Controlla i firewall

StorageGRID software

NetApp
July 23, 2026

Sommario

Controlla i firewall . . . 1
- Controlla l’accesso a StorageGRID tramite un firewall esterno . . . 1
- Gestisci i controlli firewall interni in StorageGRID . . . 2
  - Schede Elenco indirizzi privilegiati e Gestione accesso esterno . . . 2
  - ${post_edited_translations.segment} . . . 3
- Configurare il firewall interno di StorageGRID . . . 4
  - Accedi ai controlli del firewall . . . 5
  - Elenco degli indirizzi privilegiati . . . 5
  - Gestisci l’accesso esterno . . . 6
  - Rete client non affidabile . . . 6

Controlla i firewall

Controlla l'accesso a StorageGRID tramite un firewall esterno

Puoi aprire o chiudere porte specifiche sul firewall esterno.

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

Se vuoi configurare il firewall interno di StorageGRID, vedi "Configura il firewall interno".

Porta	Descrizione	Se la porta è aperta…
443	Porta HTTPS predefinita per i nodi Admin	${post_edited_translations.segment} **Nota:** Anche la porta 443 viene utilizzata per parte del traffico interno.
8443	Porta Grid Manager con restrizioni sui nodi di amministrazione	• I browser web e i client API di gestione possono accedere a Grid Manager e all'API di gestione di Grid tramite HTTPS. • I browser web e i client API di gestione non possono accedere a Tenant Manager o alla Tenant Management API. • Le richieste di contenuti interni verranno respinte.
9443	Porta Tenant Manager con restrizioni sugli Admin Node	• I browser web e i client API di gestione possono accedere a Tenant Manager e all'API di gestione Tenant tramite HTTPS. • I browser web e i client API di gestione non possono accedere a Grid Manager o alla Grid Management API. • Le richieste di contenuti interni verranno respinte.

Il single sign-on (SSO) non è disponibile sulle porte con restrizioni di Grid Manager o Tenant Manager. Devi usare la porta HTTPS predefinita (443) se vuoi che gli utenti si autentichino con il single sign-on.

Informazioni correlate

- "Accedi al Grid Manager"
- "Crea account tenant"
- "Comunicazioni esterne"

Gestisci i controlli firewall interni in StorageGRID

StorageGRID include un firewall interno su ciascun nodo che migliora la sicurezza della tua grid consentendoti di controllare l'accesso di rete al nodo. Usa il firewall per impedire l'accesso di rete su tutte le porte ad eccezione di quelle necessarie per la tua specifica implementazione della grid. Le modifiche alla configurazione che apporti nella pagina di controllo del Firewall vengono distribuite su ciascun nodo.

${post_edited_translations.segment}

- **Elenco indirizzi privilegiati**: usa questa scheda per consentire l'accesso selezionato alle porte chiuse. Puoi aggiungere indirizzi IP o subnet in notazione CIDR che possono accedere alle porte chiuse usando la scheda Gestisci accesso esterno.
- **Gestisci l'accesso esterno**: Usa questa scheda per chiudere le porte aperte per impostazione predefinita o riaprire le porte precedentemente chiuse.
- ${post_edited_translations.segment}

  Le impostazioni in questa scheda hanno la precedenza sulle impostazioni nella scheda Gestisci accesso esterno.

  - Un nodo con una Client Network non attendibile accetterà solo connessioni sulle porte endpoint del load balancer configurate su quel nodo (endpoint globali, di interfaccia del nodo e associati al tipo di nodo).
  - Le porte endpoint del load balancer sono le uniche porte aperte sulle reti client non attendibili, indipendentemente dalle impostazioni nella scheda Manage external networks.
  - Quando sono attendibili, tutte le porte aperte nella scheda Gestisci accesso esterno sono accessibili, così come tutti gli endpoint del bilanciatore di carico aperti sulla Client Network.

> Le impostazioni che modifichi in una scheda possono influenzare le modifiche di accesso che fai in un'altra scheda. Assicurati di controllare le impostazioni in tutte le schede per essere sicuro che la tua rete si comporti come ti aspetti.

Per configurare i controlli del firewall interno, consulta "${post_edited_translations.segment}".

Per ulteriori informazioni sui firewall esterni e sulla sicurezza di rete, vedi "Controlla l'accesso tramite firewall esterno".

Schede Elenco indirizzi privilegiati e Gestione accesso esterno

La scheda Elenco indirizzi privilegiati ti permette di registrare uno o più indirizzi IP a cui viene concesso l'accesso alle porte della grid che sono chiuse. La scheda Gestisci accesso esterno ti permette di chiudere l'accesso esterno a porte esterne selezionate o a tutte le porte esterne aperte (le porte esterne sono porte accessibili per impostazione predefinita dai nodi non-grid). Queste due schede spesso possono essere usate insieme per personalizzare esattamente l'accesso di rete che vuoi consentire per la tua grid.

> Gli indirizzi IP privilegiati non hanno accesso alle porte interne della griglia per impostazione predefinita.

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

Supponiamo che tu voglia utilizzare un jump host (un host con sicurezza rafforzata) per l'amministrazione della rete. Puoi seguire questi passaggi generali:

1. Usa la scheda Elenco indirizzi privilegiati per aggiungere l'indirizzo IP del jump host.
2. ${post_edited_translations.segment}

> Aggiungi l'indirizzo IP privilegiato prima di bloccare le porte 443 e 8443. 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.

Dopo aver salvato la configurazione, tutte le porte esterne sull'Admin Node nel tuo grid verranno bloccate per tutti gli host ad eccezione del jump host. Potrai quindi utilizzare il jump host per eseguire le attività di manutenzione sul tuo grid in modo più sicuro.

Esempio 2: Blocca le porte sensibili

Supponiamo che tu voglia bloccare le porte sensibili e il servizio su quella porta. Puoi seguire questi passaggi generali:

1. Utilizza la scheda Elenco indirizzi privilegiati per concedere l'accesso solo agli host che necessitano di accedere al servizio.
2. ${post_edited_translations.segment}

> Aggiungi 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). Qualsiasi utente attualmente connesso su una porta bloccata, incluso te, perderà l'accesso a Grid Manager a meno che il suo indirizzo IP non sia stato aggiunto all'elenco degli indirizzi privilegiati.

Dopo aver salvato la configurazione, la porta sensibile e il servizio su quella porta sono disponibili per gli host presenti nell'elenco degli indirizzi privilegiati. Tutti gli altri host non possono accedere al servizio, indipendentemente dall'interfaccia da cui proviene la richiesta.

Esempio 3: Disabilita l'accesso ai servizi non utilizzati

A livello di rete, puoi disabilitare alcuni servizi che non intendi utilizzare. Ad esempio, per bloccare il traffico client HTTP S3, puoi usare l'interruttore nella scheda Manage external access per bloccare la porta 18084.

${post_edited_translations.segment}

Se usi una rete client, puoi contribuire a proteggere StorageGRID da attacchi malevoli accettando il traffico client in entrata solo sugli endpoint configurati esplicitamente.

Per impostazione predefinita, la Client Network su ciascun nodo della griglia è *attendibile*. Ovvero, per impostazione predefinita, StorageGRID considera attendibili le connessioni inbound verso ciascun nodo della griglia su tutte le "porte esterne disponibili".

Puoi ridurre la minaccia di attacchi ostili al tuo sistema StorageGRID specificando che la Client Network su ciascun nodo sia *non attendibile*. Se la Client Network di un nodo non è attendibile, il nodo accetta solo connessioni inbound su porte configurate esplicitamente come endpoint del bilanciatore del carico. Vedi "${post_edited_translations.segment}" e "${post_edited_translations.segment}".

Esempio 1: Il nodo gateway accetta solo richieste S3 HTTPS

Supponiamo che tu voglia che un Gateway Node rifiuti tutto il traffico inbound sulla Client Network, tranne le richieste HTTPS S3. Dovresti seguire questi passaggi generali:

1. Dalla pagina "${post_edited_translations.segment}", configura un endpoint del bilanciatore del carico per S3 su HTTPS sulla porta 443.
2. Dalla pagina di controllo del firewall, seleziona Non attendibile per specificare che la Client Network sul Gateway Node non è attendibile.

Dopo che salvi la configurazione, tutto il traffico in entrata sulla rete client del Gateway Node viene bloccato, tranne le richieste HTTPS S3 sulla porta 443 e le richieste ICMP echo (ping).

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

Supponi di voler abilitare il traffico outbound dei servizi della piattaforma S3 da un Storage Node, ma di voler impedire qualsiasi connessione inbound a tale Storage Node sulla Client Network. Eseguiresti questo passaggio generale:

- ${post_edited_translations.segment}

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

${post_edited_translations.segment}

Supponiamo che tu voglia consentire l'accesso a Grid Manager solo su una sottorete specifica. Dovresti eseguire i seguenti passaggi:

1. ${post_edited_translations.segment}
2. Usa la scheda Rete client non attendibile per configurare la rete client come non attendibile.
3. Quando crei un endpoint del bilanciatore di carico dell'interfaccia di gestione, inserisci la porta e seleziona l'interfaccia di gestione a cui la porta accederà.
4. Seleziona **Sì** per Rete client non attendibile.
5. ${post_edited_translations.segment}

Dopo aver salvato la configurazione, solo gli host della sottorete specificata possono accedere a Grid Manager. Tutti gli altri host sono bloccati.

Configurare il firewall interno di StorageGRID

Puoi configurare il firewall di StorageGRID per controllare l'accesso di rete a porte specifiche sui nodi StorageGRID.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".
- Hai esaminato le informazioni in "Gestisci i controlli del firewall" e "Linee guida di rete".
- Se vuoi che un nodo Admin o un nodo Gateway accetti traffico in entrata solo sugli endpoint configurati esplicitamente, hai definito gli endpoint del bilanciatore di carico.

${post_edited_translations.segment}

Informazioni su questa attività

StorageGRID include un firewall interno su ciascun nodo che ti permette di aprire o chiudere alcune delle porte sui nodi della tua griglia. Puoi usare le schede di controllo del firewall per aprire o chiudere le porte che sono aperte per impostazione predefinita sulla Grid Network, Admin Network e Client Network. Puoi anche creare un elenco di indirizzi IP privilegiati che possono accedere alle porte della griglia che sono chiuse. Se usi una Client Network, puoi specificare se un nodo si fida del traffico in entrata dalla Client Network e puoi configurare l'accesso a porte specifiche sulla Client Network.

Limitare il numero di porte aperte agli indirizzi IP esterni al tuo grid solo a quelle strettamente necessarie aumenta la sicurezza del tuo grid. Usi le impostazioni su ciascuna delle tre schede di controllo del firewall per assicurarti che siano aperte solo le porte necessarie.

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

Per ulteriori informazioni sui firewall esterni e sulla sicurezza di rete, vedi "Controlla l'accesso tramite firewall esterno".

Accedi ai controlli del firewall

Passaggi

1. Seleziona **Configurazione** > **Sicurezza** > **Controllo firewall**.

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

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

   Puoi usare queste schede in qualsiasi ordine. Le configurazioni che imposti in una scheda non limitano ciò che puoi fare nelle altre schede; tuttavia, le modifiche di configurazione che apporti in una scheda potrebbero cambiare il comportamento delle porte configurate nelle altre schede.

Elenco degli indirizzi privilegiati

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

Gli indirizzi IP e le subnet privilegiate non hanno accesso alla griglia interna per impostazione predefinita. Inoltre, gli endpoint del load balancer e le porte aggiuntive aperte nella scheda Privileged address list sono accessibili anche se bloccate nella scheda Manage external access.

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

Passaggi

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

${post_edited_translations.segment}

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

> Questa opzione rimuove alcune protezioni per i servizi interni. Se possibile, lasciala disabilitata.

4. Seleziona **Salva**.

Gestisci l'accesso esterno

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

> Le impostazioni nella scheda Gestisci accesso esterno non possono sovrascrivere 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 hanno la precedenza sulle porte chiuse (come 443, 8443, 9443) sulla rete client.

Passaggi

1. Seleziona **Gestisci accesso esterno**. La scheda visualizza una tabella con tutte le porte esterne (porte accessibili per impostazione predefinita dai nodi non appartenenti alla griglia) per i nodi della tua griglia.
2. Configura le porte che vuoi aprire e chiudere usando le seguenti opzioni:
   - Usa l'interruttore accanto a ogni porta per aprire o chiudere la porta selezionata.
   - Seleziona **Apri tutte le porte visualizzate** per aprire tutte le porte elencate nella tabella.
   - Seleziona **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 sia stato aggiunto all'elenco degli indirizzi privilegiati.

> Utilizza la barra di scorrimento sul lato destro della tabella per assicurarti di aver visualizzato tutte le porte disponibili. Utilizza il campo di ricerca per trovare le impostazioni di qualsiasi porta esterna inserendo un numero di porta. Puoi inserire anche solo una parte del numero di porta. Ad esempio, se inserisci **2**, vengono visualizzate tutte le porte che hanno la stringa "2" come parte del loro nome.

3. Seleziona **Save**

Rete client non affidabile

Se la rete client di un nodo non è considerata attendibile, il nodo accetta traffico in entrata solo sulle porte configurate come endpoint del bilanciatore di carico e, facoltativamente, sulle porte aggiuntive che selezioni in questa scheda. Puoi anche usare questa scheda 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 di carico non sono stati configurati.

Le modifiche di configurazione che apporti nella scheda **Rete client non attendibile** sovrascrivono le impostazioni della scheda **Gestisci accesso esterno**.

Passaggi

1. Seleziona **Rete client non attendibile**.
2. Nella sezione Imposta impostazione predefinita per i nuovi nodi, specifica quale deve essere l'impostazione predefinita quando vengono aggiunti nuovi nodi alla grid in una procedura di espansione.

   - ${post_edited_translations.segment}
   - **Non attendibile**: Quando un nodo viene aggiunto in un'espansione, la sua Client Network non è attendibile.

     Se necessario, puoi tornare a questa scheda per modificare l'impostazione di uno specifico nuovo nodo.

     ${post_edited_translations.segment}

3. ${post_edited_translations.segment}

   - ${post_edited_translations.segment}
   - Seleziona **Considera attendibili i nodi visualizzati** per rimuovere tutti i nodi visualizzati nella tabella dall'elenco Untrusted Client Network.
   - ${post_edited_translations.segment}

     ${post_edited_translations.segment}

     Utilizza la barra di scorrimento sul lato destro della tabella per assicurarti di aver visualizzato tutti i nodi disponibili. Usa il campo di ricerca per trovare le impostazioni di qualsiasi nodo inserendo il nome del nodo. Puoi inserire anche una parte del nome. Ad esempio, se inserisci **GW**, vengono 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 interrompersi se gli endpoint del bilanciatore del carico non sono stati configurati.