búfer de carga para una gateway en una configuración de volúmenes almacenados, consulte Para configurar búfer de carga o el almacenamiento en caché adicional a la puerta de enlace. Para configurar un búfer de carga para una puerta de enlace en una configuración de volúmenes en caché, consulte Para configurar búfer de carga o el almacenamiento en caché adicional a la puerta de enlace.

En el diagrama siguiente está resaltado el destino iSCSI dentro del conjunto de la arquitectura de Storage Gateway. Para obtener más información, consulte Funcionamiento de puerta de enlace de volumen.



Puede conectarse al volumen desde un cliente de Windows o de Red Hat Linux. Si lo prefiere, puede configurar CHAP para cualquiera de estos tipos de clientes.

La gateway expone el volumen como un destino iSCSI, con el nombre que haya especificado precedido de `iqn.1997-05.com.amazon:`. Por ejemplo, si especifica el nombre de destino `myvolume`, el destino iSCSI que se usará para conectarse al volumen será `iqn.1997-05.com.amazon:myvolume`. Para obtener más información sobre cómo configurar las aplicaciones para montar volúmenes a través de iSCSI, consulte Conexión a los volúmenes de un cliente de Windows.

Para	Consulte
Conéctese al volumen desde Windows.	Conexión a un cliente Microsoft Windows
Conéctese al volumen desde Red Hat Linux.	Conexión a un cliente Red Hat Enterprise Linux
Configure la autenticación CHAP para Windows y Red Hat Linux.	Configuración de la autenticación CHAP para los destinos iSCSI

Para conectar el cliente de Windows a un volumen de almacenamiento

1. En el menú Inicio del equipo cliente Windows, introduzca **`iscsicpl.exe`** en el cuadro Buscar programas y archivos, localice el programa del iniciador iSCSI y ejecútelo.

   > **Note**
   >
   > Debe disponer de derechos de administrador en el equipo cliente para ejecutar el iniciador iSCSI.

2. Si se le pregunta, elija Sí para iniciar el servicio del iniciador iSCSI de Microsoft.
3. En el cuadro de diálogo Propiedades: Iniciador iSCSI, elija la pestaña Detección y, a continuación, elija Detectar portal.
4. En el cuadro de diálogo Detectar portal de destino, introduzca la dirección IP del destino iSCSI en Dirección IP o nombre DNS y, a continuación, elija 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 dirección IP o DNS pública en la pestaña Descripción de la EC2 consola de Amazon.

   La dirección IP aparecerá ahora en la lista Portales de destino de la pestaña Detección.

   > **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. Conecte el nuevo portal de destino al destino del volumen de almacenamiento en la gateway:

   a. Elija la pestaña Destinos.

      Se mostrará el nuevo portal de destino con el estado inactivo. El nombre de destino mostrado debe ser el mismo que el nombre que especificó para el volumen de almacenamiento en el paso 1.

   b. Seleccione el destino y, a continuación, elija Conectar.

Si el nombre del destino aún no está rellenado, introdúzcalo como se muestra en el paso 1. En el cuadro de diálogo Conectar a destino, seleccione Agregar esta conexión a la lista de destinos favoritos y, a continuación, pulse Aceptar.

c. En la pestaña Destinos, asegúrese de que el valor del campo Estado del destino sea Conectado, que indica que el destino se encuentra conectado, y elija Aceptar.

Ahora ya puede inicializar y formatear este volumen de almacenamiento para Windows, con el fin de comenzar a guardar datos en él. Para ello, utilice la herramienta Windows Disk Management.

> **Note**
>
> Aunque no es necesario para este ejercicio, se recomienda encarecidamente personalizar la configuración iSCSI para una aplicación real, tal y como se explica en Personalización de la configuración iSCSI de Windows.

Conexión de los volúmenes a un cliente de Linux

Cuando se utiliza Red Hat Enterprise Linux (RHEL), se utiliza el paquete `iscsi-initiator-utils` de RPM para conectarse a los dispositivos iSCSI de la puerta de enlace (volúmenes o dispositivos VTL).

Para conectar un cliente Linux a los destinos iSCSI

1. Instale el paquete `iscsi-initiator-utils` de RPM si aún no está instalado en el cliente.

   Puede utilizar el comando siguiente para instalar el paquete.

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

2. Asegúrese de que el daemon iSCSI se encuentre en ejecución.

   a. Utilice uno de los comandos siguientes para comprobar que el demonio iSCSI se encuentra en ejecución.

      Para RHEL 8 o 9, 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 8 o 9, utilice el siguiente comando. Por lo general, no es necesario iniciar el `iscsid` servicio de forma explícita.

   ```
   sudo service iscsid start
   ```

3. Para detectar los destinos del volumen o del dispositivo VTL definidos para una gateway, utilice el siguiente comando de detección.

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

   Sustituya la *[GATEWAY_IP]* variable del comando anterior por la dirección IP de la puerta de enlace. Encontrará la dirección IP de la puerta de enlace en las propiedades Información de destino iSCSI de un volumen en la consola de 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`

   El nombre iSCSI completo (IQN) es distinto del que se muestra anteriormente, porque los valores de los IQN son exclusivos de cada organización. El nombre del destino es el especificado al crear el volumen. También encontrará este nombre de destino en el panel de propiedades Información de destino iSCSI al seleccionar un volumen en la consola de Storage Gateway.

4. Para conectarse a un destino, utilice el siguiente comando.

   Tenga en cuenta que debe especificar el IQN correcto *[GATEWAY_IP]* 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
```

Tras configurar el iniciador, es muy recomendable que personalice la configuración de iSCSI como se explica en Personalización de la configuración de iSCSI de Linux.

Personalización de la configuración de iSCSI

Después de configurar el iniciador, es muy recomendable que personalice la configuración de iSCSI para evitar que el iniciador se desconecte de los objetivos.

Al aumentar los valores de tiempo de espera de iSCSI como se muestra en los pasos siguientes, la aplicación podrá afrontar mejor las operaciones de escritura que duren mucho tiempo y otros problemas transitorios como las interrupciones de 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 iSCSI de Windows
- Personalización de la configuración de iSCSI de Linux
- Personalización de la configuración del tiempo de espera del disco de Linux para las puertas de enlace de volumen

Personalización de la configuración iSCSI de Windows

Cuando utilice un cliente Windows, utilice el iniciador iSCSI de Microsoft para conectarse al volumen de gateway. Para obtener instrucciones sobre cómo conectarse a los volúmenes, consulte Conexión de los volúmenes al cliente.

Para personalizar la configuración iSCSI de Windows

1. Aumente el tiempo máximo para las solicitudes en la cola.

   a. Inicie el Editor del Registro (`Regedit.exe`).

   b. Vaya hasta la clave del identificador único global (GUID) para la clase de dispositivos que contiene la configuración del controlador iSCSI, que se muestra a continuación.

   > **Warning**
   >
   > Asegúrese de que está trabajando en la CurrentControlSetsubclave y no en otro conjunto de controles, como ControlSet001 o ControlSet 002.

   ```
   HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}
   ```

   c. Busque la subclave del iniciador iSCSI de Microsoft, que se muestra a continuación como. *[<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 haya instalado en el equipo, es posible que el iniciador iSCSI de Microsoft no sea la subclave `0000`. Puede asegurarse de haber seleccionado la subclave correcta al verificar que la cadena `DriverDesc` tiene el valor `Microsoft iSCSI Initiator`.

d. Para mostrar la configuración de iSCSI, elija la subclave Parameters.

e. Abra el menú contextual (haga clic con el botón derecho) del valor MaxRequestHoldTimeDWORD (32 bits), seleccione Modificar y, a continuación, cambie el valor a. **`600`**

MaxRequestHoldTimeespecifica cuántos segundos debe mantener el iniciador iSCSI de Microsoft y reintentar los comandos pendientes antes de notificar un evento a la capa superior. `Device Removal` Este valor representa un tiempo de retención de 600 segundos.

2. Puede aumentar la cantidad máxima de datos que se pueden enviar en paquetes iSCSI modificando los parámetros siguientes:

- 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.
- MaxRecvDataSegmentLengthcontrola 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 puede optimizar el software de copia de seguridad para que funcione mejor con distintas configuraciones iSCSI. 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 Disco en la subclave Servicios de la 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 de TimeOutValueDWORD (32 bits), seleccione Modificar y, a continuación, cambie el valor a. **`600`**

TimeOutValueespecifica cuántos segundos esperará el iniciador iSCSI a recibir una respuesta del destino antes de intentar recuperar la sesión interrumpiendo y restableciendo la conexión. Este valor representa un periodo de tiempo de espera de 600 segundos.

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 iSCSI de Linux

Tras configurar el iniciador para la puerta de enlace, es muy recomendable que personalice la configuración de iSCSI para evitar que el iniciador se desconecte de los objetivos. Al aumentar los valores de tiempo de espera de iSCSI como se muestra a continuación, la aplicación podrá afrontar mejor las operaciones de escritura que duren mucho tiempo y otros problemas transitorios como las interrupciones de 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 iSCSI de Linux

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. Establezca el valor en*[replacement_timeout_value]*. **600**

Establezca el *[noop_out_interval_value]* valor en**60**.

Establezca el *[noop_out_timeout_value]* valor en**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.

Establezca el *[replacement_first_burst_length_value]* valor en **262144** o en el valor predeterminado del sistema operativo Linux, el que sea superior.

Establezca el *[replacement_max_burst_length_value]* valor en **1048576** o el valor predeterminado del sistema operativo Linux, el que sea superior.

Establezca el *[replacement_segment_length_value]* valor en **262144** o el valor predeterminado del sistema operativo Linux, el que sea superior.

> **Note**
>
> Se puede optimizar el software de copia de seguridad para que funcione mejor con distintas configuraciones iSCSI. 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 una puerta de enlace de volumen, puede personalizar la siguiente configuración del tiempo de espera del disco de Linux, además de la configuración iSCSI descrita 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 utiliza el iniciador RHEL 5, abra el archivo `/etc/udev/rules.d/50-udev.rules` 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 los iniciadores RHEL 6 o 7, así que debe crearlo usando la regla siguiente.

   ```
   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 comando siguiente y, a continuación, agregue las líneas de código mostradas previamente.

```
sudo vim /etc/udev/rules.d/50-udev.rules
```

Para modificar el valor de tiempo de espera en RHEL 7, utilice el comando siguiente y, a continuación, agregue las líneas de código mostradas previamente.

```
sudo su -c "echo 600 > /sys/block/[device name]/device/timeout"
```

b. Establezca el *[timeout]* valor en**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 dispositivo iSCSI.

Configuración de la autenticación CHAP para los destinos iSCSI

Storage Gateway admite la autenticación entre la puerta de enlace y los iniciadores iSCSI mediante el protocolo de autenticación por desafío mutuo (CHAP, Challenge-Handshake Authentication Protocol). CHAP ofrece protección contra los ataques de reproducción al verificar periódicamente la identidad de un iniciador iSCSI autenticado para acceder a un volumen y un destino de dispositivo VTL.

> **Note**
>
> La configuración de CHAP es opcional, pero se recomienda encarecidamente.

CHAP debe configurarse tanto en la consola de Storage Gateway como en el software del iniciador iSCSI que se usa para conectarse al destino. Storage Gateway utiliza el protocolo CHAP mutuo, es decir, aquel en que el iniciador autentica el destino y este autentica el iniciador.

Para configurar el protocolo CHAP mutuo en los destinos

1. Configure CHAP en la consola de Storage Gateway como se explica en Para configurar CHAP para un destino de volumen en la consola de Storage Gateway.
2. En el software del iniciador del cliente, complete la configuración de CHAP:
   - Para configurar el protocolo CHAP mutuo en un cliente de Windows, consulte Para configurar el protocolo CHAP mutuo en un cliente de Windows.
   - Para configurar el protocolo CHAP mutuo en un cliente de Red Hat Linux, consulte Para configurar el protocolo CHAP mutuo en un cliente de Red Hat Linux.

Para configurar CHAP para un destino de volumen en la consola de Storage Gateway

En este procedimiento, debe especificar dos claves secretas que se utilizan para leer y escribir en un volumen. Estas mismas claves se utilizan en el procedimiento para configurar el iniciador del cliente.

1. Elija Volúmenes en el panel de navegación de la consola de Storage Gateway.
2. En Actions (Acciones), elija Configure CHAP authentication (Configurar autenticación CHAP).
3. Proporcione la información solicitada en el cuadro de diálogo Configurar la autenticación de CHAP.
   a. En Nombre del iniciador, introduzca el nombre del iniciador iSCSI. Este nombre es un nombre cualificado (IQN) iSCSI de Amazon que va precedido de `iqn.1997-05.com.amazon:` y seguido del nombre de destino. A continuación se muestra un ejemplo.

      `iqn.1997-05.com.amazon:`*`your-volume-name`*

      Encontrará el nombre del iniciador mediante el software del iniciador iSCSI. Por ejemplo, para los clientes de Windows, el nombre es el valor que figura en la pestaña Configuration (Configuración) del iniciador iSCSI. Para obtener más información, consulte Para configurar el protocolo CHAP mutuo en un cliente de Windows.

> **Note**
>
> Para cambiar el nombre de un iniciador, primero debe desactivar CHAP, luego cambiar el nombre del iniciador en el software del iniciador iSCSI y, por último, activar 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 protocolo CHAP con el destino.

c. En Secreto que se utiliza para autenticar el destino (CHAP mutuo), 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 destino debe conocer para poder participar en el protocolo 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.

4. Elija la pestaña Details (Detalles) y confirme que la opción iSCSI CHAP authentication (Autenticación CHAP para iSCSI) se encuentra establecida en true.

Para configurar el protocolo CHAP mutuo en un cliente de Windows

En este procedimiento, se configura CHAP en el iniciador iSCSI de Microsoft mediante las mismas claves que utilizó al configurar CHAP para el volumen en la consola.

1. Si el iniciador iSCSI no se está ejecutando, vaya al menú Inicio del equipo cliente Windows, elija Ejecutar, introduzca **`iscsicpl.exe`** y elija Aceptar para ejecutar el programa.
2. Configure el protocolo CHAP mutuo 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 anteriormente es el valor que usó en el cuadro de diálogo Configurar la autenticación de CHAP de la consola de 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 Secreto CHAP mutuo de iniciador iSCSI, introduzca el valor de la clave secreta del CHAP 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. Esta clave secreta es la misma que introdujo en el cuadro Secreto que se utiliza para autenticar el destino (CHAP mutuo) del cuadro de diálogo Configurar la autenticación de CHAP. Para obtener más información, consulte Configuración de la autenticación CHAP para los destinos iSCSI.

d. Si la clave que ha introducido tiene menos de 12 caracteres o más de 16, aparecerá el cuadro de diálogo de error Secreto CHAP del iniciador.

   Elija Aceptar y vuelva a introducir la clave.

3. Configure el destino con la clave secreta del iniciador para completar la configuración del protocolo CHAP mutuo.

   a. Elija la pestaña Destinos.

   b. Si el destino que desea configurar para CHAP se encuentra conectado, desconéctelo. Para ello, selecciónelo y elija Desconectar.

   c. Seleccione el destino que desea configurar para CHAP y, a continuación, elija Conectar.

   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 registro de CHAP.

      ii. Introduzca la clave secreta que se requiere para autenticar el iniciador. Esta clave secreta es la misma que escribió en el cuadro Secreto que se utiliza para autenticar el

iniciador del cuadro de diálogo Configurar la autenticación de CHAP. Para obtener más información, consulte Configuración de la autenticación CHAP para los destinos iSCSI.

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 el protocolo CHAP mutuo en un cliente de Red Hat Linux

En este procedimiento, se configura CHAP en el iniciador iSCSI de Linux mediante las mismas claves que utilizó al configurar CHAP para el volumen en la consola de Storage Gateway.

1. Asegúrese de que el demonio iSCSI se encuentre en ejecución y de haberse conectado ya a un destino. Si no ha completado estas dos tareas, consulte Conexión a un cliente Red Hat Enterprise Linux.
2. Desconéctese y elimine cualquier configuración existente del destino para el cual vaya 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 denominado **myvolume** que está definido en el nombre completo iSCSI (IQN, iSCSI Qualified Name) de Amazon. Cambie el nombre del destino y el IQN según sea necesario para la 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 de configuración iSCSI para activar 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*, *passwordusername_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
username	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 *username* valor válido.
password	Clave secreta que se utiliza para autenticar el iniciador (el cliente que está utilizando) cuando se comunica con el volumen.

Opción de configuración	Valor
username_in	IQN del volumen de destino. El valor comienza por iqn y termina por el nombre del destino. Por ejemplo, **iqn.1997-05.com.amazon:myvolume** es un *username_in* valor válido.
password_in	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 Red Hat Enterprise 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. Connect el dispositivo Storage Gateway local al AWS Direct Connect router.
3. Cree una interfaz virtual pública y configure su router local según sea necesario. Incluso con Direct Connect, los puntos finales de VPC 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.

Obtención de la dirección IP para el dispositivo de puerta de enlace

Después de elegir un host e implementar la MV de la gateway, conecte y active la gateway. Para ello, necesita la dirección IP de la MV de la gateway. Obtenga la dirección IP de la consola local de la gateway. Inicie sesión en la consola local y obtenga la dirección IP de la parte superior de la página de la consola.

Para las gateways implementadas en las instalaciones, obtenga también la dirección IP del hipervisor. En el caso de EC2 las pasarelas de Amazon, también puede obtener la dirección IP de su EC2 instancia de Amazon en Amazon EC2 Management Console. Para encontrar información cómo obtener la dirección IP de la gateway, consulte uno de los siguientes enlaces:

- VMware anfitrión: Acceder a la consola local de Gateway con VMware ESXi
- Host HyperV: Acceso a la consola local de la gateway con Microsoft Hyper-V
- Host de máquina virtual de Linux basada en el kernel (KVM): Acceso a la consola local de la gateway con Linux KVM
- EC2 anfitrión: Obtener una dirección IP de un EC2 host de Amazon

Cuando encuentre la dirección IP, anótela. A continuación, vuelva a la consola de Storage Gateway y escriba la dirección IP en la consola.

Obtener una dirección IP de un EC2 host de Amazon

Para obtener la dirección IP de la EC2 instancia de Amazon en la que está desplegada tu puerta de enlace, inicia sesión en la consola local de la EC2 instancia. A continuación, obtenga la dirección IP de la parte superior de la página de la consola. Para obtener instrucciones, consulte 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. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instances y, a continuación, seleccione la EC2 instancia en la que está desplegada la puerta de enlace.
3. Elija la pestaña Description en la parte inferior y, a continuación, anote la dirección IP pública. Utilice esta dirección IP para conectar con la gateway. Vuelva a la consola de Storage Gateway y escriba la dirección IP.

Si desea utilizar la dirección IP elástica para la activación, utilice el procedimiento siguiente.

Procedimiento 2: conectarse a la gateway mediante la dirección IP elástica

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Instances y, a continuación, seleccione la EC2 instancia en la que está desplegada la puerta de enlace.
3. Elija la pestaña Description en la parte inferior y, a continuación, anote el valor de Elastic IP. Utilice esta dirección IP elástica para conectar con la gateway. Vuelva a la consola de Storage Gateway y escriba la dirección IP elástica.
4. Una vez activada la gateway, elija la gateway que acaba de activar y, a continuación, elija la pestaña VTL devices en el panel inferior.
5. Obtenga los nombres de todos los dispositivos VTL.
6. Ejecute el siguiente comando para configurar cada uno de los destinos.

   ```
   iscsiadm -m node -o new -T [$TARGET_NAME] -p [$Elastic_IP]:3260
   ```
7. Ejecute el siguiente comando para iniciar sesión en cada uno de los destinos.

```
iscsiadm -m node -p [$ELASTIC_IP]:3260 --login
```

La puerta de enlace ahora está conectada mediante la dirección IP elástica de la EC2 instancia.

Descripción de los recursos y recursos de Storage Gateway IDs

En Storage Gateway, el recurso principal es una puerta de enlace, pero otros tipos de recursos son: volumen, cinta virtual, destino iSCSI y dispositivo de biblioteca de cintas virtuales (VTL). Se conocen como subrecursos y no existen a menos que estén asociados a una gateway.

Estos recursos y subrecursos tienen nombres de recursos de Amazon (ARNs) exclusivos asociados a ellos, como se muestra en la siguiente tabla.

Tipo de recurso	Formato de ARN
ARN de gateway	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`*
ARN de volumen	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`* `/volume/`*`volume-id`*
ARN de destino (destino iSCSI)	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`* `/target/`*`iSCSItarget`*

Storage Gateway también admite el uso de EC2 instancias y volúmenes e instantáneas de EBS. 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 ID de recurso forma parte del ARN de recurso. Un ID de recurso adopta la forma de un identificador de recurso, seguido de un guion y una combinación única de ocho letras y números. Por ejemplo, un ID de gateway presenta la forma `sgw-12A3456B` en la que `sgw` es el identificador de recurso para

puestas de enlace. Un ID de volumen adopta la forma `vol-3344CCDD` donde `vol` es el identificador de recurso para volúmenes.

Para cintas virtuales, puede anteponer un prefijo de hasta cuatro caracteres al ID de código de barra como ayuda para organizar las cintas.

IDs Los recursos de Storage Gateway están en mayúsculas. Sin embargo, cuando utilizas estos recursos IDs con la EC2 API de Amazon, Amazon EC2 espera que el recurso esté IDs en minúsculas. Debes cambiar tu ID de recurso a minúsculas para usarlo con la API. EC2 Por ejemplo, en Storage Gateway el ID para un volumen podría ser `vol-1122AABB`. Cuando utilices este ID con la EC2 API, debes cambiarlo a. `vol-1122aabb` De lo contrario, es posible que la EC2 API no se comporte como se esperaba.

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 números y letras UTF-8, el espacio y los caracteres especiales + - = . _ : / y @.

Trabajo con etiquetas

Puede trabajar con etiquetas a través de la consola de Storage Gateway, la API de Storage Gateway o la interfaz de la línea de comandos (CLI) de Storage Gateway. Los siguientes procedimientos muestran cómo agregar, editar y eliminar una etiqueta de la consola.

Para agregar una etiqueta

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. En el panel de navegación , elija el recurso que desea etiquetar.

   Por ejemplo, para etiquetar una gateway, elija Gateways y, a continuación, elija la gateway que desee etiquetar en la lista de gateways.
3. Elija Tags (Etiquetas) y, a continuación, elija Add/edit tags (Añadir o editar etiquetas).
4. En el cuadro de diálogo Add/edit tags (Añadir o editar etiquetas), elija Create tag (Crear etiqueta).
5. Escriba una clave para Key (Clave) y un valor para Value (Valor). Por ejemplo, puede escribir **`Department`** para la clave y **`Accounting`** para el valor.

   > **Note**
   >
   > Puede dejar en blanco el cuadro Value (Valor).

6. Elija Create Tag (Crear etiqueta) para agregar más etiquetas. Puede agregar varias etiquetas a un recurso.
7. Cuando haya acabado de agregar etiquetas, elija Save (Guardar).

Para editar una etiqueta

1. Abra la consola Storage Gateway en https://console.aws.amazon.com/storagegateway/casa.
2. Elija el recurso cuya etiqueta desea editar.

3. Elija Tags (Etiquetas) para abrir el cuadro de diálogo Add/edit tags (Añadir o editar etiquetas).
4. 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 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 VMware ESXi, descargue sources.tar
- Para gateways implementadas en Microsoft Hyper-V, descargue sources_hyperv.tar
- Para gateways implementadas en la máquina virtual basada en Linux Kernel (KVM), descargue Sources_KVM.tar

Este producto incluye software desarrollado por OpenSSL Project para su uso en OpenSSL Toolkit (http://www.openssl.org/). 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 los volúmenes

En la siguiente tabla se muestran las cuotas para los volúmenes.

Descripción	Volúmenes almacenados en caché	Volúmenes almacenados
Tamaño máximo de un volumen **Note** Si crea una instantánea de un volumen en caché que tiene más de 16 TiB, podrá restaurarlo en un volumen de Storage Gateway pero no en un volumen de Amazon Elastic Block Store (Amazon EBS).	32 TiB	16 TiB
Número máximo de volúmenes por gateway	32	32
Tamaño total de todos los volúmenes para una gateway	1,024 TiB	512 TiB

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 volumen en caché	150 GiB	64 TiB	150 GiB	2 TiB	—
Puerta de enlace de volumen almacenado	—	—	150 GiB	2 TiB	1 o más para el volumen o los volúmenes almacenados

> **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.

Referencia de la API para Storage Gateway

Además de usar la consola, puede usar la AWS Storage Gateway API para configurar y administrar sus puertas de enlace mediante programación. En esta sección se describen las AWS Storage Gateway operaciones, la firma de solicitudes para la autenticación y la gestión de errores. Para obtener información acerca de las regiones y los puntos de enlace disponibles para Storage Gateway, consulte Puntos de enlace y cuotas de AWS Storage Gateway en la Referencia general de AWS.

> **Note**
>
> También puede utilizarla AWS SDKs cuando desarrolle aplicaciones con AWS Storage Gateway. Las AWS SDKs versiones para Java, .NET y PHP incluyen la AWS Storage Gateway API subyacente, lo que simplifica las tareas de programación. Para obtener información sobre la descarga de las bibliotecas de SDK, consulte Código de muestra y bibliotecas.

Temas

Encabezados de solicitud obligatorios para Storage Gateway

En esta sección se describen los encabezados obligatorios que debe enviar con cada solicitud POST a Storage Gateway. Puede incluir encabezados HTTP para identificar información clave sobre la solicitud, incluidas la operación que desea invocar, la fecha de la solicitud y la información que indica su autorización como remitente de la solicitud. Los encabezados no distinguen entre mayúsculas y minúsculas y el orden de los encabezados no es importante.

El siguiente ejemplo muestra los encabezados que se utilizan en la ActivateGatewayoperación.

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120425/us-east-2/
storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target,
 Signature=9cd5a3584d1d67d57e61f120f35102d6b3649066abdd4bf4bbcf05bd9f2f8fe2
x-amz-date: 20120912T120000Z
x-amz-target: StorageGateway_20120630.ActivateGateway
```

Los siguientes son los encabezados que se deben incluir con las solicitudes POST a Storage Gateway. Los encabezados que se muestran a continuación y que comienzan por «x-amz» son encabezados específicos. AWS El resto de los encabezados que se muestran son encabezados comunes utilizados en transacciones HTTP.

Encabezado	Descripción
`Authorization`	El encabezado de autorización contiene varios elementos de informaci ón 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): `Authorization: AWS4-HMAC_SHA456 Credentials= YourAccessKey /yyymmdd/region/storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target, Signature= CalculatedSignature` En la sintaxis anterior, se especifican el año YourAccessKey, el mes y el día (aaaammdd), la región y el. CalculatedSignature El formato del encabezado de autorización viene determinado por los requisitos del proceso de firma de la versión 4. AWS Los detalles de la firma se tratan en el tema Firmar solicitudes.
`Content-Type`	Utilice `application/x-amz-json-1.1` como tipo de contenido para todas las solicitudes a Storage Gateway.

Encabezado	Descripción
	`Content-Type: application/x-amz-json-1.1`
`Host`	Utilice el encabezado de host para especificar el punto de conexión de Storage Gateway donde desea enviar la solicitud. Por ejemplo, `storagegateway.us-east-2.amazonaws.com` es el punto de conexión de la región Este de EE. UU. (Ohio). Para obtener más información 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. `Host: storagegateway. region.amazonaws.com`
`x-amz-date`	Debe proporcionar la marca de tiempo en el `Date` encabezado HTTP o en el AWS `x-amz-date` encabezado. (Algunas bibliotecas de cliente HTTP no permiten configurar el encabezado `Date`). 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 ISO86 01 Basic en el formato YYYYMMDD'T'HHMMSS'Z'. Si se utilizan tanto el encabezado como el encabezado, el `Date` formato `x-amz-date` del encabezado de fecha no tiene que ser 01. ISO86 `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`

Encabezado	Descripción
`x-amz-target`	Este encabezado especifica la versión de la API y la operación que se está solicitando. Los valores de encabezado de destino se forman concatenando la versión de la API con el nombre de la API y están en el siguiente formato. `x-amz-target: StorageGateway_ APIversion .operationName` El valor OperationName (por ejemplo, "ActivateGateway«) se encuentra en la lista de API,. Referencia de la API para Storage Gateway

Firmar solicitudes

Storage Gateway requiere que se firmen todas las solicitudes enviadas para autenticarlas. Para firmar una solicitud, se calcula una firma digital mediante una función hash criptográfica. Un hash criptográfico es una función que devuelve un valor hash único basado en la entrada. La entrada a la función hash incluye el texto de la solicitud y la clave de acceso secreta. La función hash devuelve un valor hash que se incluye en la solicitud como la firma. La firma forma parte del encabezado de la `Authorization` de la solicitud.

Tras recibir la solicitud, Storage Gateway recalcula la firma utilizando la misma función hash y los datos especificados para firmar la solicitud. Si la firma resultante coincide con la firma de la solicitud, Storage Gateway procesa la solicitud. De lo contrario, la solicitud se rechaza.

Storage Gateway admite la autenticación mediante AWS Signature Version 4. El proceso para calcular una firma se puede dividir en tres tareas:

- Tarea 1: Creación de una solicitud canónica

  Reorganice la solicitud HTTP en formato canónico. Es preciso utilizar un formato canónico, ya que Storage Gateway utiliza el mismo formato canónico cuando recalcula una firma para compararla con la que se ha enviado.
- Tarea 2: Creación de una cadena para firmar

Crear una cadena que se utilizará como uno de los valores de entrada de la función hash criptográfica. La cadena, denominada cadena para firmar, es una concatenación del nombre del algoritmo hash, la fecha de la solicitud, una cadena de ámbito de credenciales y la solicitud en formato canónico de la tarea anterior. La cadena del ámbito de credenciales es una concatenación de fecha, región e información del servicio.

- Tarea 3: Crear una firma

  Cree una firma para su solicitud mediante una función hash criptográfica que acepte dos cadenas de entrada: la cadena para firmar y una clave derivada. La clave derivada se calcula empezando por la clave de acceso secreta y utilizando la cadena del ámbito de las credenciales para crear una serie de códigos de autenticación de mensajes basados en Hash (). HMACs

Ejemplo de cálculo de firma

En el siguiente ejemplo se presentan los detalles de la creación de una firma para ListGateways. Puede utilizar el ejemplo como referencia para comprobar su método de cálculo de firmas. Encontrará otros cálculos de referencia en Conjunto de pruebas de Signature Version 4, en la Referencia general de Amazon Web Services.

El ejemplo supone lo siguiente:

- La marca temporal de la solicitud es "Mon, 10 Sep 2012 00:00:00" GMT.
- El punto de conexión es la región Este de EE. UU. (Ohio).

La sintaxis general de la solicitud (incluido el cuerpo JSON) es:

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
x-amz-Date: 20120910T000000Z
Authorization: SignatureToBeCalculated
Content-type: application/x-amz-json-1.1
x-amz-target: StorageGateway_20120630.ListGateways
{}
```

El formato canónico de la solicitud calculado para Tarea 1: Creación de una solicitud canónica es:

```
POST
```

```
/

content-type:application/x-amz-json-1.1
host:storagegateway.us-east-2.amazonaws.com
x-amz-date:20120910T000000Z
x-amz-target:StorageGateway_20120630.ListGateways

content-type;host;x-amz-date;x-amz-target
44136fa355b3678a1146ad16f7e8649e94fb4fc21fe77e8310c060f61caaff8a
```

La última línea de la solicitud canónica es el hash del cuerpo de la solicitud. Además, observe que la tercera línea de la solicitud canónica está vacía. Esto se debe a que no hay parámetros de consulta para esta API (ni para ningún Storage Gateway APIs).

La cadena para firmar de Tarea 2: Creación de una cadena para firmar es:

```
AWS4-HMAC-SHA256
20120910T000000Z
20120910/us-east-2/storagegateway/aws4_request
92c0effa6f9224ac752ca179a04cecbede3038b0959666a8160ab452c9e51b3e
```

La primera línea de la cadena para firmar es el algoritmo, la segunda es la marca temporal, la tercera es el ámbito de credenciales y la última es el hash de la solicitud canónica de la tarea 1.

En Tarea 3: Crear una firma, la clave derivada se pude representar como sigue:

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey,"20120910"),"us-
east-2"),"storagegateway"),"aws4_request")
```

Si es la clave de acceso secreta, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY, se utiliza, entonces la firma calculada es:

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

El último paso consiste en construir el encabezado `Authorization`. Para la clave de acceso de demostración AKIAIOSFODNN7EXAMPLE, el encabezado (con saltos de línea añadidos 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 respuesta de la API devuelve la excepción de error `InvalidSignatureException` si hay un problema con la firma de la solicitud. Sin embargo, el código de error de la operación `ActivationKeyInvalid` se devuelve solo para la ActivateGatewayAPI.

Según el tipo de error, Storage Gateway puede devolver solamente una excepción o puede devolver una excepción y un código de error de operación. Ejemplos de respuestas de error se muestran en Respuestas de error.

Excepciones

En la siguiente tabla se enumeran las excepciones AWS Storage Gateway de la API. Cuando una AWS Storage Gateway operación devuelve una respuesta de error, el cuerpo de la respuesta contiene una de estas excepciones. Las excepciones `InternalServerError` e `InvalidGatewayRequestException` devuelven uno de los códigos de mensaje Códigos de error de operación de los códigos de error de operación que proporcionan el código de error de operación específico.

Excepción	Mensaje	Código de estado HTTP
`IncompleteSignatureException`	La firma especificada está incompleta.	400: solicitud maligna
`InternalFailure`	El procesamiento de la solicitud ha fallado debido a un error o una excepción desconocidos.	500 Error de servidor interno
`InternalServerError`	Uno de los mensajes de código de error de operaciónCódigos de error de operación.	500 Error de servidor interno
`InvalidAction`	La acción u operación solicitada no es válida.	400: solicitud maligna
`InvalidClientTokenId`	El certificado X.509 o la ID de clave de AWS acceso proporcionados no existen en nuestros registros.	403: prohibido
`InvalidGatewayRequestException`	Uno de los mensajes de código de error de operación de Códigos de error de operación.	400: solicitud maligna
`InvalidSignatureException`	La firma de solicitud que calculamos no coincide con la firma que proporcionó. Compruebe su clave de AWS acceso y su método de firma.	400: solicitud maligna
`MissingAction`	Falta un parámetro de operación o acción en la solicitud.	400: solicitud maligna
`MissingAuthenticationToken`	La solicitud debe contener un identificador de clave de AWS acceso válido (registrado) o un certificado X.509.	403: prohibido
`RequestExpired`	La solicitud es posterior a la fecha de vencimiento o la fecha de la solicitud	400: solicitud maligna

Excepción	Mensaje	Código de estado HTTP
	(con un margen de 15) o la fecha de la solicitud ocurre más de 15 minutos en el futuro.	
`SerializationException`	Se ha producido un error durante la serialización. Compruebe que la carga útil de JSON esté bien formada.	400: solicitud maligna
`ServiceUnavailable`	La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.	503 Service Unavailable
`SubscriptionRequiredException`	El identificador de clave de AWS acceso necesita una suscripción al servicio.	400: solicitud maligna
`ThrottlingException`	Tasa superada.	400: solicitud maligna
`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

En la siguiente tabla se muestra el mapeo entre los códigos de error de AWS Storage Gateway operación y los códigos APIs que pueden devolverse. Todos los códigos de error de operación se devuelven con una o dos excepciones generales, `InternalServerError` e `InvalidGatewayRequestException` que se describen en Excepciones.

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
`ActivationKeyExpired`	La clave de activación especificada ha vencido.	ActivateGateway
`ActivationKeyInvalid`	La clave de activación especificada no es válida.	ActivateGateway
`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

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
		CreateStorediSCSIVolume
DiskDoesNotExist	El disco especificado no existe.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
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 especific ada 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`	El valor de LUN especificado es incorrecto.	CreateStorediSCSIVolume

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
`MaximumVolumeCountExceeded`	El número de volúmenes máximo se ha superado.	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes
`NetworkConfigurationChanged`	La configuración de red de la gateway ha cambiado.	CreateCachediSCSIVolume CreateStorediSCSIVolume

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
`NotSupported`	La operación especificada no es compatible.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
`OutdatedGateway`	La gateway especific ada está obsoleta.	ActivateGateway
`SnapshotInProgress Exception`	La snapshot especific ada está en curso.	DeleteVolume
`SnapshotIdInvalid`	La 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
`UnsupportedOperationForGatewayType`	La operación especificada no es válida para el tipo de gateway.	AddCache AddWorkingStorage CreateCachediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteSnapshotSchedule DescribeCache DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
`VolumeAlreadyExists`	El volumen especificado ya existe.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`VolumeIdInvalid`	El volumen especificado no es válido.	DeleteVolume
`VolumeInUse`	El volumen especificado ya se está usando.	DeleteVolume

Código de error de operación	Mensaje	Operaciones que devuelven este código de error
`VolumeNotFound`	El volumen especificado no se ha encontrado.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint DeleteVolume DescribeCachediSCSIVolumes DescribeSnapshotSchedule DescribeStorediSCSIVolumes UpdateSnapshotSchedule
`VolumeNotReady`	El volumen especificado no está listo.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

Respuestas de error

Cuando se produce un error, la información de encabezado de la respuesta contiene:

- Tipo de contenido: application/ -1.1 x-amz-json
- Un código de estado HTTP `4xx` o `5xx` adecuado

El cuerpo de una respuesta de error contiene información sobre el error que se ha producido. El siguiente ejemplo de respuesta de error muestra la sintaxis de salida de los elementos de respuesta comunes a todas las respuestas de error.

```
{
    "__type": "String",
    "message": "String",
    "error":
        { "errorCode": "String",
```

```
          "errorDetails": "String"
        }
}
```

En la tabla siguiente se explican los campos de respuesta de error JSON que se muestran en la sintaxis anterior.

__type

Una de las excepciones de Excepciones.

Tipo: cadena

error

Contiene detalles del error específicos de la API. En los errores generales (es decir, no específicos de ninguna API), esta información de error no se muestra.

Tipo: recopilación

errorCode

Uno de los códigos de error de operación .

Tipo: cadena

errorDetails

Este campo no se utiliza en la versión actual de la API.

Tipo: cadena

message

Uno de los mensajes de código de error de operación.

Tipo: cadena

Ejemplos de respuestas de error

Si utilizas la DescribeStoredi SCSIVolumes API y especificas una entrada de solicitud de ARN de puerta de enlace que no existe, se devuelve el siguiente cuerpo de JSON.

```
{
```

```
  "__type": "InvalidGatewayRequestException",
  "message": "The specified volume was not found.",
  "error": {
    "errorCode": "VolumeNotFound"
  }
}
```

El siguiente cuerpo JSON se devuelve si Storage Gateway calcula una firma que no coincida con la firma enviada con una solicitud.

```
{
  "__type": "InvalidSignatureException",
  "message": "The request signature we calculated does not match the signature you
 provided."
}
```

Operaciones en Storage Gateway

Para ver una lista completa de las operaciones de Storage Gateway, consulte Acciones en la Referencia de la API de AWS Storage Gateway .

Historial de documentos de la Guía del usuario de puerta de enlacePuerta de enlace de volumen

- Versión de la API: 30-06-2013
- 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 los cambios en esta documentación, puede suscribirse a una fuente RSS.

Cambio	Descripción	Fecha
Aviso de cambio de disponibilidad para FSx File Gateway	Amazon FSx File Gateway ya no está disponible para nuevos clientes. Los clientes actuales de FSx File Gateway pueden seguir utilizando el servicio con normalidad. Para obtener información sobre funciones similares a las de FSx File Gateway, visite esta entrada de blog.	28 de octubre de 2024
Aviso de cambio de disponibilidad para FSx File Gateway	AWS Storage Gateway de FSx File Gateway dejará de estar disponible para nuevos clientes a partir del 28 de octubre del 24 de octubre. Para utilizar el servicio, debe registrarse antes de esa fecha. Los clientes actuales de FSx File Gateway pueden seguir utilizando el servicio con normalidad. Para obtener información sobre funciones	26 de septiembre de 2024

	similares a las de FSx File Gateway, visite esta entrada de blog.	
Se ha agregado la opción de activar o desactivar las actualizaciones de mantenimiento	Storage Gateway recibe actualizaciones de mantenimiento periódicas que pueden incluir actualizaciones del sistema operativo y del software, correcciones para mejorar la estabilidad, el rendimiento y la seguridad, y acceso a nuevas características. Ahora puede configurar un ajuste para activar o desactivar estas actualizaciones para cada puerta de enlace individual en la implementación. Para obtener más información, consulte Administrar las actualizaciones de la puerta de enlace mediante la AWS Storage Gateway consola.	6 de junio de 2024
Compatibilidad obsoleta para puerta de enlace de cinta en Snowball Edge	Ya no es posible alojar la puerta de enlace de cinta en los dispositivos de 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 .	24 de octubre de 2023
Se actualizaron CloudWatch las alarmas recomendadas	La CloudWatch `HealthNotifications` alarma ahora se aplica a todos los tipos de puertas de enlace y plataformas host, y se recomienda su uso. Los ajustes de configuración recomendados también se han actualizado para `HealthNotifications` y `AvailabilityNotifications` . Para obtener más información, consulte Comprensión de CloudWatch las alarmas.	2 de octubre de 2023

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 actualiza do 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

Compatibilidad con IBM Spectrum Protect 8.1.10 en Windows y Linux para puerta de enlace de cinta	Las puertas de enlace de cinta ahora admiten IBM Spectrum Protect versión 8.1.10 que se ejecuta en Microsoft Windows Server y Linux. Para obtener más información, consulte Comprobación de la configuración mediante IBM Spectrum Protect.	24 de noviembre de 2020
Conformidad con FedRAMP	Storage Gateway ahora es compatible con FedRAMP. Para obtener más información, consulte Validación de conformidad para Storage Gateway.	24 de noviembre de 2020
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 cuadriplicado	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 bloqueo de retención de cinta y protección de cinta write-once-read-many (WORM)	Storage Gateway admite el bloqueo de retención de cinta en las cintas virtuales y escritura única y 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. Las cintas virtuales activadas con WORM 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, consulte Protección de cintas con escritura única y lectura múltiple (WORM).	19 de agosto de 2020

Pedir el dispositivo de hardware a través de la consola	Ahora puede solicitar el dispositivo de hardware a través de la AWS Storage Gateway consola. Para obtener más información, consulte Uso del dispositivo de hardware de Storage Gateway.	12 de agosto de 2020
Compatibilidad con los puntos de enlace del estándar federal de procesamiento de información (FIPS) en las regiones de AWS nuevas	Ahora puede activar una puerta de enlace con puntos de conexión FIPS en las regiones Este de EE. UU. (Ohio), Este de EE. UU. (Norte de Virginia), Oeste de EE. UU. (Norte de California), Oeste de EE. UU. (Oregón) y Canadá (centro). Para obtener más información, consulte Puntos de conexión y cuotas de AWS Storage Gateway en la Referencia general de AWS.	31 de julio de 2020
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
Compatibilidad con los puntos de enlace del estándar federal de procesamiento de información (FIPS)	Ahora puede activar una puerta de enlace con puntos de enlace de FIPS en las regiones AWS GovCloud (US) . Para elegir un punto de conexión de FIPS para una puerta de enlace de volumen, consulte Selección de un punto de conexión de servicio. Para elegir un punto de conexión de FIPS para una puerta de enlace de cinta, consulte Conexión de la puerta de enlace 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 puerta 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

Compatibilidad con hiperviso r de máquinas virtuales de Linux basadas en el kernel (KVM)	Storage Gateway ahora permite implementar una puerta de enlace en las instalaciones en la plataform a de virtualización Microsoft Hyper-V. Las puerta de enlaces implementadas en KVM tienen la misma funcional idad y características que las puerta de enlaces en las instalaciones existentes. Para obtener más informaci ón, consulte Hipervisores compatibles y requisitos de host en la Guía del usuario de Storage Gateway.	4 de febrero de 2020
Support para VMware vSphere High Availability	Storage Gateway ahora admite la alta disponibi lidad para ayudar VMware a proteger las cargas de trabajo de almacenamiento contra fallas de hardware, hipervisor o red. Para obtener más información, consulte Uso de VMware vSphere High Availability con Storage Gateway en la Guía del usuario de Storage Gateway. Esta versión también incluye mejoras de rendimiento. Para obtener más información, consulte Rendimiento en la Guía del usuario de Storage Gateway.	20 de noviembre de 2019

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
Compatibilidad con IBM Spectrum Protect versión 7.1.9 en Linux y con las puertas de enlace de cinta con un tamaño de cinta máximo aumentado a 5 TiB	Las puertas de enlace de cinta ahora son compatibles con IBM Spectrum Protect (Tivoli Storage Manager) versión 7.1.9 ejecutado en Linux, así como ejecutado en Microsoft Windows. Para obtener más información, consulte Pruebas de 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

Posibilidad de activar una puerta de enlace en una nube privada virtual (VPC)	Ahora puede activar una puerta de enlace en una VPC. Puede crear una conexión privada entre su dispositivo de software local y una infraestructura de almacenamiento basada en la nube. Para obtener más información, consulte Activación de una puerta de enlace en una nube virtual privada.	20 de junio de 2019
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

Soporte para compartir archivos SMB para Microsoft Windows ACLs	En el caso de las puertas de enlace de archivos, ahora puede utilizar las listas de control de acceso de Microsoft Windows (ACLs) para controlar el acceso a los recursos compartid os de archivos del bloque de mensajes del servidor (SMB). Para obtener más información, consulte Uso de Microsoft Windows ACLs para controlar el acceso a un recurso compartido de archivos SMB.	8 de mayo de 2019
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

Compatibilidad con Bacula Enterprise e IBM Spectrum Protect	Las puertas de enlace de cinta ahora admiten Bacula Enterprise e IBM Spectrum Protect. 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 puertas de enlace de cinta ahora admiten Microsoft System Center 2016 Data Protection Manager (DPM). Ahora puede utilizar Microsoft DPM 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 utilizando Microsoft System Center Data Protection Manager.	18 de julio de 2018

Compatibilidad con el protocolo Server Message Block (SMB)	Se ha añadido compatibilidad con el protocolo Server Message Block (SMB) para los recursos compartidos de archivos en las puertas de enlace de archivo. Para obtener más información, consulte Creación de un recurso compartido de archivos.	20 de junio de 2018
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 almacenado en caché o una cinta virtual. Actualmente, puede hacerlo mediante la API de AWS Storage Gateway . Para obtener más información, consulte Cifrado de datos mediante AWS KMS.	12 de junio de 2018

Support para NovaStor DataCenter /Network	Los Tape Gateways ahora admiten las NovaStor DataCenter/Network. You can now use NovaStor DataCente r/Network versiones 6.4 o 7.1 para hacer copias de seguridad de los datos en Amazon S3 y archivarl os directamente en un almacenamiento sin conexión (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). Para obtener más información, consulte Probar la configura ción 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 almacenam iento S3 One Zone-IA	En las puertas de enlace de archivo, ahora puede elegir S3 One Zone_IA como clase de almacenam iento 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	3 de abril de 2018

Cambio	Descripción	Fecha de modificación
	información detallada, consulta Regiones de AWS compatibles con Storage Gateway.	
Support para actualizar la memoria caché, pagar el solicitante y almacenar buckets ACLs de Amazon S3.	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 la referencia de la API de Storage Gateway. 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. Las puertas de enlace de archivo ahora le permiten conceder control total al propietario del bucket de S3 que se mapea al recurso compartido de archivos NFS. Para obtener más información, consulte Creación de un recurso compartido de archivos.	1 de marzo de 2018
Support para Dell EMC NetWorker V9.x	Las pasarelas de cinta ahora son compatibles con Dell EMC V9.x. NetWorker Ahora puede usar Dell EMC NetWorker V9.x para hacer copias de seguridad de sus datos en Amazon S3 y archivarlos directamente en un almacenamiento fuera de línea (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). Para obtener más información, consulte Probar la configuración con Dell EMC. NetWorker	27 de febrero de 2018
Nueva región de	Storage Gateway ya está disponible en la región Europa (París). Para obtener información detallada, consulta Regiones de AWS compatibles con Storage Gateway.	18 de diciembre de 2017

Cambio	Descripción	Fecha de modificación
Ayuda con las notificaciones de carga de archivos y la detección del tipo MIME	Las puertas de enlace de archivo ahora le permiten recibir una notificación cuando todos los archivos escritos en un recurso compartido de archivos NFS se han cargado en Amazon S3. Para obtener más información, consulte la referencia NotifyWhenUploadedde la API de Storage Gateway. Las puertas de enlace de archivo ahora permiten adivinar el tipo MIME de los objetos cargados en función de las extensiones de archivo. Para obtener más información, consulte Creación de un recurso compartido de archivos.	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
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

Cambio	Descripción	Fecha de modificación
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 grabados en la cinta desde la aplicación de backup 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, consulta Regiones de AWS compatibles con Storage Gateway.	02 de mayo de 2017
Actualizaciones en los ajustes de los recursos compartidos de archivos Compatibilidad con la actualización de la caché para recursos compartidos de archivos	Las puertas de enlace de archivo ahora incorporan opciones de montaje a la configuración de recursos compartidos de archivos. A partir de ahora, puede establecer opciones de agrupación y de solo lectura para el recurso compartido de archivos. Para obtener más información, consulte Creación de un recurso compartido de archivos. Las puertas de enlace de archivo ahora son capaces de encontrar objetos en el bucket de Amazon S3 que se han agregado o quitado después de que la puerta de enlace elaborase la última lista del contenido del bucket y almacenase en caché el resultado. Para obtener más información, consulte RefreshCachela referencia de la API.	28 de marzo de 2017
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	AWS Storage Gateway ahora ofrece la posibilidad de implementar un File Gateway en Amazon EC2. Puede lanzar una puerta de enlace de archivos en Amazon EC2 mediante la Amazon Machine Image (AMI) de Storage Gateway, que ahora está disponibl e como AMI comunitaria. 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 AMI de File Gateway, consulte Implement ación 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.	08 de febrero de 2017
Compatibilidad con Arcserve 17	Las puertas de enlace de cinta ahora son compatibl es 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 informaci ón, consulte Prueba de la configuración con Arcserve Backup r17.0.	17 de enero de 2017
Nueva región de	Storage Gateway ya está disponible en la región UE (Londres). Para obtener información detallada, consulta Regiones de AWS compatibles con Storage Gateway.	13 de diciembre de 2016
Nueva región de	Storage Gateway ya está disponible en la región Canadá (centro). Para obtener información detallada, consulta Regiones de AWS compatibles con Storage Gateway.	08 de diciembre de 2016

Cambio	Descripción	Fecha de modificación
Compatibilidad con la puerta de enlace de archivos	Además de puerta de enlace de volumen y puerta de enlace de cinta, Storage Gateway ahora ofrece puerta de enlace de archivo. La puerta de enlace de archivo combina un servicio y dispositivo de software virtual, lo que le permite almacenar y recuperar objetos en Amazon S3 a través de protocolos de archivo estándar del sector como Network File System (NFS). La puerta de enlace proporciona acceso a objetos de Amazon S3 como archivos en un punto de montaje NFS.	29 de noviembre de 2016
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	La puerta de enlace de cinta ahora es compatible con Micro Focus (HPE) Data Protector 9.x. Ahora puede utilizar HPE Data Protector 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 Comprobación de la configuración mediante 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 , consulta 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 configura r, administrar y supervisar las puertas de enlace, los volúmenes y las cintas virtuales. La interfaz de usuario ahora ofrece vistas que se pueden filtrar y proporcio na enlaces directos a AWS servicios integrados como CloudWatch Amazon EBS. Para obtener más información, consulte Inscríbase en AWS Storage Gateway.	30 de agosto de 2016
Compatibilidad con Veeam Backup & Replicati on 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 posterior es). 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
Volumen e instantáneas más largos 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
Nueva región de Compatibilidad con almacenamiento de hasta 512 TiB para volúmenes almacenados Otras actualizaciones de la puerta de enlace y mejoras de la consola local de Storage Gateway	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. 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. 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. 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.	21 de marzo de 2016
Compatibilidad con Dell EMC 8.x NetWorker	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 fuera de línea (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). Para obtener más información, consulte Probar la configuración con Dell EMC NetWorker.	29 de febrero de 2016

Cambio	Descripción	Fecha de modificación
Support para VMware ESXi Hypervisor versión 6.0 y el iniciador iSCSI Red Hat Enterprise Linux 7	AWS Storage Gateway ahora es compatible con la versión 6.0 del VMware ESXi hipervisor y el iniciador iSCSI Red Hat Enterprise Linux 7. Para obtener más información, consulte Hipervisores compatibles y requisitos de host y Iniciadores iSCSI compatibles.	20 de octubre de 2015
Reestructuración del contenido	Esta versión incluye esta mejora: la documenta ción ahora incluye una sección de administración de la gateway activada, que combina las tareas de administración que son comunes a todas las solucione s de gateway. A continuación, encontrará instrucci ones sobre cómo administrar la gateway después de haberla implementado y activado. Para obtener más información, consulte Administración de la gateway de volúmenes.	

Cambio	Descripción	Fecha de modificación
Compatibilidad con almacenamiento de hasta 1024 TiB para volúmenes en caché Support para el tipo de adaptador de red VMXNET3 (10 GbE) en el VMware ESXi hipervisor Mejoras de desempeño Diversas mejoras y actualizaciones de la consola local de Storage Gateway	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. 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 puerta de enlace. 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. 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.	16 de septiembre de 2015
Compatibilidad con el etiquetado	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.	2 de septiembre de 2015

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 directame nte en un almacenamiento sin conexión (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). Para obtener más información, consulte Probar su configura ción 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 del sistema (núcleos de CPU virtual, tamaño de volumen raíz y RAM) son suficientes para que la gateway funcione correctamente. Para obtener más información, consulte Visualización del estado de los recursos de sistema de la puerta de enlace o Visualización del estado de los recursos de sistema de la puerta de enlace.	
Compatibilidad con el iniciador iSCSI de Red Hat Enterprise Linux 6	Storage Gateway ya es compatible con el iniciador iSCSI de Red Hat Enterprise Linux 6. Para obtener más información, consulte Requisitos para configurar puerta de enlace de volumen.	
	Esta versión incluye las siguientes mejoras y actualizaciones de Storage Gateway: • 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 Administración de actualizaciones de puertas de enlace. •	

Cambio	Descripción	Fecha de modificación
	Storage Gateway ya ofrece una API que puede utilizar para enumerar los iniciadores iSCSI conectados a los volúmenes de almacenamiento. Para obtener más información, consulte ListVolumeInitiators en la referencia de la API.	
Compatibilidad con las versiones 2012 y 2012 R2 del hipervisor Microsoft Hyper-V	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.	30 de abril de 2015
Compatibilidad con Symantec Backup Exec 15	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.	6 de abril de 2015
Compatibilidad con la autenticación CHAP en los volúmenes de almacenamiento	Storage Gateway ahora admite la configuración de la autenticación CHAP en los volúmenes de almacenamiento. Para obtener más información, consulte Configuración de la autenticación CHAP para los volúmenes.	2 de abril de 2015

Cambio	Descripción	Fecha de modificación
Support para las versiones 5.1 y 5.5 de VMware ESXi Hypervisor	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.	30 de marzo de 2015
Compatibilidad con la utilidad CHKDSK de Windows	Storage Gateway ahora es compatible con la utilidad CHKDSK de Windows. Puede utilizar esta utilidad para comprobar la integridad de los volúmenes y corregir errores en ellos. Para obtener más informaci ón, consulte la Solución de problemas con volúmenes.	04 de marzo de 2015
Integración con AWS CloudTrai l para capturar llamadas a la API	Storage Gateway ahora está integrado con AWS CloudTrail. AWS CloudTrail captura las llamadas a la API 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. Esta versión incluye la siguiente mejora y actualiza ción de Storage Gateway: • Ahora, las cintas virtuales que tienen datos incorrect os 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 informaci ón, consulte Recuperar una cinta virtual de una puerta de enlace no recuperable.	16 de diciembre de 2014

Cambio	Descripción	Fecha de modificación
Compatibilidad con software de backup adicional y cambiador de medios	La puerta de enlace de cinta ahora es compatible con el software de copia de seguridad siguiente: • Symantec Backup Exec 2014 • Microsoft System Center 2012 R2 Data Protection Manager • Veeam Backup & Replication V7 • Veeam Backup & Replication V8 Ahora puede utilizar estos cuatro productos de software de copia de seguridad con la biblioteca de cintas virtuales (VTL) de Storage Gateway para hacer copias de seguridad en Amazon S3 y archivar 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. A partir de ahora, Storage Gateway ofrece un cambiador de medios adicional que funciona con el nuevo software de copia de seguridad. Esta versión incluye varias AWS Storage Gateway mejoras y actualizaciones.	3 de noviembre de 2014
Región de Europa (Fráncfort)	Ahora Storage Gateway también está disponible en la región de Europa (Fráncfort). Para obtener informaci ón detallada, consulta Regiones de AWS compatibles con Storage Gateway.	23 de octubre de 2014

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
Compatibilidad con Clústeres de conmutación por error de Windows Server Support for VMware ESX Initiator Compatibilidad con la realización de tareas de configuración en la consola local de Storage Gateway	• A partir de ahora, Storage Gateway permite conectar varios hosts al mismo volumen si los hosts coordinan el acceso mediante Clústeres de conmutación por error de Windows Server (WSFC). Sin embargo, no se pueden conectar varios hosts al mismo volumen si no se usa WSFC. • A partir de ahora, Storage Gateway permite administrar la conectividad del almacenamiento directamente a través del host de ESX. Esto proporciona una alternativa al uso de iniciadores residentes en el sistema operativo huésped de su sistema operativo. VMs • Storage Gateway ahora es compatible con la realización de tareas de configuración en la consola local de Storage Gateway. Para obtener informaci ón 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	31 de enero de 2014

Cambio	Descripción	Fecha de modificación
Compatibilidad con bibliotecas de cintas virtuales (VTL) e introducción del API versión 2013-06-30	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 las puertas de enlace de volumen (volúmenes en caché y almacenados), a partir de ahora Storage Gateway admite las bibliotecas 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 comandos de SCSI, por lo que sus aplicaciones de backup on-premise funcionarán sin modificaciones. Para obtener más información, consulte los siguientes temas en la Guía del usuario de AWS Storage Gateway . • 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.	5 de noviembre de 2013
Compatibilidad con Microsoft Hyper-V	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.	10 de abril de 2013

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 (Amazon EC2). Puede lanzar una instancia de puerta de enlace en Amazon EC2 mediante la AMI de Storage Gateway disponible en AWS Marketplace. Para comenzar a implementar una puerta de enlace mediante la AMI de Storage Gateway, consulte Implemente una EC2 instancia de Amazon personalizada para Volume Gateway.	15 de enero de 2013

Cambio	Descripción	Fecha de modificación
Compatibilidad con los volúmenes en caché e introducción del API versión 2012-06-30	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 con un tamaño de hasta 32 TiB y montarlos como dispositivos iSCSI desde los 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. En esta versión, Storage Gateway también presenta una nueva versión del API que, además de ser compatible con las operaciones actuales, ofrece nuevas operaciones para admitir los volúmenes en caché. Para obtener más información sobre las dos soluciones de Storage Gateway, consulte Funcionamiento de puerta de enlace de volumen.	29 de octubre de 2012

Cambio	Descripción	Fecha de modificación
	También puede probar una configuración de prueba. Para obtener instrucciones, consulte Creación de una puerta de enlace de cinta.	
Compatibilidad con API e IAM	En esta versión, Storage Gateway presenta la compatibilidad con las API y con AWS Identity and Access Management(IAM). • Compatibilidad con el API: ahora puede configura r y administrar los recursos de Storage Gateway mediante programación. Para obtener más información sobre la API, consulte Referencia de la API para Storage Gateway en la Guía del usuario de AWS Storage Gateway . • Compatibilidad con IAM: AWS Identity and Access Management (IAM) permite crear usuarios y administrar el acceso de los usuarios a los recursos de Storage Gateway mediante políticas de IAM. Para obtener algunos ejemplos de políticas de IAM, consulte Identity and Access Management para AWS Storage Gateway. Para obtener más informaci ón sobre IAM, consulte la página de información detallada de AWS Identity and Access Managemen t (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 de puerta de enlace de volumen

Estas notas de la versión describen las características, mejoras y correcciones nuevas y actualizadas que se incluyen con cada versión del dispositivo de Puerta de enlace de volumen. Cada versión de software se identifica por su fecha de lanzamiento y un número de versión único.

Para determinar el número de versión del software de una puerta de enlace, consulte su página de detalles en la consola de Storage Gateway o llame a la acción de la DescribeGatewayInformationAPI mediante un AWS CLI comando similar al siguiente:

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

El número de versión se devuelve en el campo de `SoftwareVersion` de la respuesta de la API.

> **Note**
>
> Una puerta de enlace no proporcionará información sobre la versión de software en las siguientes circunstancias:
>
> - La puerta de enlace está fuera de línea.
> - La puerta de enlace ejecuta software antiguo que no admite la generación de informes de versiones.
> - El tipo de puerta de enlace es FSx File Gateway.

Para obtener más información sobre las actualizaciones de Volume Gateway, incluida la forma de modificar la programación automática predeterminada de mantenimiento y actualización de una puerta de enlace, consulte Gestión de las actualizaciones de la puerta de enlace mediante la consola AWS Storage Gateway.

Fecha de lanzamiento	Versión del software	Notas de la versión
2025-07-01	2.12.11	• Se actualizaron los elementos del sistema

Fecha de lanzamiento	Versión del software	Notas de la versión
		operativo y del software para mejorar la seguridad y el rendimiento de las pasarelas nuevas y existentes
2025-06-02	2.12.10	• Se actualizaron los elementos del sistema operativo y del software para mejorar la seguridad y el rendimiento de las pasarelas nuevas y existentes
2025-05-01	2.12.9	• Se actualizaron los elementos del sistema operativo y del software para mejorar la seguridad y el rendimiento de las pasarelas nuevas y existentes
2025-05-01	2.12.8	• Se actualizaron los elementos del sistema operativo y del software para mejorar la seguridad y el rendimiento de las pasarelas nuevas y existentes

Fecha de lanzamiento	Versión del software	Notas de la versión
01-04-01	2.12.7	• Se actualizaron los elementos del sistema operativo y del software para mejorar la seguridad y el rendimiento de las pasarelas nuevas y existentes
04-03-2025	2.12.6	• Se actualizaron los elementos del sistema operativo y del software para mejorar la seguridad y el rendimiento de las pasarelas nuevas y existentes
2025-02-04	2.12.5	• Se actualizaron los elementos del sistema operativo y del software para mejorar la seguridad y el rendimiento de las pasarelas nuevas y existentes • Se solucionó un problema que provocaba que las puertas de enlace se quedaran bloqueadas al apagarse después de una actualización de software

Fecha de lanzamiento	Versión del software	Notas de la versión
07/01/2020	2.12.3	• Se actualizaron los elementos del sistema operativo y del software para mejorar la seguridad y el rendimiento de las pasarelas nuevas y existentes
6 de diciembre de 2022	2.12.2	• Se actualizaron los elementos del sistema operativo y del software para mejorar la seguridad y el rendimiento de las pasarelas nuevas y existentes
06/11/2022	2.12.1	• Se actualizaron los elementos del sistema operativo y del software para mejorar la seguridad y el rendimiento de las pasarelas nuevas y existentes

Fecha de lanzamiento	Versión del software	Notas de la versión
03 de octubre de 2024	2.12.0	• Se ha corregido un problema por el que el iniciador iSCSI no se reconectaba automátic amente con los volúmenes tras el reinicio de la puerta de enlace o la actualización del software de la puerta de enlace • Se actualizaron los elementos del sistema operativo y del software para mejorar la seguridad y el rendimiento de las pasarelas nuevas y existentes
30 de agosto de 2024/	2.11.0	• Se actualizaron el sistema operativo y los elementos de software para mejorar la seguridad y el rendimien to de las puertas de enlace nuevas y existentes
29-07-2020	2.10.0	• Se actualizaron el sistema operativo y los elementos de software para mejorar la seguridad y el rendimien to de las puertas de enlace nuevas y existentes • Varias correcciones y mejoras de errores

Fecha de lanzamiento	Versión del software	Notas de la versión
-17 de junio de 2024	2.9.2	• Se actualizaron los elementos del sistema operativo y del software para mejorar la seguridad y el rendimiento de las pasarelas nuevas y existentes
28-05-2022	2.9.0	• Se ha reducido el 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
2024-05-08	2.8.3	• Se solucionó el problema de conectividad a la nube al usar un proxy SOCKS5
10 de abril de 2022	2.8.1	• Se ha corregido un problema de uso de memoria ingresado en 2.8.0 • Actualizaciones del parche de seguridad • Se ha mejorado el proceso de actualización de software • Se ha corregido la falta del componente Protocolo de tiempo de red (NTP) para las nuevas puertas de enlace

Fecha de lanzamiento	Versión del software	Notas de la versión
2024-03-06	2.8.0	• Se actualizaron los elementos del sistema operativo y del software para mejorar la seguridad y el rendimiento de las nuevas puertas de enlace • Actualizaciones del parche de seguridad
-19 de diciembre de 2023	2.7.0	• Se actualizaron los elementos del sistema operativo y del software para mejorar la seguridad y el rendimiento de las nuevas puertas de enlace
14 de diciembre de 2023	2.6.6	• Versión de mantenimiento

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