



Administración de redes de clientes que no son de confianza

StorageGRID 11.5

NetApp
April 11, 2024

Tabla de contenidos

- Administración de redes de clientes que no son de confianza 1
 - Ejemplo 1: Gateway Node solo acepta solicitudes HTTPS S3 1
 - Ejemplo 2: El nodo de almacenamiento envía solicitudes de servicios de plataforma S3 1
 - La especificación de la red de cliente de un nodo no es de confianza 2

Administración de redes de clientes 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 cuadrícula en todos los puertos externos disponibles (consulte la información acerca de las comunicaciones externas en las directrices de red).

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.

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. En la página Load Balancer Endpoints, configure un extremo de equilibrador de carga para S3 a través de HTTPS en el puerto 443.
2. En la página redes de cliente no fiables, especifique que la red de 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

Supongamos que desea habilitar el tráfico saliente del servicio de la plataforma S3 desde un nodo de almacenamiento, pero desea impedir las conexiones entrantes a ese nodo de almacenamiento en la red cliente. Debe realizar este paso general:

- En la página redes de cliente no fiables, indique que la red de clientes del 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 solicitudes salientes a Amazon Web Services.

Información relacionada

["Directrices de red"](#)

["Configuración de los extremos del equilibrador de carga"](#)

La especificación de la red de cliente de un nodo no es de confianza

Si utiliza una red de cliente, puede especificar si la red de cliente de cada nodo es de confianza o no es de confianza. También puede especificar la configuración predeterminada para los nuevos nodos agregados en una ampliación.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener el permiso acceso raíz.
- 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.



Las conexiones de cliente existentes podrían fallar si no se han configurado extremos de equilibrador de carga.

Pasos

1. Seleccione **Configuración > Configuración de red > Red de cliente no confiable**.

Aparece la página redes de cliente no fiables.

Esta página muestra todos los nodos del sistema StorageGRID. La columna motivo no disponible incluye una entrada si la red de cliente del nodo debe ser de confianza.

Untrusted Client Networks

If you are using a Client Network, you can specify whether a node trusts inbound traffic from the Client Network. If the Client Network is untrusted, the node only accepts inbound traffic on ports configured as [load balancer endpoints](#).

Set New Node Default

This setting applies to new nodes expanded into the grid.

New Node Client Network Default Trusted Untrusted

Select Untrusted Client Network Nodes

Select nodes that should have untrusted Client Network enforcement.

<input type="checkbox"/>	Node Name	Unavailable Reason
<input type="checkbox"/>	DC1-ADM1	
<input type="checkbox"/>	DC1-G1	
<input type="checkbox"/>	DC1-S1	
<input type="checkbox"/>	DC1-S2	
<input type="checkbox"/>	DC1-S3	
<input type="checkbox"/>	DC1-S4	

Client Network untrusted on 0 nodes.

Save

- 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.
 - Trusted:** Cuando se agrega un nodo en una expansión, su red de 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 página para cambiar la configuración de un nuevo nodo concreto.



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

- En la sección **Seleccionar nodos de red de cliente no confiable**, seleccione los nodos que deben permitir conexiones de cliente sólo en puntos finales de equilibrador de carga configurados explícitamente.

Puede seleccionar o anular la selección de la casilla de comprobación en el título para seleccionar o anular la selección de todos los nodos.

- Haga clic en **Guardar**.

Las nuevas reglas de firewall se agregan y aplican inmediatamente. Las conexiones de cliente existentes podrían fallar si no se han configurado extremos de equilibrador de carga.

Información relacionada

["Configuración de los extremos del equilibrador de carga"](#)

Información de copyright

Copyright © 2024 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 INTERRUPTIÓN 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.