Controle los firewalls

StorageGRID 11.8

NetApp
March 19, 2024

Tabla de contenidos

Controle los firewalls

Controle el acceso a un firewall externo

Puede abrir o cerrar puertos específicos en el firewall externo.

Puede controlar el acceso a las interfaces de usuario y las API de los nodos de administrador de StorageGRID. Para ello, abra y cierre puertos específicos en el firewall externo. Por ejemplo, es posible que desee evitar que los inquilinos puedan conectarse a 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 "Configure el firewall interno".

Puerto	Descripción	Si el puerto está abierto…
443	Puerto HTTPS predeterminado para nodos de administración	Los exploradores web y los clientes de la API de gestión pueden acceder a Grid Manager, a la API de gestión de grid, al administrador de inquilinos y a la API de gestión de inquilinos. **Nota:** el puerto 443 también se utiliza para tráfico interno.
8443	Puerto de Grid Manager restringido en nodos de administración	• Los exploradores web y los clientes de la API de gestión pueden acceder a Grid Manager y a la API de gestión de grid mediante HTTPS. • Los exploradores web y los clientes de API de gestión no pueden acceder al administrador de inquilinos ni a la API de gestión de inquilinos. • Se rechazarán las solicitudes de contenido interno.
9443	Puerto de administrador de inquilinos restringido en los nodos de administrador	• Los exploradores web y los clientes de API de gestión pueden acceder al administrador de inquilinos y a la API de gestión de inquilinos mediante HTTPS. • Los exploradores web y los clientes de API de gestión no pueden acceder a Grid Manager ni a la API de administración de grid. • Se rechazarán las solicitudes de contenido interno.

El inicio de sesión único (SSO) no está disponible en los puertos de administrador de grid restringido o de administrador de inquilinos. Debe utilizar el puerto HTTPS predeterminado (443) si desea que los usuarios se autentiquen con inicio de sesión único.

Información relacionada

- "Inicie sesión en Grid Manager"

- "Cree una cuenta de inquilino"
- "Comunicaciones externas"

Gestionar los controles internos del firewall

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

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

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

  La configuración de esta ficha sustituye a la configuración de la ficha Administrar acceso externo.

  - Un nodo con una red de cliente que no sea de confianza aceptará solo conexiones en los puertos de punto final del equilibrador de carga configurados en ese nodo (puntos finales enlazados de tipo de nodo, interfaz de nodo y global).
  - Los puertos de punto final del equilibrador de carga *son los únicos puertos abiertos* en redes de cliente que no son de confianza, independientemente de la configuración de la pestaña Administrar redes externas.
  - Cuando se confía, se puede acceder a todos los puertos abiertos en la pestaña Administrar acceso externo, así como a cualquier punto final del equilibrador de carga abierto en la red cliente.

> La configuración que realice en una pestaña puede afectar a los cambios de acceso que realice en otra pestaña. Asegúrese de comprobar la configuración en todas las pestañas para asegurarse de que su red se comporta de la forma que espera.

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

Para obtener más información sobre los firewalls externos y la seguridad de la red, consulte "Controle el acceso a un firewall externo".

Lista de direcciones con privilegios y pestañas Gestionar acceso externo

El separador Lista de Direcciones con Privilegios permite registrar una o más direcciones IP a las que se les concede acceso a los puertos de grid que están cerrados. La pestaña Administrar acceso externo permite cerrar el acceso externo a los puertos externos seleccionados o a todos los puertos externos abiertos (los puertos externos son puertos a los que pueden acceder los nodos que no son de cuadrícula de forma predeterminada). Estas dos pestañas a menudo se pueden utilizar juntas para personalizar el acceso exacto a la red que necesita para su grid.

Las direcciones IP con privilegios no tienen acceso de puerto de grid interno por defecto.

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

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

1. Utilice el separador Lista de Direcciones con Privilegios para agregar la dirección IP del host de salto.
2. Utilice la pestaña Gestionar acceso externo para bloquear todos los puertos.

Agregue la dirección IP con privilegios antes de bloquear los puertos 443 y 8443. Cualquier usuario conectado actualmente 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 con privilegios.

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

Ejemplo 2: Limitar el acceso a Grid Manager y al administrador de inquilinos

Supongamos que desea limitar el acceso a Grid Manager y al gestor de inquilinos (puertos predefinidos) por motivos de seguridad. Puede utilizar estos pasos generales:

1. Utilice el conmutador en la pestaña Administrar acceso externo para bloquear el puerto 443.
2. Utilice el conmutador en la pestaña Administrar acceso externo para permitir el acceso al puerto 8443.
3. Utilice el conmutador en la pestaña Administrar acceso externo para permitir el acceso al puerto 9443.

Después de guardar la configuración, los hosts no podrán acceder al puerto 443, pero podrán acceder a Grid Manager a través del puerto 8443 y al gestor de inquilinos a través del puerto 9443.

Los puertos 443, 8443 y 9443 son los puertos predefinidos para Grid Manager y Tenant Manager. Puede alternar cualquier puerto para limitar el acceso a un gestor de inquilinos o Grid Manager específico.

Ejemplo 3: Bloquear puertos sensibles

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

1. Utilice el separador Lista de Direcciones con Privilegios para otorgar acceso sólo a los hosts que necesitan acceso al servicio.
2. Utilice la pestaña Gestionar acceso externo para bloquear todos los puertos.

Agregue la dirección IP con privilegios antes de bloquear el acceso a los puertos asignados para acceder a Grid Manager y al gestor de inquilinos (los puertos predefinidos son 443 y 8443). Cualquier usuario conectado actualmente 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 con privilegios.

Después de guardar la configuración, el puerto 22 y el servicio SSH estarán disponibles para los hosts de la

lista de direcciones con privilegios. Se denegará el acceso al servicio a todos los demás hosts sin importar de qué interfaz proviene la solicitud.

Ejemplo 4: Desactivar el acceso a los servicios no utilizados

A nivel de red, puede desactivar algunos servicios que no desea utilizar. Por ejemplo, si no proporcionará acceso Swift, debe realizar los siguientes pasos generales:

1. Utilice el conmutador en la pestaña Administrar acceso externo para bloquear el puerto 18083.
2. Utilice el conmutador en la pestaña Administrar acceso externo para bloquear el puerto 18085.

Después de guardar la configuración, el nodo de almacenamiento ya no permite la conectividad Swift, pero sigue permitiendo el acceso a otros servicios en puertos no bloqueados.

Pestaña Redes de cliente que no son de confianza

Si está utilizando una red de cliente, puede ayudar a proteger StorageGRID de ataques hostiles aceptando tráfico de cliente entrante sólo en puntos finales configurados explícitamente.

De forma predeterminada, la red de cliente de cada nodo de cuadrícula es *Trusted*. Es decir, de forma predeterminada, StorageGRID confía en las conexiones entrantes a cada nodo de grid en All "puertos externos disponibles".

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

Ejemplo 1: Gateway Node solo acepta solicitudes HTTPS S3

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

1. Desde la "Puntos finales del equilibrador de carga" Configure un punto final del equilibrador de carga para S3 sobre HTTPS en el puerto 443.
2. En la página de control de firewall, seleccione Sin confianza para especificar que la red cliente del nodo de puerta de enlace no sea de confianza.

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

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

Suponga que desea habilitar el tráfico de servicios de la plataforma S3 saliente desde un nodo de almacenamiento, pero desea evitar las conexiones entrantes a ese nodo de almacenamiento en la red de clientes. Debe realizar este paso general:

- En la pestaña Redes de cliente sin confianza de la página de control de firewall, indique que la red de cliente en el nodo de almacenamiento no es de confianza.

Después de guardar la configuración, el nodo de almacenamiento ya no acepta ningún tráfico entrante en la red cliente, pero continúa permitiendo las 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 de Grid Manager solo en una subred específica. Debe realizar los siguientes pasos:

1. Conecte la red cliente de sus nodos de administración a la subred.
2. Utilice la pestaña Red de cliente sin confianza para configurar la red cliente como no confiable.
3. Cuando cree un extremo del balanceador de carga de la interfaz de gestión, introduzca el puerto y seleccione la interfaz de gestión a la que accederá el puerto.
4. Seleccione **Sí** para Red cliente no confiable.
5. Utilice el separador Gestionar acceso externo para bloquear todos los puertos externos (con o sin direcciones IP con privilegios definidas para hosts fuera de esa subred).

Después de guardar la configuración, solo los hosts de la subred especificada pueden acceder a Grid Manager. Todos los demás hosts están bloqueados.

Configure el firewall interno

Puede configurar el firewall de StorageGRID para controlar el acceso a la red a puertos específicos de los nodos de StorageGRID.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".
- Ha revisado la información de "Gestionar los controles del firewall" y.. "Directrices sobre redes".
- Si desea que un nodo de administración o un nodo de puerta de enlace acepte tráfico entrante sólo en puntos finales configurados explícitamente, ha definido los puntos finales del equilibrador de carga.

> Al cambiar la configuración de la red cliente, las conexiones de cliente existentes pueden fallar si no se han configurado los puntos finales del equilibrador 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 del grid. Puede utilizar las pestañas de control del firewall para abrir o cerrar los puertos que están abiertos de forma predeterminada en la red de grid, la red de administración y la red de cliente. También puede crear una lista de direcciones IP con privilegios que pueden acceder a los puertos de cuadrícula que están cerrados. Si utiliza una red cliente, puede especificar si un nodo confía en el tráfico entrante de la red cliente y puede configurar el acceso de puertos específicos en la red cliente.

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

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

Para obtener más información sobre los firewalls externos y la seguridad de la red, consulte "Controle el acceso a un firewall externo".

Acceda a los controles del cortafuegos

Pasos

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

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

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

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

Lista de direcciones con privilegios

Utilice el separador Lista de Direcciones con Privilegios para otorgar a los hosts acceso a los puertos que están cerrados por defecto o cerrados por valores en el separador Gestionar Acceso Externo.

Las direcciones IP y subredes con privilegios no tienen acceso interno a la cuadrícula por defecto. Además, los puntos finales del equilibrador de carga y los puertos adicionales abiertos en la pestaña de lista de direcciones con privilegios son accesibles incluso si están bloqueados en la pestaña Gestionar acceso externo.

> La configuración de la pestaña Lista de direcciones con privilegios no puede sustituir la configuración de la pestaña Red de clientes sin confianza.

Pasos

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

   > Agregue el menor número posible de direcciones a la lista de privilegios.

3. Opcionalmente, seleccione **Permitir direcciones IP privilegiadas para acceder a los puertos internos de StorageGRID**. Consulte "Puertos internos StorageGRID".

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

4. Seleccione **Guardar**.

Gestione el acceso externo

Cuando se cierra un puerto en la pestaña Administrar acceso externo, ninguna dirección IP que no sea de grid puede acceder al puerto a menos que agregue la dirección IP a la lista de direcciones con privilegios. Solo puede cerrar los puertos que están abiertos de forma predeterminada y sólo puede abrir los puertos que haya cerrado.

La configuración de la pestaña Administrar acceso externo no puede sustituir la configuración de la pestaña Red de cliente no confiable. Por ejemplo, si un nodo no es de confianza, el puerto SSH/22 se bloquea en la red cliente incluso si está abierto en la pestaña Gestionar acceso externo. La configuración de la pestaña Red de cliente no confiable anula los puertos cerrados (como 443, 8443, 9443) en la red cliente.

Pasos

1. Selecciona **Administrar acceso externo**. El separador muestra una tabla con todos los puertos externos (puertos a los que pueden acceder los nodos que no son de cuadrícula por defecto) para los nodos de la cuadrícula.
2. Configure los puertos que desea abrir y cerrar mediante las siguientes opciones:
   - Utilice la palanca situada 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, cualquier usuario conectado actualmente 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 con privilegios.

   Utilice la barra de desplazamiento situada a la derecha de la tabla para asegurarse de que ha visto todos los puertos disponibles. Utilice el campo de búsqueda para buscar la configuración de cualquier puerto externo introduciendo un número de puerto. Puede introducir un número de puerto parcial. Por ejemplo, si introduce un **2**, se mostrarán todos los puertos que tengan la cadena “2” como parte de su nombre.
3. Seleccione **Guardar**

Red cliente no confiable

Si la red cliente de un nodo no es de confianza, el nodo solo acepta el tráfico entrante en los puertos configurados como puntos finales de equilibrio de carga y, opcionalmente, los puertos adicionales que seleccione en esta pestaña. También puede usar 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 extremos de equilibrador de carga.

Los cambios de configuración que realice en la pestaña **Red de clientes sin confianza** anulan la configuración de la pestaña **Administrar acceso externo**.

Pasos

1. Seleccione **Red cliente no confiable**.
2. En la sección Definir Nuevo Nodo por Defecto, especifique cuál debe ser el valor por defecto cuando se agregan nuevos nodos a la cuadrícula en un procedimiento de expansión.
   - **De confianza** (por defecto): Cuando se agrega un nodo en una expansión, su red cliente es de confianza.

- **No fiable**: Cuando se agrega un nodo en una expansión, su red cliente no es de confianza.

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

  Esta configuración no afecta a los nodos existentes del sistema StorageGRID.

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

   - Seleccione **Untrust on Visualized Nodes** para agregar todos los nodos mostrados en la tabla a la lista Untrusted Client Network.
   - Seleccione **Confiar en los nodos mostrados** para eliminar todos los nodos mostrados en la tabla de la lista Red de clientes sin confianza.
   - Utilice el conmutador situado junto a cada nodo para establecer la red cliente como de confianza o no de confianza para el nodo seleccionado.

     Por ejemplo, puede seleccionar **Untrust on displayed nodes** para agregar todos los nodos a la lista Untrusted Client Network y, a continuación, usar el conmutador junto a un nodo individual para agregar ese nodo a la lista Trusted Client Network.

     Use la barra de desplazamiento en la parte derecha de la tabla para asegurarse de que ha visto todos los nodos disponibles. Utilice el campo de búsqueda para encontrar la configuración de cualquier nodo introduciendo el nombre del nodo. Puede introducir un nombre parcial. Por ejemplo, si introduce 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 aplica inmediatamente. Las conexiones de cliente existentes podrían fallar si no se han configurado extremos de equilibrador de carga.