



Verwalten von nicht vertrauenswürdigen Client-Netzwerken

StorageGRID 11.5

NetApp
April 11, 2024

Inhalt

- Verwalten von nicht vertrauenswürdigen Client-Netzwerken 1
 - Beispiel 1: Der Gateway-Node akzeptiert nur HTTPS-S3-Anforderungen 1
 - Beispiel 2: Storage-Node sendet Anforderungen von S3-Plattform-Services 1
 - Das Festlegen des Client-Netzwerks eines Knotens ist nicht vertrauenswürdig 2

Verwalten von nicht vertrauenswürdigen Client-Netzwerken

Wenn Sie ein Client-Netzwerk verwenden, können Sie StorageGRID vor feindlichen Angriffen schützen, indem Sie eingehenden Client-Datenverkehr nur auf explizit konfigurierten Endpunkten akzeptieren.

Standardmäßig ist das Client-Netzwerk auf jedem Grid-Knoten *Trusted*. Das heißt, StorageGRID vertraut standardmäßig eingehende Verbindungen zu jedem Grid-Knoten auf allen verfügbaren externen Ports (siehe Informationen über externe Kommunikation in den Netzwerkrichtlinien).

Sie können die Bedrohung durch feindliche Angriffe auf Ihrem StorageGRID-System verringern, indem Sie angeben, dass das Client-Netzwerk auf jedem Knoten *unvertrauenswürdig* ist. Wenn das Client-Netzwerk eines Node nicht vertrauenswürdig ist, akzeptiert der Knoten nur eingehende Verbindungen an Ports, die explizit als Load Balancer-Endpunkte konfiguriert sind.

Beispiel 1: Der Gateway-Node akzeptiert nur HTTPS-S3-Anforderungen

Angenommen, ein Gateway-Node soll den gesamten eingehenden Datenverkehr im Client-Netzwerk mit Ausnahme von HTTPS S3-Anforderungen ablehnen. Sie würden folgende allgemeine Schritte durchführen:

1. Konfigurieren Sie auf der Seite Load Balancer Endpoints einen Endpunkt für den Load Balancer für S3 über HTTPS am Port 443.
2. Geben Sie auf der Seite nicht vertrauenswürdige Clientnetzwerke an, dass das Client-Netzwerk auf dem Gateway-Node nicht vertrauenswürdig ist.

Nachdem Sie Ihre Konfiguration gespeichert haben, wird der gesamte eingehende Datenverkehr im Client-Netzwerk des Gateway-Knotens außer HTTPS-S3-Anfragen auf Port 443- und ICMP-Echo-(Ping-)Anfragen verworfen.

Beispiel 2: Storage-Node sendet Anforderungen von S3-Plattform-Services

Angenommen, Sie möchten den Datenverkehr des Outbound-S3-Plattformdienstes von einem Speicherknoten aktivieren, jedoch eingehende Verbindungen zu diesem Storage-Node im Client-Netzwerk verhindern. Sie würden diesen allgemeinen Schritt durchführen:

- Geben Sie auf der Seite nicht vertrauenswürdige Clientnetzwerke an, dass das Client-Netzwerk auf dem Speicherknoten nicht vertrauenswürdig ist.

Nachdem Sie Ihre Konfiguration gespeichert haben, akzeptiert der Speicherknoten keinen eingehenden Datenverkehr im Client-Netzwerk mehr, aber er erlaubt weiterhin ausgehende Anfragen an Amazon Web Services.

Verwandte Informationen

["Netzwerkrichtlinien"](#)

["Konfigurieren von Load Balancer-Endpunkten"](#)

Das Festlegen des Client-Netzwerks eines Knotens ist nicht vertrauenswürdig

Wenn Sie ein Client-Netzwerk verwenden, können Sie angeben, ob das Client-Netzwerk jedes Node vertrauenswürdig oder nicht vertrauenswürdig ist. Sie können auch die Standardeinstellung für neue Knoten festlegen, die in einer Erweiterung hinzugefügt werden.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.
- Wenn ein Admin-Node oder Gateway-Node nur eingehenden Datenverkehr auf explizit konfigurierten Endpunkten annehmen soll, haben Sie die Load Balancer-Endpunkte definiert.



Vorhandene Client-Verbindungen können fehlschlagen, wenn die Load Balancer-Endpunkte nicht konfiguriert wurden.

Schritte

1. Wählen Sie **Konfiguration > Netzwerkeinstellungen > Nicht Vertrauenswürdiges Clientnetzwerk**.

Die Seite nicht vertrauenswürdige Clientnetzwerke wird angezeigt.

Auf dieser Seite werden alle Knoten in Ihrem StorageGRID-System aufgelistet. Die Spalte „nicht verfügbar“ enthält einen Eintrag, wenn das Client-Netzwerk auf dem Knoten vertrauenswürdig sein muss.

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

- Geben Sie im Abschnitt **Neue Knoten Standard** festlegen an, was die Standardeinstellung sein soll, wenn neue Knoten in einem Erweiterungsvorgang zum Raster hinzugefügt werden.
 - Trusted:** Wenn ein Knoten in einer Erweiterung hinzugefügt wird, wird seinem Client-Netzwerk vertraut.
 - UnTrusted:** Wenn ein Knoten in einer Erweiterung hinzugefügt wird, ist sein Client-Netzwerk nicht vertrauenswürdig. Sie können bei Bedarf zu dieser Seite zurückkehren, um die Einstellung für einen bestimmten neuen Knoten zu ändern.



Diese Einstellung hat keine Auswirkung auf die vorhandenen Nodes im StorageGRID System.

- Wählen Sie im Abschnitt **nicht vertrauenswürdige Client-Netzwerkknoten auswählen** die Knoten aus, die Clientverbindungen nur auf explizit konfigurierten Load-Balancer-Endpunkten zulassen sollen.

Sie können das Kontrollkästchen im Titel auswählen oder deaktivieren, um alle Knoten auszuwählen oder zu deaktivieren.

- Klicken Sie Auf **Speichern**.

Die neuen Firewall-Regeln werden sofort hinzugefügt und durchgesetzt. Vorhandene Client-Verbindungen können fehlschlagen, wenn die Load Balancer-Endpunkte nicht konfiguriert wurden.

Verwandte Informationen

["Konfigurieren von Load Balancer-Endpunkten"](#)

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.