Gestione delle reti e delle connessioni StorageGRID

StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/it-it/storagegrid-115/admin/guidelines-for-storagegrid-networks.html on October 03, 2025. Always check docs.netapp.com for the latest.

Sommario

Gestione delle reti e delle connessioni StorageGRID . . . 1
- Linee guida per le reti StorageGRID . . . 1
  - Grid Network . . . 1
  - Admin Network (rete amministrativa) . . . 1
  - Rete client . . . 1
  - Linee guida . . . 2
- Visualizzazione degli indirizzi IP . . . 2
- Crittografia supportata per le connessioni TLS in uscita . . . 3
  - Versioni supportate di TLS . . . 3
  - Suite di crittografia TLS 1.2 supportate . . . 3
  - Suite di crittografia TLS 1.3 supportate . . . 4
- Modifica della crittografia del trasferimento di rete . . . 4
- Configurazione dei certificati del server . . . 5
  - Tipi supportati di certificati server personalizzati . . . 5
  - Certificati per gli endpoint del bilanciamento del carico . . . 5
  - Configurazione di un certificato server personalizzato per Grid Manager e Tenant Manager . . . 5
  - Ripristino dei certificati server predefiniti per Grid Manager e Tenant Manager . . . 7
  - Configurazione di un certificato server personalizzato per le connessioni al nodo di storage o al servizio CLB . . . 7
  - Ripristino dei certificati server predefiniti per gli endpoint S3 e Swift REST API . . . 8
  - Copia del certificato CA del sistema StorageGRID . . . 9
  - Configurazione dei certificati StorageGRID per FabricPool . . . 10
  - Creazione di un certificato server autofirmato per l'interfaccia di gestione . . . 10
- Configurazione delle impostazioni del proxy di storage . . . 12
- Configurazione delle impostazioni del proxy amministratore . . . 13
- Gestione delle policy di classificazione del traffico . . . 15
  - Regole corrispondenti e limiti opzionali . . . 15
  - Limitazione del traffico . . . 16
  - Utilizzo delle policy di classificazione del traffico con gli SLA . . . 16
  - Creazione di criteri di classificazione del traffico . . . 16
  - Modifica di una policy di classificazione del traffico . . . 23
  - Eliminazione di una policy di classificazione del traffico . . . 25
  - Visualizzazione delle metriche del traffico di rete . . . 25
- Quali sono i costi di collegamento . . . 28
  - Aggiornamento dei costi di collegamento . . . 30

Gestione delle reti e delle connessioni StorageGRID

È possibile utilizzare Grid Manager per configurare e gestire le reti e le connessioni StorageGRID.

Vedere "Configurazione delle connessioni dei client S3 e Swift" Per scoprire come connettere i client S3 o Swift.

- "Linee guida per le reti StorageGRID"
- "Visualizzazione degli indirizzi IP"
- "Crittografia supportata per le connessioni TLS in uscita"
- "Modifica della crittografia del trasferimento di rete"
- "Configurazione dei certificati del server"
- "Configurazione delle impostazioni del proxy di storage"
- "Configurazione delle impostazioni del proxy amministratore"
- "Gestione delle policy di classificazione del traffico"
- "Quali sono i costi di collegamento"

Linee guida per le reti StorageGRID

StorageGRID supporta fino a tre interfacce di rete per nodo di rete, consentendo di configurare la rete per ogni singolo nodo di rete in modo che corrisponda ai requisiti di sicurezza e accesso.

Per modificare o aggiungere una rete per un nodo griglia, consultare le istruzioni di ripristino e manutenzione. Per ulteriori informazioni sulla topologia di rete, consultare le istruzioni di rete.

Grid Network

Obbligatorio. La rete griglia viene utilizzata per tutto il traffico StorageGRID interno. Fornisce connettività tra tutti i nodi della rete, in tutti i siti e le subnet.

Admin Network (rete amministrativa)

Opzionale. La rete di amministrazione viene generalmente utilizzata per l'amministrazione e la manutenzione del sistema. Può essere utilizzato anche per l'accesso al protocollo client. La rete di amministrazione è in genere una rete privata e non deve essere instradabile tra i siti.

Rete client

Opzionale. La rete client è una rete aperta, generalmente utilizzata per fornire l'accesso alle applicazioni client S3 e Swift, in modo che la rete grid possa essere isolata e protetta. La rete client può comunicare con qualsiasi subnet raggiungibile tramite il gateway locale.

Linee guida

- Ogni nodo della griglia StorageGRID richiede un'interfaccia di rete dedicata, un indirizzo IP, una subnet mask e un gateway per ciascuna rete a cui è assegnato.
- Un nodo Grid non può avere più di un'interfaccia su una rete.
- È supportato un singolo gateway, per rete, per nodo di rete, che deve trovarsi sulla stessa sottorete del nodo. Se necessario, è possibile implementare un routing più complesso nel gateway.
- Su ciascun nodo, ogni rete viene mappata a una specifica interfaccia di rete.

Rete	Nome dell'interfaccia
Griglia	eth0
Admin (opzionale)	eth1
Client (opzionale)	eth2

- Se il nodo è collegato a un'appliance StorageGRID, vengono utilizzate porte specifiche per ciascuna rete. Per ulteriori informazioni, consultare le istruzioni di installazione dell'apparecchio.
- Il percorso predefinito viene generato automaticamente, per nodo. Se eth2 è attivato, 0.0.0.0/0 utilizza la rete client su eth2. Se eth2 non è abilitato, 0.0.0.0/0 utilizza Grid Network su eth0.
- La rete client non diventa operativa fino a quando il nodo grid non si è Unito alla griglia
- La rete amministrativa può essere configurata durante l'implementazione del nodo grid per consentire l'accesso all'interfaccia utente dell'installazione prima che la griglia sia completamente installata.

Informazioni correlate

"Mantieni Ripristina"

"Linee guida per la rete"

Visualizzazione degli indirizzi IP

È possibile visualizzare l'indirizzo IP di ciascun nodo della griglia nel sistema StorageGRID. È quindi possibile utilizzare questo indirizzo IP per accedere al nodo Grid dalla riga di comando ed eseguire varie procedure di manutenzione.

Di cosa hai bisogno

È necessario accedere a Grid Manager utilizzando un browser supportato.

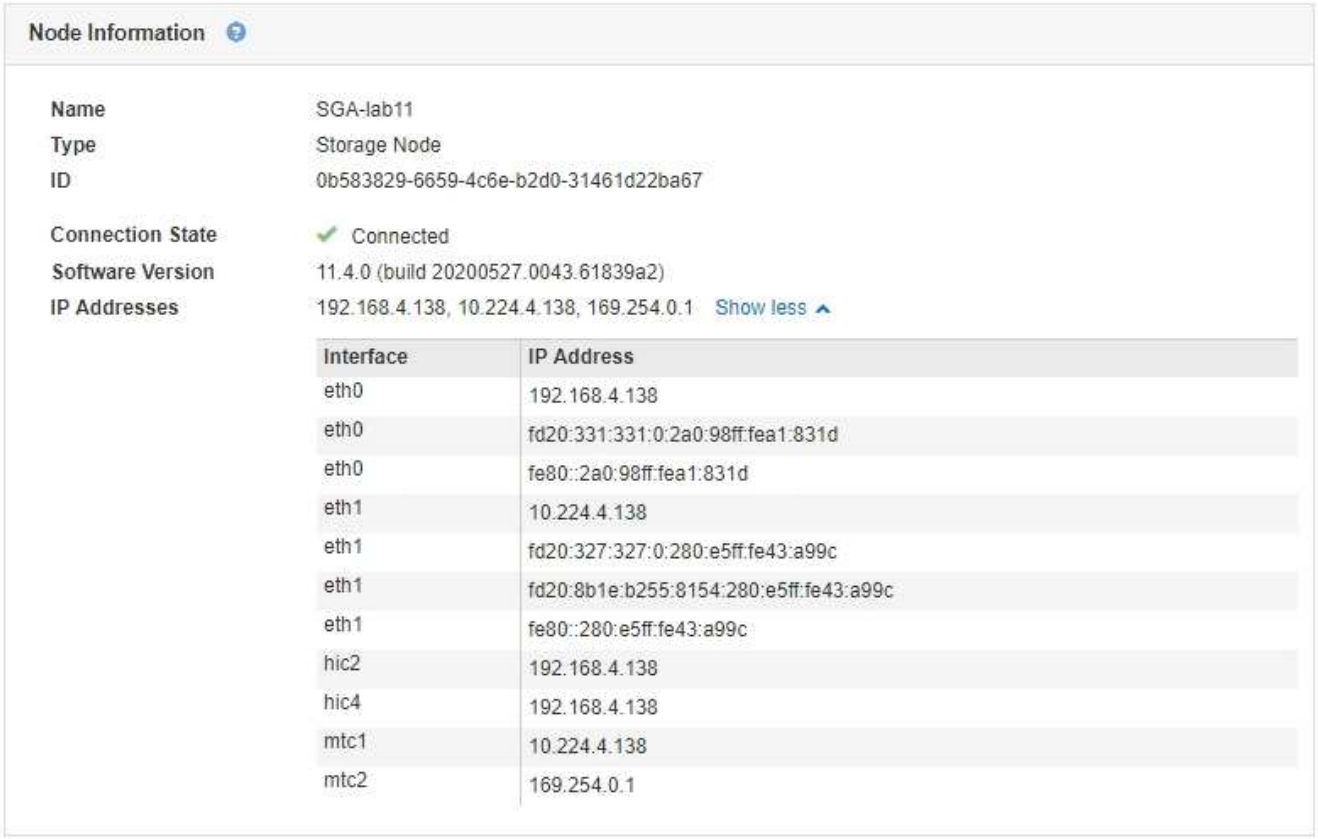
A proposito di questa attività

Per informazioni sulla modifica degli indirizzi IP, consultare le istruzioni di ripristino e manutenzione.

Fasi

1. Selezionare **Nodes *Grid Node* Overview**.
2. Fare clic su **Mostra altri** a destra del titolo indirizzi IP.

   Gli indirizzi IP per il nodo della griglia sono elencati in una tabella.



Informazioni correlate

"Mantieni Ripristina"

Crittografia supportata per le connessioni TLS in uscita

Il sistema StorageGRID supporta un set limitato di suite di crittografia per le connessioni TLS (Transport Layer Security) ai sistemi esterni utilizzati per la federazione di identità e i pool di storage cloud.

Versioni supportate di TLS

StorageGRID supporta TLS 1.2 e TLS 1.3 per le connessioni a sistemi esterni utilizzati per la federazione delle identità e i pool di storage cloud.

I cifrari TLS supportati per l'utilizzo con sistemi esterni sono stati selezionati per garantire la compatibilità con una vasta gamma di sistemi esterni. L'elenco è più grande dell'elenco di cifrature supportate per l'utilizzo con le applicazioni client S3 o Swift.

> Le opzioni di configurazione TLS, quali versioni di protocollo, crittografia, algoritmi di scambio delle chiavi e algoritmi MAC, non sono configurabili in StorageGRID. Se hai richieste specifiche su queste impostazioni, contatta il tuo rappresentante NetApp.

Suite di crittografia TLS 1.2 supportate

Sono supportate le seguenti suite di crittografia TLS 1.2:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

Suite di crittografia TLS 1.3 supportate

Sono supportate le seguenti suite di crittografia TLS 1.3:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

Modifica della crittografia del trasferimento di rete

Il sistema StorageGRID utilizza TLS (Transport Layer Security) per proteggere il traffico di controllo interno tra i nodi di rete. L'opzione Network Transfer Encryption (crittografia trasferimento di rete) imposta l'algoritmo utilizzato da TLS per crittografare il traffico di controllo tra i nodi della griglia. Questa impostazione non influisce sulla crittografia dei dati.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

Per impostazione predefinita, la crittografia del trasferimento di rete utilizza l'algoritmo AES256-SHA. Il traffico di controllo può anche essere crittografato utilizzando l'algoritmo AES128-SHA.

Fasi

1. Selezionare **Configurazione Impostazioni di sistema Opzioni griglia**.
2. Nella sezione Network Options (Opzioni di rete), impostare Network Transfer Encryption (crittografia trasferimento di rete) su **AES128-SHA** o **AES256-SHA** (impostazione predefinita).

3. Fare clic su **Save** (Salva).

Configurazione dei certificati del server

È possibile personalizzare i certificati server utilizzati dal sistema StorageGRID.

Il sistema StorageGRID utilizza certificati di sicurezza per diversi scopi distinti:

- Management Interface Server Certificates: Utilizzato per proteggere l'accesso a Grid Manager, tenant Manager, Grid Management API e tenant Management API.
- Storage API Server Certificates: Utilizzato per proteggere l'accesso ai nodi di storage e ai nodi gateway, le applicazioni client API utilizzate per caricare e scaricare i dati degli oggetti.

È possibile utilizzare i certificati predefiniti creati durante l'installazione oppure sostituire uno o entrambi i tipi di certificati predefiniti con certificati personalizzati.

Tipi supportati di certificati server personalizzati

Il sistema StorageGRID supporta certificati server personalizzati crittografati con RSA o ECDSA (algoritmo di firma digitale a curva ellittica).

Per ulteriori informazioni su come StorageGRID protegge le connessioni client per l'API REST, consultare le guide all'implementazione di S3 o Swift.

Certificati per gli endpoint del bilanciamento del carico

StorageGRID gestisce separatamente i certificati utilizzati per gli endpoint del bilanciamento del carico. Per configurare i certificati di bilanciamento del carico, consultare le istruzioni per la configurazione degli endpoint di bilanciamento del carico.

Informazioni correlate

"Utilizzare S3"

"USA Swift"

"Configurazione degli endpoint del bilanciamento del carico"

Configurazione di un certificato server personalizzato per Grid Manager e Tenant Manager

È possibile sostituire il certificato del server StorageGRID predefinito con un singolo certificato server personalizzato che consente agli utenti di accedere a Grid Manager e a Tenant Manager senza incontrare avvisi di sicurezza.

A proposito di questa attività

Per impostazione predefinita, ogni nodo amministrativo riceve un certificato firmato dalla CA della griglia. Questi certificati firmati dalla CA possono essere sostituiti da un singolo certificato server personalizzato comune e dalla chiave privata corrispondente.

Poiché per tutti i nodi di amministrazione viene utilizzato un singolo certificato server personalizzato, è necessario specificare il certificato come carattere jolly o certificato multidominio se i client devono verificare il nome host durante la connessione a Grid Manager e Tenant Manager. Definire il certificato personalizzato in

modo che corrisponda a tutti i nodi Admin nella griglia.

È necessario completare la configurazione sul server e, a seconda dell'autorità di certificazione (CA) di origine in uso, gli utenti potrebbero dover installare il certificato CA di origine nel browser Web utilizzato per accedere a Grid Manager e a Tenant Manager.

> Per garantire che le operazioni non vengano interrotte da un certificato del server guasto, l'avviso **scadenza del certificato del server per l'interfaccia di gestione** e l'allarme MCEP (Management Interface Certificate Expiry) legacy vengono attivati quando il certificato del server sta per scadere. In base alle esigenze, è possibile visualizzare il numero di giorni che devono essere trascorsi prima della scadenza del certificato di servizio corrente selezionando **supporto Strumenti topologia griglia**. Quindi, selezionare ***Primary Admin Node*** **CMN Resources**.

> Se si accede a Grid Manager o Tenant Manager utilizzando un nome di dominio invece di un indirizzo IP, il browser mostra un errore di certificato senza l'opzione di ignorare se si verifica una delle seguenti condizioni:
>
> - Il certificato del server dell'interfaccia di gestione personalizzata scade.
> - Viene ripristinato il certificato del server di un'interfaccia di gestione personalizzata al certificato del server predefinito.

Fasi

1. Selezionare **Configurazione Impostazioni di rete certificati server**.
2. Nella sezione Management Interface Server Certificate (certificato server interfaccia di gestione), fare clic su **Install Custom Certificate** (Installa certificato personalizzato).
3. Caricare i file dei certificati del server richiesti:
   - **Server Certificate**: Il file di certificato del server personalizzato (`.crt`).
   - **Server Certificate Private Key** (chiave privata certificato server): Il file di chiave privata del certificato del server personalizzato (`.key`).

     > Le chiavi private EC devono essere 224 bit o superiori. Le chiavi private RSA devono essere 2048 bit o superiori.

   - **Bundle CA**: Un singolo file contenente i certificati di ciascuna CA intermedia. Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati in ordine di catena del certificato.
4. Fare clic su **Save** (Salva).

   I certificati server personalizzati vengono utilizzati per tutte le nuove connessioni client successive.

   Selezionare una scheda per visualizzare informazioni dettagliate sul certificato del server StorageGRID predefinito o su un certificato firmato dalla CA caricato.

   > Dopo aver caricato un nuovo certificato, attendere fino a un giorno per eliminare eventuali avvisi relativi alla scadenza del certificato (o allarmi legacy).

5. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

Ripristino dei certificati server predefiniti per Grid Manager e Tenant Manager

È possibile ripristinare l'utilizzo dei certificati server predefiniti per Grid Manager e Tenant Manager.

Fasi

1. Selezionare **Configurazione Impostazioni di rete certificati server**.
2. Nella sezione Manage Interface Server Certificate (Gestisci certificato server interfaccia), fare clic su **Use Default Certificates** (Usa certificati predefiniti)
3. Fare clic su **OK** nella finestra di dialogo di conferma.

   Quando si ripristinano i certificati del server predefiniti, i file dei certificati del server personalizzati configurati vengono cancellati e non possono essere ripristinati dal sistema. I certificati server predefiniti vengono utilizzati per tutte le nuove connessioni client successive.

4. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

Configurazione di un certificato server personalizzato per le connessioni al nodo di storage o al servizio CLB

È possibile sostituire il certificato del server utilizzato per le connessioni client S3 o Swift al nodo di storage o al servizio CLB (obsoleto) sul nodo gateway. Il certificato del server personalizzato sostitutivo è specifico dell'organizzazione.

A proposito di questa attività

Per impostazione predefinita, ogni nodo di storage viene emesso un certificato server X.509 firmato dalla CA della griglia. Questi certificati firmati dalla CA possono essere sostituiti da un singolo certificato server personalizzato comune e dalla chiave privata corrispondente.

Per tutti i nodi di storage viene utilizzato un singolo certificato server personalizzato, pertanto è necessario specificare il certificato come certificato wildcard o multi-dominio se i client devono verificare il nome host durante la connessione all'endpoint di storage. Definire il certificato personalizzato in modo che corrisponda a tutti i nodi di storage nella griglia.

Una volta completata la configurazione sul server, gli utenti potrebbero anche aver bisogno di installare il certificato CA principale nel client S3 o Swift API che utilizzeranno per accedere al sistema, a seconda dell'autorità di certificazione (CA) root in uso.

> Per garantire che le operazioni non vengano interrotte da un certificato del server guasto, l'avviso **scadenza del certificato del server per gli endpoint API di storage** e l'allarme scadenza del certificato (SCEP) degli endpoint del servizio API di storage legacy vengono attivati quando il certificato del server root sta per scadere. In base alle esigenze, è possibile visualizzare il numero di giorni che devono essere trascorsi prima della scadenza del certificato di servizio corrente selezionando **supporto Strumenti topologia griglia**. Quindi, selezionare ***Primary Admin Node* CMN Resources**.

I certificati personalizzati vengono utilizzati solo se i client si connettono a StorageGRID utilizzando il servizio CLB obsoleto sui nodi gateway o se si connettono direttamente ai nodi di storage. I client S3 o Swift che si connettono a StorageGRID utilizzando il servizio bilanciamento del carico sui nodi di amministrazione o gateway utilizzano il certificato configurato per l'endpoint del bilanciamento del carico.

L'avviso **scadenza del certificato endpoint del bilanciamento del carico** viene attivato per gli endpoint del bilanciamento del carico che scadranno a breve.

Fasi

1. Selezionare **Configurazione Impostazioni di rete certificati server**.
2. Nella sezione Object Storage API Service Endpoints Server Certificate, fare clic su **Install Custom Certificate** (Installa certificato personalizzato).
3. Caricare i file dei certificati del server richiesti:
   - **Server Certificate**: Il file di certificato del server personalizzato (`.crt`).
   - **Server Certificate Private Key** (chiave privata certificato server): Il file di chiave privata del certificato del server personalizzato (`.key`).

     Le chiavi private EC devono essere 224 bit o superiori. Le chiavi private RSA devono essere 2048 bit o superiori.

   - **Bundle CA**: Un singolo file contenente i certificati di ciascuna CA intermedia. Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati in ordine di catena del certificato.
4. Fare clic su **Save** (Salva).

   Il certificato del server personalizzato viene utilizzato per tutte le nuove connessioni client API successive.

   Selezionare una scheda per visualizzare informazioni dettagliate sul certificato del server StorageGRID predefinito o su un certificato firmato dalla CA caricato.

   Dopo aver caricato un nuovo certificato, attendere fino a un giorno per eliminare eventuali avvisi relativi alla scadenza del certificato (o allarmi legacy).

5. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

Informazioni correlate

"Utilizzare S3"

"USA Swift"

"Configurazione dei nomi di dominio degli endpoint S3 API"

Ripristino dei certificati server predefiniti per gli endpoint S3 e Swift REST API

È possibile ripristinare l'utilizzo dei certificati server predefiniti per gli endpoint S3 e Swift REST API.

Fasi

1. Selezionare **Configurazione Impostazioni di rete certificati server**.
2. Nella sezione Object Storage API Service Endpoints Server Certificate, fare clic su **Use Default Certificates** (Usa certificati predefiniti).
3. Fare clic su **OK** nella finestra di dialogo di conferma.

   Quando si ripristinano i certificati server predefiniti per gli endpoint API dello storage a oggetti, i file di

certificato del server personalizzati configurati vengono cancellati e non possono essere ripristinati dal sistema. I certificati server predefiniti vengono utilizzati per tutte le nuove connessioni client API successive.

4. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

Copia del certificato CA del sistema StorageGRID

StorageGRID utilizza un'autorità di certificazione (CA) interna per proteggere il traffico interno. Questo certificato non cambia se si caricano i propri certificati.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

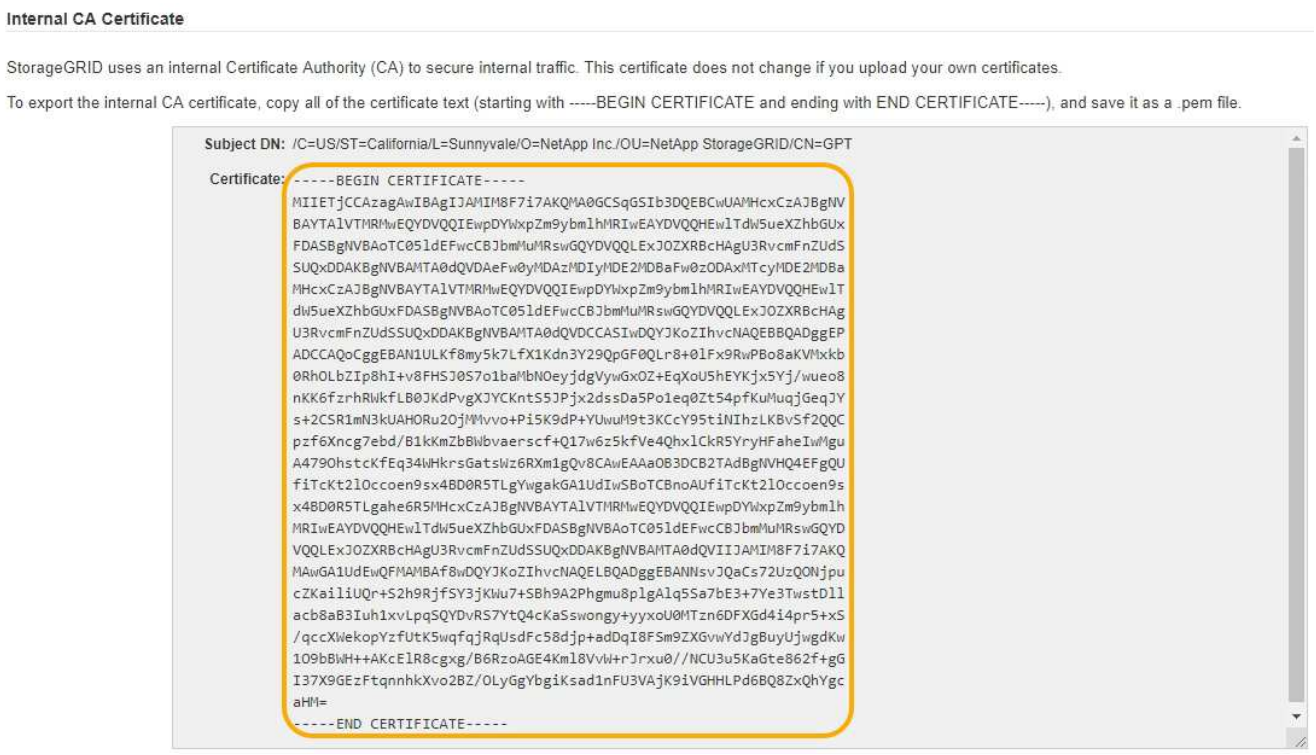
A proposito di questa attività

Se è stato configurato un certificato server personalizzato, le applicazioni client devono verificare il server utilizzando il certificato server personalizzato. Non devono copiare il certificato CA dal sistema StorageGRID.

Fasi

1. Selezionare **Configurazione Impostazioni di rete certificati server**.
2. Nella sezione **certificato CA interno**, selezionare tutto il testo del certificato.

   È necessario includere `-----BEGIN CERTIFICATE-----` e. `-----END CERTIFICATE-----` nella selezione.



3. Fare clic con il pulsante destro del mouse sul testo selezionato e selezionare **Copia**.
4. Incollare il certificato copiato in un editor di testo.
5. Salvare il file con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

Configurazione dei certificati StorageGRID per FabricPool

Per i client S3 che eseguono una convalida rigorosa del nome host e non supportano la disattivazione della convalida rigorosa del nome host, ad esempio i client ONTAP che utilizzano FabricPool, è possibile generare o caricare un certificato server quando si configura l'endpoint del bilanciamento del carico.

Di cosa hai bisogno

- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario accedere a Grid Manager utilizzando un browser supportato.

A proposito di questa attività

Quando si crea un endpoint di bilanciamento del carico, è possibile generare un certificato server autofirmato o caricare un certificato firmato da un'autorità di certificazione (CA) nota. Negli ambienti di produzione, è necessario utilizzare un certificato firmato da una CA nota. I certificati firmati da una CA possono essere ruotati senza interruzioni. Sono inoltre più sicuri perché offrono una migliore protezione contro gli attacchi man-in-the-middle.

La procedura riportata di seguito fornisce linee guida generali per i client S3 che utilizzano FabricPool. Per informazioni e procedure più dettagliate, consultare le istruzioni per la configurazione di StorageGRID per FabricPool.

> Il servizio separato di bilanciamento del carico di connessione (CLB) sui nodi gateway è obsoleto e non è più consigliato per l'utilizzo con FabricPool.

Fasi

1. Facoltativamente, configurare un gruppo ad alta disponibilità (ha) da utilizzare per FabricPool.
2. Creare un endpoint di bilanciamento del carico S3 da utilizzare per FabricPool.

   Quando si crea un endpoint di bilanciamento del carico HTTPS, viene richiesto di caricare il certificato del server, la chiave privata del certificato e il bundle CA.

3. Collega StorageGRID come Tier cloud in ONTAP.

   Specificare la porta endpoint del bilanciamento del carico e il nome di dominio completo utilizzato nel certificato CA caricato. Quindi, fornire il certificato CA.

   > Se una CA intermedia ha emesso il certificato StorageGRID, è necessario fornire il certificato CA intermedio. Se il certificato StorageGRID è stato emesso direttamente dalla CA principale, è necessario fornire il certificato della CA principale.

Informazioni correlate

"Configurare StorageGRID per FabricPool"

Creazione di un certificato server autofirmato per l'interfaccia di gestione

È possibile utilizzare uno script per generare un certificato server autofirmato per i client

API di gestione che richiedono una convalida rigorosa del nome host.

Di cosa hai bisogno

- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario disporre di `Passwords.txt` file.

A proposito di questa attività

Negli ambienti di produzione, è necessario utilizzare un certificato firmato da un'autorità di certificazione nota (CA). I certificati firmati da una CA possono essere ruotati senza interruzioni. Sono inoltre più sicuri perché offrono una migliore protezione contro gli attacchi man-in-the-middle.

Fasi

1. Ottenere il nome di dominio completo (FQDN) di ciascun nodo di amministrazione.
2. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.
3. Configurare StorageGRID con un nuovo certificato autofirmato.

   ```
   $ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
   ```

   - Per `--domains`, Utilizzare i caratteri jolly per rappresentare i nomi di dominio completi di tutti i nodi di amministrazione. Ad esempio, `*.ui.storagegrid.example.com` utilizza il carattere jolly * per rappresentare `admin1.ui.storagegrid.example.com` e. `admin2.ui.storagegrid.example.com`.
   - Impostare `--type` a. `management` Per configurare il certificato utilizzato da Grid Manager e Tenant Manager.
   - Per impostazione predefinita, i certificati generati sono validi per un anno (365 giorni) e devono essere ricreati prima della scadenza. È possibile utilizzare `--days` argomento per eseguire l'override del periodo di validità predefinito.

     > Il periodo di validità di un certificato inizia quando `make-certificate` è eseguito. È necessario assicurarsi che il client API di gestione sia sincronizzato con la stessa origine temporale di StorageGRID; in caso contrario, il client potrebbe rifiutare il certificato.

     ```
     $ sudo make-certificate --domains *.ui.storagegrid.example.com --type
     management --days 365
     ```

     L'output risultante contiene il certificato pubblico necessario al client API di gestione.
4. Selezionare e copiare il certificato.

Includere i tag BEGIN e END nella selezione.

5. Disconnettersi dalla shell dei comandi. `$ exit`
6. Verificare che il certificato sia stato configurato:
   a. Accedere a Grid Manager.
   b. Selezionare **Configuration Server Certificates Management Interface Server Certificate**.
7. Configurare il client API di gestione in modo che utilizzi il certificato pubblico copiato. Includere i tag inizio e FINE.

Configurazione delle impostazioni del proxy di storage

Se si utilizzano servizi di piattaforma o Cloud Storage Pool, è possibile configurare un proxy non trasparente tra i nodi di storage e gli endpoint S3 esterni. Ad esempio, potrebbe essere necessario un proxy non trasparente per consentire l'invio dei messaggi dei servizi della piattaforma a endpoint esterni, ad esempio un endpoint su Internet.

Di cosa hai bisogno

- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario accedere a Grid Manager utilizzando un browser supportato.

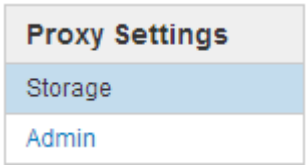
A proposito di questa attività

È possibile configurare le impostazioni per un singolo Storage Proxy.

Fasi

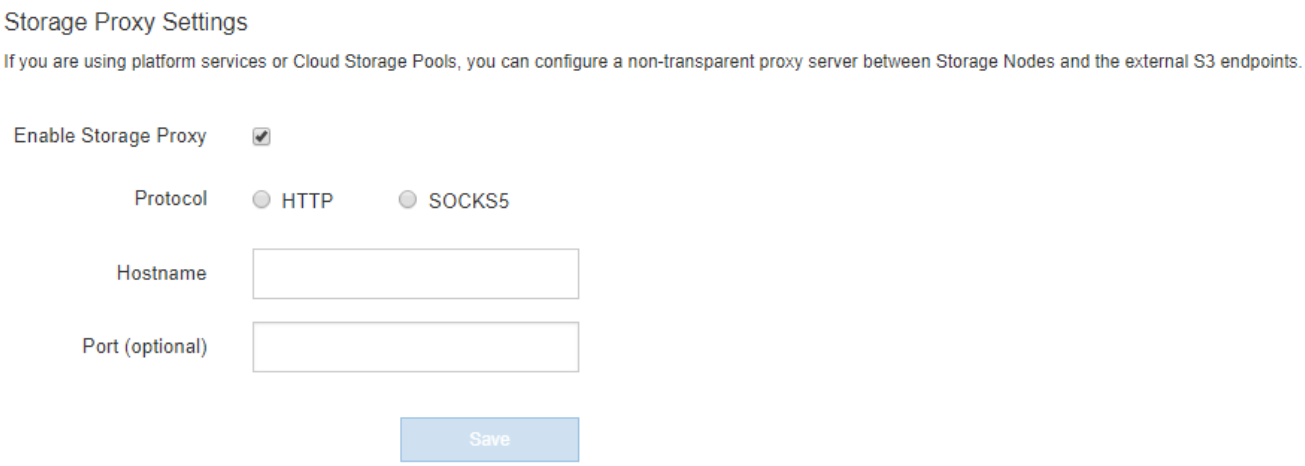
1. Selezionare **Configurazione Impostazioni di rete Impostazioni proxy**.

   Viene visualizzata la pagina Storage Proxy Settings (Impostazioni proxy storage). Per impostazione predefinita, nel menu della barra laterale è selezionata l'opzione **Storage**.

2. Selezionare la casella di controllo **Enable Storage Proxy** (attiva proxy di storage).

   Vengono visualizzati i campi per la configurazione di un proxy di storage.



3. Selezionare il protocollo per il proxy dello storage non trasparente.
4. Immettere il nome host o l'indirizzo IP del server proxy.
5. Facoltativamente, inserire la porta utilizzata per connettersi al server proxy.

   È possibile lasciare vuoto questo campo se si utilizza la porta predefinita per il protocollo: 80 per HTTP o 1080 per SOCKS5.

6. Fare clic su **Save** (Salva).

   Una volta salvato il proxy dello storage, è possibile configurare e testare i nuovi endpoint per i servizi della piattaforma o i pool di cloud storage.

   > Le modifiche del proxy possono richiedere fino a 10 minuti.

7. Controllare le impostazioni del server proxy per assicurarsi che i messaggi relativi al servizio della piattaforma da StorageGRID non vengano bloccati.

Al termine

Se è necessario disattivare un proxy di storage, deselezionare la casella di controllo **Enable Storage Proxy** (attiva proxy di storage) e fare clic su **Save** (Salva).

Informazioni correlate

"Networking e porte per i servizi della piattaforma"

"Gestire gli oggetti con ILM"

Configurazione delle impostazioni del proxy amministratore

Se si inviano messaggi AutoSupport utilizzando HTTP o HTTPS, è possibile configurare un server proxy non trasparente tra i nodi di amministrazione e il supporto tecnico (AutoSupport).

Di cosa hai bisogno

- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario accedere a Grid Manager utilizzando un browser supportato.

A proposito di questa attività

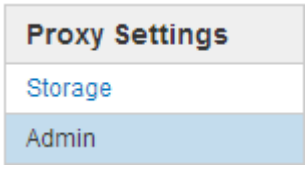
È possibile configurare le impostazioni per un singolo proxy Admin.

Fasi

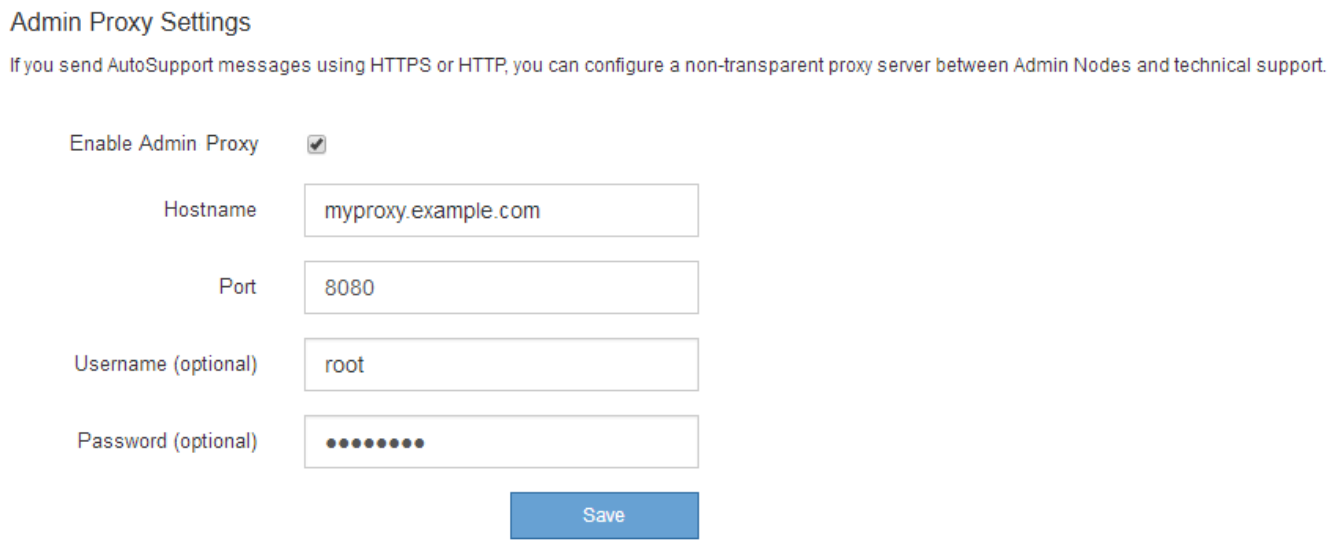
1. Selezionare **Configurazione Impostazioni di rete Impostazioni proxy**.

   Viene visualizzata la pagina Admin Proxy Settings (Impostazioni proxy amministratore). Per impostazione predefinita, nel menu della barra laterale è selezionata l'opzione **Storage**.

2. Dal menu della barra laterale, selezionare **Admin**.



3. Selezionare la casella di controllo **Enable Admin Proxy** (attiva proxy amministratore).



4. Immettere il nome host o l'indirizzo IP del server proxy.
5. Inserire la porta utilizzata per la connessione al server proxy.
6. Se si desidera, inserire il nome utente del proxy.

   Lasciare vuoto questo campo se il server proxy non richiede un nome utente.

7. Se si desidera, inserire la password del proxy.

   Lasciare vuoto questo campo se il server proxy non richiede una password.

8. Fare clic su **Save** (Salva).

   Una volta salvato il proxy Admin, viene configurato il server proxy tra i nodi Admin e il supporto tecnico.

   Le modifiche del proxy possono richiedere fino a 10 minuti.

9. Per disattivare il proxy, deselezionare la casella di controllo **Enable Admin Proxy** (attiva proxy

amministratore) e fare clic su **Save** (Salva).

Informazioni correlate

"Specifica del protocollo per i messaggi AutoSupport"

Gestione delle policy di classificazione del traffico

Per migliorare la qualità del servizio (QoS), è possibile creare policy di classificazione del traffico per identificare e monitorare diversi tipi di traffico di rete. Queste policy possono essere utili per la limitazione e il monitoraggio del traffico.

I criteri di classificazione del traffico vengono applicati agli endpoint del servizio bilanciamento del carico StorageGRID per i nodi gateway e i nodi di amministrazione. Per creare criteri di classificazione del traffico, è necessario aver già creato endpoint di bilanciamento del carico.

Regole corrispondenti e limiti opzionali

Ogni policy di classificazione del traffico contiene una o più regole corrispondenti per identificare il traffico di rete correlato a una o più delle seguenti entità:

- Bucket
- Tenant
- Subnet (subnet IPv4 contenente il client)
- Endpoint (endpoint del bilanciamento del carico)

StorageGRID monitora il traffico che corrisponde a qualsiasi regola all'interno del criterio in base agli obiettivi della regola. Qualsiasi traffico corrispondente a qualsiasi regola di un criterio viene gestito da tale criterio. Al contrario, è possibile impostare le regole in modo che corrispondano a tutto il traffico ad eccezione di un'entità specificata.

Facoltativamente, è possibile impostare limiti per una policy in base ai seguenti parametri:

- Larghezza di banda aggregata in
- Larghezza di banda aggregata in uscita
- Richieste di lettura simultanee
- Richieste di scrittura simultanee
- Larghezza di banda per richiesta in
- Larghezza di banda per richiesta in uscita
- Velocità richiesta di lettura
- Tasso di richieste di scrittura

> È possibile creare policy per limitare la larghezza di banda aggregata o per limitare la larghezza di banda per richiesta. Tuttavia, StorageGRID non può limitare entrambi i tipi di larghezza di banda contemporaneamente. I limiti di larghezza di banda aggregati potrebbero imporre un ulteriore impatto minore sulle performance sul traffico non limitato.

Limitazione del traffico

Una volta creati i criteri di classificazione del traffico, il traffico viene limitato in base al tipo di regole e limiti impostati. Per i limiti di larghezza di banda aggregati o per richiesta, le richieste vengono trasmesse in streaming alla velocità impostata. StorageGRID può applicare una sola velocità, quindi la corrispondenza di policy più specifica, in base al tipo di matcher, è quella applicata. Per tutti gli altri tipi di limite, le richieste client vengono ritardate di 250 millisecondi e ricevono una risposta lenta di 503 per le richieste che superano qualsiasi limite di policy corrispondente.

In Grid Manager, è possibile visualizzare i diagrammi di traffico e verificare che i criteri stiano applicando i limiti di traffico previsti.

Utilizzo delle policy di classificazione del traffico con gli SLA

È possibile utilizzare le policy di classificazione del traffico insieme ai limiti di capacità e alla protezione dei dati per applicare gli SLA (Service-Level Agreement) che forniscono specifiche per capacità, protezione dei dati e performance.

I limiti di classificazione del traffico vengono implementati per bilanciamento del carico. Se il traffico viene distribuito simultaneamente tra più bilanciatori di carico, i tassi massimi totali sono un multiplo dei limiti di velocità specificati.

Nell'esempio riportato di seguito vengono illustrati tre livelli di uno SLA. È possibile creare criteri di classificazione del traffico per raggiungere gli obiettivi di performance di ciascun livello SLA.

Livello di servizio	Capacità	Protezione dei dati	Performance	Costo
Oro	1 PB di storage consentito	3 copia regola ILM	25 K richieste/sec Larghezza di banda di 5 GB/sec (40 Gbps)	€ al mese
Argento	250 TB di storage consentiti	2 copia regola ILM	10 K richieste/sec Larghezza di banda di 1.25 GB/sec (10 Gbps)	dollari al mese
Bronzo	100 TB di storage consentiti	2 copia regola ILM	5 K richieste/sec Larghezza di banda di 1 GB/sec (8 Gbps)	dollari al mese

Creazione di criteri di classificazione del traffico

È possibile creare criteri di classificazione del traffico se si desidera monitorare e, facoltativamente, limitare il traffico di rete per bucket, tenant, subnet IP o endpoint del bilanciamento del carico. Facoltativamente, è possibile impostare limiti per una policy in base alla larghezza di banda, al numero di richieste simultanee o alla velocità di richiesta.

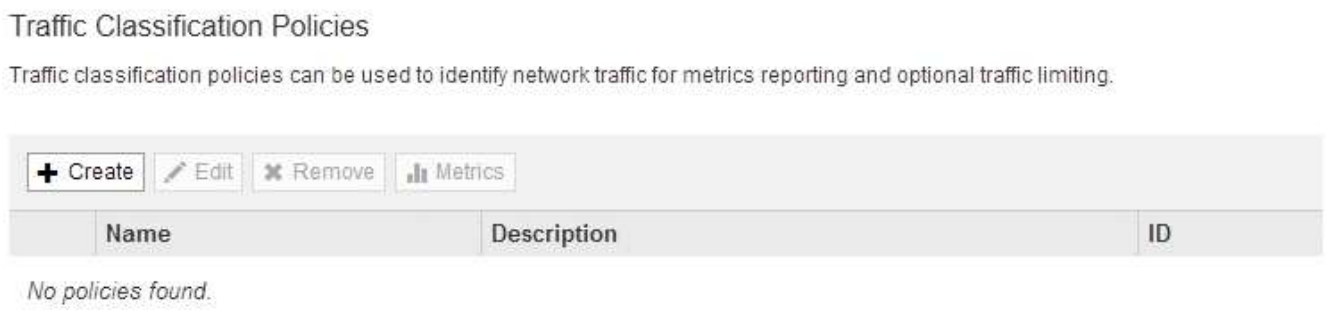
Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione di accesso root.
- È necessario aver creato tutti gli endpoint del bilanciamento del carico che si desidera associare.
- È necessario aver creato tutti i tenant che si desidera abbinare.

Fasi

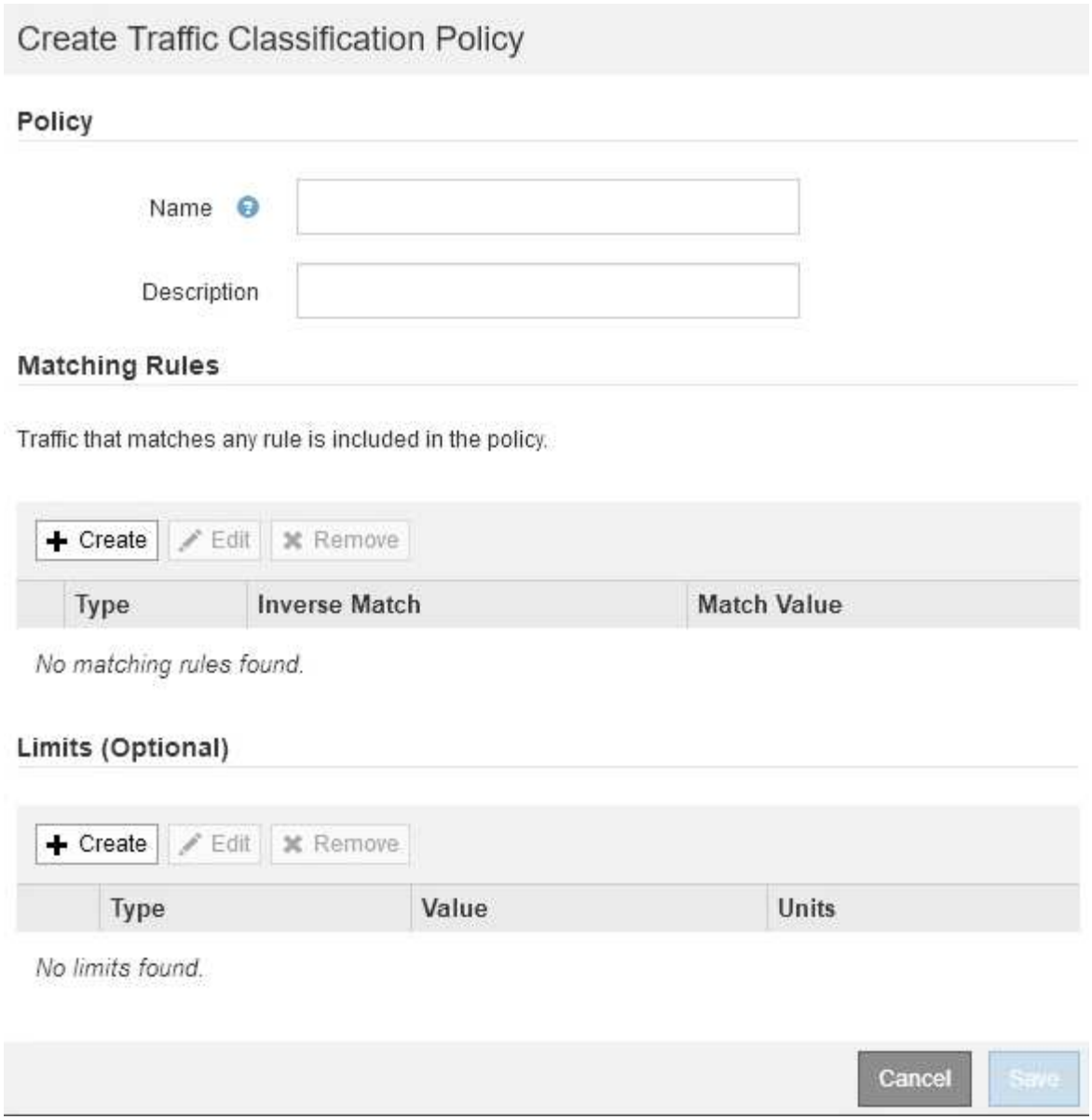
1. Selezionare **Configurazione** > **Impostazioni di rete** > **classificazione del traffico**.

   Viene visualizzata la pagina Criteri di classificazione del traffico.



2. Fare clic su **Create** (Crea).

   Viene visualizzata la finestra di dialogo Crea policy di classificazione del traffico.



3. Nel campo **Nome**, immettere un nome per la policy.

   Immettere un nome descrittivo per poter riconoscere il criterio.

4. Facoltativamente, aggiungere una descrizione per la policy nel campo **Descrizione**.

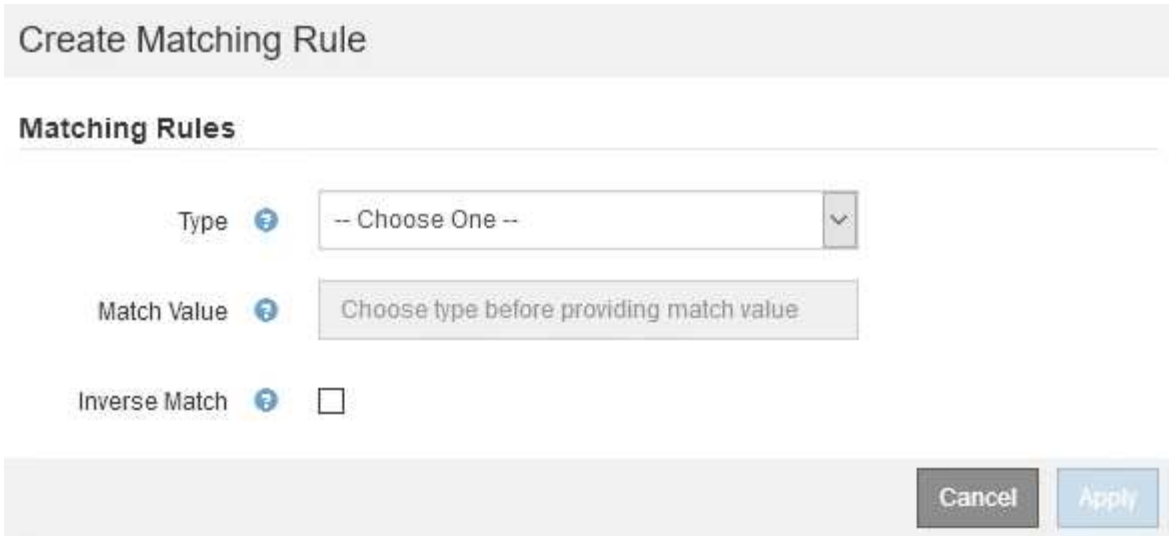
   Ad esempio, descrivi a cosa si applica questa policy di classificazione del traffico e a cosa limiterà.

5. Creare una o più regole corrispondenti per il criterio.

   Le regole corrispondenti controllano le entità interessate da questa policy di classificazione del traffico. Ad esempio, selezionare tenant se si desidera che questo criterio venga applicato al traffico di rete di un tenant specifico. In alternativa, selezionare Endpoint se si desidera applicare questo criterio al traffico di rete su un endpoint specifico del bilanciamento del carico.

   a. Fare clic su **Crea** nella sezione **regole corrispondenti**.

      Viene visualizzata la finestra di dialogo Create Matching Rule (Crea regola corrispondente).



b. Dal menu a discesa **Type**, selezionare il tipo di entità da includere nella regola di corrispondenza.

c. Nel campo **valore di corrispondenza**, immettere un valore di corrispondenza in base al tipo di entità scelta.

   - Bucket (bucket): Immettere il nome di un bucket.
   - Bucket Regex (Regex bucket): Immettere un'espressione regolare che verrà utilizzata per far corrispondere un set di nomi di bucket.

     L'espressione regolare non è ancorata. Utilizzare l'ancora ^ per trovare la corrispondenza all'inizio del nome del bucket e utilizzare l'ancora per la corrispondenza alla fine del nome.

   - CIDR: Immettere una subnet IPv4, nella notazione CIDR, che corrisponda alla subnet desiderata.
   - Endpoint: Selezionare un endpoint dall'elenco degli endpoint esistenti. Questi sono gli endpoint del bilanciamento del carico definiti nella pagina endpoint del bilanciamento del carico.
   - Tenant (tenant): Selezionare un tenant dall'elenco dei tenant esistenti. L'abbinamento dei tenant si basa sulla proprietà del bucket a cui si accede. L'accesso anonimo a un bucket corrisponde al tenant proprietario del bucket.

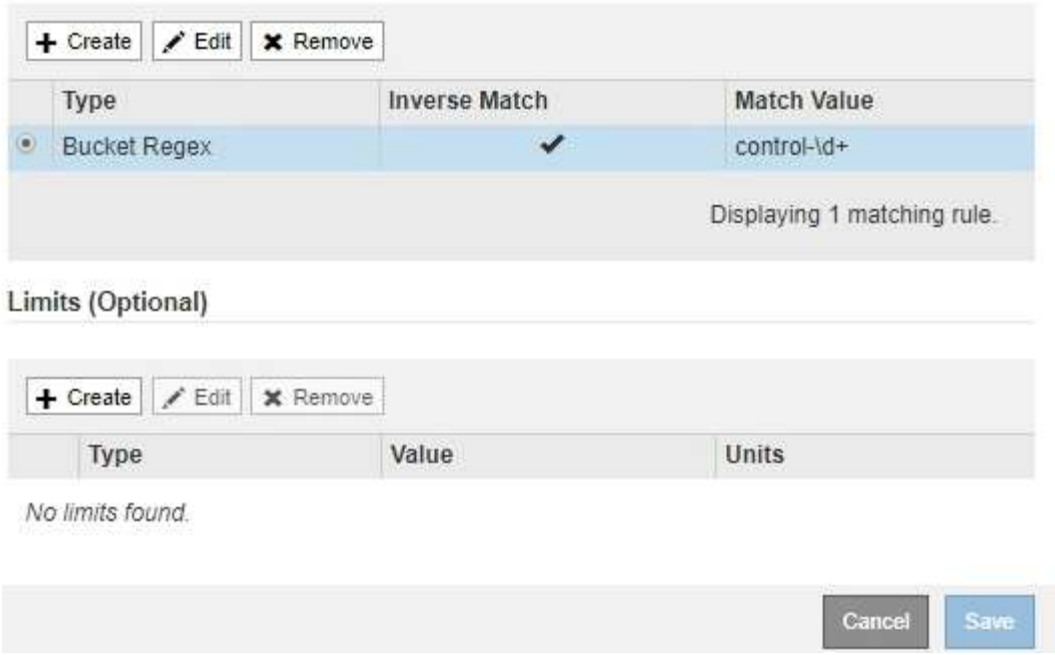
d. Se si desidera far corrispondere tutto il traffico di rete *tranne* corrispondente al valore Type and Match appena definito, selezionare la casella di controllo **Inverse**. In caso contrario, lasciare deselezionata la casella di controllo.

   Ad esempio, se si desidera che questo criterio venga applicato a tutti gli endpoint del bilanciamento del carico tranne uno, specificare l'endpoint del bilanciamento del carico da escludere e selezionare **inverso**.

   > Per un criterio contenente più adattatori in cui almeno uno è un adattatore inverso, fare attenzione a non creare un criterio che corrisponda a tutte le richieste.

e. Fare clic su **Apply** (Applica).

   La regola viene creata ed elencata nella tabella regole corrispondenti.



a. Ripetere questi passaggi per ogni regola che si desidera creare per il criterio.

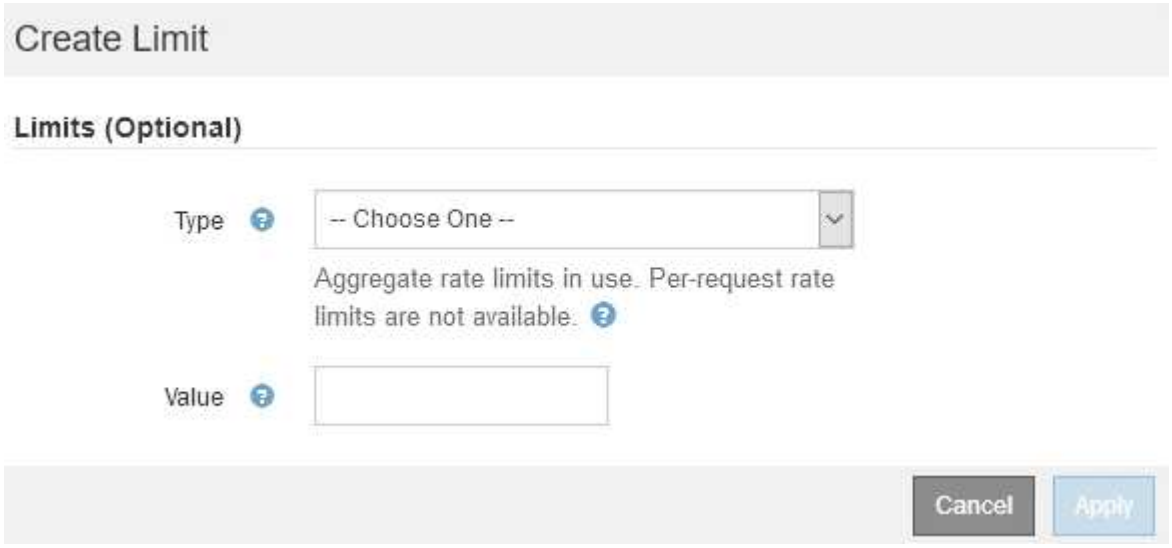
> Il traffico che corrisponde a qualsiasi regola viene gestito dal criterio.

6. Facoltativamente, creare limiti per la policy.

> Anche se non si creano limiti, StorageGRID raccoglie le metriche in modo da poter monitorare il traffico di rete corrispondente alla policy.

a. Fare clic su **Crea** nella sezione **limiti**.

Viene visualizzata la finestra di dialogo Create Limit (Crea limite).



b. Nell'elenco a discesa **tipo**, selezionare il tipo di limite che si desidera applicare al criterio.

Nell'elenco seguente, **in** si riferisce al traffico dai client S3 o Swift al bilanciamento del carico StorageGRID, mentre **out** si riferisce al traffico dal bilanciamento del carico ai client S3 o Swift.

- Larghezza di banda aggregata in
- Larghezza di banda aggregata in uscita
- Richieste di lettura simultanee
- Richieste di scrittura simultanee
- Larghezza di banda per richiesta in
- Larghezza di banda per richiesta in uscita
- Velocità richiesta di lettura
- Tasso di richieste di scrittura

> È possibile creare policy per limitare la larghezza di banda aggregata o per limitare la larghezza di banda per richiesta. Tuttavia, StorageGRID non può limitare entrambi i tipi di larghezza di banda contemporaneamente. I limiti di larghezza di banda aggregati potrebbero imporre un ulteriore impatto minore sulle performance sul traffico non limitato.

Per i limiti di larghezza di banda, StorageGRID applica la policy che meglio corrisponde al tipo di limite impostato. Ad esempio, se si dispone di una policy che limita il traffico in una sola direzione, il traffico nella direzione opposta sarà illimitato, anche se il traffico corrisponde a criteri aggiuntivi con limiti di larghezza di banda. StorageGRID implementa le corrispondenze "Best" per i limiti di larghezza di banda nel seguente ordine:

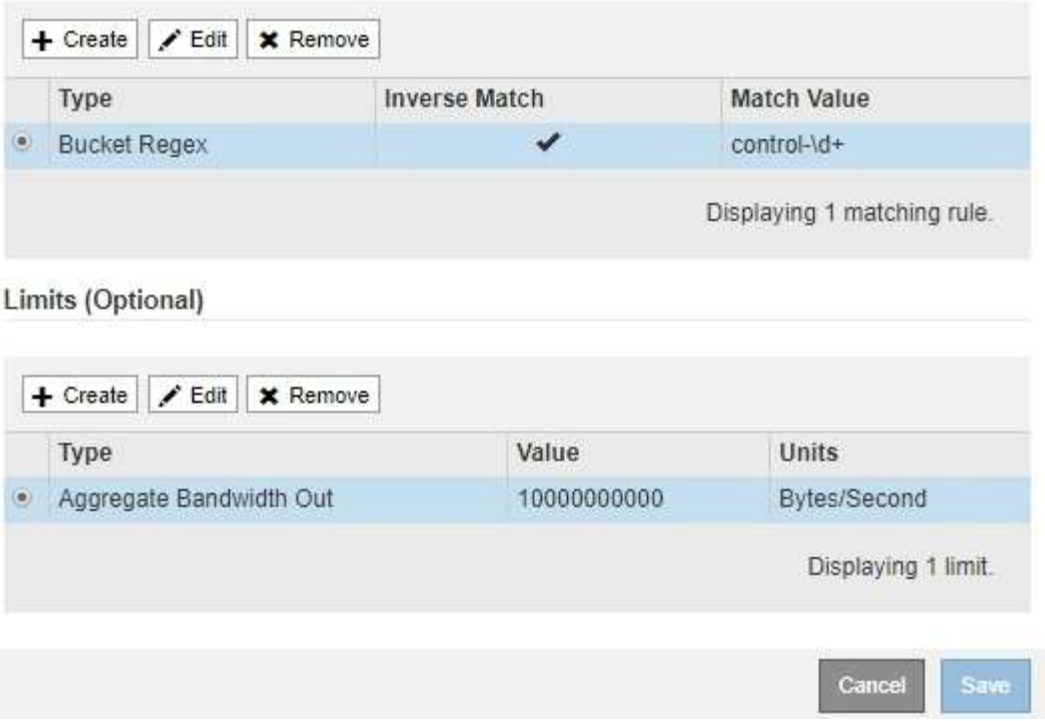
- Indirizzo IP esatto (/32 mask)
- Nome esatto del bucket
- Regex. Bucket
- Tenant
- Endpoint
- Corrispondenze CIDR non esatte (non /32)
- Corrispondenze inverse

c. Nel campo **valore**, immettere un valore numerico per il tipo di limite scelto.

   Le unità previste vengono visualizzate quando si seleziona un limite.

d. Fare clic su **Apply** (Applica).

   Il limite viene creato ed è elencato nella tabella dei limiti.



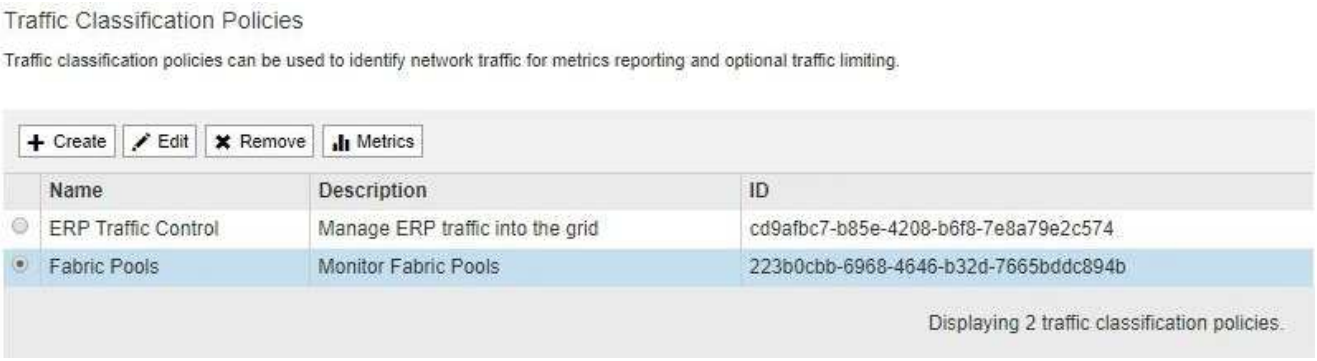
e. Ripetere questi passaggi per ciascun limite che si desidera aggiungere al criterio.

   Ad esempio, se si desidera creare un limite di larghezza di banda di 40 Gbps per un livello SLA, creare un limite di larghezza di banda aggregata in limite e un limite di larghezza di banda aggregato in uscita e impostare ciascuno su 40 Gbps.

   Per convertire megabyte al secondo in gigabit al secondo, moltiplicare per otto. Ad esempio, 125 MB/s equivale a 1,000 Mbps o 1 Gbps.

7. Al termine della creazione di regole e limiti, fare clic su **Save** (Salva).

   La policy viene salvata ed è elencata nella tabella Traffic Classification Policies (Criteri di classificazione del traffico).



   Il traffico dei client S3 e Swift viene ora gestito in base alle policy di classificazione del traffico. È possibile visualizzare i diagrammi di traffico e verificare che i criteri stiano applicando i limiti di traffico previsti.

Informazioni correlate

"Gestione del bilanciamento del carico"

"Visualizzazione delle metriche del traffico di rete"

Modifica di una policy di classificazione del traffico

È possibile modificare un criterio di classificazione del traffico per modificarne il nome o la descrizione oppure per creare, modificare o eliminare eventuali regole o limiti per il criterio.

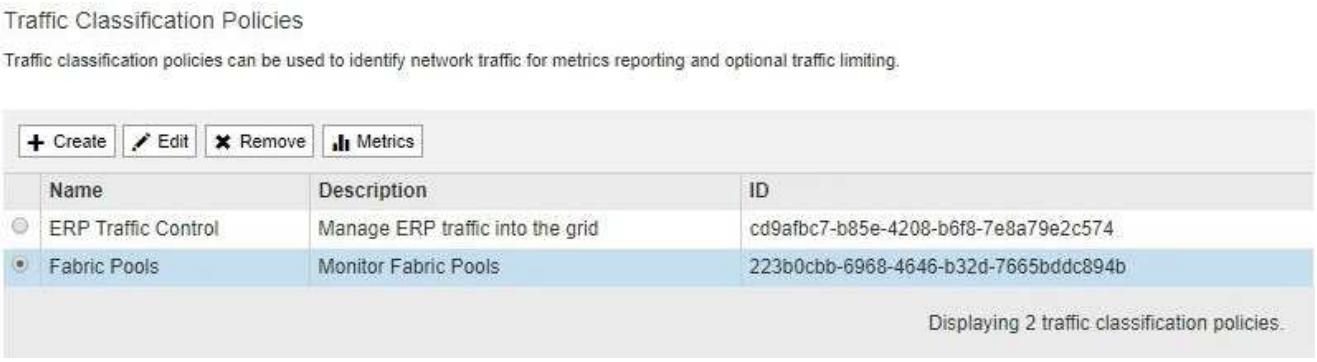
Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione di accesso root.

Fasi

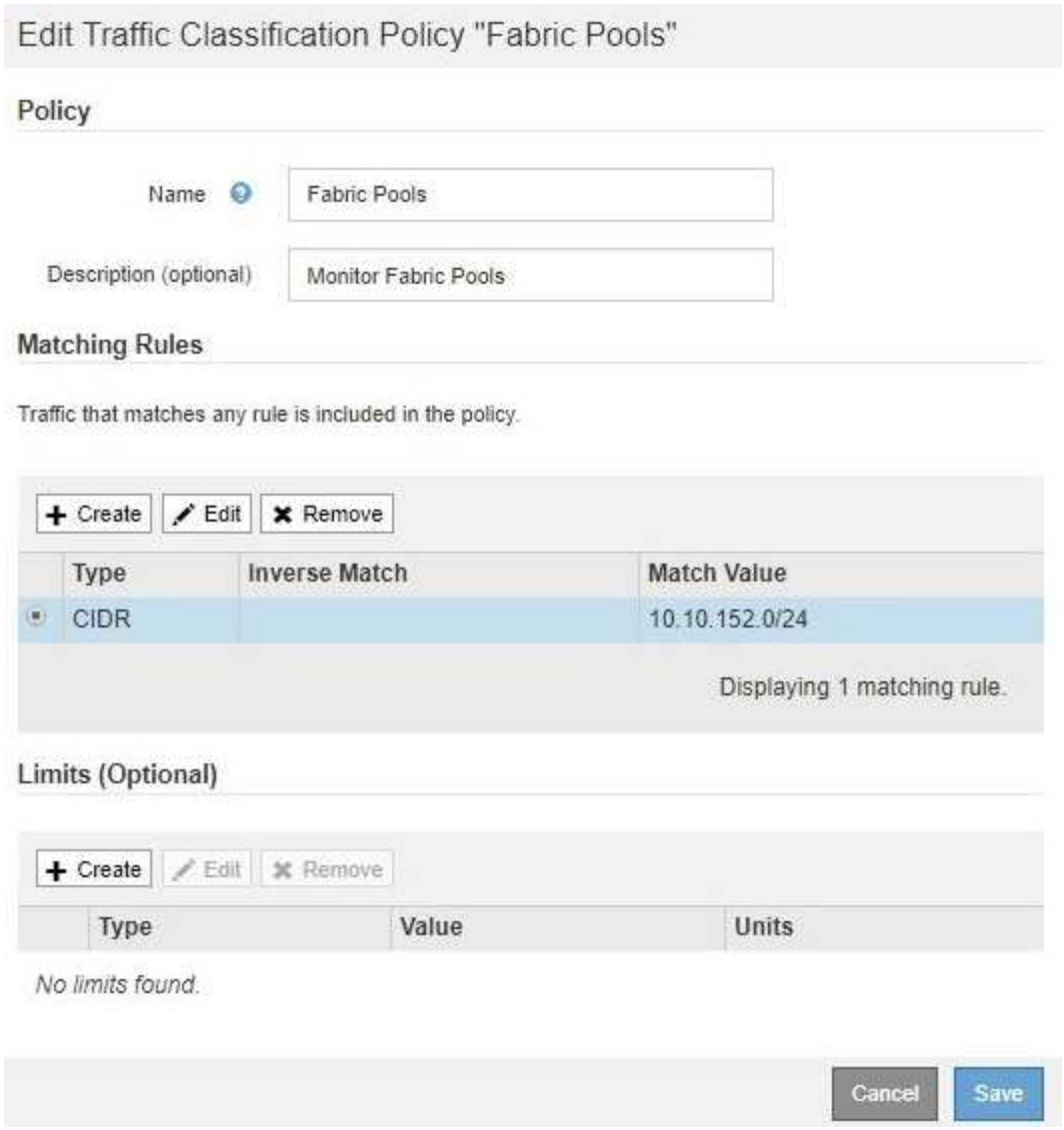
1. Selezionare **Configurazione** > **Impostazioni di rete** > **classificazione del traffico**.

   Viene visualizzata la pagina Traffic Classification Policies (Criteri di classificazione del traffico) e i criteri esistenti sono elencati nella tabella.



2. Selezionare il pulsante di opzione a sinistra del criterio che si desidera modificare.
3. Fare clic su **Edit** (Modifica).

   Viene visualizzata la finestra di dialogo Modifica policy di classificazione del traffico.



4. Creare, modificare o rimuovere regole e limiti corrispondenti in base alle esigenze.
   a. Per creare una regola o un limite corrispondente, fare clic su **Crea** e seguire le istruzioni per creare una regola o un limite.
   b. Per modificare una regola o un limite corrispondente, selezionare il pulsante di opzione corrispondente alla regola o al limite, fare clic su **Edit** nella sezione **Matching Rules** (regole corrispondenti) o nella sezione **Limits** (limiti) e seguire le istruzioni per creare una regola o un limite.
   c. Per rimuovere una regola o un limite corrispondente, selezionare il pulsante di opzione corrispondente alla regola o al limite e fare clic su **Rimuovi**. Quindi, fare clic su **OK** per confermare che si desidera rimuovere la regola o il limite.
5. Una volta creata o modificata una regola o un limite, fare clic su **Apply** (Applica).
6. Una volta terminata la modifica del criterio, fare clic su **Save** (Salva).

   Le modifiche apportate alla policy vengono salvate e il traffico di rete viene gestito in base alle policy di classificazione del traffico. È possibile visualizzare i diagrammi di traffico e verificare che i criteri stiano applicando i limiti di traffico previsti.

Eliminazione di una policy di classificazione del traffico

Se non è più necessario un criterio di classificazione del traffico, è possibile eliminarlo.

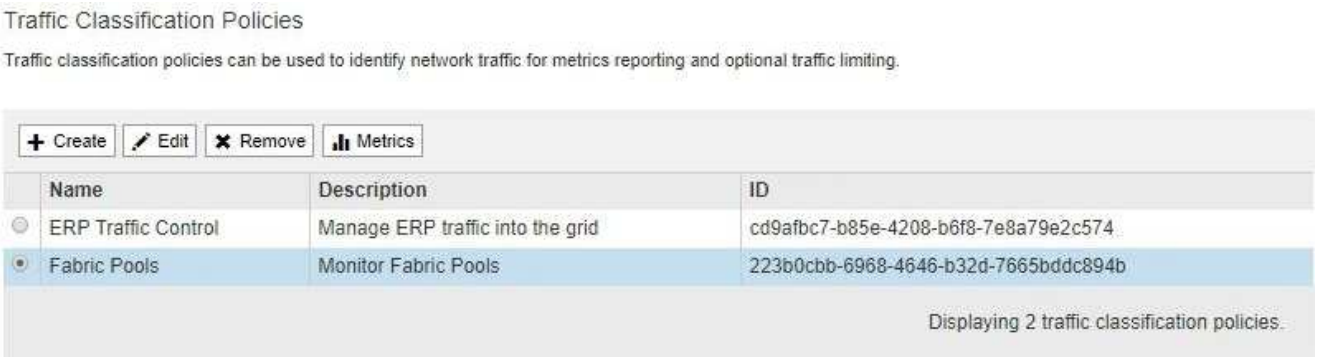
Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione di accesso root.

Fasi

1. Selezionare **Configurazione** > **Impostazioni di rete** > **classificazione del traffico**.

   Viene visualizzata la pagina Traffic Classification Policies (Criteri di classificazione del traffico) e i criteri esistenti sono elencati nella tabella.



2. Selezionare il pulsante di opzione a sinistra del criterio che si desidera eliminare.
3. Fare clic su **Rimuovi**.

   Viene visualizzata la finestra di dialogo Avviso.

4. Fare clic su **OK** per confermare che si desidera eliminare il criterio.

   La policy viene eliminata.

Visualizzazione delle metriche del traffico di rete

È possibile monitorare il traffico di rete visualizzando i grafici disponibili nella pagina Traffic Classification Policies (Criteri di classificazione del traffico).

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.

- È necessario disporre dell'autorizzazione di accesso root.

A proposito di questa attività

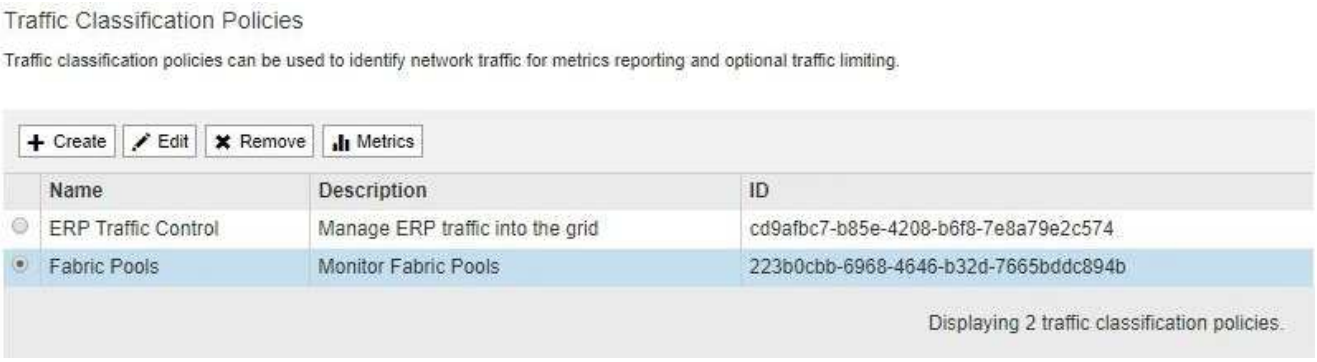
Per qualsiasi criterio di classificazione del traffico esistente, è possibile visualizzare le metriche per il servizio Load Balancer per determinare se il criterio limita correttamente il traffico nella rete. I dati nei grafici possono aiutare a determinare se è necessario modificare la policy.

Anche se non vengono impostati limiti per una policy di classificazione del traffico, vengono raccolte le metriche e i grafici forniscono informazioni utili per comprendere le tendenze del traffico.

Fasi

1. Selezionare **Configurazione** > **Impostazioni di rete** > **classificazione del traffico**.

   Viene visualizzata la pagina Traffic Classification Policies (Criteri di classificazione del traffico) e i criteri esistenti sono elencati nella tabella.



2. Selezionare il pulsante di opzione a sinistra della policy per la quale si desidera visualizzare le metriche.
3. Fare clic su **metriche**.

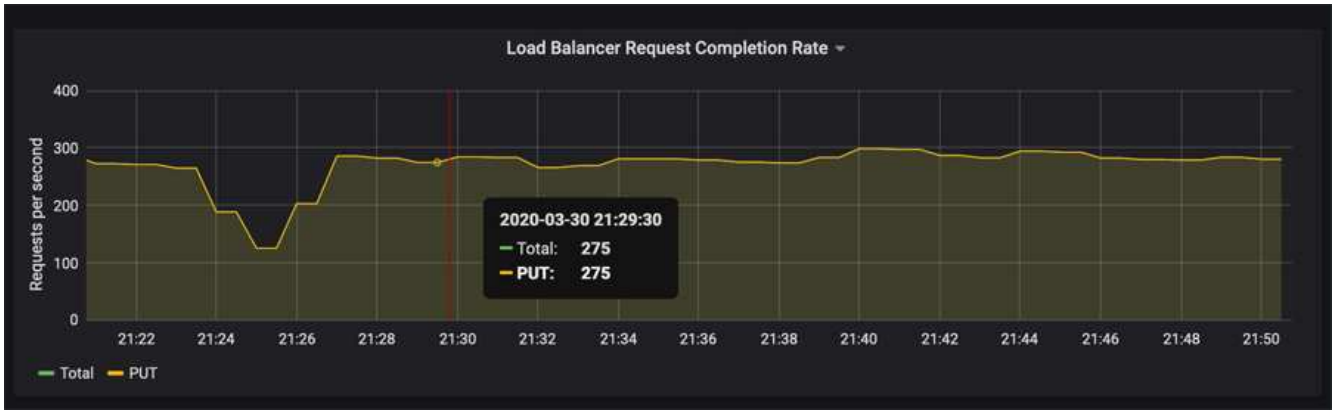
   Viene visualizzata una nuova finestra del browser e i grafici della policy di classificazione del traffico. I grafici visualizzano le metriche solo per il traffico corrispondente al criterio selezionato.

   È possibile selezionare altri criteri da visualizzare utilizzando l'elenco a discesa **policy**.

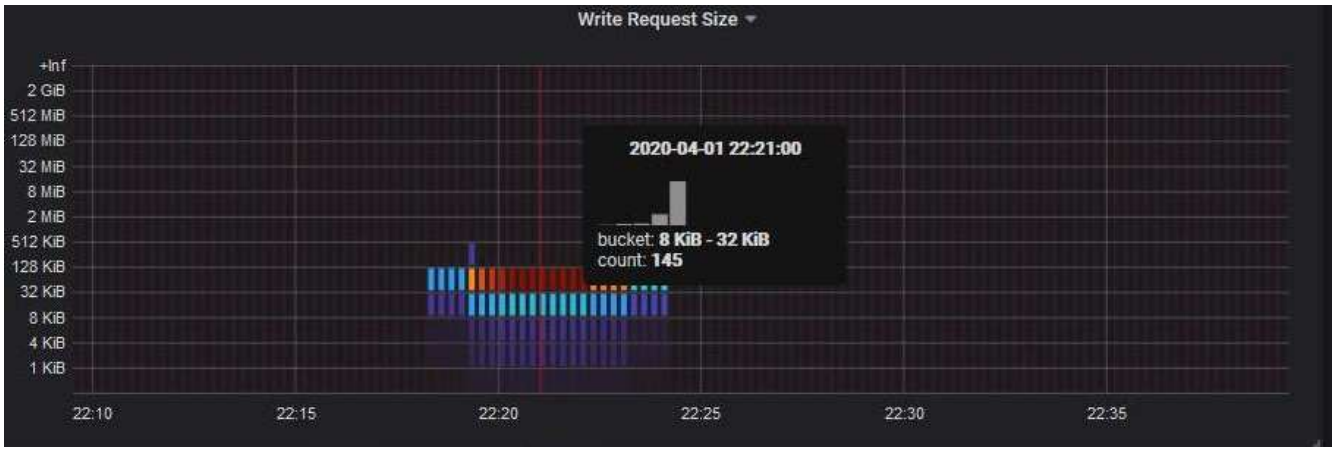
I grafici seguenti sono inclusi nella pagina Web.

- Load Balancer Request Traffic: Questo grafico fornisce una media mobile di 3 minuti del throughput dei dati trasmessi tra gli endpoint del bilanciamento del carico e i client che eseguono le richieste, in bit al secondo.
- Tasso di completamento della richiesta di bilanciamento del carico: Questo grafico fornisce una media mobile di 3 minuti del numero di richieste completate al secondo, suddiviso per tipo di richiesta (GET, PUT, HEAD e DELETE). Questo valore viene aggiornato quando le intestazioni di una nuova richiesta sono state convalidate.
- Tasso di risposta agli errori: Questo grafico fornisce una media mobile di 3 minuti del numero di risposte agli errori restituite ai client al secondo, suddiviso per codice di risposta agli errori.
- Durata media della richiesta (non errore): Questo grafico fornisce una media mobile di 3 minuti delle durate della richiesta, suddivisa per tipo di richiesta (GET, PUT, HEAD e DELETE). Ogni durata della richiesta inizia quando un'intestazione di richiesta viene analizzata dal servizio Load Balancer e termina quando il corpo di risposta completo viene restituito al client.
- Write Request Rate by Object Size (velocità di richiesta di scrittura per dimensione oggetto): Questa mappa termica fornisce una media mobile di 3 minuti della velocità di completamento delle richieste di scrittura in base alle dimensioni dell'oggetto. In questo contesto, le richieste di scrittura si riferiscono solo alle richieste PUT.
- Read Request Rate by Object Size (velocità richiesta di lettura per dimensione oggetto): Questa mappa termica fornisce una media mobile di 3 minuti della velocità di completamento delle richieste di lettura in base alle dimensioni dell'oggetto. In questo contesto, le richieste di lettura si riferiscono solo alle richieste GET. I colori nella mappa termica indicano la frequenza relativa delle dimensioni di un oggetto all'interno di un singolo grafico. I colori più freddi (ad esempio, viola e blu) indicano tassi relativi inferiori, mentre i colori più caldi (ad esempio, arancione e rosso) indicano tassi relativi più elevati.

4. Posizionare il cursore su un grafico a linee per visualizzare una finestra a comparsa di valori su una parte specifica del grafico.



5. Spostare il cursore su una mappa termica per visualizzare una finestra a comparsa che mostra la data e l'ora del campione, le dimensioni degli oggetti aggregati nel conteggio e il numero di richieste al secondo durante tale periodo di tempo.



6. Utilizzare l'elenco a discesa **Policy** in alto a sinistra per selezionare un criterio diverso.

   Vengono visualizzati i grafici relativi al criterio selezionato.

7. In alternativa, accedere ai grafici dal menu **supporto**.
   a. Selezionare **supporto Strumenti metriche**.
   b. Nella sezione **Grafana** della pagina, selezionare **Traffic Classification Policy**.
   c. Selezionare il criterio dall'elenco a discesa in alto a sinistra nella pagina.

      Le policy di classificazione del traffico sono identificate dal loro ID. Gli ID policy sono elencati nella pagina Traffic Classification Policies.

8. Analizzare i grafici per determinare la frequenza con cui il criterio limita il traffico e se è necessario modificare il criterio.

Informazioni correlate

"Monitor risoluzione dei problemi"

Quali sono i costi di collegamento

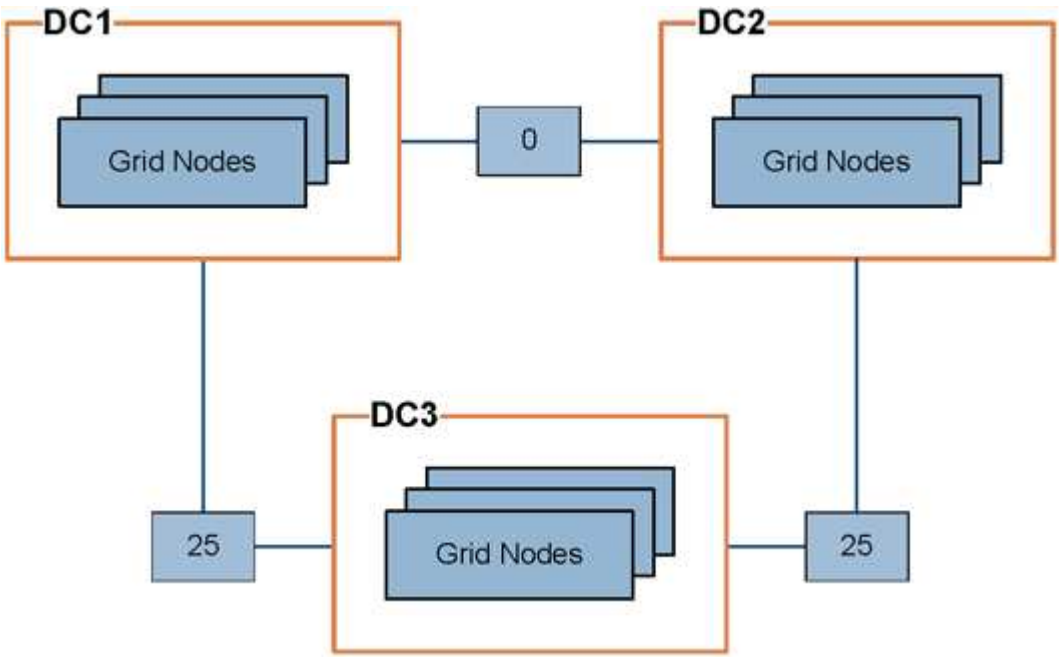
I costi di collegamento consentono di assegnare la priorità al sito del data center che fornisce un servizio richiesto quando esistono due o più siti del data center. È possibile

regolare i costi di collegamento in modo da riflettere la latenza tra i siti.

- I costi di collegamento vengono utilizzati per assegnare la priorità alla copia oggetto utilizzata per soddisfare i recuperi di oggetti.
- I costi di collegamento vengono utilizzati dall'API di gestione del grid e dall'API di gestione del tenant per determinare i servizi StorageGRID interni da utilizzare.
- I costi di collegamento vengono utilizzati dal servizio CLB sui nodi gateway per indirizzare le connessioni client.

> Il servizio CLB è obsoleto.

Il diagramma mostra una griglia a tre siti con costi di collegamento configurati tra i siti:



- Il servizio CLB sui nodi gateway distribuisce in modo uguale le connessioni client a tutti i nodi di storage nello stesso sito del data center e a qualsiasi sito del data center con un costo di collegamento pari a 0.

  Nell'esempio, un nodo gateway nel sito 1 del data center (DC1) distribuisce in modo uguale le connessioni client ai nodi di storage in DC1 e ai nodi di storage in DC2. Un nodo gateway in DC3 invia le connessioni client solo ai nodi di storage in DC3.

- Quando si recupera un oggetto che esiste come copie replicate multiple, StorageGRID recupera la copia nel data center che ha il costo di collegamento più basso.

  Nell'esempio, se un'applicazione client in DC2 recupera un oggetto memorizzato sia in DC1 che in DC3, l'oggetto viene recuperato da DC1, perché il costo del collegamento da DC1 a D2 è 0, che è inferiore al costo del collegamento da DC3 a DC2 (25).

I costi di collegamento sono numeri relativi arbitrari senza unità di misura specifica. Ad esempio, un costo di collegamento di 50 viene utilizzato in modo meno preferenziale rispetto a un costo di collegamento di 25. La tabella mostra i costi di collegamento comunemente utilizzati.

Collegamento	Costo del collegamento	Note
Tra siti fisici di data center	25 (impostazione predefinita)	Data center connessi tramite un collegamento WAN.
Tra i siti del data center logico nella stessa posizione fisica	0	Data center logici nello stesso edificio fisico o campus connessi da una LAN.

Informazioni correlate

"Come funziona il bilanciamento del carico - servizio CLB"

Aggiornamento dei costi di collegamento

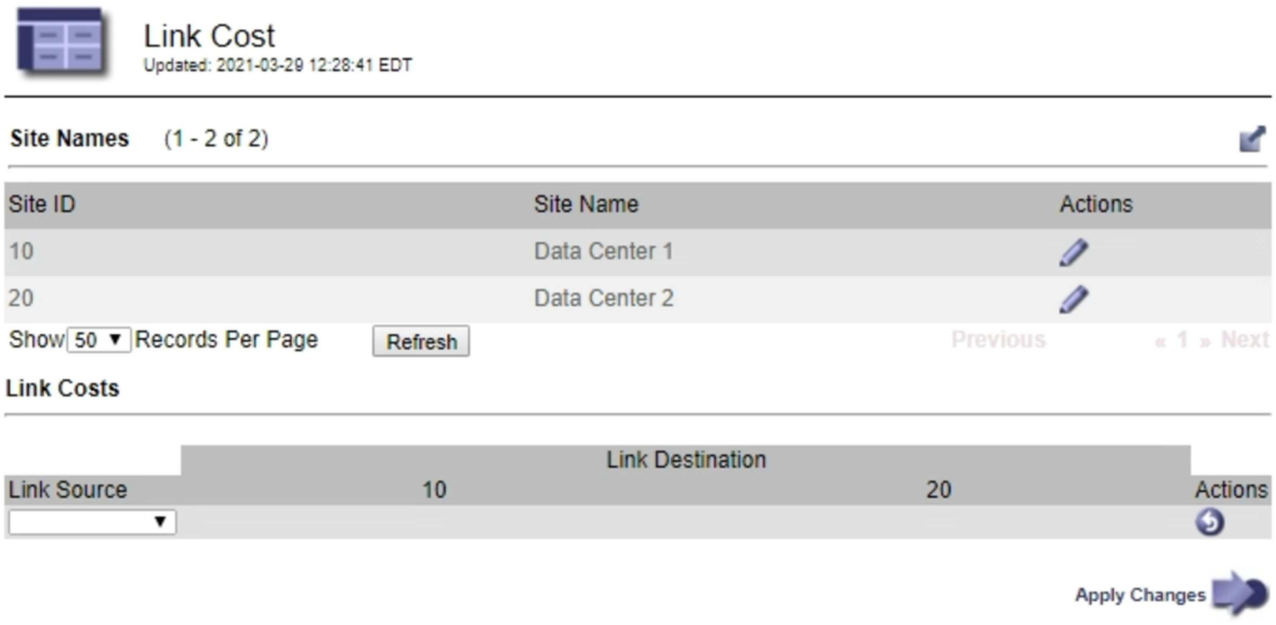
È possibile aggiornare i costi di collegamento tra i siti del data center per riflettere la latenza tra i siti.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione Grid Topology Page Configuration (Configurazione pagina topologia griglia).

Fasi

1. Selezionare **Configurazione Impostazioni di rete costo collegamento**.



2. Selezionare un sito in **link Source** (origine collegamento) e immettere un valore di costo compreso tra 0 e 100 in **link Destination** (destinazione collegamento).

   Non è possibile modificare il costo del collegamento se l'origine è la stessa della destinazione.

   Per annullare le modifiche, fare clic su **Ripristina**.

3. Fare clic su **Applica modifiche**.

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.