Controla los cortafuegos

StorageGRID software

NetApp
July 23, 2026

Tabla de contenidos

Controla los cortafuegos

Controla el acceso a StorageGRID en un firewall externo

Puedes abrir o cerrar puertos específicos en el firewall externo.

Puedes controlar el acceso a las interfaces de usuario y a las API en los Admin Nodes de StorageGRID abriendo o cerrando puertos específicos en el firewall externo. Por ejemplo, es posible que quieras evitar que los inquilinos puedan conectarse al Grid Manager en el firewall, además de utilizar otros métodos para controlar el acceso al sistema.

Si quieres configurar el firewall interno de StorageGRID, consulta "Configura el cortafuegos interno".

Puerto	Descripción	${post_edited_translations.segment}
443	${post_edited_translations.segment}	Los navegadores web y los clientes de la API de gestión pueden acceder al Grid Manager, a la Grid Management API, al Tenant Manager y a la Tenant Management API. **Nota:** El puerto 443 también se utiliza para parte del tráfico interno.
8443	Puerto restringido de Grid Manager en los nodos de administración	• Los navegadores web y los clientes de la API de gestión pueden acceder al Grid Manager y a la Grid Management API mediante HTTPS. • ${post_edited_translations.segment} • Se rechazarán las solicitudes de contenido interno.
9443	Puerto restringido de Tenant Manager en los nodos de administración	• Los navegadores web y los clientes de la API de gestión pueden acceder al Tenant Manager y a la Tenant Management API mediante HTTPS. • Los navegadores web y los clientes de la API de gestión no pueden acceder al Grid Manager ni a la Grid Management API. • Se rechazarán las solicitudes de contenido interno.

El inicio de sesión único (SSO) no está disponible en los puertos restringidos de Grid Manager o Tenant Manager. Debes utilizar el puerto HTTPS predeterminado (443) si quieres que los usuarios se autentiquen con el inicio de sesión único.

Información relacionada

- "Inicia sesión en Grid Manager"
- "Crear cuenta de inquilino"
- "Comunicaciones externas"

Administra los controles internos de firewall en StorageGRID

StorageGRID incluye un cortafuegos interno en cada nodo que mejora la seguridad de tu grid al permitirte controlar el acceso de red al nodo. Usa el cortafuegos para evitar el acceso de red en todos los puertos excepto en los necesarios para tu implementación específica de grid. Los cambios de configuración que hagas en la página de control del cortafuegos se aplican a cada nodo.

${post_edited_translations.segment}

- **Lista de direcciones con privilegios**: utiliza esta pestaña para permitir el acceso seleccionado a los puertos cerrados. Puedes añadir direcciones IP o subredes en notación CIDR que puedan acceder a los puertos cerrados mediante la pestaña Gestionar acceso externo.
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

  La configuración de esta pestaña prevalece sobre la de la pestaña Gestionar acceso externo.

  - Un nodo con una red de clientes no fiable solo aceptará conexiones en los puertos de los puntos finales del equilibrador de carga configurados en dicho nodo (puntos finales globales, de interfaz de nodo y vinculados al tipo de nodo).
  - ${post_edited_translations.segment}
  - Cuando se consideran de confianza, se puede acceder a todos los puertos abiertos en la pestaña Gestionar acceso externo, así como a cualquier endpoint del equilibrador de carga abierto en la Client Network.

> La configuración que realices en una pestaña puede afectar a los cambios de acceso que realices en otra pestaña. Asegúrate de comprobar la configuración de todas las pestañas para garantizar que tu red funcione tal y como esperas.

Para configurar los controles del cortafuegos interno, consulta "Configura los controles del cortafuegos".

Para obtener más información sobre los firewalls externos y la seguridad de la red, consulta "Controla el acceso en el cortafuegos externo".

${post_edited_translations.segment}

La pestaña Privileged address list te permite registrar una o más direcciones IP para permitirles el acceso a los puertos de la grid que están cerrados. La pestaña Manage external access te permite cerrar el acceso externo a los puertos externos seleccionados o a todos los puertos externos abiertos (los puertos externos son aquellos a los que pueden acceder los nodos que no pertenecen a la grid de forma predeterminada). A menudo puedes utilizar estas dos pestañas juntas para personalizar el acceso exacto a la red que necesitas permitir para tu grid.

> ${post_edited_translations.segment}

Ejemplo 1: usa un servidor de enlace para tareas de mantenimiento

Supón que quieres usar un jump host (un host con seguridad reforzada) para la administración de la red. Podrías seguir estos pasos generales:

1. Utiliza la pestaña «Lista de direcciones privilegiadas» para añadir la dirección IP del jump host.
2. ${post_edited_translations.segment}

> Añade la dirección IP privilegiada antes de bloquear los puertos 443 y 8443. Cualquier usuario que esté conectado actualmente a un puerto bloqueado, incluido tú, perderá el acceso a Grid Manager a menos que su dirección IP se haya añadido a la lista de direcciones privilegiadas.

Después de guardar tu configuración, todos los puertos externos del Admin Node de tu grid se bloquearán para todos los hosts, excepto para el jump host. Luego puedes usar el jump host para realizar tareas de mantenimiento en tu grid de forma más segura.

${post_edited_translations.segment}

Supongamos que quieres bloquear los puertos sensibles y el servicio en ese puerto. Podrías seguir estos pasos generales:

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}

> Añade la dirección IP privilegiada antes de bloquear el acceso a cualquier puerto asignado para acceder a Grid Manager y Tenant Manager (los puertos preestablecidos son 443 y 8443). Cualquier usuario que esté conectado actualmente a un puerto bloqueado, incluido tú, perderá el acceso a Grid Manager a menos que su dirección IP se haya añadido a la lista de direcciones privilegiadas.

Después de que guardes tu configuración, el puerto sensible y el servicio en ese puerto estarán disponibles para los hosts en la lista de direcciones privilegiadas. A todos los demás hosts se les negará el acceso al servicio sin importar desde qué interfaz provenga la solicitud.

Ejemplo 3: desactivar el acceso a los servicios que no se utilizan

A nivel de red, puedes desactivar algunos servicios que no tengas previsto utilizar. Por ejemplo, para bloquear el tráfico de clientes HTTP S3, usarías el interruptor de la pestaña Manage external access para bloquear el puerto 18084.

${post_edited_translations.segment}

Si utilizas una red de clientes, puedes ayudar a proteger StorageGRID de ataques hostiles aceptando el tráfico entrante de clientes solo en los endpoints configurados explícitamente.

De forma predeterminada, la red de clientes de cada nodo de grid es de *confianza*. Es decir, de forma predeterminada, StorageGRID confía en las conexiones entrantes a cada nodo de grid en todos los "puertos externos disponibles".

Puedes reducir la amenaza de ataques hostiles contra tu sistema StorageGRID especificando que la Client Network de cada nodo sea *untrusted*. Si la Client Network de un nodo es untrusted, el nodo solo acepta conexiones entrantes en los puertos configurados explícitamente como endpoints del load balancer. Consulta "Configura los puntos de conexión del equilibrador de carga" y "Configura los controles del cortafuegos".

Ejemplo 1: el nodo de puerta de enlace solo acepta solicitudes HTTPS S3

Supongamos que quieres que un nodo de puerta de enlace rechace todo el tráfico entrante en la red del cliente, excepto las solicitudes HTTPS S3. Para ello, deberías seguir estos pasos generales:

1. Desde la página "${post_edited_translations.segment}", configura un endpoint del equilibrador de carga para S3 sobre HTTPS en el puerto 443.
2. En la página de control del cortafuegos, selecciona No fiable para indicar que la Client Network en el Gateway Node no es fiable.

${post_edited_translations.segment}

${post_edited_translations.segment}

Supongamos que quieres habilitar el tráfico saliente de los servicios de la plataforma S3 desde un nodo de almacenamiento, pero quieres impedir cualquier conexión entrante a ese nodo de almacenamiento desde la red del cliente. Realizarías este paso general:

- ${post_edited_translations.segment}

${post_edited_translations.segment}

Ejemplo 3: limitar el acceso a Grid Manager a una subred

Supongamos que quieres permitir el acceso a Grid Manager únicamente en una subred concreta. Realiza los siguientes pasos:

1. Conecta la red de clientes de tus nodos de administración a la subred.
2. Utiliza la pestaña Untrusted Client Network para configurar la Client Network como no fiable.
3. Cuando creas un punto de conexión del equilibrador de carga de la interfaz de gestión, introduce el puerto y selecciona la interfaz de gestión a la que accederá el puerto.
4. ${post_edited_translations.segment}
5. Utiliza la pestaña «Gestionar acceso externo» para bloquear todos los puertos externos (con o sin direcciones IP privilegiadas configuradas para los hosts fuera de esa subred).

Una vez que guardes tu configuración, solo los hosts de la subred que especificaste podrán acceder al Grid Manager. Todos los demás hosts quedarán bloqueados.

Configura el firewall interno de StorageGRID

Puedes configurar el firewall de StorageGRID para controlar el acceso de red a puertos específicos en tus nodos de StorageGRID.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes "permisos de acceso específicos".
- Has revisado la información en "Gestiona los controles del cortafuegos" y "${post_edited_translations.segment}".
- ${post_edited_translations.segment}

${post_edited_translations.segment}

Acerca de esta tarea

StorageGRID incluye un cortafuegos interno en cada nodo que te permite abrir o cerrar algunos de los puertos de los nodos de tu grid. Puedes usar las pestañas de control del cortafuegos para abrir o cerrar los puertos que están abiertos por defecto en la Grid Network, Admin Network y Client Network. También puedes crear una lista de direcciones IP privilegiadas que pueden acceder a los puertos del grid que estén cerrados. Si estás usando una Client Network, puedes especificar si un nodo confía en el tráfico entrante de la Client Network y puedes configurar el acceso a puertos específicos en la Client Network.

Limitar el número de puertos abiertos a direcciones IP fuera de tu grid a solo aquellos que sean absolutamente necesarios mejora la seguridad de tu grid. Usas la configuración de cada una de las tres pestañas de control del Firewall para asegurarte de que solo estén abiertos los puertos necesarios.

Para obtener más información sobre el uso de los controles del firewall, incluidos algunos ejemplos, consulta "Gestiona los controles del cortafuegos".

Para obtener más información sobre los firewalls externos y la seguridad de la red, consulta "Controla el acceso en el cortafuegos externo".

Accede a los controles del cortafuegos

Pasos

1. Selecciona **Configuración** > **Seguridad** > **Control del cortafuegos**.

   Las tres pestañas de esta página se describen en "Gestiona los controles del cortafuegos".

2. Selecciona cualquier pestaña para configurar los controles del cortafuegos.

   Puedes utilizar estas pestañas en cualquier orden. Las configuraciones que establezcas en una pestaña no limitan lo que puedes hacer en las demás; sin embargo, los cambios de configuración que realices en una pestaña podrían modificar el comportamiento de los puertos configurados en otras pestañas.

Lista de direcciones privilegiadas

La pestaña «Lista de direcciones privilegiadas» sirve para conceder a los hosts acceso a los puertos que están cerrados por defecto o que se han cerrado mediante la configuración de la pestaña «Manage external access».

Las direcciones IP y subredes con privilegios no tienen acceso al grid interno de forma predeterminada. Además, los endpoints del equilibrador de carga y los puertos adicionales que abras en la pestaña Lista de direcciones con privilegios seguirán estando accesibles aunque los bloquees en la pestaña Administrar acceso externo.

La configuración de la pestaña «Lista de direcciones privilegiadas» no puede anular la configuración de la pestaña «Red de clientes no fiables».

Pasos

1. En la pestaña «Lista de direcciones privilegiadas», introduce la dirección o la subred IP a la que quieres conceder acceso a los puertos cerrados.
2. Si lo deseas, selecciona **Add another IP address or subnet in CIDR notation** para añadir clientes con

privilegios adicionales.

Agrega la menor cantidad posible de direcciones a la lista de direcciones privilegiadas.

3. Si lo deseas, selecciona **Permitir que las direcciones IP con privilegios accedan a los puertos internos de StorageGRID**. Consulta "Puertos internos de StorageGRID".

Esta opción elimina algunas protecciones para los servicios internos. Si es posible, déjala desactivada.

4. Selecciona **Guardar**.

Gestiona el acceso externo

Cuando se cierra un puerto en la pestaña Gestionar acceso externo, el puerto no puede ser accedido por ninguna dirección IP que no sea de la grid, a menos que añadas la dirección IP a la lista de direcciones privilegiadas. Solo puedes cerrar los puertos que están abiertos por defecto, y solo puedes abrir los puertos que hayas cerrado.

La configuración de la pestaña Manage external access no puede anular la configuración de la pestaña Untrusted Client Network. Por ejemplo, si un nodo no es de confianza, el puerto SSH/22 se bloquea en la Client Network aunque esté abierto en la pestaña Manage external access. La configuración de la pestaña Untrusted Client Network anula los puertos cerrados (como 443, 8443, 9443) en la Client Network.

Pasos

1. Selecciona **Gestionar acceso externo**. La pestaña muestra una tabla con todos los puertos externos (puertos a los que pueden acceder por defecto los nodos que no forman parte del grid) de los nodos de tu grid.
2. Configura los puertos que quieras abrir y cerrar utilizando las siguientes opciones:
   - ${post_edited_translations.segment}
   - Selecciona **Abrir todos los puertos mostrados** para abrir todos los puertos que aparecen en la tabla.
   - ${post_edited_translations.segment}

Si cierras los puertos 443 u 8443 de Grid Manager, cualquier usuario que esté conectado en ese momento a un puerto bloqueado, incluido tú, perderá el acceso a Grid Manager a menos que su dirección IP se haya añadido a la lista de direcciones privilegiadas.

Utiliza la barra de desplazamiento situada a la derecha de la tabla para asegurarte de que has visto todos los puertos disponibles. Utiliza el campo de búsqueda para encontrar la configuración de cualquier puerto externo introduciendo un número de puerto. Puedes introducir un número de puerto parcial. Por ejemplo, si introduces **2**, se mostrarán todos los puertos que tengan la cadena "2" como parte de su nombre.

3. Selecciona **Guardar**

${post_edited_translations.segment}

Si la red de cliente de un nodo no es de confianza, el nodo solo acepta tráfico entrante en los puertos configurados como puntos finales del equilibrador de carga y, opcionalmente, en los puertos adicionales que selecciones en esta pestaña. También puedes utilizar esta pestaña para especificar la configuración predeterminada para los nuevos nodos añadidos en una ampliación.

Las conexiones de los clientes existentes podrían fallar si no se han configurado los endpoints del equilibrador de carga.

${post_edited_translations.segment}

Pasos

1. Selecciona **Red de cliente no fiable**.
2. En la sección «Establecer valor predeterminado para nuevos nodos», especifica cuál debe ser la configuración predeterminada cuando se añadan nuevos nodos a la grid en un procedimiento de ampliación.

   - **De confianza** (por defecto): Cuando se añade un nodo en una ampliación, su Client Network es de confianza.
   - **No fiable**: Cuando se añade un nodo en una ampliación, su red de cliente no es fiable.

     Si lo necesitas, puedes volver a esta pestaña para cambiar la configuración de un nodo nuevo concreto.

     ${post_edited_translations.segment}

3. Utiliza las siguientes opciones para seleccionar los nodos que solo deben permitir conexiones de clientes en los puntos finales del equilibrador de carga configurados explícitamente o en puertos adicionales seleccionados:

   - Selecciona **Marcar como no fiable los nodos mostrados** para añadir todos los nodos que aparecen en la tabla a la lista de Red de clientes no fiables.
   - Selecciona **Confiar en los nodos mostrados** para eliminar todos los nodos que aparecen en la tabla de la lista de Untrusted Client Network.
   - Utiliza el botón de alternancia situado junto a cada nodo para configurar la red del cliente como de confianza o no de confianza para el nodo seleccionado.

     ${post_edited_translations.segment}

     Utiliza la barra de desplazamiento situada a la derecha de la tabla para asegurarte de que has visto todos los nodos disponibles. Utiliza el campo de búsqueda para encontrar la configuración de cualquier nodo introduciendo el nombre de nodo. Puedes introducir un nombre parcial. Por ejemplo, si introduces **GW**, se mostrarán todos los nodos que tengan la cadena "GW" como parte de su nombre.

4. Selecciona **Guardar**.

   La nueva configuración del cortafuegos se aplica y se hace efectiva de forma inmediata. Las conexiones de los clientes existentes podrían fallar si no se han configurado los endpoints del balanceador de carga.