Controlar cortafuegos

StorageGRID software

NetApp
December 03, 2025

Tabla de contenidos

Controlar cortafuegos

Controlar el acceso al firewall externo

Puede abrir o cerrar puertos específicos en el firewall externo.

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

Si desea configurar el firewall interno de StorageGRID , consulte"Configurar el firewall interno" .

Puerto	Descripción	Si el puerto está abierto…
443	Puerto HTTPS predeterminado para nodos de administración	Los navegadores web y los clientes de API de administración pueden acceder al Administrador de Grid, la API de administración de Grid, el Administrador de inquilinos y la API de administración de inquilinos. **Nota:** El puerto 443 también se utiliza para cierto tráfico interno.
8443	Puerto de Grid Manager restringido en los nodos de administración	• Los navegadores web y los clientes de API de administración pueden acceder al Administrador de Grid y a la API de administración de Grid mediante HTTPS. • Los navegadores web y los clientes de API de administración no pueden acceder al Administrador de inquilinos ni a la API de administración de inquilinos. • Las solicitudes de contenido interno serán rechazadas.
9443	Puerto de administrador de inquilinos restringido en nodos de administración	• Los navegadores web y los clientes de API de administración pueden acceder al Administrador de inquilinos y a la API de administración de inquilinos mediante HTTPS. • Los navegadores web y los clientes de API de administración no pueden acceder al Administrador de Grid ni a la API de administración de Grid. • Las solicitudes de contenido interno serán rechazadas.

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

Información relacionada

- "Sign in en el Administrador de cuadrícula"
- "Crear una cuenta de inquilino"
- "Comunicaciones externas"

Administrar los controles internos del firewall

StorageGRID incluye un firewall interno en cada nodo que mejora la seguridad de su red al permitirle controlar el acceso de la red al nodo. Utilice el firewall para evitar el acceso a la red en todos los puertos excepto aquellos necesarios para su implementación de red específica. Los cambios de configuración que realice en la página de control del Firewall se implementarán en cada nodo.

Utilice las tres pestañas de la página de control de Firewall para personalizar el acceso que necesita para su red.

- **Lista de direcciones privilegiadas**: utilice esta pestaña para permitir el acceso seleccionado a puertos cerrados. Puede agregar direcciones IP o subredes en notación CIDR que puedan acceder a puertos cerrados mediante la pestaña Administrar acceso externo.
- **Administrar acceso externo**: utilice esta pestaña para cerrar puertos que están abiertos de forma predeterminada o reabrir puertos previamente cerrados.
- **Red de cliente no confiable**: utilice esta pestaña para especificar si un nodo confía en el tráfico entrante de la red de cliente.

  La configuración de esta pestaña anula la configuración de la pestaña Administrar acceso externo.

  - Un nodo con una red de cliente no confiable solo aceptará conexiones en los puertos de punto final del balanceador de carga configurados en ese nodo (puntos finales globales, de interfaz de nodo y enlazados al tipo de nodo).
  - Los puertos finales del equilibrador de carga *son los únicos puertos abiertos* en redes de cliente que no son de confianza, independientemente de la configuración en la pestaña Administrar redes externas.
  - Cuando es confiable, todos los puertos abiertos en la pestaña Administrar acceso externo son accesibles, así como también cualquier punto final del balanceador de carga abierto en la red del cliente.

> Las configuraciones que realice en una pestaña pueden afectar los cambios de acceso que realice en otra pestaña. Asegúrese de verificar la configuración en todas las pestañas para asegurarse de que su red se comporte de la manera esperada.

Para configurar los controles internos del firewall, consulte"Configurar los controles del firewall" .

Para obtener más información sobre firewalls externos y seguridad de red, consulte"Controlar el acceso al firewall externo" .

Lista de direcciones privilegiadas y pestañas para administrar acceso externo

La pestaña Lista de direcciones privilegiadas le permite registrar una o más direcciones IP a las que se les concede acceso a los puertos de la red que están cerrados. La pestaña Administrar acceso externo le permite

cerrar el acceso externo a puertos externos seleccionados o a todos los puertos externos abiertos (los puertos externos son puertos a los que pueden acceder los nodos que no pertenecen a la red de manera predeterminada). Estas dos pestañas a menudo se pueden usar juntas para personalizar el acceso de red exacto que necesita permitir para su red.

> Las direcciones IP privilegiadas no tienen acceso al puerto de la red interna de forma predeterminada.

Ejemplo 1: Utilizar un host de salto para tareas de mantenimiento

Supongamos que desea utilizar un host de salto (un host con seguridad reforzada) para la administración de la red. Podrías utilizar estos pasos generales:

1. Utilice la pestaña Lista de direcciones privilegiadas para agregar la dirección IP del host de salto.
2. Utilice la pestaña Administrar acceso externo para bloquear todos los puertos.

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

Después de guardar su configuración, todos los puertos externos en el nodo de administración de su red se bloquearán para todos los hosts excepto el host de salto. Luego, puede utilizar el host de salto para realizar tareas de mantenimiento en su red de forma más segura.

Ejemplo 2: Bloquear puertos sensibles

Supongamos que desea bloquear puertos sensibles y el servicio en ese puerto (por ejemplo, SSH en el puerto 22). Podrías utilizar los siguientes pasos generales:

1. Utilice la pestaña Lista de direcciones privilegiadas para otorgar acceso solo a los hosts que necesitan acceso al servicio.
2. Utilice la pestaña Administrar acceso externo para bloquear todos los puertos.

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

Después de guardar su configuración, el puerto 22 y el servicio SSH 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 de qué interfaz provenga la solicitud.

Ejemplo 3: Deshabilitar el acceso a servicios no utilizados

A nivel de red, podrías deshabilitar algunos servicios que no deseas utilizar. Por ejemplo, para bloquear el tráfico del cliente HTTP S3, deberá utilizar el interruptor en la pestaña Administrar acceso externo para bloquear el puerto 18084.

Pestaña Redes de clientes no confiables

Si utiliza una red de cliente, puede ayudar a proteger StorageGRID de ataques hostiles al aceptar tráfico de

cliente entrante solo en puntos finales configurados explícitamente.

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

Puede reducir la amenaza de ataques hostiles en su sistema StorageGRID especificando que la red de cliente en cada nodo sea *no confiable*. Si la red de cliente de un nodo no es confiable, el nodo solo acepta conexiones entrantes en puertos configurados explícitamente como puntos finales del balanceador de carga. Ver"Configurar los puntos finales del balanceador de carga" y"Configurar los controles del firewall" .

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

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

1. Desde"Puntos finales del balanceador de carga" página, configure un punto final de balanceador de carga para S3 sobre HTTPS en el puerto 443.
2. Desde la página de control de Firewall, seleccione No confiable para especificar que la red de cliente en el nodo de puerta de enlace no es confiable.

Después de guardar su configuración, se descarta todo el tráfico entrante en la red de cliente del nodo de puerta de enlace, excepto las solicitudes HTTPS S3 en el puerto 443 y las solicitudes de eco ICMP (ping).

Ejemplo 2: El nodo de almacenamiento envía solicitudes de servicios de la plataforma S3

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

- Desde la pestaña Redes de clientes no confiables de la página de control de Firewall, indique que la red de clientes en el nodo de almacenamiento no es confiable.

Después de guardar su configuración, el nodo de almacenamiento ya no acepta tráfico entrante en la red del cliente, pero continúa permitiendo solicitudes salientes a los destinos de servicios de plataforma configurados.

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

Supongamos que desea permitir el acceso a Grid Manager solo en una subred específica. Realizarías los siguientes pasos:

1. Conecte la red de cliente de sus nodos de administración a la subred.
2. Utilice la pestaña Red de cliente no confiable para configurar la red de cliente como no confiable.
3. Cuando crea un punto final de balanceador de carga de interfaz de administración, ingrese el puerto y seleccione la interfaz de administración a la que accederá el puerto.
4. Seleccione **Sí** para Red de cliente no confiable.
5. Utilice la pestaña Administrar acceso externo para bloquear todos los puertos externos (con o sin direcciones IP privilegiadas configuradas para hosts fuera de esa subred).

Después de guardar su configuración, solo los hosts en la subred que especificó podrán acceder al Administrador de Grid. Todos los demás hosts están bloqueados.

Configurar el firewall interno

Puede configurar el firewall de StorageGRID para controlar el acceso de red a puertos específicos en sus nodos de StorageGRID .

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tienes"permisos de acceso específicos" .
- Has revisado la información en"Administrar los controles del firewall" y"Pautas para establecer redes" .
- Si desea que un nodo de administración o un nodo de puerta de enlace acepte tráfico entrante solo en puntos finales configurados explícitamente, debe definir los puntos finales del equilibrador de carga.

> Al cambiar la configuración de la red del cliente, las conexiones de cliente existentes podrían fallar si no se han configurado los puntos finales del balanceador de carga.

Acerca de esta tarea

StorageGRID incluye un firewall interno en cada nodo que le permite abrir o cerrar algunos de los puertos en los nodos de su red. Puede utilizar las pestañas de control de Firewall para abrir o cerrar puertos que están abiertos de manera predeterminada en la red de cuadrícula, la red de administración y la red de cliente. También puede crear una lista de direcciones IP privilegiadas que pueden acceder a los puertos de la red que están cerrados. Si está utilizando una red de cliente, puede especificar si un nodo confía en el tráfico entrante de la red de cliente y puede configurar el acceso a puertos específicos en la red de cliente.

Limitar la cantidad de puertos abiertos a direcciones IP fuera de su red a solo aquellos que sean absolutamente necesarios mejora la seguridad de su red. Utilice la configuración de cada una de las tres pestañas de control del Firewall para asegurarse de que solo los puertos necesarios estén abiertos.

Para obtener más información sobre el uso de los controles de firewall, incluidos ejemplos, consulte"Administrar los controles del firewall" .

Para obtener más información sobre firewalls externos y seguridad de red, consulte"Controlar el acceso al firewall externo" .

Controles de firewall de acceso

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Control de firewall**.

   Las tres pestañas de esta página se describen en"Administrar los controles del firewall" .

2. Seleccione cualquier pestaña para configurar los controles del firewall.

   Puede utilizar estas pestañas en cualquier orden. Las configuraciones que establezca en una pestaña no limitan lo que puede hacer en las otras pestañas; sin embargo, los cambios de configuración que realice en una pestaña podrían cambiar el comportamiento de los puertos configurados en otras pestañas.

Lista de direcciones privilegiadas

Utilice la pestaña Lista de direcciones privilegiadas para otorgar a los hosts acceso a puertos que están cerrados de manera predeterminada o cerrados por la configuración de la pestaña Administrar acceso

externo.

Las direcciones IP y subredes privilegiadas no tienen acceso a la red interna de forma predeterminada. Además, los puntos finales del balanceador de carga y los puertos adicionales abiertos en la pestaña Lista de direcciones privilegiadas son accesibles incluso si están bloqueados en la pestaña Administrar acceso externo.

> Las configuraciones en la pestaña Lista de direcciones privilegiadas no pueden anular las configuraciones en la pestaña Red de cliente no confiable.

Pasos

1. En la pestaña Lista de direcciones privilegiadas, ingrese la dirección o subred IP a la que desea otorgar acceso a los puertos cerrados.
2. Opcionalmente, seleccione **Agregar otra dirección IP o subred en notación CIDR** para agregar clientes privilegiados adicionales.

   > Agregue la menor cantidad posible de direcciones a la lista privilegiada.

3. Opcionalmente, seleccione *Permitir que las direcciones IP privilegiadas accedan a los puertos internos de StorageGRID *. Ver "Puertos internos de StorageGRID" .

   > Esta opción elimina algunas protecciones para los servicios internos. Déjelo deshabilitado si es posible.

4. Seleccione **Guardar**.

Gestionar el acceso externo

Cuando se cierra un puerto en la pestaña Administrar acceso externo, ninguna dirección IP que no sea de la red podrá acceder al puerto a menos que agregue la dirección IP a la lista de direcciones privilegiadas. Solo puedes cerrar puertos que estén abiertos de forma predeterminada y solo puedes abrir puertos que hayas cerrado.

> Las configuraciones en la pestaña Administrar acceso externo no pueden anular las configuraciones en la pestaña Red de cliente no confiable. Por ejemplo, si un nodo no es confiable, el puerto SSH/22 se bloquea en la red del cliente incluso si está abierto en la pestaña Administrar acceso externo. Las configuraciones en la pestaña Red de cliente no confiable anulan los puertos cerrados (como 443, 8443, 9443) en la red del cliente.

Pasos

1. Seleccione **Administrar acceso externo**. La pestaña muestra una tabla con todos los puertos externos (puertos a los que pueden acceder los nodos que no pertenecen a la red de manera predeterminada) para los nodos de su red.
2. Configure los puertos que desea abrir y cerrar utilizando las siguientes opciones:
   - Utilice el interruptor junto a cada puerto para abrir o cerrar el puerto seleccionado.
   - Seleccione **Abrir todos los puertos mostrados** para abrir todos los puertos enumerados en la tabla.
   - Seleccione **Cerrar todos los puertos mostrados** para cerrar todos los puertos enumerados en la tabla.

Si cierra los puertos 443 o 8443 de Grid Manager, todos los usuarios que estén conectados actualmente en un puerto bloqueado, incluido usted, perderán el acceso a Grid Manager a menos que su dirección IP se haya agregado a la lista de direcciones privilegiadas.

Utilice la barra de desplazamiento en el lado derecho de la tabla para asegurarse de haber visto todos los puertos disponibles. Utilice el campo de búsqueda para encontrar la configuración de cualquier puerto externo ingresando un número de puerto. Puede ingresar un número de puerto parcial. Por ejemplo, si ingresa un **2**, se mostrarán todos los puertos que tengan la cadena "2" como parte de su nombre.

3. Seleccione **Guardar**

Red de clientes no confiables

Si la red de cliente de un nodo no es confiable, el nodo solo acepta tráfico entrante en los puertos configurados como puntos finales del balanceador de carga y, opcionalmente, puertos adicionales que seleccione en esta pestaña. También puede utilizar esta pestaña para especificar la configuración predeterminada para los nuevos nodos agregados en una expansión.

Las conexiones de cliente existentes podrían fallar si no se han configurado los puntos finales del balanceador de carga.

Los cambios de configuración que realice en la pestaña **Red de cliente no confiable** anulan las configuraciones de la pestaña **Administrar acceso externo**.

Pasos

1. Seleccione **Red de cliente no confiable**.
2. En la sección Establecer nuevo nodo predeterminado, especifique cuál debe ser la configuración predeterminada cuando se agregan nuevos nodos a la cuadrícula en un procedimiento de expansión.
   - **Confiable** (predeterminado): cuando se agrega un nodo en una expansión, su red de cliente es confiable.
   - **No confiable**: cuando se agrega un nodo en una expansión, su red de cliente no es confiable.

     Según sea necesario, puede regresar a esta pestaña para cambiar la configuración de un nuevo nodo específico.

     Esta configuración no afecta a los nodos existentes en su sistema StorageGRID .
3. Utilice las siguientes opciones para seleccionar los nodos que deben permitir conexiones de clientes solo en puntos finales del balanceador de carga configurados explícitamente o en puertos seleccionados adicionales:
   - Seleccione **No confiar en los nodos mostrados** para agregar todos los nodos que se muestran en la tabla a la lista de Red de clientes no confiables.
   - Seleccione **Confiar en los nodos mostrados** para eliminar todos los nodos que se muestran en la tabla de la lista Red de clientes no confiables.
   - Utilice el interruptor junto a cada nodo para configurar la red del cliente como confiable o no confiable para el nodo seleccionado.

Por ejemplo, puede seleccionar **No confiar en los nodos mostrados** para agregar todos los nodos a la lista de Red de clientes no confiables y luego usar el botón junto a un nodo individual para agregar ese único nodo a la lista de Red de clientes confiables.

> Utilice la barra de desplazamiento en el lado derecho de la tabla para asegurarse de haber visto todos los nodos disponibles. Utilice el campo de búsqueda para encontrar la configuración de cualquier nodo ingresando el nombre del nodo. Puede introducir un nombre parcial. Por ejemplo, si ingresa un **GW**, se mostrarán todos los nodos que tengan la cadena "GW" como parte de su nombre.

4. Seleccione **Guardar**.

   La nueva configuración del firewall se aplica y se ejecuta de inmediato. Las conexiones de cliente existentes podrían fallar si no se han configurado los puntos finales del balanceador de carga.

Información de copyright

Información de la marca comercial