



Configurar conexiones de cliente

StorageGRID software

NetApp
December 03, 2025

Tabla de contenidos

Configurar conexiones de cliente	1
Configurar conexiones de cliente S3	1
Tareas de configuración	1
Información necesaria para adjuntar StorageGRID a una aplicación cliente	2
Seguridad para clientes S3	3
Resumen	3
Cómo StorageGRID proporciona seguridad para las aplicaciones cliente	4
Algoritmos de cifrado y hash compatibles con bibliotecas TLS	4
Utilice el asistente de configuración de S3	5
Utilizar el asistente de configuración de S3: Consideraciones y requisitos	5
Acceda y complete el asistente de configuración de S3	6
Administrar grupos de alta disponibilidad	14
¿Qué son los grupos de alta disponibilidad (HA)?	14
¿Cómo se utilizan los grupos HA?	17
Opciones de configuración para grupos de alta disponibilidad	18
Configurar grupos de alta disponibilidad	19
Gestionar el equilibrio de carga	25
Consideraciones para el equilibrio de carga	25
Configurar los puntos finales del balanceador de carga	29
Configurar nombres de dominio de puntos finales S3	39
Agregar un nombre de dominio de punto final S3	40
Cambiar el nombre de un dominio de punto final S3	41
Eliminar un nombre de dominio de punto final S3	41
Resumen: Direcciones IP y puertos para conexiones de cliente	41
URL de ejemplo	42
Dónde encontrar direcciones IP	42

Configurar conexiones de cliente

Configurar conexiones de cliente S3

Como administrador de la red, usted administra las opciones de configuración que controlan cómo las aplicaciones cliente S3 se conectan a su sistema StorageGRID para almacenar y recuperar datos.



Se han eliminado los detalles rápidos de esta versión del sitio de documentación. Ver ["StorageGRID 11.8: Configurar conexiones de cliente S3 y Swift"](#) .

Tareas de configuración

1. Realice tareas previas requeridas en StorageGRID, según cómo la aplicación cliente se conectará a StorageGRID.

Tareas requeridas

Debes obtener:

- Direcciones IP
- Nombres de dominio
- Certificado SSL

Tareas opcionales

Opcionalmente, configure:

- Federación de identidades
- SSO

1. Utilice StorageGRID para obtener los valores que la aplicación necesita para conectarse a la red. Puede utilizar el asistente de configuración de S3 o configurar cada entidad StorageGRID manualmente.

Utilice el asistente de configuración de S3

Siga los pasos del asistente de configuración de S3.

Configurar manualmente

1. Crear un grupo de alta disponibilidad
2. Crear un punto final del balanceador de carga
3. Crear una cuenta de inquilino
4. Crear bucket y claves de acceso
5. Configurar reglas y políticas de ILM

1. Utilice la aplicación S3 para completar la conexión a StorageGRID. Cree entradas DNS para asociar direcciones IP a cualquier nombre de dominio que planee utilizar.

Según sea necesario, realice configuraciones adicionales de la aplicación.

2. Realice tareas continuas en la aplicación y en StorageGRID para administrar y monitorear el almacenamiento de objetos a lo largo del tiempo.

Información necesaria para adjuntar StorageGRID a una aplicación cliente

Antes de poder conectar StorageGRID a una aplicación cliente S3, debe realizar pasos de configuración en StorageGRID y obtener cierto valor.

¿Qué valores necesito?

La siguiente tabla muestra los valores que debe configurar en StorageGRID y dónde la aplicación S3 y el servidor DNS utilizan esos valores.

Valor	Donde se configura el valor	Dónde se utiliza el valor
Direcciones IP virtuales (VIP)	StorageGRID > Grupo de alta disponibilidad	Entrada DNS
Puerto	StorageGRID > Punto final del balanceador de carga	Aplicación cliente
Certificado SSL	StorageGRID > Punto final del balanceador de carga	Aplicación cliente
Nombre del servidor (FQDN)	StorageGRID > Punto final del balanceador de carga	<ul style="list-style-type: none">• Aplicación cliente• Entrada DNS
ID de clave de acceso S3 y clave de acceso secreta	StorageGRID > Inquilino y depósito	Aplicación cliente
Nombre del cubo/contenedor	StorageGRID > Inquilino y depósito	Aplicación cliente

¿Cómo obtengo estos valores?

Dependiendo de sus necesidades, puede realizar cualquiera de las siguientes acciones para obtener la información que necesita:

- *Utilice el ["Asistente de configuración de S3"](#) *. El asistente de configuración de S3 le ayuda a configurar rápidamente los valores necesarios en StorageGRID y genera uno o dos archivos que puede usar al configurar la aplicación S3. El asistente lo guía a través de los pasos necesarios y lo ayuda a garantizar que su configuración se ajuste a las mejores prácticas de StorageGRID .



Si está configurando una aplicación S3, se recomienda utilizar el asistente de configuración S3 a menos que sepa que tiene requisitos especiales o que su implementación requerirá una personalización significativa.

- *Utilice el ["Asistente de configuración de FabricPool"](#) *. Similar al asistente de configuración de S3, el asistente de configuración de FabricPool lo ayuda a configurar rápidamente los valores requeridos y

genera un archivo que puede usar cuando configura un nivel de nube de FabricPool en ONTAP.



Si planea utilizar StorageGRID como sistema de almacenamiento de objetos para un nivel de nube de FabricPool, se recomienda utilizar el asistente de configuración de FabricPool a menos que sepa que tiene requisitos especiales o que su implementación requerirá una personalización significativa.

- **Configurar elementos manualmente.** Si se conecta a una aplicación S3 y prefiere no utilizar el asistente de configuración S3, puede obtener los valores necesarios realizando la configuración manualmente. Siga estos pasos:
 - a. Configure el grupo de alta disponibilidad (HA) que desea utilizar para la aplicación S3. Ver "[Configurar grupos de alta disponibilidad](#)".
 - b. Cree el punto final del equilibrador de carga que utilizará la aplicación S3. Ver "[Configurar los puntos finales del balanceador de carga](#)".
 - c. Cree la cuenta de inquilino que utilizará la aplicación S3. Ver "[Crear una cuenta de inquilino](#)".
 - d. Para un inquilino S3, inicie sesión en la cuenta del inquilino y genere una ID de clave de acceso y una clave de acceso secreta para cada usuario que accederá a la aplicación. Ver "[Crea tus propias claves de acceso](#)".
 - e. Cree uno o más depósitos S3 dentro de la cuenta del inquilino. Para S3, consulte "[Crear un depósito S3](#)".
 - f. Para agregar instrucciones de ubicación específicas para los objetos que pertenecen al nuevo inquilino o contenedor, cree una nueva regla ILM y active una nueva política ILM para usar esa regla. Ver "[Crear regla ILM](#)" y "[Crear una política ILM](#)".

Seguridad para clientes S3

Las cuentas de inquilino de StorageGRID utilizan aplicaciones cliente S3 para guardar datos de objetos en StorageGRID. Debe revisar las medidas de seguridad implementadas para las aplicaciones cliente.

Resumen

La siguiente lista resume cómo se implementa la seguridad para la API REST de S3:

Seguridad de la conexión

TLS

Autenticación del servidor

Certificado de servidor X.509 firmado por la CA del sistema o certificado de servidor personalizado proporcionado por el administrador

Autenticación de cliente

ID de clave de acceso de la cuenta S3 y clave de acceso secreta

Autorización del cliente

Propiedad del depósito y todas las políticas de control de acceso aplicables

Cómo StorageGRID proporciona seguridad para las aplicaciones cliente

Las aplicaciones cliente S3 pueden conectarse al servicio Load Balancer en nodos de puerta de enlace o nodos de administración o directamente a nodos de almacenamiento.

- Los clientes que se conectan al servicio Load Balancer pueden usar HTTPS o HTTP, según cómo ["configurar el punto final del balanceador de carga"](#) .

Se recomienda utilizar HTTPS para proporcionar una comunicación segura cifrada mediante TLS. Debe adjuntar un certificado de seguridad al punto final.

HTTP proporciona una comunicación menos segura y sin cifrar y solo debe usarse para redes que no sean de producción o de prueba.

- Los clientes que se conectan a los nodos de almacenamiento también pueden usar HTTPS o HTTP.

HTTPS es el predeterminado y se recomienda.

HTTP proporciona una comunicación menos segura y sin cifrar, pero puede ser opcional. ["activado"](#) para redes que no sean de producción o de prueba.

- Las comunicaciones entre StorageGRID y el cliente están cifradas mediante TLS.
- Las comunicaciones entre el servicio Load Balancer y los nodos de almacenamiento dentro de la red están cifradas independientemente de si el punto final del balanceador de carga está configurado para aceptar conexiones HTTP o HTTPS.
- Los clientes deben suministrar ["Encabezados de autenticación HTTP"](#) a StorageGRID para realizar operaciones de API REST.

Certificados de seguridad y aplicaciones cliente

En todos los casos, las aplicaciones cliente pueden realizar conexiones TLS utilizando un certificado de servidor personalizado cargado por el administrador de la red o un certificado generado por el sistema StorageGRID :

- Cuando las aplicaciones cliente se conectan al servicio Load Balancer, utilizan el certificado que se configuró para el punto final del balanceador de carga. Cada punto final del equilibrador de carga tiene su propio certificado: un certificado de servidor personalizado cargado por el administrador de la red o un certificado que el administrador de la red generó en StorageGRID al configurar el punto final.

Ver ["Consideraciones para el equilibrio de carga"](#) .

- Cuando las aplicaciones cliente se conectan directamente a un nodo de almacenamiento, utilizan los certificados de servidor generados por el sistema que se generaron para los nodos de almacenamiento cuando se instaló el sistema StorageGRID (que están firmados por la autoridad de certificación del sistema) o un único certificado de servidor personalizado que proporciona un administrador de la red para la red. Ver ["agregar un certificado API S3 personalizado"](#) .

Los clientes deben configurarse para confiar en la autoridad de certificación que firmó el certificado que utilizan para establecer conexiones TLS.

Algoritmos de cifrado y hash compatibles con bibliotecas TLS

El sistema StorageGRID admite un conjunto de conjuntos de cifrado que las aplicaciones cliente pueden usar al establecer una sesión TLS. Para configurar cifrados, vaya a **CONFIGURACIÓN > Seguridad >**

Configuración de seguridad y seleccione Políticas TLS y SSH.

Versiones compatibles de TLS

StorageGRID admite TLS 1.2 y TLS 1.3.



SSLv3 y TLS 1.1 (o versiones anteriores) ya no son compatibles.

Utilice el asistente de configuración de S3

Utilizar el asistente de configuración de S3: Consideraciones y requisitos

Puede utilizar el asistente de configuración de S3 para configurar StorageGRID como el sistema de almacenamiento de objetos para una aplicación S3.

Cuándo utilizar el asistente de configuración de S3

El asistente de configuración de S3 lo guía a través de cada paso de la configuración de StorageGRID para su uso con una aplicación S3. Como parte de completar el asistente, descargará archivos que puede usar para ingresar valores en la aplicación S3. Utilice el asistente para configurar su sistema más rápidamente y asegurarse de que sus configuraciones se ajusten a las mejores prácticas de StorageGRID .

Si tienes el ["Permiso de acceso root"](#) Puede completar el asistente de configuración de S3 cuando comience a utilizar StorageGRID Grid Manager o puede acceder al asistente y completarlo en cualquier momento posterior. Dependiendo de sus requisitos, también puede configurar algunos o todos los elementos necesarios manualmente y luego usar el asistente para reunir los valores que necesita una aplicación S3.

Antes de utilizar el asistente

Antes de utilizar el asistente, confirme que ha completado estos requisitos previos.

Obtener direcciones IP y configurar interfaces VLAN

Si configura un grupo de alta disponibilidad (HA), sabrá a qué nodos se conectará la aplicación S3 y qué red StorageGRID se utilizará. También sabe qué valores ingresar para el CIDR de subred, la dirección IP de puerta de enlace y las direcciones IP virtuales (VIP).

Si planea utilizar una LAN virtual para segregar el tráfico de la aplicación S3, ya ha configurado la interfaz VLAN. Ver ["Configurar interfaces VLAN"](#) .

Configurar la federación de identidades y el SSO

Si planea utilizar la federación de identidad o el inicio de sesión único (SSO) para su sistema StorageGRID , debe habilitar estas funciones. También sabe qué grupo federado debe tener acceso raíz para la cuenta de inquilino que utilizará la aplicación S3. Ver ["Utilizar la federación de identidades"](#) y ["Configurar el inicio de sesión único"](#) .

Obtener y configurar nombres de dominio

Sabe qué nombre de dominio completo (FQDN) utilizar para StorageGRID. Las entradas del servidor de nombres de dominio (DNS) asignarán este FQDN a las direcciones IP virtuales (VIP) del grupo de alta disponibilidad que cree mediante el asistente.

Si planea utilizar solicitudes alojadas virtuales de estilo S3, debe tener ["nombres de dominio de punto final S3 configurados"](#) . Se recomienda utilizar solicitudes de estilo alojado virtual.

Revisar los requisitos del balanceador de carga y del certificado de seguridad

Si planea utilizar el balanceador de carga StorageGRID , ha revisado las consideraciones generales para el balanceo de carga. Tienes los certificados que cargarás o los valores que necesitas para generar un certificado.

Si planea utilizar un punto final de balanceador de carga externo (de terceros), debe tener el nombre de dominio completo (FQDN), el puerto y el certificado para ese balanceador de carga.

Configurar cualquier conexión de federación de red

Si desea permitir que el inquilino de S3 clone datos de cuenta y replique objetos de bucket a otra red mediante una conexión de federación de red, confirme lo siguiente antes de iniciar el asistente:

- Tienes ["configuró la conexión de la federación de red"](#) .
- El estado de la conexión es **Conectado**.
- Tienes permiso de acceso root.

Acceda y complete el asistente de configuración de S3

Puede utilizar el asistente de configuración de S3 para configurar StorageGRID para su uso con una aplicación S3. El asistente de configuración proporciona los valores que la aplicación necesita para acceder a un depósito StorageGRID y guardar objetos.

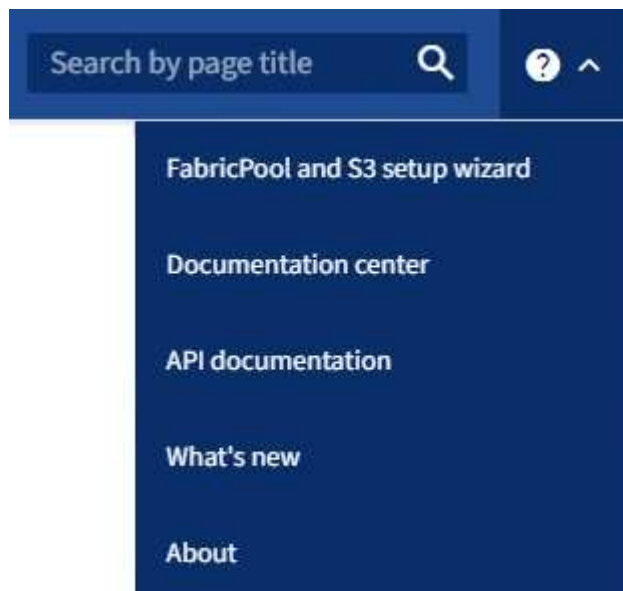
Antes de empezar

- Tú tienes el ["Permiso de acceso root"](#) .
- Usted ha revisado el ["Consideraciones y requisitos"](#) para utilizar el asistente.

Acceder al asistente

Pasos

1. Sign in en Grid Manager usando un ["navegador web compatible"](#) .
2. Si aparece el banner **Asistente de configuración de FabricPool y S3** en el panel, seleccione el enlace en el banner. Si el banner ya no aparece, seleccione el ícono de ayuda en la barra de encabezado en el Administrador de cuadrícula y seleccione **Asistente de configuración de FabricPool y S3**.



3. En la sección de aplicación S3 de la página del asistente de configuración de FabricPool y S3, seleccione **Configurar ahora**.

Paso 1 de 6: Configurar el grupo de alta disponibilidad

Un grupo de alta disponibilidad es una colección de nodos que contienen cada uno el servicio StorageGRID Load Balancer. Un grupo de alta disponibilidad puede contener nodos de puerta de enlace, nodos de administración o ambos.

Puede utilizar un grupo HA para ayudar a mantener disponibles las conexiones de datos S3. Si la interfaz activa en el grupo HA falla, una interfaz de respaldo puede administrar la carga de trabajo con poco impacto en las operaciones de S3.

Para obtener más detalles sobre esta tarea, consulte ["Administrar grupos de alta disponibilidad"](#).

Pasos

1. Si planea utilizar un balanceador de carga externo, no necesita crear un grupo de alta disponibilidad. Seleccione **Omitir este paso** y vaya a [Paso 2 de 6: Configurar el punto final del balanceador de carga](#).
2. Para utilizar el equilibrador de carga StorageGRID, puede crear un nuevo grupo de HA o utilizar un grupo de HA existente.

Crear un grupo de alta disponibilidad

- a. Para crear un nuevo grupo de HA, seleccione **Crear grupo de HA**.
- b. Para el paso **Ingresar detalles**, complete los siguientes campos.

Campo	Descripción
Nombre del grupo HA	Un nombre para mostrar único para este grupo HA.
Descripción (opcional)	La descripción de este grupo HA.

- c. Para el paso **Agregar interfaces**, seleccione las interfaces de nodo que desea utilizar en este grupo de HA.

Utilice los encabezados de columna para ordenar las filas o ingrese un término de búsqueda para localizar interfaces más rápidamente.

Puede seleccionar uno o más nodos, pero solo puede seleccionar una interfaz para cada nodo.

- d. Para el paso **Priorizar interfaces**, determine la interfaz principal y cualquier interfaz de respaldo para este grupo de HA.

Arrastre filas para cambiar los valores en la columna **Orden de prioridad**.

La primera interfaz de la lista es la interfaz principal. La interfaz principal es la interfaz activa a menos que ocurra una falla.

Si el grupo HA incluye más de una interfaz y la interfaz activa falla, las direcciones IP virtuales (VIP) se mueven a la primera interfaz de respaldo en el orden de prioridad. Si esa interfaz falla, las direcciones VIP pasan a la siguiente interfaz de respaldo, y así sucesivamente. Cuando se resuelven las fallas, las direcciones VIP vuelven a la interfaz de mayor prioridad disponible.

- e. Para el paso **Ingresar direcciones IP**, complete los siguientes campos.

Campo	Descripción
CIDR de subred	La dirección de la subred VIP en notación CIDR: una dirección IPv4 seguida de una barra y la longitud de la subred (0-32). La dirección de red no debe tener ningún bit de host configurado. Por ejemplo, 192.16.0.0/22 .
Dirección IP de la puerta de enlace (opcional)	Si las direcciones IP de S3 utilizadas para acceder a StorageGRID no están en la misma subred que las direcciones VIP de StorageGRID , ingrese la dirección IP de la puerta de enlace local VIP de StorageGRID . La dirección IP de la puerta de enlace local debe estar dentro de la subred VIP.

Campo	Descripción
Dirección IP virtual	<p>Ingrese al menos una y no más de diez direcciones VIP para la interfaz activa en el grupo HA. Todas las direcciones VIP deben estar dentro de la subred VIP.</p> <p>Al menos una dirección debe ser IPv4. Opcionalmente, puede especificar direcciones IPv4 e IPv6 adicionales.</p>

f. Seleccione **Crear grupo HA** y luego seleccione **Finalizar** para regresar al asistente de configuración de S3.

g. Seleccione **Continuar** para ir al paso del balanceador de carga.

Utilizar el grupo HA existente

a. Para utilizar un grupo de HA existente, seleccione el nombre del grupo de HA en **Seleccionar un grupo de HA**.

b. Seleccione **Continuar** para ir al paso del balanceador de carga.

Paso 2 de 6: Configurar el punto final del balanceador de carga

StorageGRID utiliza un equilibrador de carga para administrar la carga de trabajo de las aplicaciones cliente. El equilibrio de carga maximiza la velocidad y la capacidad de conexión en múltiples nodos de almacenamiento.

Puede utilizar el servicio StorageGRID Load Balancer, que existe en todos los nodos de puerta de enlace y de administración, o puede conectarse a un balanceador de carga externo (de terceros). Se recomienda utilizar el balanceador de carga StorageGRID .

Para obtener más detalles sobre esta tarea, consulte ["Consideraciones para el equilibrio de carga"](#) .

Para utilizar el servicio StorageGRID Load Balancer, seleccione la pestaña * StorageGRID load balancer* y luego cree o seleccione el punto final del balanceador de carga que desee utilizar. Para utilizar un balanceador de carga externo, seleccione la pestaña **Balanceador de carga externo** y proporcione detalles sobre el sistema que ya ha configurado.

Crear punto final

Pasos

1. Para crear un punto final de balanceador de carga, seleccione **Crear punto final**.
2. Para el paso **Ingresar detalles del punto final**, complete los siguientes campos.

Campo	Descripción
Nombre	Un nombre descriptivo para el punto final.
Puerto	<p>El puerto StorageGRID que desea utilizar para equilibrar la carga. Este campo tiene como valor predeterminado 10433 para el primer punto final que cree, pero puede ingresar cualquier puerto externo no utilizado. Si ingresa 80 o 443, el punto final se configura solo en los nodos de puerta de enlace, porque estos puertos están reservados en los nodos de administración.</p> <p>Nota: No se permiten los puertos utilizados por otros servicios de red. Ver el "Referencia del puerto de red".</p>
Tipo de cliente	Debe ser S3 .
Protocolo de red	<p>Seleccione HTTPS.</p> <p>Nota: Se admite la comunicación con StorageGRID sin cifrado TLS, pero no se recomienda.</p>

3. Para el paso **Seleccionar modo de enlace**, especifique el modo de enlace. El modo de enlace controla cómo se accede al punto final utilizando cualquier dirección IP o utilizando direcciones IP e interfaces de red específicas.

Modo	Descripción
Global (predeterminado)	<p>Los clientes pueden acceder al punto final utilizando la dirección IP de cualquier nodo de puerta de enlace o nodo de administración, la dirección IP virtual (VIP) de cualquier grupo de alta disponibilidad en cualquier red o un FQDN correspondiente.</p> <p>Utilice la configuración Global (predeterminada) a menos que necesite restringir la accesibilidad de este punto final.</p>
IP virtuales de grupos de alta disponibilidad	<p>Los clientes deben usar una dirección IP virtual (o FQDN correspondiente) de un grupo de HA para acceder a este punto final.</p> <p>Todos los puntos finales con este modo de enlace pueden usar el mismo número de puerto, siempre que los grupos de HA que seleccione para los puntos finales no se superpongan.</p>
Interfaces de nodo	Los clientes deben utilizar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas para acceder a este punto final.

Modo	Descripción
Tipo de nodo	Según el tipo de nodo que seleccione, los clientes deben usar la dirección IP (o FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o FQDN correspondiente) de cualquier nodo de puerta de enlace para acceder a este punto final.

4. Para el paso de acceso de inquilino, seleccione una de las siguientes opciones:

Campo	Descripción
Permitir a todos los inquilinos (predeterminado)	Todas las cuentas de inquilinos pueden usar este punto final para acceder a sus depósitos.
Permitir inquilinos seleccionados	Solo las cuentas de inquilinos seleccionadas pueden usar este punto final para acceder a sus depósitos.
Bloquear inquilinos seleccionados	Las cuentas de inquilinos seleccionadas no pueden usar este punto final para acceder a sus depósitos. Todos los demás inquilinos pueden utilizar este punto final.

5. Para el paso **Adjuntar certificado**, seleccione una de las siguientes opciones:

Campo	Descripción
Subir certificado (recomendado)	Utilice esta opción para cargar un certificado de servidor firmado por una CA, una clave privada de certificado y un paquete de CA opcional.
Generar certificado	Utilice esta opción para generar un certificado autofirmado. Ver " Configurar los puntos finales del balanceador de carga " para obtener detalles de qué ingresar.
Utilice el certificado StorageGRID S3	Utilice esta opción solo si ya ha cargado o generado una versión personalizada del certificado global de StorageGRID . Ver " Configurar certificados de API S3 " Para más detalles.

6. Seleccione **Finalizar** para regresar al asistente de configuración de S3.

7. Seleccione **Continuar** para ir al paso de inquilino y depósito.



Los cambios en un certificado de punto final pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Utilice el punto final del balanceador de carga existente

Pasos

1. Para utilizar un punto final existente, seleccione su nombre en **Seleccionar un punto final del balanceador de carga**.
2. Seleccione **Continuar** para ir al paso de inquilino y depósito.

Utilice un balanceador de carga externo

Pasos

1. Para utilizar un balanceador de carga externo, complete los siguientes campos.

Campo	Descripción
Nombre de dominio completo (FQDN)	El nombre de dominio completo (FQDN) del balanceador de carga externo.
Puerto	El número de puerto que utilizará la aplicación S3 para conectarse al balanceador de carga externo.
Certificado	Copie el certificado del servidor para el balanceador de carga externo y péguelo en este campo.

2. Seleccione **Continuar** para ir al paso de inquilino y depósito.

Paso 3 de 6: Crear inquilino y depósito

Un inquilino es una entidad que puede utilizar aplicaciones S3 para almacenar y recuperar objetos en StorageGRID. Cada inquilino tiene sus propios usuarios, claves de acceso, depósitos, objetos y un conjunto específico de capacidades.

Un bucket es un contenedor que se utiliza para almacenar objetos y metadatos de objetos de un inquilino. Aunque los inquilinos pueden tener muchos grupos, el asistente le ayuda a crear un inquilino y un grupo de la forma más rápida y sencilla. Si necesita agregar depósitos o configurar opciones más adelante, puede utilizar el Administrador de inquilinos.

Para obtener más detalles sobre esta tarea, consulte ["Crear una cuenta de inquilino"](#) y ["Crear un depósito S3"](#).

Pasos

1. Introduzca un nombre para la cuenta de inquilino.

Los nombres de los inquilinos no necesitan ser únicos. Cuando se crea la cuenta de inquilino, recibe un ID de cuenta numérico único.

2. Defina el acceso raíz para la cuenta de inquilino, en función de si su sistema StorageGRID utiliza ["federación de identidades"](#), ["inicio de sesión único \(SSO\)"](#), o ambos.

Opción	Haz esto
Si la federación de identidad no está habilitada	Especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si la federación de identidad está habilitada	<ol style="list-style-type: none">a. Seleccione un grupo federado existente para tener "Permiso de acceso root" para el inquilino.b. Opcionalmente, especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.

Opción	Haz esto
Si tanto la federación de identidad como el inicio de sesión único (SSO) están habilitados	Seleccione un grupo federado existente para tener " Permiso de acceso root " para el inquilino. Ningún usuario local puede iniciar sesión.

- Si desea que el asistente cree la ID de clave de acceso y la clave de acceso secreta para el usuario raíz, seleccione **Crear clave de acceso S3 del usuario raíz automáticamente**.

Seleccione esta opción si el único usuario del inquilino será el usuario raíz. Si otros usuarios utilizarán este inquilino, "[utilizar el Administrador de inquilinos](#)" para configurar claves y permisos.

- Si desea crear un depósito para este inquilino ahora, seleccione **Crear depósito para este inquilino**.



Si el Bloqueo de objetos S3 está habilitado para la cuadrícula, el depósito creado en este paso no tendrá el Bloqueo de objetos S3 habilitado. Si necesita utilizar un depósito de bloqueo de objetos S3 para esta aplicación S3, no seleccione crear un depósito ahora. En su lugar, utilice el Administrador de inquilinos para "[crear el cubo](#)" más tarde.

- Introduzca el nombre del depósito que utilizará la aplicación S3. Por ejemplo, `s3-bucket`.

No puedes cambiar el nombre del depósito después de crearlo.

- Seleccione la **Región** para este bucket.


Utilice la región predeterminada (`us-east-1`) a menos que espere utilizar ILM en el futuro para filtrar objetos según la región del depósito.

- Seleccione **Crear y continuar**.

Paso 4 de 6: Descargar datos

En el paso de descarga de datos, puede descargar uno o dos archivos para guardar los detalles de lo que acaba de configurar.

Pasos

- Si seleccionó **Crear clave de acceso S3 de usuario raíz automáticamente**, realice una o ambas de las siguientes acciones:
 - Seleccione **Descargar claves de acceso** para descargar una `.csv` archivo que contiene el nombre de la cuenta del inquilino, el ID de la clave de acceso y la clave de acceso secreta.
 - Seleccione el icono de copia () para copiar el ID de la clave de acceso y la clave de acceso secreta al portapapeles.
- Seleccione **Descargar valores de configuración** para descargar un `.txt` archivo que contiene las configuraciones para el punto final del balanceador de carga, el inquilino, el depósito y el usuario raíz.
- Guarde esta información en un lugar seguro.



No cierre esta página hasta que haya copiado ambas claves de acceso. Las claves no estarán disponibles después de cerrar esta página. Asegúrese de guardar esta información en una ubicación segura porque puede usarse para obtener datos de su sistema StorageGRID.

4. Si se le solicita, seleccione la casilla de verificación para confirmar que ha descargado o copiado las claves.
5. Seleccione **Continuar** para ir al paso de reglas y políticas de ILM.

Paso 5 de 6: Revisar la regla y la política de ILM para S3

Las reglas de administración del ciclo de vida de la información (ILM) controlan la ubicación, la duración y el comportamiento de ingesta de todos los objetos en su sistema StorageGRID . La política ILM incluida con StorageGRID realiza dos copias replicadas de todos los objetos. Esta política estará vigente hasta que active al menos una nueva política.

Pasos

1. Revise la información proporcionada en la página.
2. Si desea agregar instrucciones específicas para los objetos que pertenecen al nuevo inquilino o depósito, cree una nueva regla y una nueva política. Ver "[Crear regla ILM](#)" y "[Utilice las políticas de ILM](#)".
3. Seleccione **He revisado estos pasos y entiendo lo que necesito hacer**.
4. Seleccione la casilla de verificación para indicar que comprende qué hacer a continuación.
5. Seleccione **Continuar** para ir a **Resumen**.

Paso 6 de 6: Revisar el resumen

Pasos

1. Revise el resumen.
2. Tome nota de los detalles en los próximos pasos, que describen la configuración adicional que podría ser necesaria antes de conectarse al cliente S3. Por ejemplo, si selecciona * Sign in como root*, accederá al Administrador de inquilinos, donde podrá agregar usuarios inquilinos, crear depósitos adicionales y actualizar la configuración de los depósitos.
3. Seleccione **Finalizar**.
4. Configure la aplicación utilizando el archivo que descargó de StorageGRID o los valores que obtuvo manualmente.

Administrar grupos de alta disponibilidad

¿Qué son los grupos de alta disponibilidad (HA)?

Los grupos de alta disponibilidad (HA) proporcionan conexiones de datos de alta disponibilidad para clientes S3 y conexiones de alta disponibilidad para Grid Manager y Tenant Manager.

Puede agrupar las interfaces de red de varios nodos de administración y de puerta de enlace en un grupo de alta disponibilidad (HA). Si la interfaz activa en el grupo HA falla, una interfaz de respaldo puede administrar la carga de trabajo.

Cada grupo HA proporciona acceso a los servicios compartidos en los nodos seleccionados.

- Los grupos de alta disponibilidad que incluyen nodos de puerta de enlace, nodos de administración o ambos proporcionan conexiones de datos de alta disponibilidad para clientes S3.
- Los grupos de HA que incluyen solo nodos de administración proporcionan conexiones de alta

disponibilidad al Administrador de red y al Administrador de inquilinos.

- Un grupo de alta disponibilidad que incluye solo dispositivos de servicios y nodos de software basados en VMware puede proporcionar conexiones de alta disponibilidad para ["Inquilinos de S3 que utilizan S3 Select"](#) . Se recomiendan grupos HA cuando se utiliza S3 Select, pero no son obligatorios.

¿Cómo se crea un grupo HA?

1. Selecciona una interfaz de red para uno o más nodos de administración o nodos de puerta de enlace. Puede utilizar una interfaz de red de cuadrícula (eth0), una interfaz de red de cliente (eth2), una interfaz VLAN o una interfaz de acceso que haya agregado al nodo.



No se puede agregar una interfaz a un grupo HA si tiene una dirección IP asignada por DHCP.

2. Debe especificar una interfaz para que sea la interfaz principal. La interfaz principal es la interfaz activa a menos que ocurra una falla.
3. Usted determina el orden de prioridad para cualquier interfaz de respaldo.
4. Asigna de una a diez direcciones IP virtuales (VIP) al grupo. Las aplicaciones clientes pueden usar cualquiera de estas direcciones VIP para conectarse a StorageGRID.

Para obtener instrucciones, consulte ["Configurar grupos de alta disponibilidad"](#) .

¿Qué es la interfaz activa?

Durante el funcionamiento normal, todas las direcciones VIP del grupo HA se agregan a la interfaz principal, que es la primera interfaz en el orden de prioridad. Mientras la interfaz principal permanezca disponible, se utilizará cuando los clientes se conecten a cualquier dirección VIP del grupo. Es decir, durante el funcionamiento normal, la interfaz principal es la interfaz "activa" para el grupo.

De manera similar, durante el funcionamiento normal, cualquier interfaz de menor prioridad para el grupo HA actúa como interfaz de "respaldo". Estas interfaces de respaldo no se utilizan a menos que la interfaz principal (actualmente activa) deje de estar disponible.

Ver el estado actual del grupo HA de un nodo

Para ver si un nodo está asignado a un grupo de alta disponibilidad y determinar su estado actual, seleccione **NODOS > nodo**.

Si la pestaña **Descripción general** incluye una entrada para **Grupos de HA**, el nodo se asigna a los grupos de HA enumerados. El valor después del nombre del grupo es el estado actual del nodo en el grupo HA:

- **Activo:** El grupo HA está alojado actualmente en este nodo.
- **Copia de seguridad:** El grupo HA no está utilizando actualmente este nodo; esta es una interfaz de copia de seguridad.
- **Detenido:** El grupo HA no se puede alojar en este nodo porque el servicio de alta disponibilidad (keepalived) se detuvo manualmente.
- **Error:** El grupo HA no se puede alojar en este nodo debido a uno o más de los siguientes motivos:
 - El servicio Load Balancer (nginx-gw) no se está ejecutando en el nodo.
 - La interfaz eth0 o VIP del nodo está inactiva.
 - El nodo está caído.

En este ejemplo, el nodo de administración principal se ha agregado a dos grupos de alta disponibilidad. Este nodo es actualmente la interfaz activa para el grupo de clientes de administración y una interfaz de respaldo para el grupo de clientes de FabricPool .

DC1-ADM1 (Primary Admin Node) [🔗](#)

Overview Hardware Network Storage Load balancer Tasks

Node information [?](#)

Name:	DC1-ADM1
Type:	Primary Admin Node
ID:	ce00d9c8-8a79-4742-bdef-c9c658db5315
Connection state:	✔ Connected
Software version:	11.6.0 (build 20211207.1804.614bc17)
HA groups:	<div>Admin clients (Active)</div> <div>FabricPool clients (Backup)</div>
IP addresses:	<div>172.16.1.225 - eth0 (Grid Network)</div> <div>10.224.1.225 - eth1 (Admin Network)</div> <div>47.47.0.2, 47.47.1.225 - eth2 (Client Network)</div> <div>Show additional IP addresses ▼</div>

¿Qué sucede cuando falla la interfaz activa?

La interfaz que actualmente aloja las direcciones VIP es la interfaz activa. Si el grupo HA incluye más de una interfaz y la interfaz activa falla, las direcciones VIP se mueven a la primera interfaz de respaldo disponible en el orden de prioridad. Si esa interfaz falla, las direcciones VIP pasan a la siguiente interfaz de respaldo disponible, y así sucesivamente.

La conmutación por error se puede activar por cualquiera de estos motivos:

- El nodo en el que está configurada la interfaz deja de funcionar.
- El nodo en el que está configurada la interfaz pierde conectividad con todos los demás nodos durante al menos 2 minutos.
- La interfaz activa deja de funcionar.
- El servicio Load Balancer se detiene.
- El servicio de Alta Disponibilidad se detiene.



Es posible que la conmutación por error no se active por fallas de red externas al nodo que aloja la interfaz activa. De manera similar, la conmutación por error no es activada por los servicios del Administrador de red o del Administrador de inquilinos.

El proceso de conmutación por error generalmente toma sólo unos segundos y es lo suficientemente rápido como para que las aplicaciones cliente experimenten poco impacto y puedan confiar en los comportamientos de reintento normales para continuar la operación.

Cuando se resuelve la falla y vuelve a estar disponible una interfaz de mayor prioridad, las direcciones VIP se mueven automáticamente a la interfaz de mayor prioridad que esté disponible.

¿Cómo se utilizan los grupos HA?

Puede utilizar grupos de alta disponibilidad (HA) para proporcionar conexiones de alta disponibilidad a StorageGRID para datos de objetos y para uso administrativo.

- Un grupo HA puede proporcionar conexiones administrativas de alta disponibilidad al administrador de red o al administrador de inquilinos.
- Un grupo HA puede proporcionar conexiones de datos de alta disponibilidad para clientes S3.
- Un grupo HA que contiene solo una interfaz le permite proporcionar muchas direcciones VIP y configurar explícitamente direcciones IPv6.

Un grupo de alta disponibilidad solo puede proporcionar alta disponibilidad si todos los nodos incluidos en el grupo brindan los mismos servicios. Al crear un grupo de alta disponibilidad, agregue interfaces de los tipos de nodos que brindan los servicios que necesita.

- **Nodos de administración:** incluye el servicio Load Balancer y habilita el acceso al Grid Manager o al Tenant Manager.
- **Nodos de puerta de enlace:** incluye el servicio Load Balancer.

Propósito del grupo HA	Agregue nodos de este tipo al grupo HA
Acceso al Administrador de Red	<ul style="list-style-type: none">• Nodo de administración principal (Principal)• Nodos de administración no principales <p>Nota: El nodo de administración principal debe ser la interfaz principal. Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal.</p>
Acceso únicamente al administrador de inquilinos	<ul style="list-style-type: none">• Nodos de administración primarios o no primarios
Acceso de cliente S3: servicio Load Balancer	<ul style="list-style-type: none">• Nodos de administración• Nodos de puerta de enlace
Acceso de cliente S3 para "S3 Seleccionar"	<ul style="list-style-type: none">• Servicios de electrodomésticos• Nodos de software basados en VMware <p>Nota: Se recomiendan grupos HA cuando se utiliza S3 Select, pero no son obligatorios.</p>

Limitaciones del uso de grupos de alta disponibilidad con Grid Manager o Tenant Manager

Si falla un servicio de Grid Manager o Tenant Manager, no se activa la conmutación por error del grupo HA.

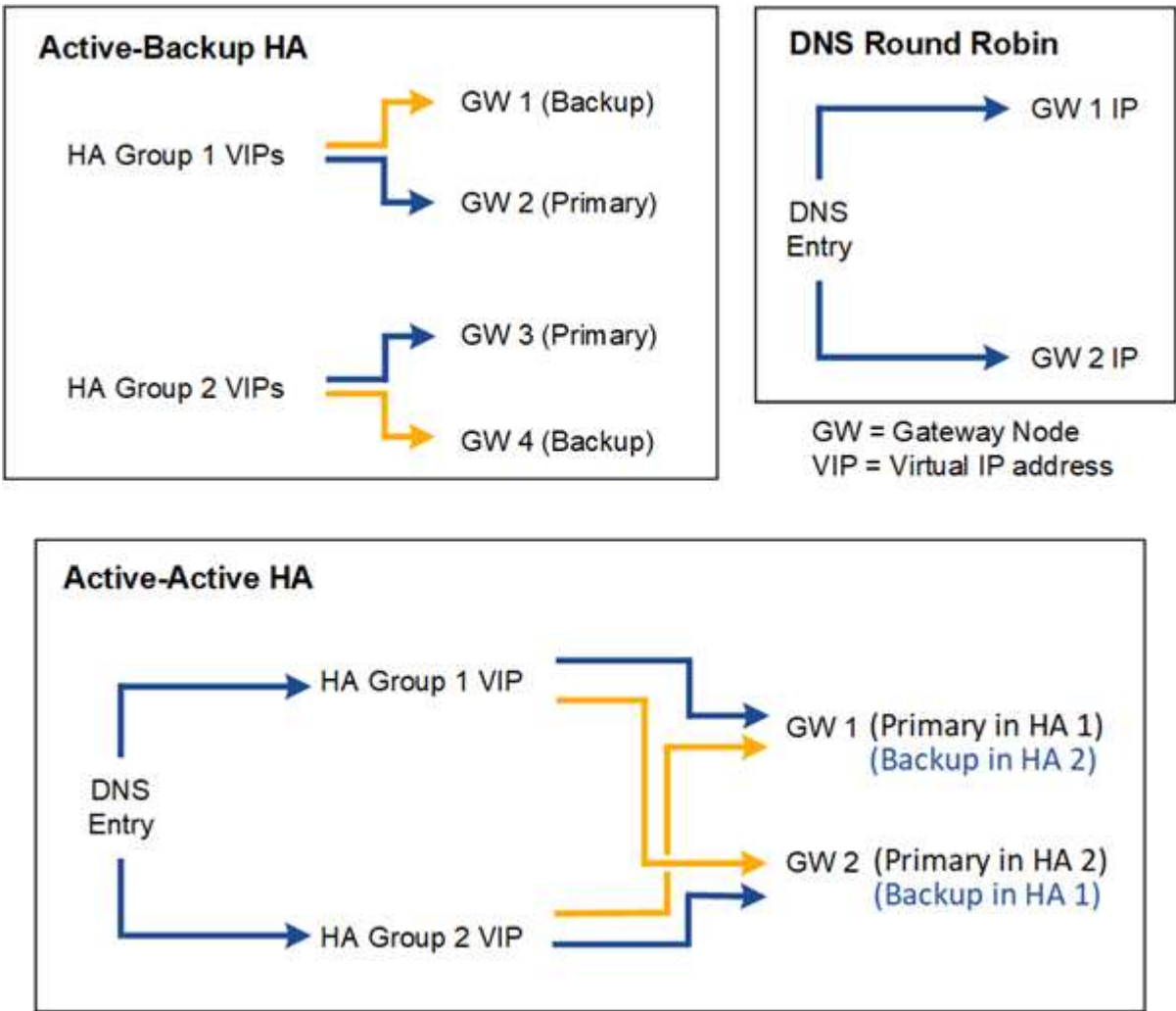
Si ha iniciado sesión en Grid Manager o Tenant Manager cuando se produce una conmutación por error, cerrará la sesión y deberá iniciar sesión nuevamente para reanudar su tarea.

Algunos procedimientos de mantenimiento no se pueden realizar cuando el nodo de administración principal no está disponible. Durante la conmutación por error, puede utilizar el Administrador de cuadrícula para supervisar su sistema StorageGRID .

Opciones de configuración para grupos de alta disponibilidad

Los siguientes diagramas proporcionan ejemplos de diferentes formas en las que se pueden configurar grupos de HA. Cada opción tiene ventajas y desventajas.

En los diagramas, el azul indica la interfaz principal en el grupo HA y el amarillo indica la interfaz de respaldo en el grupo HA.



La tabla resume los beneficios de cada configuración de HA que se muestra en el diagrama.

Configuración	Ventajas	Desventajas
Alta disponibilidad de respaldo activo	<ul style="list-style-type: none">• Administrado por StorageGRID sin dependencias externas.• Conmutación por error rápida.	<ul style="list-style-type: none">• Solo un nodo en un grupo HA está activo. Al menos un nodo por grupo HA estará inactivo.

Configuración	Ventajas	Desventajas
DNS Round Robin	<ul style="list-style-type: none"> • Aumento del rendimiento agregado. • No hay hosts inactivos. 	<ul style="list-style-type: none"> • Conmutación por error lenta, que podría depender del comportamiento del cliente. • Requiere configuración de hardware fuera de StorageGRID. • Necesita un control de salud implementado por el cliente.
HA activo-activo	<ul style="list-style-type: none"> • El tráfico se distribuye entre varios grupos de alta disponibilidad. • Alto rendimiento agregado que escala con la cantidad de grupos de HA. • Conmutación por error rápida. 	<ul style="list-style-type: none"> • Más complejo de configurar. • Requiere configuración de hardware fuera de StorageGRID. • Necesita un control de salud implementado por el cliente.

Configurar grupos de alta disponibilidad

Puede configurar grupos de alta disponibilidad (HA) para proporcionar acceso de alta disponibilidad a los servicios en los nodos de administración o los nodos de puerta de enlace.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["Permiso de acceso root"](#).
- Si planea utilizar una interfaz VLAN en un grupo HA, habrá creado la interfaz VLAN. Ver ["Configurar interfaces VLAN"](#).
- Si planea utilizar una interfaz de acceso para un nodo en un grupo de alta disponibilidad, ha creado la interfaz:
 - **Red Hat Enterprise Linux (antes de instalar el nodo):** ["Crear archivos de configuración de nodos"](#)
 - **Ubuntu o Debian (antes de instalar el nodo):** ["Crear archivos de configuración de nodos"](#)
 - **Linux (después de instalar el nodo):** ["Linux: Agregar interfaces troncales o de acceso a un nodo"](#)
 - **VMware (después de instalar el nodo):** ["VMware: Agregar interfaces troncales o de acceso a un nodo"](#)

Crear un grupo de alta disponibilidad

Cuando se crea un grupo de alta disponibilidad, se selecciona una o más interfaces y se organizan en orden de prioridad. Luego, asigna una o más direcciones VIP al grupo.

Una interfaz debe ser para que un nodo de puerta de enlace o un nodo de administración se incluya en un grupo de alta disponibilidad. Un grupo de HA solo puede usar una interfaz para un nodo determinado; sin embargo, se pueden usar otras interfaces para el mismo nodo en otros grupos de HA.

Acceder al asistente

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Grupos de alta disponibilidad**.
2. Seleccione **Crear**.

Introduzca detalles para el grupo HA

Pasos

1. Proporcione un nombre único para el grupo HA.
2. Opcionalmente, ingrese una descripción para el grupo HA.
3. Seleccione **Continuar**.

Agregar interfaces al grupo HA

Pasos

1. Seleccione una o más interfaces para agregar a este grupo de HA.

Utilice los encabezados de columna para ordenar las filas o ingrese un término de búsqueda para localizar interfaces más rápidamente.

Add interfaces to the HA group

Select one or more interfaces for this HA group. You can select only one interface for each node.

Total interface count: 4

	Node ?	Interface ?	Site ?	IPv4 subnet	Node type ?
<input type="checkbox"/>	DC1-ADM1-104-96	eth0 ?	DC1	10.96.104.0/22	Primary Admin Node
<input type="checkbox"/>	DC1-ADM1-104-96	eth2 ?	DC1	—	Primary Admin Node
<input type="checkbox"/>	DC2-ADM1-104-103	eth0 ?	DC2	10.96.104.0/22	Admin Node
<input type="checkbox"/>	DC2-ADM1-104-103	eth2 ?	DC2	—	Admin Node

0 interfaces selected



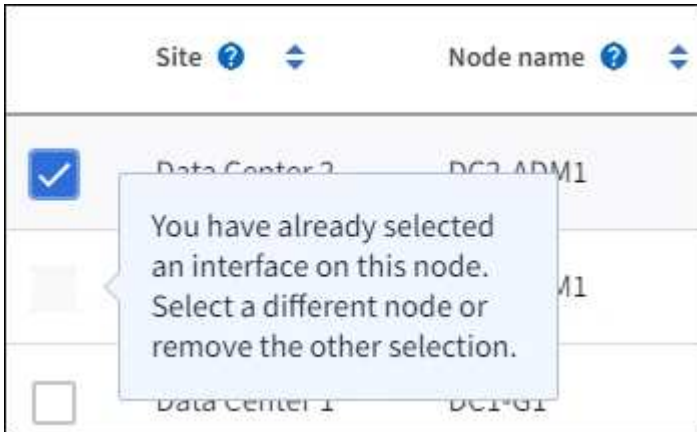
Después de crear una interfaz VLAN, espere hasta 5 minutos para que la nueva interfaz aparezca en la tabla.

Directrices para la selección de interfaces

- Debes seleccionar al menos una interfaz.
- Puede seleccionar solo una interfaz para un nodo.
- Si el grupo HA es para la protección de HA de los servicios del nodo de administración, que incluyen el administrador de red y el administrador de inquilinos, seleccione interfaces solo en los nodos de

administración.

- Si el grupo HA es para la protección de HA del tráfico del cliente S3, seleccione interfaces en los nodos de administración, los nodos de puerta de enlace o ambos.
- Si selecciona interfaces en diferentes tipos de nodos, aparece una nota informativa. Se le recuerda que si se produce una conmutación por error, es posible que los servicios proporcionados por el nodo previamente activo no estén disponibles en el nuevo nodo activo. Por ejemplo, un nodo de puerta de enlace de respaldo no puede brindar protección de alta disponibilidad a los servicios del nodo de administración. De manera similar, un nodo de administración de respaldo no puede realizar todos los procedimientos de mantenimiento que el nodo de administración principal puede proporcionar.
- Si no puede seleccionar una interfaz, su casilla de verificación estará deshabilitada. La información sobre herramientas proporciona más información.



- No puede seleccionar una interfaz si su valor de subred o puerta de enlace entra en conflicto con otra interfaz seleccionada.
- No puede seleccionar una interfaz configurada si no tiene una dirección IP estática.

2. Seleccione **Continuar**.

Determinar el orden de prioridad

Si el grupo HA incluye más de una interfaz, puede determinar cuál es la interfaz principal y cuáles son las interfaces de respaldo (conmutación por error). Si la interfaz principal falla, las direcciones VIP se mueven a la interfaz de mayor prioridad que esté disponible. Si esa interfaz falla, las direcciones VIP pasan a la siguiente interfaz de mayor prioridad que esté disponible, y así sucesivamente.

Pasos

1. Arrastre filas en la columna **Orden de prioridad** para determinar la interfaz principal y cualquier interfaz de respaldo.

La primera interfaz de la lista es la interfaz principal. La interfaz principal es la interfaz activa a menos que ocurra una falla.

Determine the priority order

Determine the primary interface and the backup (failover) interfaces for this HA group. Drag and drop rows or select the arrows.

Priority order ?	Node	Interface ?	Node type ?
1 (Primary interface)	⬆ DC1-ADM1-104-96	eth2	Primary Admin Node
2	⬆ DC2-ADM1-104-103	eth2	Admin Node



Si el grupo HA proporciona acceso al Administrador de red, debe seleccionar una interfaz en el Nodo de administración principal para que sea la interfaz principal. Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal.

2. Seleccione **Continuar**.

Introduzca direcciones IP

Pasos

1. En el campo **Subred CIDR**, especifique la subred VIP en notación CIDR: una dirección IPv4 seguida de una barra y la longitud de la subred (0-32).

La dirección de red no debe tener ningún bit de host configurado. Por ejemplo, 192.16.0.0/22.



Si utiliza un prefijo de 32 bits, la dirección de red VIP también sirve como dirección de puerta de enlace y dirección VIP.

Enter details for the HA group

Subnet CIDR ?

Specify the subnet in CIDR notation. The optional gateway IP and all VIPs must be in this subnet.

IPv4 address followed by a slash and the subnet length (0-32)

Gateway IP address (optional) ?

Optionally specify the IP address of the gateway, which must be in the subnet. If the subnet address length is 32, the gateway IP address is automatically set to the subnet IP.

Virtual IP address ?

Specify at least 1 and no more than 10 virtual IPs for the HA group. All virtual IPs must be in the same subnet. If the subnet length is 32, only one VIP is allowed, which is automatically set to the subnet/gateway IP.

[Add another IP address](#)

- De manera opcional, si algún cliente administrativo o inquilino de S3 accederá a estas direcciones VIP desde una subred diferente, ingrese la **dirección IP de puerta de enlace**. La dirección de la puerta de enlace debe estar dentro de la subred VIP.

Los usuarios clientes y administradores utilizarán esta puerta de enlace para acceder a las direcciones IP virtuales.

- Ingrese al menos una y no más de diez direcciones VIP para la interfaz activa en el grupo HA. Todas las direcciones VIP deben estar dentro de la subred VIP y todas estarán activas al mismo tiempo en la interfaz activa.

Debe proporcionar al menos una dirección IPv4. Opcionalmente, puede especificar direcciones IPv4 e IPv6 adicionales.

- Seleccione **Crear grupo HA** y seleccione **Finalizar**.

Se crea el grupo HA y ahora puede utilizar las direcciones IP virtuales configuradas.

Próximos pasos

Si va a utilizar este grupo HA para equilibrar la carga, cree un punto final del equilibrador de carga para determinar el puerto y el protocolo de red y para adjuntar los certificados necesarios. Ver "[Configurar los puntos finales del balanceador de carga](#)".

Editar un grupo de alta disponibilidad

Puede editar un grupo de alta disponibilidad (HA) para cambiar su nombre y descripción, agregar o eliminar interfaces, cambiar el orden de prioridad o agregar o actualizar direcciones IP virtuales.

Por ejemplo, es posible que necesite editar un grupo de alta disponibilidad si desea eliminar el nodo asociado

con una interfaz seleccionada en un procedimiento de desmantelamiento de sitio o nodo.

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Grupos de alta disponibilidad**.

La página Grupos de alta disponibilidad muestra todos los grupos de alta disponibilidad existentes.

2. Seleccione la casilla de verificación del grupo HA que desea editar.
3. Realice una de las siguientes acciones, según lo que desee actualizar:
 - Seleccione **Acciones > Editar dirección IP virtual** para agregar o eliminar direcciones VIP.
 - Seleccione **Acciones > Editar grupo de HA** para actualizar el nombre o la descripción del grupo, agregar o eliminar interfaces, cambiar el orden de prioridad o agregar o eliminar direcciones VIP.
4. Si seleccionó **Editar dirección IP virtual**:
 - a. Actualice las direcciones IP virtuales para el grupo HA.
 - b. Seleccione **Guardar**.
 - c. Seleccione **Finalizar**.
5. Si seleccionó **Editar grupo HA**:
 - a. Opcionalmente, actualice el nombre o la descripción del grupo.
 - b. Opcionalmente, seleccione o desmarque las casillas de verificación para agregar o eliminar interfaces.



Si el grupo HA proporciona acceso al Administrador de red, debe seleccionar una interfaz en el Nodo de administración principal para que sea la interfaz principal. Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal

- c. Opcionalmente, arrastre filas para cambiar el orden de prioridad de la interfaz principal y cualquier interfaz de respaldo para este grupo de HA.
- d. Opcionalmente, actualice las direcciones IP virtuales.
- e. Seleccione **Guardar** y luego seleccione **Finalizar**.

Eliminar un grupo de alta disponibilidad

Puede eliminar uno o más grupos de alta disponibilidad (HA) a la vez.



No se puede eliminar un grupo de alta disponibilidad si está vinculado a un punto final del equilibrador de carga. Para eliminar un grupo de HA, debe quitarlo de todos los puntos finales del balanceador de carga que lo utilicen.

Para evitar interrupciones del cliente, actualice cualquier aplicación cliente S3 afectada antes de eliminar un grupo de alta disponibilidad. Actualice cada cliente para conectarse utilizando otra dirección IP, por ejemplo, la dirección IP virtual de un grupo de HA diferente o la dirección IP que se configuró para una interfaz durante la instalación.

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Grupos de alta disponibilidad**.
2. Revise la columna **Puntos finales del balanceador de carga** para cada grupo de HA que desee eliminar. Si se enumeran puntos finales del balanceador de carga:

- a. Vaya a **CONFIGURACIÓN > Red > Puntos finales del balanceador de carga**.
 - b. Seleccione la casilla de verificación para el punto final.
 - c. Seleccione **Acciones > Editar modo de enlace de punto final**.
 - d. Actualice el modo de enlace para eliminar el grupo HA.
 - e. Seleccione **Guardar cambios**.
3. Si no se enumeran puntos finales del balanceador de carga, seleccione la casilla de verificación para cada grupo de alta disponibilidad que desee eliminar.
 4. Seleccione **Acciones > Eliminar grupo HA**.
 5. Revise el mensaje y seleccione **Eliminar grupo HA** para confirmar su selección.

Se eliminan todos los grupos HA que seleccionó. Aparece un banner de éxito verde en la página de grupos de alta disponibilidad.

Gestionar el equilibrio de carga

Consideraciones para el equilibrio de carga

Puede utilizar el equilibrio de carga para gestionar cargas de trabajo de ingesta y recuperación de clientes S3.

¿Qué es el equilibrio de carga?

Cuando una aplicación cliente guarda o recupera datos de un sistema StorageGRID, StorageGRID utiliza un equilibrador de carga para administrar la carga de trabajo de ingesta y recuperación. El equilibrio de carga maximiza la velocidad y la capacidad de conexión al distribuir la carga de trabajo entre múltiples nodos de almacenamiento.

El servicio StorageGRID Load Balancer está instalado en todos los nodos de administración y en todos los nodos de puerta de enlace y proporciona equilibrio de carga de capa 7. Realiza la terminación de seguridad de la capa de transporte (TLS) de las solicitudes de los clientes, inspecciona las solicitudes y establece nuevas conexiones seguras con los nodos de almacenamiento.

El servicio Load Balancer en cada nodo funciona de forma independiente al reenviar el tráfico del cliente a los nodos de almacenamiento. A través de un proceso de ponderación, el servicio Load Balancer dirige más solicitudes a los nodos de almacenamiento con mayor disponibilidad de CPU.



Si bien el servicio StorageGRID Load Balancer es el mecanismo de equilibrio de carga recomendado, es posible que desee integrar un equilibrador de carga de terceros. Para obtener más información, comuníquese con su representante de cuenta de NetApp o consulte ["TR-4626: Balanceadores de carga globales y de terceros de StorageGRID"](#).

¿Cuántos nodos de equilibrio de carga necesito?

Como práctica recomendada general, cada sitio en su sistema StorageGRID debe incluir dos o más nodos con el servicio Load Balancer. Por ejemplo, un sitio puede incluir dos nodos de puerta de enlace o un nodo de administración y un nodo de puerta de enlace. Asegúrese de que haya una infraestructura de red, hardware o virtualización adecuada para cada nodo de equilibrio de carga, independientemente de que utilice dispositivos de servicios, nodos físicos o nodos basados en máquinas virtuales (VM).

¿Qué es un punto final de balanceador de carga?

Un punto final del balanceador de carga define el puerto y el protocolo de red (HTTPS o HTTP) que las solicitudes de aplicaciones cliente entrantes y salientes utilizarán para acceder a aquellos nodos que contienen el servicio del balanceador de carga. El punto final también define el tipo de cliente (S3), el modo de enlace y, opcionalmente, una lista de inquilinos permitidos o bloqueados.

Para crear un punto final del balanceador de carga, seleccione **CONFIGURACIÓN > Red > Puntos finales del balanceador de carga** o complete el asistente de configuración de FabricPool y S3. Para obtener instrucciones:

- ["Configurar los puntos finales del balanceador de carga"](#)
- ["Utilice el asistente de configuración de S3"](#)
- ["Utilice el asistente de configuración de FabricPool"](#)

Consideraciones para el puerto

El puerto para un punto final del balanceador de carga tiene como valor predeterminado 10433 para el primer punto final que cree, pero puede especificar cualquier puerto externo no utilizado entre 1 y 65535. Si usa el puerto 80 o 443, el punto final utilizará el servicio Load Balancer solo en los nodos de puerta de enlace. Estos puertos están reservados en los nodos de administración. Si utiliza el mismo puerto para más de un punto final, debe especificar un modo de enlace diferente para cada punto final.

No se permiten puertos utilizados por otros servicios de la red. Ver el ["Referencia del puerto de red"](#).

Consideraciones para el protocolo de red

En la mayoría de los casos, las conexiones entre las aplicaciones cliente y StorageGRID deben utilizar el cifrado de seguridad de la capa de transporte (TLS). Se admite la conexión a StorageGRID sin cifrado TLS, pero no se recomienda, especialmente en entornos de producción. Al seleccionar el protocolo de red para el punto final del balanceador de carga StorageGRID, debe seleccionar **HTTPS**.

Consideraciones sobre los certificados de punto final del equilibrador de carga

Si selecciona **HTTPS** como protocolo de red para el punto final del balanceador de carga, deberá proporcionar un certificado de seguridad. Puede utilizar cualquiera de estas tres opciones al crear el punto final del equilibrador de carga:

- **Subir un certificado firmado (recomendado).** Este certificado puede estar firmado por una autoridad de certificación (CA) privada o de confianza pública. La mejor práctica es utilizar un certificado de servidor CA de confianza pública para proteger la conexión. A diferencia de los certificados generados, los certificados firmados por una CA se pueden rotar sin interrupciones, lo que puede ayudar a evitar problemas de vencimiento.

Debe obtener los siguientes archivos antes de crear el punto final del equilibrador de carga:

- El archivo de certificado de servidor personalizado.
- El archivo de clave privada del certificado de servidor personalizado.
- Opcionalmente, un paquete CA de los certificados de cada autoridad de certificación emisora intermedia.
- **Generar un certificado autofirmado.**
- **Utilice el certificado global StorageGRID S3.** Debe cargar o generar una versión personalizada de este certificado antes de poder seleccionarlo para el punto final del balanceador de carga. Ver ["Configurar](#)

¿Qué valores necesito?

Para crear el certificado, debe conocer todos los nombres de dominio y direcciones IP que las aplicaciones cliente S3 usarán para acceder al punto final.

La entrada **DN del sujeto** (nombre distinguido) del certificado debe incluir el nombre de dominio completo que la aplicación cliente utilizará para StorageGRID. Por ejemplo:

```
Subject DN:  
/C=Country/ST=State/O=Company, Inc./CN=s3.storagegrid.example.com
```

Según sea necesario, el certificado puede usar caracteres comodín para representar los nombres de dominio completos de todos los nodos de administración y nodos de puerta de enlace que ejecutan el servicio Load Balancer. Por ejemplo, `*.storagegrid.example.com` utiliza el comodín `*` para representar `adm1.storagegrid.example.com` y `gn1.storagegrid.example.com`.

Si planea utilizar solicitudes alojadas virtuales de estilo S3, el certificado también debe incluir una entrada **Nombre alternativo** para cada una. "[Nombre de dominio del punto final S3](#)" que haya configurado, incluidos los nombres comodín. Por ejemplo:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```



Si utiliza comodines para los nombres de dominio, revise la "[Pautas de refuerzo para certificados de servidor](#)".

También debe definir una entrada DNS para cada nombre en el certificado de seguridad.

¿Cómo gestiono los certificados que expiran?



Si el certificado utilizado para proteger la conexión entre la aplicación S3 y StorageGRID caduca, la aplicación podría perder temporalmente el acceso a StorageGRID.

Para evitar problemas de vencimiento de certificados, siga estas prácticas recomendadas:

- Supervise atentamente cualquier alerta que advierta sobre fechas de vencimiento de certificados próximas, como las alertas **Vencimiento del certificado del punto final del equilibrador de carga** y **Vencimiento del certificado del servidor global para la API de S3**.
- Mantenga siempre sincronizadas las versiones del certificado de StorageGRID y de la aplicación S3. Si reemplaza o renueva el certificado utilizado para un punto final del balanceador de carga, debe reemplazar o renovar el certificado equivalente utilizado por la aplicación S3.
- Utilice un certificado CA firmado públicamente. Si utiliza un certificado firmado por una CA, puede reemplazar certificados que estén próximos a vencer sin interrupciones.
- Si ha generado un certificado StorageGRID autofirmado y dicho certificado está a punto de caducar, debe reemplazarlo manualmente tanto en StorageGRID como en la aplicación S3 antes de que caduque el certificado existente.

Consideraciones para el modo de enlace

El modo de enlace le permite controlar qué direcciones IP se pueden usar para acceder a un punto final del balanceador de carga. Si un punto final utiliza un modo de enlace, las aplicaciones cliente solo pueden acceder al punto final si usan una dirección IP permitida o su nombre de dominio completo (FQDN) correspondiente. Las aplicaciones cliente que utilicen cualquier otra dirección IP o FQDN no pueden acceder al punto final.

Puede especificar cualquiera de los siguientes modos de enlace:

- **Global** (predeterminado): Las aplicaciones cliente pueden acceder al punto final utilizando la dirección IP de cualquier nodo de puerta de enlace o nodo de administración, la dirección IP virtual (VIP) de cualquier grupo de alta disponibilidad en cualquier red o un FQDN correspondiente. Utilice esta configuración a menos que necesite restringir la accesibilidad de un punto final.
- **IP virtuales de grupos HA**. Las aplicaciones cliente deben utilizar una dirección IP virtual (o FQDN correspondiente) de un grupo de alta disponibilidad.
- **Interfaces de nodo**. Los clientes deben utilizar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas.
- **Tipo de nodo**. Según el tipo de nodo que seleccione, los clientes deben usar la dirección IP (o FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o FQDN correspondiente) de cualquier nodo de puerta de enlace.

Consideraciones para el acceso de los inquilinos

El acceso de inquilinos es una función de seguridad opcional que le permite controlar qué cuentas de inquilinos de StorageGRID pueden usar un punto final del balanceador de carga para acceder a sus buckets. Puede permitir que todos los inquilinos accedan a un punto final (predeterminado) o puede especificar una lista de inquilinos permitidos o bloqueados para cada punto final.

Puede utilizar esta función para proporcionar un mejor aislamiento de seguridad entre los inquilinos y sus puntos finales. Por ejemplo, puede utilizar esta función para garantizar que los materiales altamente clasificados o de alto secreto propiedad de un inquilino permanezcan completamente inaccesibles para los demás inquilinos.



A los efectos del control de acceso, el inquilino se determina a partir de las claves de acceso utilizadas en la solicitud del cliente; si no se proporcionan claves de acceso como parte de la solicitud (como en el caso del acceso anónimo), se utiliza el propietario del depósito para determinar el inquilino.

Ejemplo de acceso de inquilinos

Para comprender cómo funciona esta característica de seguridad, considere el siguiente ejemplo:

1. Ha creado dos puntos finales de equilibrador de carga, de la siguiente manera:
 - Punto final **público**: utiliza el puerto 10443 y permite el acceso a todos los inquilinos.
 - Punto final **alto secreto**: utiliza el puerto 10444 y permite el acceso únicamente al inquilino **alto secreto**. Todos los demás inquilinos tienen bloqueado el acceso a este punto final.
2. El `top-secret.pdf` está en un cubo propiedad del inquilino **alto secreto**.

Para acceder a la `top-secret.pdf`, un usuario en el inquilino **Top secret** puede emitir una solicitud GET a `https://w.x.y.z:10444/top-secret.pdf`. Debido a que a este inquilino se le permite usar el punto final 10444, el usuario puede acceder al objeto. Sin embargo, si un usuario que pertenece a otro inquilino

emite la misma solicitud a la misma URL, recibirá inmediatamente un mensaje de acceso denegado. Se deniega el acceso incluso si las credenciales y la firma son válidas.

Disponibilidad de CPU

El servicio Load Balancer en cada nodo de administración y nodo de puerta de enlace funciona de forma independiente al reenviar tráfico S3 a los nodos de almacenamiento. A través de un proceso de ponderación, el servicio Load Balancer dirige más solicitudes a los nodos de almacenamiento con mayor disponibilidad de CPU. La información de carga de la CPU del nodo se actualiza cada pocos minutos, pero la ponderación podría actualizarse con mayor frecuencia. A todos los nodos de almacenamiento se les asigna un valor de peso base mínimo, incluso si un nodo informa una utilización del 100 % o no informa su utilización.

En algunos casos, la información sobre la disponibilidad de la CPU se limita al sitio donde se encuentra el servicio Load Balancer.

Configurar los puntos finales del balanceador de carga

Los puntos finales del balanceador de carga determinan los puertos y los protocolos de red que los clientes S3 pueden usar cuando se conectan al balanceador de carga StorageGRID en los nodos de puerta de enlace y de administración. También puede utilizar puntos finales para acceder al Administrador de red, al Administrador de inquilinos o a ambos.



Se han eliminado los detalles rápidos de esta versión del sitio de documentación. Ver ["Configurar conexiones de cliente S3 y Swift"](#).

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["Permiso de acceso root"](#).
- Usted ha revisado el ["Consideraciones para el equilibrio de carga"](#).
- Si anteriormente reasignó un puerto que desea utilizar para el punto final del balanceador de carga, debe ["Se eliminó la reasignación del puerto"](#).
- Ha creado todos los grupos de alta disponibilidad (HA) que planea utilizar. Se recomiendan los grupos HA, pero no son obligatorios. Ver ["Administrar grupos de alta disponibilidad"](#).
- Si el punto final del balanceador de carga será utilizado por ["Inquilinos de S3 para S3 Select"](#), no debe utilizar las direcciones IP o FQDN de ningún nodo físico. Solo se permiten dispositivos de servicios y nodos de software basados en VMware para los puntos finales del equilibrador de carga utilizados para S3 Select.
- Ha configurado todas las interfaces VLAN que planea utilizar. Ver ["Configurar interfaces VLAN"](#).
- Si está creando un punto final HTTPS (recomendado), tiene la información del certificado del servidor.



Los cambios en un certificado de punto final pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

- Para cargar un certificado, necesita el certificado del servidor, la clave privada del certificado y, opcionalmente, un paquete de CA.
- Para generar un certificado, necesita todos los nombres de dominio y direcciones IP que los clientes S3 usarán para acceder al punto final. También debes conocer el tema (Nombre Distinguido).

- Si desea utilizar el certificado API S3 de StorageGRID (que también se puede usar para conexiones directas a nodos de almacenamiento), ya ha reemplazado el certificado predeterminado con un certificado personalizado firmado por una autoridad de certificación externa. Ver "[Configurar certificados de API S3](#)".

Crear un punto final de balanceador de carga

Cada punto final del balanceador de carga del cliente S3 especifica un puerto, un tipo de cliente (S3) y un protocolo de red (HTTP o HTTPS). Los puntos finales del balanceador de carga de la interfaz de administración especifican un puerto, un tipo de interfaz y una red de cliente no confiable.

Acceder al asistente

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Puntos finales del balanceador de carga**.
2. Para crear un punto final para un cliente S3 o Swift, seleccione la pestaña **Cliente S3 o Swift**.
3. Para crear un punto final para acceder al Administrador de red, al Administrador de inquilinos o a ambos, seleccione la pestaña **Interfaz de administración**.
4. Seleccione **Crear**.

Ingrese los detalles del punto final

Pasos

1. Seleccione las instrucciones adecuadas para ingresar detalles para el tipo de punto final que desea crear.

Cliente S3 o Swift

Campo	Descripción
Nombre	Un nombre descriptivo para el punto final, que aparecerá en la tabla de la página Puntos finales del balanceador de carga.
Puerto	<p>El puerto StorageGRID que desea utilizar para equilibrar la carga. Este campo tiene como valor predeterminado 10433 para el primer punto final que cree, pero puede ingresar cualquier puerto externo no utilizado del 1 al 65535.</p> <p>Si ingresa 80 o 8443, el punto final se configura solo en los nodos de puerta de enlace, a menos que haya liberado el puerto 8443. Luego, puede usar el puerto 8443 como punto final S3, y el puerto se configurará tanto en los nodos de puerta de enlace como en los de administración.</p>
Tipo de cliente	El tipo de aplicación cliente que utilizará este punto final, ya sea S3 o Swift .
Protocolo de red	<p>El protocolo de red que utilizarán los clientes cuando se conecten a este punto final.</p> <ul style="list-style-type: none">• Seleccione HTTPS para una comunicación segura y cifrada con TLS (recomendado). Debe adjuntar un certificado de seguridad antes de poder guardar el punto final.• Seleccione HTTP para una comunicación menos segura y sin cifrar. Utilice HTTP únicamente para una cuadrícula que no sea de producción.

Interfaz de gestión

Campo	Descripción
Nombre	Un nombre descriptivo para el punto final, que aparecerá en la tabla de la página Puntos finales del balanceador de carga.
Puerto	<p>El puerto StorageGRID que desea utilizar para acceder al Administrador de Grid, al Administrador de inquilinos o a ambos.</p> <ul style="list-style-type: none">• Administrador de red: 8443• Gerente de inquilinos: 9443• Tanto el administrador de la red como el administrador de inquilinos: 443 <p>Nota: Puede utilizar estos puertos preestablecidos u otros puertos disponibles.</p>
Tipo de interfaz	Seleccione el botón de opción para la interfaz StorageGRID a la que accederá mediante este punto final.

Campo	Descripción
Red de clientes no confiables	<p>Seleccione Sí si este punto final debe ser accesible para redes de clientes que no son de confianza. De lo contrario, seleccione No.</p> <p>Cuando selecciona Sí, el puerto se abre en todas las redes de cliente que no son de confianza.</p> <p>Nota: Solo puede configurar un puerto para que esté abierto o cerrado para redes de clientes que no sean de confianza cuando crea el punto final del balanceador de carga.</p>

1. Seleccione **Continuar**.

Seleccionar un modo de enlace

Pasos

1. Seleccione un modo de enlace para el punto final para controlar cómo se accede a él utilizando cualquier dirección IP o utilizando direcciones IP e interfaces de red específicas.

Algunos modos de enlace están disponibles para puntos finales de cliente o puntos finales de interfaz de administración. Aquí se enumeran todos los modos para ambos tipos de puntos finales.

Modo	Descripción
Global (predeterminado para puntos finales del cliente)	<p>Los clientes pueden acceder al punto final utilizando la dirección IP de cualquier nodo de puerta de enlace o nodo de administración, la dirección IP virtual (VIP) de cualquier grupo de alta disponibilidad en cualquier red o un FQDN correspondiente.</p> <p>Utilice la configuración Global a menos que necesite restringir la accesibilidad de este punto final.</p>
IP virtuales de grupos de alta disponibilidad	<p>Los clientes deben usar una dirección IP virtual (o FQDN correspondiente) de un grupo de HA para acceder a este punto final.</p> <p>Todos los puntos finales con este modo de enlace pueden usar el mismo número de puerto, siempre que los grupos de HA que seleccione para los puntos finales no se superpongan.</p>
Interfaces de nodo	<p>Los clientes deben utilizar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas para acceder a este punto final.</p>
Tipo de nodo (solo puntos finales del cliente)	<p>Según el tipo de nodo que seleccione, los clientes deben usar la dirección IP (o FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o FQDN correspondiente) de cualquier nodo de puerta de enlace para acceder a este punto final.</p>

Modo	Descripción
Todos los nodos de administración (predeterminado para los puntos finales de la interfaz de administración)	Los clientes deben usar la dirección IP (o FQDN correspondiente) de cualquier nodo de administración para acceder a este punto final.

Si más de un punto final usa el mismo puerto, StorageGRID usa este orden de prioridad para decidir qué punto final usar: **IP virtuales de grupos de alta disponibilidad** > **Interfaces de nodo** > **Tipo de nodo** > **Global**.

Si está creando puntos finales de interfaz de administración, solo se permiten nodos de administración.

2. Si seleccionó **IP virtuales de grupos de HA**, seleccione uno o más grupos de HA.

Si está creando puntos finales de interfaz de administración, seleccione VIP asociados únicamente con nodos de administración.

3. Si seleccionó **Interfaces de nodo**, seleccione una o más interfaces de nodo para cada nodo de administración o nodo de puerta de enlace que desee asociar con este punto final.
4. Si seleccionó **Tipo de nodo**, seleccione Nodos de administración, que incluye tanto el nodo de administración principal como cualquier nodo de administración no principal, o Nodos de puerta de enlace.

Controlar el acceso de los inquilinos



Un punto final de interfaz de administración puede controlar el acceso de los inquilinos solo cuando el punto final tiene la [Tipo de interfaz del administrador de inquilinos](#).

Pasos

1. Para el paso **Acceso de inquilino**, seleccione una de las siguientes opciones:

Campo	Descripción
Permitir a todos los inquilinos (predeterminado)	Todas las cuentas de inquilinos pueden usar este punto final para acceder a sus depósitos. Debe seleccionar esta opción si aún no ha creado ninguna cuenta de inquilino. Después de agregar cuentas de inquilino, puede editar el punto final del balanceador de carga para permitir o bloquear cuentas específicas.
Permitir inquilinos seleccionados	Solo las cuentas de inquilinos seleccionadas pueden usar este punto final para acceder a sus depósitos.
Bloquear inquilinos seleccionados	Las cuentas de inquilinos seleccionadas no pueden usar este punto final para acceder a sus depósitos. Todos los demás inquilinos pueden utilizar este punto final.

2. Si está creando un punto final **HTTP**, no necesita adjuntar un certificado. Seleccione **Crear** para agregar el

nuevo punto final del balanceador de carga. Luego, ve a [Después de terminar](#) . De lo contrario, seleccione **Continuar** para adjuntar el certificado.

Adjuntar certificado

Pasos

1. Si está creando un punto final **HTTPS**, seleccione el tipo de certificado de seguridad que desea adjuntar al punto final.

El certificado protege las conexiones entre los clientes S3 y el servicio Load Balancer en los nodos de administración o de puerta de enlace.

- **Subir certificado.** Seleccione esta opción si tiene certificados personalizados para cargar.
- **Generar certificado.** Seleccione esta opción si tiene los valores necesarios para generar un certificado personalizado.
- **Utilice el certificado StorageGRID S3.** Seleccione esta opción si desea utilizar el certificado API S3 global, que también se puede usar para conexiones directas a nodos de almacenamiento.

No puede seleccionar esta opción a menos que haya reemplazado el certificado API S3 predeterminado, que está firmado por la CA de la red, con un certificado personalizado firmado por una autoridad de certificación externa. Ver "[Configurar certificados de API S3](#)".

- **Utilizar certificado de interfaz de administración.** Seleccione esta opción si desea utilizar el certificado de interfaz de administración global, que también se puede utilizar para conexiones directas a los nodos de administración.
2. Si no está utilizando el certificado StorageGRID S3, cargue o genere el certificado.

Subir certificado

a. Seleccione **Subir certificado**.

b. Cargue los archivos de certificado de servidor necesarios:

- **Certificado de servidor:** el archivo de certificado de servidor personalizado en codificación PEM.
- **Clave privada del certificado:** El archivo de clave privada del certificado del servidor personalizado(`.key`).



Las claves privadas EC deben tener 224 bits o más. Las claves privadas RSA deben tener 2048 bits o más.

- **Paquete CA:** un único archivo opcional que contiene los certificados de cada autoridad de certificación (CA) emisora intermedia. El archivo debe contener cada uno de los archivos de certificado CA codificados en PEM, concatenados en el orden de la cadena de certificados.

c. Expande **Detalles del certificado** para ver los metadatos de cada certificado que hayas cargado. Si cargó un paquete de CA opcional, cada certificado se muestra en su propia pestaña.

- Seleccione **Descargar certificado** para guardar el archivo de certificado o seleccione **Descargar paquete de CA** para guardar el paquete de certificados.

Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

- Seleccione **Copiar certificado PEM** o **Copiar paquete CA PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

d. Seleccione **Crear**. + Se crea el punto final del equilibrador de carga. El certificado personalizado se utiliza para todas las nuevas conexiones posteriores entre los clientes S3 o la interfaz de administración y el punto final.

Generar certificado

a. Seleccione **Generar certificado**.

b. Especifique la información del certificado:

Campo	Descripción
Nombre de dominio	Uno o más nombres de dominio completos para incluir en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
Propiedad intelectual	Una o más direcciones IP para incluir en el certificado.
Asunto (opcional)	Sujeto X.509 o nombre distinguido (DN) del propietario del certificado. Si no se ingresa ningún valor en este campo, el certificado generado utiliza el primer nombre de dominio o dirección IP como nombre común del sujeto (CN).

Campo	Descripción
Días válidos	Número de días después de su creación que expira el certificado.
Agregar extensiones de uso de claves	<p>Si se selecciona (predeterminado y recomendado), las extensiones de uso de clave y uso de clave extendido se agregan al certificado generado.</p> <p>Estas extensiones definen el propósito de la clave contenida en el certificado.</p> <p>Nota: Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes más antiguos cuando los certificados incluyan estas extensiones.</p>

c. Seleccione **Generar**.

d. Seleccione **Detalles del certificado** para ver los metadatos del certificado generado.

- Seleccione **Descargar certificado** para guardar el archivo del certificado.

Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

- Seleccione **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

e. Seleccione **Crear**.

Se crea el punto final del equilibrador de carga. El certificado personalizado se utiliza para todas las nuevas conexiones posteriores entre los clientes S3 o la interfaz de administración y este punto final.

Después de terminar

Pasos

1. Si utiliza un DNS, asegúrese de que el DNS incluya un registro para asociar el nombre de dominio completo (FQDN) de StorageGRID a cada dirección IP que los clientes usarán para realizar conexiones.

La dirección IP que ingrese en el registro DNS depende de si está utilizando un grupo HA de nodos de equilibrio de carga:

- Si ha configurado un grupo de alta disponibilidad, los clientes se conectarán a las direcciones IP virtuales de ese grupo de alta disponibilidad.
- Si no utiliza un grupo de alta disponibilidad, los clientes se conectarán al servicio StorageGRID Load Balancer mediante la dirección IP de un nodo de puerta de enlace o de administración.

También debe asegurarse de que el registro DNS haga referencia a todos los nombres de dominio de punto final requeridos, incluidos todos los nombres comodín.

2. Proporcionar a los clientes S3 la información necesaria para conectarse al punto final:

- Número de puerto
- Nombre de dominio completo o dirección IP
- Cualquier detalle del certificado requerido

Ver y editar puntos finales del balanceador de carga

Puede ver los detalles de los puntos finales del balanceador de carga existentes, incluidos los metadatos del certificado para un punto final seguro. Puede cambiar ciertas configuraciones para un punto final.

- Para ver información básica de todos los puntos finales del balanceador de carga, revise las tablas en la página Puntos finales del balanceador de carga.
- Para ver todos los detalles sobre un punto final específico, incluidos los metadatos del certificado, seleccione el nombre del punto final en la tabla. La información mostrada varía según el tipo de punto final y cómo esté configurado.

S3 load balancer endpoint

Port:	10443
Client type:	S3
Network protocol:	HTTPS
Binding mode:	Global
Endpoint ID:	3d02c126-9437-478c-8b24-08384401d3cb

[Remove](#)

Binding mode


Certificate

Tenant access (2 allowed)

You can select a different binding mode or change IP addresses for the current binding mode.

[Edit binding mode](#)

Binding mode: Global

 This endpoint uses the Global binding mode. Unless there are one or more overriding endpoints for the same port, clients can access this endpoint using the IP address of any Gateway Node, any Admin Node, or the virtual IP of any HA group on any network.


- Para editar un punto final, utilice el menú **Acciones** en la página Puntos finales del balanceador de carga.



Si pierde el acceso a Grid Manager mientras edita el puerto de un punto final de la interfaz de administración, actualice la URL y el puerto para recuperar el acceso.



Después de editar un punto final, es posible que deba esperar hasta 15 minutos para que los cambios se apliquen a todos los nodos.

Tarea	Menú de acciones	Página de detalles
Editar el nombre del punto final	<ul style="list-style-type: none"> a. Seleccione la casilla de verificación para el punto final. b. Seleccione Acciones > Editar nombre del punto final. c. Introduzca el nuevo nombre. d. Seleccione Guardar. 	<ul style="list-style-type: none"> a. Seleccione el nombre del punto final para mostrar los detalles. b. Seleccione el icono de edición  . c. Introduzca el nuevo nombre. d. Seleccione Guardar.
Editar el puerto del punto final	<ul style="list-style-type: none"> a. Seleccione la casilla de verificación para el punto final. b. Seleccione Acciones > Editar puerto de punto final c. Introduzca un número de puerto válido. d. Seleccione Guardar. 	<i>n / A</i>
Editar el modo de enlace del punto final	<ul style="list-style-type: none"> a. Seleccione la casilla de verificación para el punto final. b. Seleccione Acciones > Editar modo de enlace de punto final. c. Actualice el modo de enlace según sea necesario. d. Seleccione Guardar cambios. 	<ul style="list-style-type: none"> a. Seleccione el nombre del punto final para mostrar los detalles. b. Seleccione Editar modo de enlace. c. Actualice el modo de enlace según sea necesario. d. Seleccione Guardar cambios.
Editar el certificado del punto final	<ul style="list-style-type: none"> a. Seleccione la casilla de verificación para el punto final. b. Seleccione Acciones > Editar certificado de punto final. c. Cargue o genere un nuevo certificado personalizado o comience a utilizar el certificado S3 global, según sea necesario. d. Seleccione Guardar cambios. 	<ul style="list-style-type: none"> a. Seleccione el nombre del punto final para mostrar los detalles. b. Seleccione la pestaña Certificado. c. Seleccione Editar certificado. d. Cargue o genere un nuevo certificado personalizado o comience a utilizar el certificado S3 global, según sea necesario. e. Seleccione Guardar cambios.

Tarea	Menú de acciones	Página de detalles
Editar el acceso de los inquilinos	a. Seleccione la casilla de verificación para el punto final. b. Seleccione Acciones > Editar acceso de inquilino . c. Elija una opción de acceso diferente, seleccione o elimine inquilinos de la lista, o haga ambas cosas. d. Seleccione Guardar cambios .	a. Seleccione el nombre del punto final para mostrar los detalles. b. Seleccione la pestaña Acceso de inquilinos . c. Seleccione Editar acceso de inquilino . d. Elija una opción de acceso diferente, seleccione o elimine inquilinos de la lista, o haga ambas cosas. e. Seleccione Guardar cambios .

Eliminar puntos finales del balanceador de carga

Puede eliminar uno o más puntos finales mediante el menú **Acciones**, o puede eliminar un solo punto final desde la página de detalles.



Para evitar interrupciones del cliente, actualice cualquier aplicación cliente S3 afectada antes de eliminar un punto final del balanceador de carga. Actualice cada cliente para conectarse usando un puerto asignado a otro punto final del balanceador de carga. Asegúrese de actualizar también cualquier información del certificado requerida.



Si pierde el acceso a Grid Manager mientras elimina un punto final de la interfaz de administración, actualice la URL.

- Para eliminar uno o más puntos finales:
 - Desde la página Balanceador de carga, seleccione la casilla de verificación para cada punto final que desee eliminar.
 - Seleccione **Acciones > Eliminar**.
 - Seleccione **Aceptar**.
- Para eliminar un punto final de la página de detalles:
 - Desde la página Balanceador de carga, seleccione el nombre del punto final.
 - Seleccione **Eliminar** en la página de detalles.
 - Seleccione **Aceptar**.

Configurar nombres de dominio de puntos finales S3

Para admitir solicitudes de estilo alojado virtualmente S3, debe usar Grid Manager para configurar la lista de nombres de dominio de puntos finales S3 a los que se conectan los clientes S3.



No se admite el uso de una dirección IP para un nombre de dominio de punto final. Las versiones futuras evitarán esta configuración.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tienes ["permisos de acceso específicos"](#) .
- Ha confirmado que no hay ninguna actualización de la red en curso.



No realice ningún cambio en la configuración del nombre de dominio cuando haya una actualización de la red en curso.

Acerca de esta tarea

Para permitir que los clientes utilicen nombres de dominio de punto final S3, debe realizar todo lo siguiente:

- Utilice Grid Manager para agregar los nombres de dominio del punto final S3 al sistema StorageGRID .
- Asegúrese de que el ["Certificado que el cliente utiliza para conexiones HTTPS a StorageGRID"](#) Está firmado para todos los nombres de dominio que requiera el cliente.

Por ejemplo, si el punto final es `s3.company.com` , debe asegurarse de que el certificado utilizado para las conexiones HTTPS incluya el `s3.company.com` punto final y el nombre alternativo del sujeto (SAN) comodín del punto final: `*.s3.company.com` .

- Configurar el servidor DNS utilizado por el cliente. Incluya registros DNS para las direcciones IP que los clientes usan para realizar conexiones y asegúrese de que los registros hagan referencia a todos los nombres de dominio de punto final S3 requeridos, incluidos todos los nombres comodín.



Los clientes pueden conectarse a StorageGRID utilizando la dirección IP de un nodo de puerta de enlace, un nodo de administración o un nodo de almacenamiento, o conectándose a la dirección IP virtual de un grupo de alta disponibilidad. Debe comprender cómo se conectan las aplicaciones cliente a la red para incluir las direcciones IP correctas en los registros DNS.

Los clientes que utilizan conexiones HTTPS (recomendadas) a la red pueden usar cualquiera de estos certificados:

- Los clientes que se conectan a un punto final del equilibrador de carga pueden usar un certificado personalizado para ese punto final. Cada punto final del equilibrador de carga se puede configurar para reconocer diferentes nombres de dominio de punto final S3.
- Los clientes que se conectan a un punto final del balanceador de carga o directamente a un nodo de almacenamiento pueden personalizar el certificado API S3 global para incluir todos los nombres de dominio de punto final S3 requeridos.



Si no agrega nombres de dominio de punto final S3 y la lista está vacía, se deshabilita la compatibilidad con solicitudes de estilo alojado virtualmente S3.

Agregar un nombre de dominio de punto final S3

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Nombres de dominio de punto final S3**.
2. Introduzca el nombre de dominio en el campo **Nombre de dominio 1**. Seleccione **Agregar otro nombre de dominio** para agregar más nombres de dominio.

3. Seleccione **Guardar**.
4. Asegúrese de que los certificados de servidor que utilizan los clientes coincidan con los nombres de dominio de punto final S3 requeridos.
 - Si los clientes se conectan a un punto final del balanceador de carga que utiliza su propio certificado, ["Actualizar el certificado asociado con el punto final"](#) .
 - Si los clientes se conectan a un punto final del balanceador de carga que utiliza el certificado de API S3 global o directamente a los nodos de almacenamiento, ["actualizar el certificado API global de S3"](#) .
5. Agregue los registros DNS necesarios para garantizar que se puedan resolver las solicitudes de nombre de dominio del punto final.

Resultado

Ahora, cuando los clientes utilizan el punto final `bucket.s3.company.com` , el servidor DNS se resuelve en el punto final correcto y el certificado autentica el punto final como se esperaba.

Cambiar el nombre de un dominio de punto final S3

Si cambia un nombre utilizado por aplicaciones S3, las solicitudes de estilo alojado virtualmente fallarán.


Pasos

1. Seleccione **CONFIGURACIÓN > Red > Nombres de dominio de punto final S3**.
2. Seleccione el campo de nombre de dominio que desea editar y realice los cambios necesarios.
3. Seleccione **Guardar**.
4. Seleccione **Sí** para confirmar su cambio.

Eliminar un nombre de dominio de punto final S3

Si elimina un nombre utilizado por aplicaciones S3, las solicitudes de estilo alojado virtualmente fallarán.

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Nombres de dominio de punto final S3**.
2. Seleccione el icono de eliminar  junto al nombre de dominio.
3. Seleccione **Sí** para confirmar la eliminación.

Información relacionada

- ["Utilice la API REST de S3"](#)
- ["Ver direcciones IP"](#)
- ["Configurar grupos de alta disponibilidad"](#)

Resumen: Direcciones IP y puertos para conexiones de cliente

Para almacenar o recuperar objetos, las aplicaciones cliente S3 se conectan al servicio Load Balancer, que está incluido en todos los nodos de administración y nodos de puerta de enlace, o al servicio Local Distribution Router (LDR), que está incluido en todos los nodos de almacenamiento.

Las aplicaciones cliente pueden conectarse a StorageGRID utilizando la dirección IP de un nodo de la red y el número de puerto del servicio en ese nodo. Opcionalmente, puede crear grupos de alta disponibilidad (HA) de nodos de equilibrio de carga para proporcionar conexiones de alta disponibilidad que utilicen direcciones IP virtuales (VIP). Si desea conectarse a StorageGRID utilizando un nombre de dominio completo (FQDN) en lugar de una dirección IP o VIP, puede configurar entradas DNS.

Esta tabla resume las diferentes formas en que los clientes pueden conectarse a StorageGRID y las direcciones IP y los puertos que se utilizan para cada tipo de conexión. Si ya ha creado puntos finales de equilibrador de carga y grupos de alta disponibilidad (HA), consulte [Dónde encontrar direcciones IP](#) para localizar estos valores en el Administrador de cuadrícula.

Donde se establece la conexión	Servicio al que se conecta el cliente	Dirección IP	Puerto
Grupo HA	Balanceador de carga	Dirección IP virtual de un grupo de alta disponibilidad	Puerto asignado al punto final del balanceador de carga
Nodo de administración	Balanceador de carga	Dirección IP del nodo de administración	Puerto asignado al punto final del balanceador de carga
Nodo de puerta de enlace	Balanceador de carga	Dirección IP del nodo de enlace	Puerto asignado al punto final del balanceador de carga
Nodo de almacenamiento	LDR	Dirección IP del nodo de almacenamiento	Puertos S3 predeterminados: <ul style="list-style-type: none"> • HTTPS: 18082 • HTTP: 18084

URL de ejemplo

Para conectar una aplicación cliente al punto final del balanceador de carga de un grupo de alta disponibilidad de nodos de puerta de enlace, utilice una URL estructurada como se muestra a continuación:

```
https://VIP-of-HA-group:LB-endpoint-port
```

Por ejemplo, si la dirección IP virtual del grupo HA es 192.0.2.5 y el número de puerto del punto final del balanceador de carga es 10443, entonces una aplicación podría usar la siguiente URL para conectarse a StorageGRID:

```
https://192.0.2.5:10443
```

Dónde encontrar direcciones IP

1. Sign in en Grid Manager usando un ["navegador web compatible"](#).
2. Para encontrar la dirección IP de un nodo de la red:
 - a. Seleccione **NODOS**.

- b. Seleccione el nodo de administración, el nodo de puerta de enlace o el nodo de almacenamiento al que desea conectarse.
- c. Seleccione la pestaña **Descripción general**.
- d. En la sección Información del nodo, anote las direcciones IP del nodo.
- e. Seleccione **Mostrar más** para ver las direcciones IPv6 y las asignaciones de interfaces.

Puede establecer conexiones desde aplicaciones cliente a cualquiera de las direcciones IP de la lista:

- **eth0**: Red de cuadrícula
- **eth1**: Red de administración (opcional)
- **eth2**: Red de cliente (opcional)



Si está viendo un nodo de administración o un nodo de puerta de enlace y es el nodo activo en un grupo de alta disponibilidad, la dirección IP virtual del grupo de alta disponibilidad se muestra en eth2.

3. Para encontrar la dirección IP virtual de un grupo de alta disponibilidad:
 - a. Seleccione **CONFIGURACIÓN > Red > Grupos de alta disponibilidad**.
 - b. En la tabla, anote la dirección IP virtual del grupo HA.
4. Para encontrar el número de puerto de un punto final del balanceador de carga:
 - a. Seleccione **CONFIGURACIÓN > Red > Puntos finales del balanceador de carga**.
 - b. Anote el número de puerto del punto final que desea utilizar.



Si el número de puerto es 80 o 443, el punto final se configura solo en los nodos de puerta de enlace, porque esos puertos están reservados en los nodos de administración. Todos los demás puertos se configuran tanto en los nodos de puerta de enlace como en los nodos de administración.

- c. Seleccione el nombre del punto final de la tabla.
- d. Confirme que el **Tipo de cliente** (S3) coincida con la aplicación cliente que utilizará el punto final.

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.