Controllare i firewall

StorageGRID software

NetApp
December 03, 2025

This PDF was generated from https://docs.netapp.com/it-it/storagegrid-119/admin/controlling-access-through-firewalls.html on December 03, 2025. Always check docs.netapp.com for the latest.

Sommario

Controllare i firewall

Controllare l’accesso al firewall esterno

È possibile aprire o chiudere porte specifiche sul firewall esterno.

È possibile controllare l’accesso alle interfacce utente e alle API sui nodi di amministrazione StorageGRID aprendo o chiudendo porte specifiche sul firewall esterno. Ad esempio, potresti voler impedire ai tenant di connettersi a Grid Manager tramite il firewall, oltre a utilizzare altri metodi per controllare l’accesso al sistema.

Se si desidera configurare il firewall interno StorageGRID , vedere"Configurare il firewall interno" .

Porta	Descrizione	Se la porta è aperta…
443	Porta HTTPS predefinita per i nodi di amministrazione	I browser Web e i client API di gestione possono accedere a Grid Manager, Grid Management API, Tenant Manager e Tenant Management API. **Nota:** la porta 443 viene utilizzata anche per parte del traffico interno.
8443	Porta Grid Manager limitata sui nodi amministrativi	• I browser Web e i client API di gestione possono accedere a Grid Manager e alla Grid Management API tramite HTTPS. • I browser Web e i client API di gestione non possono accedere a Tenant Manager o all’API Tenant Management. • Le richieste di contenuti interni verranno respinte.
9443	Porta Tenant Manager limitata sui nodi amministrativi	• I browser Web e i client API di gestione possono accedere a Tenant Manager e all’API Tenant Management tramite HTTPS. • I browser Web e i client API di gestione non possono accedere a Grid Manager o all’API Grid Management. • Le richieste di contenuti interni verranno respinte.

L’accesso Single Sign-On (SSO) non è disponibile sulle porte riservate di Grid Manager o Tenant Manager. Se si desidera che gli utenti eseguano l’autenticazione tramite Single Sign-On, è necessario utilizzare la porta HTTPS predefinita (443).

Informazioni correlate

- "Sign in a Grid Manager"
- "Crea un account inquilino"
- "Comunicazioni esterne"

Gestire i controlli del firewall interno

StorageGRID include un firewall interno su ciascun nodo che migliora la sicurezza della griglia consentendo di controllare l'accesso di rete al nodo. Utilizzare il firewall per impedire l'accesso alla rete su tutte le porte, ad eccezione di quelle necessarie per la distribuzione specifica della griglia. Le modifiche alla configurazione apportate nella pagina di controllo del firewall vengono distribuite a ciascun nodo.

Utilizza le tre schede nella pagina di controllo del firewall per personalizzare l'accesso necessario per la tua griglia.

- **Elenco indirizzi privilegiati**: utilizzare questa scheda per consentire l'accesso selezionato alle porte chiuse. È possibile aggiungere indirizzi IP o subnet in notazione CIDR che possono accedere alle porte chiuse utilizzando la scheda Gestisci accesso esterno.
- **Gestisci accesso esterno**: usa questa scheda per chiudere le porte aperte per impostazione predefinita o per riaprire quelle chiuse in precedenza.
- **Rete client non attendibile**: utilizzare questa scheda per specificare se un nodo considera attendibile il traffico in entrata dalla rete client.

  Le impostazioni in questa scheda sostituiscono quelle nella scheda Gestisci accesso esterno.

  - Un nodo con una rete client non attendibile accetterà solo connessioni sulle porte degli endpoint del bilanciatore del carico configurate su quel nodo (endpoint globali, interfaccia nodo e tipo nodo).
  - Le porte degli endpoint del bilanciatore del carico *sono le uniche porte aperte* sulle reti client non attendibili, indipendentemente dalle impostazioni nella scheda Gestisci reti esterne.
  - Se attendibili, tutte le porte aperte nella scheda Gestisci accesso esterno sono accessibili, così come tutti gli endpoint del bilanciatore del carico aperti sulla rete client.

> Le impostazioni effettuate in una scheda possono influire sulle modifiche di accesso effettuate in un'altra scheda. Assicurati di controllare le impostazioni in tutte le schede per verificare che la tua rete si comporti come previsto.

Per configurare i controlli del firewall interno, vedere"Configurare i controlli del firewall" .

Per ulteriori informazioni sui firewall esterni e sulla sicurezza di rete, vedere"Controllare l'accesso al firewall esterno" .

Elenco indirizzi privilegiati e schede Gestisci accesso esterno

La scheda Elenco indirizzi privilegiati consente di registrare uno o più indirizzi IP a cui è concesso l'accesso alle porte della griglia chiuse. La scheda Gestisci accesso esterno consente di chiudere l'accesso esterno alle porte esterne selezionate o a tutte le porte esterne aperte (le porte esterne sono porte accessibili per impostazione predefinita dai nodi non di griglia). Spesso è possibile utilizzare insieme queste due schede per personalizzare l'esatto accesso alla rete che si desidera consentire alla propria griglia.

> Per impostazione predefinita, gli indirizzi IP privilegiati non hanno accesso alla porta della griglia interna.

Esempio 1: utilizzare un jump host per le attività di manutenzione

Supponiamo di voler utilizzare un jump host (un host con sicurezza rafforzata) per l'amministrazione della rete. Potresti seguire questi passaggi generali:

1. Utilizzare la scheda Elenco indirizzi privilegiati per aggiungere l'indirizzo IP dell'host jump.
2. Utilizzare la scheda Gestisci accesso esterno per bloccare tutte le porte.

> Aggiungere l'indirizzo IP privilegiato prima di bloccare le porte 443 e 8443. Tutti gli utenti attualmente connessi a una porta bloccata, incluso te, perderanno l'accesso a Grid Manager a meno che il loro indirizzo IP non sia stato aggiunto all'elenco degli indirizzi privilegiati.

Dopo aver salvato la configurazione, tutte le porte esterne sul nodo di amministrazione nella griglia verranno bloccate per tutti gli host, ad eccezione dell'host jump. È quindi possibile utilizzare l'host jump per eseguire attività di manutenzione sulla griglia in modo più sicuro.

Esempio 2: Bloccare le porte sensibili

Supponiamo di voler bloccare porte sensibili e il servizio su quella porta (ad esempio, SSH sulla porta 22). È possibile seguire i seguenti passaggi generali:

1. Utilizzare la scheda Elenco indirizzi privilegiati per concedere l'accesso solo agli host che necessitano di accedere al servizio.
2. Utilizzare la scheda Gestisci accesso esterno per bloccare tutte le porte.

> Aggiungere l'indirizzo IP privilegiato prima di bloccare l'accesso a qualsiasi porta assegnata per accedere a Grid Manager e Tenant Manager (le porte preimpostate sono 443 e 8443). Tutti gli utenti attualmente connessi a una porta bloccata, incluso te, perderanno l'accesso a Grid Manager a meno che il loro indirizzo IP non sia stato aggiunto all'elenco degli indirizzi privilegiati.

Dopo aver salvato la configurazione, la porta 22 e il servizio SSH saranno disponibili per gli host nell'elenco degli indirizzi privilegiati. A tutti gli altri host verrà negato l'accesso al servizio, indipendentemente dall'interfaccia da cui proviene la richiesta.

Esempio 3: Disabilitare l'accesso ai servizi non utilizzati

A livello di rete, potresti disattivare alcuni servizi che non intendi utilizzare. Ad esempio, per bloccare il traffico client HTTP S3, è necessario utilizzare l'interruttore nella scheda Gestisci accesso esterno per bloccare la porta 18084.

Scheda Reti client non attendibili

Se si utilizza una rete client, è possibile proteggere StorageGRID da attacchi ostili accettando il traffico client in entrata solo su endpoint configurati in modo esplicito.

Per impostazione predefinita, la rete client su ciascun nodo della griglia è *attendibile*. Ciò significa che, per impostazione predefinita, StorageGRID considera attendibili le connessioni in ingresso a ciascun nodo della griglia su tutti"porte esterne disponibili" .

È possibile ridurre la minaccia di attacchi ostili al sistema StorageGRID specificando che la rete client su ciascun nodo sia *non attendibile*. Se la rete client di un nodo non è attendibile, il nodo accetta solo connessioni in entrata su porte configurate esplicitamente come endpoint del bilanciatore del carico. Vedere"Configurare gli

endpoint del bilanciatore del carico" E"Configurare i controlli del firewall" .

Esempio 1: il nodo gateway accetta solo richieste HTTPS S3

Supponiamo di voler far sì che un nodo gateway rifiuti tutto il traffico in entrata sulla rete client, ad eccezione delle richieste HTTPS S3. Dovresti eseguire questi passaggi generali:

1. Dal"Endpoint del bilanciatore del carico" pagina, configura un endpoint del bilanciatore del carico per S3 su HTTPS sulla porta 443.
2. Nella pagina Controllo firewall, selezionare Non attendibile per specificare che la rete client sul nodo gateway non è attendibile.

Dopo aver salvato la configurazione, tutto il traffico in entrata sulla rete client del nodo gateway viene interrotto, ad eccezione delle richieste HTTPS S3 sulla porta 443 e delle richieste ICMP echo (ping).

Esempio 2: il nodo di archiviazione invia richieste di servizi della piattaforma S3

Supponiamo di voler abilitare il traffico dei servizi della piattaforma S3 in uscita da un nodo di archiviazione, ma di voler impedire qualsiasi connessione in ingresso a tale nodo di archiviazione sulla rete client. Dovresti eseguire questo passaggio generale:

- Dalla scheda Reti client non attendibili della pagina di controllo del firewall, indicare che la rete client sul nodo di archiviazione non è attendibile.

Dopo aver salvato la configurazione, il nodo di archiviazione non accetta più traffico in entrata sulla rete client, ma continua a consentire richieste in uscita verso le destinazioni dei servizi della piattaforma configurati.

Esempio 3: limitazione dell'accesso a Grid Manager a una subnet

Supponiamo di voler consentire l'accesso a Grid Manager solo su una subnet specifica. Dovresti eseguire i seguenti passaggi:

1. Collega la rete client dei tuoi nodi amministrativi alla subnet.
2. Utilizzare la scheda Rete client non attendibile per configurare la rete client come non attendibile.
3. Quando si crea un endpoint del bilanciatore del carico dell'interfaccia di gestione, immettere la porta e selezionare l'interfaccia di gestione a cui la porta accederà.
4. Selezionare **Sì** per Rete client non attendibile.
5. Utilizzare la scheda Gestisci accesso esterno per bloccare tutte le porte esterne (con o senza indirizzi IP privilegiati impostati per gli host esterni a quella subnet).

Dopo aver salvato la configurazione, solo gli host nella subnet specificata potranno accedere a Grid Manager. Tutti gli altri host sono bloccati.

Configurare il firewall interno

È possibile configurare il firewall StorageGRID per controllare l'accesso alla rete a porte specifiche sui nodi StorageGRID .

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Hai"autorizzazioni di accesso specifiche" .

- Hai esaminato le informazioni in"Gestire i controlli del firewall" E"Linee guida per il networking" .
- Se si desidera che un nodo di amministrazione o un nodo gateway accetti il traffico in entrata solo su endpoint configurati in modo esplicito, è necessario definire gli endpoint del bilanciatore del carico.

> Quando si modifica la configurazione della rete client, le connessioni client esistenti potrebbero non funzionare se gli endpoint del bilanciatore del carico non sono stati configurati.

Informazioni su questo compito

StorageGRID include un firewall interno su ciascun nodo che consente di aprire o chiudere alcune porte sui nodi della griglia. È possibile utilizzare le schede di controllo Firewall per aprire o chiudere le porte aperte per impostazione predefinita sulla rete Grid, sulla rete di amministrazione e sulla rete client. È anche possibile creare un elenco di indirizzi IP privilegiati che possono accedere alle porte della griglia chiuse. Se si utilizza una rete client, è possibile specificare se un nodo si fida del traffico in entrata dalla rete client e configurare l'accesso di porte specifiche sulla rete client.

Limitare il numero di porte aperte agli indirizzi IP esterni alla rete solo a quelle assolutamente necessarie aumenta la sicurezza della rete stessa. Utilizzare le impostazioni in ciascuna delle tre schede di controllo del firewall per garantire che siano aperte solo le porte necessarie.

Per ulteriori informazioni sull'utilizzo dei controlli del firewall, inclusi esempi, vedere"Gestire i controlli del firewall" .

Per ulteriori informazioni sui firewall esterni e sulla sicurezza di rete, vedere"Controllare l'accesso al firewall esterno" .

Controlli del firewall di accesso

Passi

1. Selezionare **CONFIGURAZIONE** > **Sicurezza** > **Controllo firewall**.

   Le tre schede in questa pagina sono descritte in"Gestire i controlli del firewall" .

2. Selezionare una scheda qualsiasi per configurare i controlli del firewall.

   È possibile utilizzare queste schede in qualsiasi ordine. Le configurazioni impostate in una scheda non limitano le operazioni eseguibili nelle altre schede; tuttavia, le modifiche apportate alla configurazione in una scheda potrebbero modificare il comportamento delle porte configurate nelle altre schede.

Elenco indirizzi privilegiati

Utilizzare la scheda Elenco indirizzi privilegiati per concedere agli host l'accesso alle porte chiuse per impostazione predefinita o chiuse dalle impostazioni nella scheda Gestisci accesso esterno.

Per impostazione predefinita, gli indirizzi IP e le subnet privilegiati non dispongono di accesso alla griglia interna. Inoltre, gli endpoint del bilanciatore del carico e le porte aggiuntive aperte nella scheda Elenco indirizzi privilegiati sono accessibili anche se bloccati nella scheda Gestisci accesso esterno.

> Le impostazioni nella scheda Elenco indirizzi privilegiati non possono sovrascrivere le impostazioni nella scheda Rete client non attendibile.

Passi

1. Nella scheda Elenco indirizzi privilegiati, immettere l'indirizzo o la subnet IP a cui si desidera concedere l'accesso alle porte chiuse.
2. Facoltativamente, seleziona **Aggiungi un altro indirizzo IP o subnet in notazione CIDR** per aggiungere altri client privilegiati.

   Aggiungere il minor numero possibile di indirizzi all'elenco privilegiato.

3. Facoltativamente, seleziona *Consenti agli indirizzi IP privilegiati di accedere alle porte interne StorageGRID *. Vedere "Porte interne StorageGRID" .

   Questa opzione rimuove alcune protezioni per i servizi interni. Se possibile, lascialo disattivato.

4. Seleziona **Salva**.

Gestisci l'accesso esterno

Quando una porta viene chiusa nella scheda Gestisci accesso esterno, non è possibile accedervi da nessun indirizzo IP non in rete, a meno che non si aggiunga l'indirizzo IP all'elenco degli indirizzi privilegiati. Puoi chiudere solo le porte che sono aperte per impostazione predefinita e puoi aprire solo le porte che hai chiuso.

Le impostazioni nella scheda Gestisci accesso esterno non possono sostituire le impostazioni nella scheda Rete client non attendibile. Ad esempio, se un nodo non è attendibile, la porta SSH/22 viene bloccata sulla rete client anche se è aperta nella scheda Gestisci accesso esterno. Le impostazioni nella scheda Rete client non attendibile sovrascrivono le porte chiuse (ad esempio 443, 8443, 9443) sulla rete client.

Passi

1. Seleziona **Gestisci accesso esterno**. La scheda visualizza una tabella con tutte le porte esterne (porte accessibili per impostazione predefinita dai nodi non in griglia) per i nodi nella griglia.
2. Configura le porte che vuoi aprire e chiudere utilizzando le seguenti opzioni:
   - Utilizzare il pulsante accanto a ciascuna porta per aprire o chiudere la porta selezionata.
   - Selezionare **Apri tutte le porte visualizzate** per aprire tutte le porte elencate nella tabella.
   - Selezionare **Chiudi tutte le porte visualizzate** per chiudere tutte le porte elencate nella tabella.

     Se chiudi le porte 443 o 8443 di Grid Manager, tutti gli utenti attualmente connessi su una porta bloccata, incluso te, perderanno l'accesso a Grid Manager, a meno che il loro indirizzo IP non sia stato aggiunto all'elenco degli indirizzi privilegiati.

     Utilizzare la barra di scorrimento sul lato destro della tabella per assicurarsi di aver visualizzato tutte le porte disponibili. Utilizzare il campo di ricerca per trovare le impostazioni per qualsiasi porta esterna inserendo un numero di porta. È possibile immettere un numero di porta parziale. Ad esempio, se si immette **2**, vengono visualizzate tutte le porte che contengono la stringa "2" nel loro nome.

3. Seleziona **Salva**

Rete client non attendibile

Se la rete client di un nodo non è attendibile, il nodo accetta solo il traffico in entrata sulle porte configurate come endpoint del bilanciatore del carico e, facoltativamente, sulle porte aggiuntive selezionate in questa scheda. È possibile utilizzare questa scheda anche per specificare l'impostazione predefinita per i nuovi nodi aggiunti in un'espansione.

> Le connessioni client esistenti potrebbero non riuscire se gli endpoint del bilanciatore del carico non sono stati configurati.

Le modifiche alla configurazione apportate nella scheda **Rete client non attendibile** sovrascrivono le impostazioni nella scheda **Gestisci accesso esterno**.

Passi

1. Selezionare **Rete client non attendibile**.
2. Nella sezione Imposta nuovo nodo predefinito, specificare quale deve essere l'impostazione predefinita quando vengono aggiunti nuovi nodi alla griglia in una procedura di espansione.
   - **Affidabile** (predefinito): quando un nodo viene aggiunto in un'espansione, la sua rete client è attendibile.
   - **Non attendibile**: quando un nodo viene aggiunto a un'espansione, la sua rete client non è attendibile.

     Se necessario, è possibile tornare a questa scheda per modificare l'impostazione per un nuovo nodo specifico.

     > Questa impostazione non influisce sui nodi esistenti nel sistema StorageGRID .
3. Utilizzare le seguenti opzioni per selezionare i nodi che devono consentire connessioni client solo su endpoint del bilanciatore del carico configurati in modo esplicito o porte aggiuntive selezionate:
   - Selezionare **Non considerare attendibili i nodi visualizzati** per aggiungere tutti i nodi visualizzati nella tabella all'elenco Reti client non attendibili.
   - Selezionare **Considera attendibili i nodi visualizzati** per rimuovere tutti i nodi visualizzati nella tabella dall'elenco Reti client non attendibili.
   - Utilizzare il pulsante di attivazione/disattivazione accanto a ciascun nodo per impostare la rete client come attendibile o non attendibile per il nodo selezionato.

     Ad esempio, è possibile selezionare **Non considerare attendibili i nodi visualizzati** per aggiungere tutti i nodi all'elenco Reti client non attendibili e quindi utilizzare il pulsante di attivazione/disattivazione accanto a un singolo nodo per aggiungere quel singolo nodo all'elenco Reti client attendibili.

     > Utilizzare la barra di scorrimento sul lato destro della tabella per assicurarsi di aver visualizzato tutti i nodi disponibili. Utilizzare il campo di ricerca per trovare le impostazioni di qualsiasi nodo immettendone il nome. È possibile immettere un nome parziale. Ad esempio, se si immette **GW**, verranno visualizzati tutti i nodi che hanno la stringa "GW" come parte del loro nome.
4. Seleziona **Salva**.

   Le nuove impostazioni del firewall vengono applicate e rese effettive immediatamente. Le connessioni client esistenti potrebbero non riuscire se gli endpoint del bilanciatore del carico non sono stati configurati.

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.