



Kontrollieren Sie Firewalls

StorageGRID 11.8

NetApp
May 10, 2024

Inhalt

- Kontrollieren Sie Firewalls 1
 - Kontrolle des Zugriffs über externe Firewall 1
 - Interne Firewall-Kontrollen verwalten 2
 - Konfigurieren Sie die interne Firewall 5

Kontrollieren Sie Firewalls

Kontrolle des Zugriffs über externe Firewall

Sie können bestimmte Ports an der externen Firewall öffnen oder schließen.

Sie können den Zugriff auf die Benutzeroberflächen und APIs auf StorageGRID-Administratorknoten steuern, indem Sie bestimmte Ports an der externen Firewall öffnen oder schließen. Beispielsweise möchten Sie verhindern, dass Mandanten sich an der Firewall mit dem Grid Manager verbinden können, und zwar zusätzlich über andere Methoden zur Steuerung des Systemzugriffs.

Informationen zum Konfigurieren der internen StorageGRID-Firewall finden Sie unter "[Konfigurieren Sie die interne Firewall](#)".

Port	Beschreibung	Port offen...
443	Standard-HTTPS-Port für Admin-Nodes	Webbrowser und Management-API-Clients können auf den Grid Manager, die Grid Management API, den Mandanten-Manager und die Mandanten-Management-API zugreifen. Hinweis: Port 443 wird auch für einen internen Verkehr genutzt.
8443	Eingeschränkter Grid Manager-Port an Admin-Nodes	<ul style="list-style-type: none">• Webbrowser und Management-API-Clients können mithilfe von HTTPS auf den Grid Manager und die Grid Management API zugreifen.• Webbrowser und Management-API-Clients können nicht auf den Tenant Manager oder die Mandanten-Management-API zugreifen.• Anfragen nach internen Inhalten werden abgelehnt.
9443	Eingeschränkter Mandantenmanager-Port an Admin-Nodes	<ul style="list-style-type: none">• Webbrowser und Management-API-Clients können mithilfe von HTTPS auf den Mandanten-Manager und die Mandanten-Management-API zugreifen.• Webbrowser und Management-API-Clients können nicht auf den Grid Manager oder die Grid-Management-API zugreifen.• Anfragen nach internen Inhalten werden abgelehnt.



Single Sign-On (SSO) ist auf den Ports Restricted Grid Manager oder Tenant Manager nicht verfügbar. Sie müssen den Standard-HTTPS-Port (443) verwenden, wenn Benutzer sich mit Single Sign-On authentifizieren möchten.

Verwandte Informationen

- ["Melden Sie sich beim Grid Manager an"](#)
- ["Erstellen eines Mandantenkontos"](#)
- ["Externe Kommunikation"](#)

Interne Firewall-Kontrollen verwalten

StorageGRID verfügt über eine interne Firewall auf jedem Node, die die Sicherheit Ihres Grids erhöht, indem Sie den Netzwerkzugriff auf den Node kontrollieren können. Verwenden Sie die Firewall, um den Netzwerkzugriff auf allen Ports zu verhindern, außer den für Ihre spezifische Grid-Bereitstellung erforderlichen Ports. Die Konfigurationsänderungen, die Sie auf der Seite Firewall-Steuerung vornehmen, werden für jeden Knoten bereitgestellt.

Verwenden Sie die drei Registerkarten auf der Seite „Firewall-Steuerung“, um den für Ihr Raster erforderlichen Zugriff anzupassen.

- **Privilegierte Adressliste:** Verwenden Sie diese Registerkarte, um ausgewählten Zugriff auf geschlossene Ports zu ermöglichen. Sie können IP-Adressen oder Subnetze in CIDR-Notation hinzufügen, die über die Registerkarte externen Zugriff managen auf geschlossene Ports zugreifen können.
- **Externen Zugriff verwalten:** Verwenden Sie diese Registerkarte, um Ports zu schließen, die standardmäßig geöffnet sind, oder um zuvor geschlossene Ports wieder zu öffnen.
- **Nicht vertrauenswürdiges Client-Netzwerk:** Verwenden Sie diese Registerkarte, um anzugeben, ob ein Knoten eingehenden Datenverkehr vom Client-Netzwerk anvertraut.

Die Einstellungen auf dieser Registerkarte überschreiben die Einstellungen auf der Registerkarte externen Zugriff verwalten.

- Ein Knoten mit einem nicht vertrauenswürdigen Client-Netzwerk akzeptiert nur Verbindungen auf den an diesem Knoten konfigurierten Load-Balancer-Endpunktports (global, Knotenschnittstelle und Knotentyp gebundene Endpunkte).
- Load Balancer-Endpunkt-Ports *sind die einzigen offenen Ports* in nicht vertrauenswürdigen Client-Netzwerken, unabhängig von den Einstellungen auf der Registerkarte Externe Netzwerke verwalten.
- Wenn vertrauenswürdig, sind alle Ports, die auf der Registerkarte externen Zugriff managen geöffnet sind, sowie alle im Client-Netzwerk geöffneten Load Balancer-Endpunkte zugänglich.



Die Einstellungen, die Sie auf einer Registerkarte vornehmen, können sich auf die Zugriffsänderungen auswirken, die Sie auf einer anderen Registerkarte vornehmen. Überprüfen Sie die Einstellungen auf allen Registerkarten, um sicherzustellen, dass sich Ihr Netzwerk wie erwartet verhält.

Informationen zum Konfigurieren der internen Firewall-Steuerelemente finden Sie unter ["Konfigurieren Sie die Firewall-Steuerelemente"](#).

Weitere Informationen zu externen Firewalls und Netzwerksicherheit finden Sie unter ["Kontrolle des Zugriffs über externe Firewall"](#).

Liste privilegierter Adressen und Verwaltung externer Zugriffsregisterkarten

Auf der Registerkarte Liste der privilegierten Adressen können Sie eine oder mehrere IP-Adressen registrieren,

denen Zugriff auf geschlossene Grid-Ports gewährt wird. Auf der Registerkarte externen Zugriff verwalten können Sie den externen Zugriff auf ausgewählte externe Ports oder alle offenen externen Ports schließen (externe Ports sind Ports, auf die standardmäßig nicht-Grid-Nodes zugreifen können). Diese beiden Registerkarten können häufig zusammen verwendet werden, um den genauen Netzwerkzugriff anzupassen, den Sie für Ihr Raster benötigen.



Privilegierte IP-Adressen haben standardmäßig keinen internen Grid-Port-Zugriff.

Beispiel 1: Verwenden Sie einen Jump-Host für Wartungsaufgaben

Angenommen, Sie möchten einen Jump-Host (einen sicherheitsgesicherten Host) für die Netzwerkadministration verwenden. Sie können die folgenden allgemeinen Schritte verwenden:

1. Verwenden Sie die Registerkarte Liste der privilegierten Adressen, um die IP-Adresse des Jump-Hosts hinzuzufügen.
2. Verwenden Sie die Registerkarte externen Zugriff verwalten, um alle Ports zu blockieren.



Fügen Sie die privilegierte IP-Adresse hinzu, bevor Sie die Ports 443 und 8443 blockieren. Alle Benutzer, die derzeit mit einem blockierten Port verbunden sind, einschließlich Ihnen, verlieren den Zugriff auf Grid Manager, es sei denn, ihre IP-Adresse wurde der Liste der privilegierten Adressen hinzugefügt.

Nachdem Sie Ihre Konfiguration gespeichert haben, werden alle externen Ports auf dem Admin-Knoten in Ihrem Grid für alle Hosts außer dem Jump-Host gesperrt. Sie können dann den Jump-Host verwenden, um Wartungsarbeiten am Grid sicherer durchzuführen.

Beispiel 2: Beschränken Sie den Zugriff auf den Grid-Manager und den Tenant Manager

Angenommen, Sie möchten aus Sicherheitsgründen den Zugriff auf Grid Manager und Tenant Manager (voreingestellte Ports) einschränken. Sie können die folgenden allgemeinen Schritte verwenden:

1. Verwenden Sie den Umschalter auf der Registerkarte externen Zugriff verwalten, um Port 443 zu blockieren.
2. Verwenden Sie die Umschalttaste auf der Registerkarte externen Zugriff verwalten, um den Zugriff auf Port 8443 zu ermöglichen.
3. Verwenden Sie die Umschalttaste auf der Registerkarte externen Zugriff verwalten, um den Zugriff auf Port 9443 zu ermöglichen.

Nachdem Sie Ihre Konfiguration gespeichert haben, können Hosts nicht auf Port 443 zugreifen, aber sie können dennoch über Port 8443 und den Tenant Manager über Port 9443 auf den Grid Manager zugreifen.



Die Ports 443, 8443 und 9443 sind die voreingestellten Ports für Grid Manager und Tenant Manager. Sie können jeden beliebigen Port umschalten, um den Zugriff auf einen bestimmten Grid Manager oder Tenant Manager zu beschränken.

Beispiel 3: Sperren sensibler Ports

Angenommen, Sie möchten sensible Ports und den Dienst auf diesem Port sperren (z. B. SSH an Port 22). Sie können die folgenden allgemeinen Schritte verwenden:

1. Verwenden Sie die Registerkarte Liste der privilegierten Adressen, um nur den Hosts Zugriff zu gewähren, die Zugriff auf den Dienst benötigen.

2. Verwenden Sie die Registerkarte externen Zugriff verwalten, um alle Ports zu blockieren.



Fügen Sie die privilegierte IP-Adresse hinzu, bevor Sie den Zugriff auf alle Ports blockieren, die dem Zugriff auf Grid Manager und Tenant Manager zugewiesen sind (voreingestellte Ports sind 443 und 8443). Alle Benutzer, die derzeit mit einem blockierten Port verbunden sind, einschließlich Ihnen, verlieren den Zugriff auf Grid Manager, es sei denn, ihre IP-Adresse wurde der Liste der privilegierten Adressen hinzugefügt.

Nachdem Sie die Konfiguration gespeichert haben, stehen den Hosts auf der Liste der privilegierten Adressen Port 22 und SSH-Dienst zur Verfügung. Allen anderen Hosts wird der Zugriff auf den Dienst verweigert, unabhängig davon, von welcher Schnittstelle die Anforderung stammt.

Beispiel 4: Deaktivieren Sie den Zugriff auf nicht verwendete Dienste

Auf Netzwerkebene können Sie einige Dienste deaktivieren, die Sie nicht verwenden möchten. Wenn Sie beispielsweise keinen Swift-Zugriff bereitstellen, führen Sie die folgenden allgemeinen Schritte aus:

1. Verwenden Sie den Umschalter auf der Registerkarte externen Zugriff verwalten, um Port 18083 zu blockieren.
2. Verwenden Sie den Umschalter auf der Registerkarte externen Zugriff verwalten, um Port 18085 zu blockieren.

Nachdem Sie die Konfiguration gespeichert haben, lässt der Storage Node die Swift-Konnektivität nicht mehr zu, erlaubt aber weiterhin den Zugriff auf andere Dienste auf nicht blockierten Ports.

Registerkarte nicht vertrauenswürdige Client-Netzwerke

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, standardmäßig vertraut StorageGRID eingehende Verbindungen zu jedem Grid-Knoten auf allen "[Verfügbare externe Ports](#)".

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. Siehe "[Konfigurieren von Load Balancer-Endpunkten](#)" Und "[Konfigurieren Sie die Firewall-Steuerelemente](#)".

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. Von "[Load Balancer-Endpunkte](#)" Konfigurieren Sie einen Load Balancer-Endpunkt für S3 über HTTPS an Port 443.
2. Wählen Sie auf der Seite Firewall-Steuerung die Option nicht vertrauenswürdig aus, um anzugeben, dass das Client-Netzwerk auf dem Gateway-Knoten 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 ausgehenden Datenverkehr der S3-Platforddienste von einem Storage-Node aktivieren, möchten jedoch eingehende Verbindungen zu diesem Storage-Node im Client-Netzwerk verhindern. Sie würden diesen allgemeinen Schritt durchführen:

- Geben Sie auf der Registerkarte nicht vertrauenswürdige Client-Netzwerke der Seite Firewall-Steuerung an, dass das Client-Netzwerk auf dem Storage Node nicht vertrauenswürdig ist.

Nachdem Sie die Konfiguration gespeichert haben, akzeptiert der Storage Node keinen eingehenden Datenverkehr mehr im Client-Netzwerk, erlaubt jedoch weiterhin ausgehende Anfragen an konfigurierte Plattforddienstziele.

Beispiel 3: Zugriff auf Grid Manager auf ein Subnetz beschränken

Angenommen, Sie möchten den Zugriff des Grid-Managers nur auf ein bestimmtes Subnetz zulassen. Führen Sie die folgenden Schritte aus:

1. Verbinden Sie das Client-Netzwerk Ihrer Admin-Knoten mit dem Subnetz.
2. Verwenden Sie die Registerkarte nicht vertrauenswürdige Clientnetzwerk, um das Clientnetzwerk als nicht vertrauenswürdig zu konfigurieren.
3. Wenn Sie einen Load Balancer-Endpunkt der Managementoberfläche erstellen, geben Sie den Port ein und wählen Sie die Managementoberfläche aus, auf die der Port zugreifen soll.
4. Wählen Sie **Ja** für nicht vertrauenswürdige Client-Netzwerk aus.
5. Verwenden Sie die Registerkarte externen Zugriff verwalten, um alle externen Ports zu blockieren (mit oder ohne privilegierte IP-Adressen für Hosts außerhalb dieses Subnetzes).

Nachdem Sie die Konfiguration gespeichert haben, können nur Hosts in dem von Ihnen angegebenen Subnetz auf den Grid Manager zugreifen. Alle anderen Hosts sind blockiert.

Konfigurieren Sie die interne Firewall

Sie können die StorageGRID Firewall konfigurieren, um den Netzwerkzugriff auf bestimmte Ports auf Ihren StorageGRID Nodes zu steuern.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Das ist schon ["Bestimmte Zugriffsberechtigungen"](#).
- Sie haben die Informationen in geprüft ["Management der Firewall-Kontrollen"](#) Und ["Netzwerkrichtlinien"](#).
- Wenn ein Admin-Node oder Gateway-Node nur eingehenden Datenverkehr auf explizit konfigurierten Endpunkten annehmen soll, haben Sie die Load Balancer-Endpunkte definiert.



Wenn Sie die Konfiguration des Client-Netzwerks ändern, können bestehende Clientverbindungen fehlschlagen, wenn die Load Balancer-Endpunkte nicht konfiguriert wurden.

Über diese Aufgabe

StorageGRID verfügt über eine interne Firewall auf jedem Node, über die Sie einige Ports an den Nodes des Grids öffnen oder schließen können. Sie können die Registerkarten für die Firewall-Steuerung verwenden, um

Ports zu öffnen oder zu schließen, die standardmäßig im Grid-Netzwerk, im Admin-Netzwerk und im Client-Netzwerk geöffnet sind. Sie können auch eine Liste mit privilegierten IP-Adressen erstellen, die auf gesperrte Grid-Ports zugreifen können. Wenn Sie ein Client-Netzwerk verwenden, können Sie angeben, ob ein Knoten eingehenden Datenverkehr vom Client-Netzwerk anvertraut, und Sie können den Zugriff bestimmter Ports auf dem Client-Netzwerk konfigurieren.

Die Beschränkung der Anzahl der offenen Ports auf IP-Adressen außerhalb Ihres Grids auf nur die absolut notwendigen Ports erhöht die Sicherheit Ihres Grids. Mithilfe der Einstellungen auf den drei Registerkarten für die Firewall-Steuerung stellen Sie sicher, dass nur die erforderlichen Ports geöffnet sind.

Weitere Informationen zur Verwendung von Firewall-Kontrollen, einschließlich Beispiele, finden Sie unter ["Management der Firewall-Kontrollen"](#).

Weitere Informationen zu externen Firewalls und Netzwerksicherheit finden Sie unter ["Kontrolle des Zugriffs über externe Firewall"](#).

Firewall-Kontrollen für den Zugriff

Schritte

1. Wählen Sie **CONFIGURATION > Security > Firewall Control**.

Die drei Registerkarten auf dieser Seite werden unter beschrieben ["Management der Firewall-Kontrollen"](#).

2. Wählen Sie eine beliebige Registerkarte aus, um die Firewall-Steuerelemente zu konfigurieren.

Sie können diese Registerkarten in beliebiger Reihenfolge verwenden. Die Konfigurationen, die Sie auf einer Registerkarte festlegen, beschränken nicht, was Sie auf den anderen Registerkarten tun können. Konfigurationsänderungen, die Sie auf einer Registerkarte vornehmen, können jedoch das Verhalten der auf anderen Registerkarten konfigurierten Ports ändern.

Liste privilegierter Adressen

Sie verwenden die Registerkarte Liste der privilegierten Adressen, um Hosts Zugriff auf Ports zu gewähren, die standardmäßig geschlossen oder durch Einstellungen auf der Registerkarte externen Zugriff verwalten geschlossen sind.

Privilegierte IP-Adressen und Subnetze haben standardmäßig keinen internen Grid-Zugriff. Zudem sind die Load Balancer-Endpunkte und zusätzliche Ports, die auf der Registerkarte „privilegierte Adressen“ geöffnet wurden, auch dann verfügbar, wenn sie auf der Registerkarte „externen Zugriff verwalten“ gesperrt sind.



Einstellungen auf der Registerkarte „Liste privilegierter Adressen“ können die Einstellungen auf der Registerkarte „nicht vertrauenswürdigen Clientnetzwerk“ nicht außer Kraft setzen.

Schritte

1. Geben Sie auf der Registerkarte Liste der privilegierten Adressen die Adresse oder das IP-Subnetz ein, die Sie Zugriff auf geschlossene Ports gewähren möchten.
2. Wählen Sie optional **Add another IP address or subnet in CIDR Notation** aus, um weitere privilegierte Clients hinzuzufügen.



Fügen Sie so wenig Adressen wie möglich zur Liste der privilegierten Adressen hinzu.

3. Wählen Sie optional **privilegierten IP-Adressen erlauben, auf interne StorageGRID-Ports zuzugreifen**.

Siehe "Interne StorageGRID-Ports".



Diese Option entfernt einige Schutzmaßnahmen für interne Dienste. Lassen Sie sie nach Möglichkeit deaktiviert.

4. Wählen Sie **Speichern**.

Management des externen Zugriffs

Wenn ein Port auf der Registerkarte externen Zugriff verwalten geschlossen wird, kann keine IP-Adresse ohne Grid auf den Port zugegriffen werden, es sei denn, Sie fügen die IP-Adresse der Liste privilegierter Adressen hinzu. Sie können nur Ports schließen, die standardmäßig geöffnet sind, und Sie können nur Ports öffnen, die Sie geschlossen haben.



Einstellungen auf der Registerkarte „externen Zugriff verwalten“ können die Einstellungen auf der Registerkarte „nicht vertrauenswürdiger Client-Netzwerk“ nicht außer Kraft setzen. Wenn ein Knoten beispielsweise nicht vertrauenswürdig ist, wird Port SSH/22 im Client-Netzwerk gesperrt, selbst wenn er auf der Registerkarte externen Zugriff verwalten geöffnet ist. Die Einstellungen auf der Registerkarte nicht vertrauenswürdiger Client-Netzwerk überschreiben geschlossene Ports (z. B. 443, 8443, 9443) im Client-Netzwerk.

Schritte

1. Wählen Sie **externen Zugriff verwalten**. Auf der Registerkarte wird eine Tabelle mit allen externen Ports (Ports, auf die standardmäßig nicht-Grid-Nodes zugreifen können) für die Nodes in Ihrem Grid angezeigt.
2. Konfigurieren Sie die Ports, die geöffnet und geschlossen werden sollen, mithilfe der folgenden Optionen:
 - Verwenden Sie den Umschalter neben jedem Port, um den ausgewählten Port zu öffnen oder zu schließen.
 - Wählen Sie **Alle angezeigten Ports öffnen**, um alle in der Tabelle aufgeführten Ports zu öffnen.
 - Wählen Sie **Alle angezeigten Ports schließen**, um alle in der Tabelle aufgeführten Ports zu schließen.



Wenn Sie die Grid-Manager-Ports 443 oder 8443 schließen, verlieren alle Benutzer, die derzeit an einem blockierten Port verbunden sind, einschließlich Ihnen, den Zugriff auf Grid Manager, es sei denn, ihre IP-Adresse wurde der Liste der privilegierten Adressen hinzugefügt.



Verwenden Sie die Bildlaufleiste auf der rechten Seite der Tabelle, um sicherzustellen, dass Sie alle verfügbaren Ports angezeigt haben. Verwenden Sie das Suchfeld, um die Einstellungen für einen externen Port zu finden, indem Sie eine Portnummer eingeben. Sie können einen Teil der Portnummer eingeben. Wenn Sie beispielsweise einen **2** eingeben, werden alle Ports angezeigt, die den String "2" als Teil ihres Namens haben.

3. Wählen Sie **Speichern**

Nicht Vertrauenswürdiger Client-Netzwerk

Wenn das Client-Netzwerk für einen Knoten nicht vertrauenswürdig ist, akzeptiert der Knoten nur eingehenden Datenverkehr an Ports, die als Load Balancer-Endpunkte konfiguriert sind, und optional zusätzliche Ports, die Sie auf dieser Registerkarte auswählen. Auf dieser Registerkarte können Sie auch die Standardeinstellung für neue Knoten festlegen, die in einer Erweiterung hinzugefügt wurden.



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

Die Konfigurationsänderungen, die Sie auf der Registerkarte **nicht vertrauenswürdiges Client-Netzwerk** vornehmen, überschreiben die Einstellungen auf der Registerkarte **externen Zugriff verwalten**.

Schritte

1. Wählen Sie **Nicht Vertrauenswürdiges Client-Netzwerk**.
2. Geben Sie im Abschnitt „Standard für neuen Knoten festlegen“ an, welche Standardeinstellung verwendet werden soll, wenn in einem Erweiterungsverfahren neue Knoten zum Raster hinzugefügt werden.
 - **Trusted** (Standard): Wenn ein Knoten in einer Erweiterung hinzugefügt wird, wird sein Client-Netzwerk vertrauenswürdig.
 - **UnTrusted**: Wenn ein Knoten in einer Erweiterung hinzugefügt wird, ist sein Client-Netzwerk nicht vertrauenswürdig.

Bei Bedarf können Sie zu dieser Registerkarte zurückkehren, um die Einstellung für einen bestimmten neuen Knoten zu ändern.



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

3. Verwenden Sie die folgenden Optionen, um die Knoten auszuwählen, die Clientverbindungen nur an explizit konfigurierten Endpunkten des Lastausgleichs oder zusätzlichen ausgewählten Ports zulassen sollen:
 - Wählen Sie **Untrust on displayed Nodes** aus, um alle in der Tabelle angezeigten Knoten zur Liste UnTrusted Client Network hinzuzufügen.
 - Wählen Sie **Trust on displayed Nodes** aus, um alle in der Tabelle angezeigten Knoten aus der Liste UnTrusted Client Network zu entfernen.
 - Verwenden Sie den Umschalter neben den einzelnen Knoten, um das Client-Netzwerk für den ausgewählten Knoten als vertrauenswürdig oder nicht vertrauenswürdig festzulegen.

Sie können beispielsweise **Untrust on displayed Nodes** auswählen, um alle Knoten zur Liste UnTrusted Client Network hinzuzufügen, und dann den Umschalter neben einem einzelnen Knoten verwenden, um diesen einzelnen Knoten zur Liste Trusted Client Network hinzuzufügen.



Verwenden Sie die Bildlaufleiste auf der rechten Seite der Tabelle, um sicherzustellen, dass Sie alle verfügbaren Knoten angezeigt haben. Verwenden Sie das Suchfeld, um die Einstellungen für jeden Knoten durch Eingabe des Knotennamens zu suchen. Sie können einen Teilnamen eingeben. Wenn Sie beispielsweise einen **GW** eingeben, werden alle Knoten angezeigt, die den String "GW" als Teil ihres Namens haben.

4. Wählen Sie **Speichern**.

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

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, BEISPIELHAFTE 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.