Gestisci il bilanciamento del carico

StorageGRID software

NetApp
July 23, 2026

This PDF was generated from https://docs.netapp.com/it-it/storagegrid-120/admin/managing-load-balancing.html on July 23, 2026. Always check docs.netapp.com for the latest.

Sommario

Gestisci il bilanciamento del carico

Scopri il bilanciamento del carico di StorageGRID

Puoi usare il bilanciamento del carico per gestire i carichi di lavoro di ingest e recupero dai client S3.

${post_edited_translations.segment}

Quando un'applicazione client salva o recupera dati da un sistema StorageGRID, StorageGRID utilizza un bilanciatore del carico per gestire il carico di lavoro di acquisizione e recupero. Il bilanciamento del carico massimizza la velocità e la capacità di connessione distribuendo il carico di lavoro su più Storage Node.

Il servizio StorageGRID Load Balancer è installato su tutti i nodi di amministrazione e su tutti i nodi gateway e fornisce bilanciamento del carico Layer 7. Esegue la terminazione Transport Layer Security (TLS) delle richieste dei client, ispeziona le richieste e stabilisce nuove connessioni sicure ai nodi Storage.

Il servizio Load Balancer su ciascun nodo opera in modo indipendente durante l'inoltro del traffico client ai Storage Node. Attraverso un processo di ponderazione, il servizio Load Balancer instrada più richieste ai Storage Node con una maggiore disponibilità di CPU.

> Sebbene il servizio StorageGRID Load Balancer sia il meccanismo di bilanciamento del carico consigliato, potresti voler integrare un bilanciatore di carico di terze parti. Per informazioni, contatta il tuo NetApp account representative o consulta "Utilizza bilanciatori di carico di terze parti con StorageGRID".

Di quanti nodi di bilanciamento del carico hai bisogno?

Come best practice generale, ogni sito nel tuo sistema StorageGRID dovrebbe includere due o più nodi con il servizio Load Balancer. Ad esempio, un sito potrebbe includere due Gateway Node oppure sia un Admin Node che un Gateway Node. Assicurati che ci sia un'infrastruttura di rete, hardware o virtualizzazione adeguata per ogni nodo di bilanciamento del carico, che tu stia utilizzando servizi appliance, nodi bare metal o nodi basati su macchine virtuali (VM).

${post_edited_translations.segment}

Un endpoint del load balancer definisce la porta e il protocollo di rete (HTTPS o HTTP) che le richieste delle applicazioni client in entrata e in uscita utilizzeranno per accedere ai nodi che contengono il servizio Load Balancer. L'endpoint definisce anche il tipo di client (S3), la modalità di binding e, facoltativamente, un elenco di tenant consentiti o bloccati.

Per creare un endpoint del bilanciatore del carico, utilizza il Grid Manager oppure completa i wizard di setup di S3 e FabricPool:

- "${post_edited_translations.segment}"
- "Usa la setup wizard"
- "Utilizza il setup wizard di FabricPool"

Considerazioni sulla memorizzazione nella cache del bilanciatore di carico

La memorizzazione nella cache migliora significativamente le prestazioni quando un carico di lavoro opera su un sottoinsieme di dati e accede agli oggetti più volte. Inoltre, la memorizzazione nella cache consente l'accesso remoto allo storage a oggetti senza una completa implementazione della grid. La memorizzazione nella cache del load balancer è disponibile solo per i Gateway Nodes.

Quando crei gli endpoint del bilanciamento del carico:

- Abilita la memorizzazione nella cache solo per i carichi di lavoro che sono memorizzabili nella cache. I carichi di lavoro che accedono ai dati non memorizzati nella cache più spesso dei dati memorizzati nella cache avranno prestazioni peggiori rispetto a quelli che non sarebbero stati gestiti dalla cache. In alcuni casi, i carichi di lavoro con elevati tassi di sovrascrittura e rimozione potrebbero anche superare la durata di scrittura garantita dell'unità.
- Valuta di aggiungere ulteriori endpoint o nodi per la memorizzazione nella cache dei singoli carichi di lavoro che sono buoni candidati per la cache.
- Usa endpoint distinti per i carichi di lavoro memorizzabili nella cache e per quelli non memorizzabili nella cache. Questa separazione garantisce che i meccanismi di caching vengano applicati correttamente e non interferiscano con l'elaborazione dei dati non memorizzabili nella cache.
- Valuta un potenziale carico di lavoro memorizzabile nella cache indirizzandolo all'endpoint abilitato alla cache. Monitora e verifica il tasso di cache hit per determinare l'idoneità del carico di lavoro per la memorizzazione nella cache. Questa valutazione aiuta a ottimizzare le prestazioni e a garantire un uso efficiente delle risorse di cache.
- "${post_edited_translations.segment}" per determinare se un carico di lavoro esistente sia un buon candidato per la memorizzazione nella cache. Per un determinato periodo di tempo, determina quale percentuale di GET è per oggetti univoci. Per essere adatto alla memorizzazione nella cache, questo valore deve essere inferiore al 50%.

Esempi di carichi di lavoro che potrebbero essere buoni candidati per la memorizzazione nella cache

- Data lake
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- asset management multimediale
- Produzione video

- È possibile memorizzare nella cache più versioni di un oggetto.
- Sono supportate le operazioni di lettura di intervalli.

Esempi di carichi di lavoro che non sono buoni candidati per la memorizzazione nella cache

- FabricPool
- ${post_edited_translations.segment}
- Tiering dello storage

Se un qualsiasi contenuto che deve essere fornito dalla cache richiede la crittografia a riposo, "abilita la crittografia del nodo o dell'unità" sul nodo di cache.

Tipi di oggetti e richieste che non verranno memorizzati nella cache

- Il `response-content-encoding` parametro di query
- Il `partNumber` parametro di query
- ${post_edited_translations.segment}
  - `If-Match`
  - `If-Modified-Since`
  - `If-None-Match`
  - `If-Unmodified-Since`
- ${post_edited_translations.segment}
  - ${post_edited_translations.segment}
  - SSE-C (crittografia lato server con chiavi fornite dal cliente)
  - ${post_edited_translations.segment}

Tutte le richieste che non sono memorizzate nella cache vengono inoltrate a un LDR a monte come se la cache non fosse abilitata.

Informazioni correlate

- "Risolvi i problemi di caching del bilanciatore di carico"
- Per ulteriori informazioni sulla cache del bilanciatore di carico, contatta il supporto tecnico.

Considerazioni per la porta

La porta per un endpoint del bilanciatore del carico ha come valore predefinito 10433 per il primo endpoint che crei, ma puoi specificare qualsiasi porta esterna inutilizzata tra 1 e 65535. Se usi la porta 80 o 443, l'endpoint utilizzerà il servizio di bilanciamento del carico solo sui nodi Gateway. Queste porte sono riservate sui nodi Admin. Se usi la stessa porta per più di un endpoint, devi specificare una modalità di associazione diversa per ciascun endpoint.

Le porte utilizzate da altri servizi di grid non sono consentite. Vedi "Porte interne di StorageGRID".

Considerazioni sul protocollo di rete

Nella maggior parte dei casi, le connessioni tra le applicazioni client e StorageGRID dovrebbero utilizzare la crittografia Transport Layer Security (TLS). La connessione a StorageGRID senza crittografia TLS è supportata ma non consigliata, in particolare negli ambienti di produzione. Quando selezioni il protocollo di rete per l'endpoint del bilanciatore del carico di StorageGRID, dovresti selezionare **HTTPS**.

Considerazioni relative ai certificati degli endpoint del bilanciatore di carico

Se selezioni **HTTPS** come protocollo di rete per l'endpoint del bilanciatore del carico, devi fornire un certificato di sicurezza. Puoi utilizzare una qualsiasi di queste tre opzioni quando crei l'endpoint del bilanciatore del carico:

- **Carica un certificato firmato (consigliato)**. Questo certificato può essere firmato da un'autorità di certificazione (CA) pubblica attendibile o privata. L'utilizzo di un certificato server CA pubblico attendibile per proteggere la connessione è la best practice. A differenza dei certificati generati, i certificati firmati da una CA possono essere ruotati senza interruzioni, il che può aiutare a evitare problemi di scadenza.

Devi ottenere i seguenti file prima di creare l'endpoint del bilanciamento del carico:

  - ${post_edited_translations.segment}
  - Il file della chiave privata del certificato server personalizzato.
  - Facoltativamente, un pacchetto CA dei certificati di ciascuna autorità di certificazione emittente intermedia.

- ${post_edited_translations.segment}
- **Usa il certificato S3 globale di StorageGRID**. Devi caricare o generare una versione personalizzata di questo certificato prima di poterlo selezionare per l'endpoint del bilanciamento del carico. Consulta "Configura i certificati API S3".

Di quali valori hai bisogno?

Per creare il certificato, devi conoscere tutti i nomi di dominio e gli indirizzi IP che le applicazioni client S3 utilizzeranno per accedere all'endpoint.

La voce **Subject DN** (Distinguished Name) del certificato deve includere il fully qualified domain name che l'applicazione client utilizzerà per StorageGRID. Ad esempio:

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

Come richiesto, il certificato può utilizzare caratteri jolly per rappresentare i fully qualified domain names di tutti i nodi Admin e Gateway che eseguono il servizio Load Balancer. Ad esempio, `*.storagegrid.example.com` usa il carattere jolly * per rappresentare `adm1.storagegrid.example.com` e `gn1.storagegrid.example.com`.

Se vuoi utilizzare richieste in stile S3 virtual hosted, il certificato deve includere anche una voce **Nome alternativo** per ogni "domain name endpoint S3" che hai configurato, inclusi eventuali nomi wildcard. Per esempio:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

Se usi i caratteri jolly per i domain name, rivedi il "${post_edited_translations.segment}".

${post_edited_translations.segment}

${post_edited_translations.segment}

Se il certificato utilizzato per proteggere la connessione tra l'applicazione S3 e StorageGRID scade, l'applicazione potrebbe perdere temporaneamente l'accesso a StorageGRID.

${post_edited_translations.segment}

- Monitora attentamente tutti gli avvisi che segnalano l'imminente scadenza dei certificati, come gli avvisi **Expiration of load balancer endpoint certificate** e **Expiration of global server certificate for S3 API**.
- Mantieni sempre sincronizzate le versioni del certificato di StorageGRID e dell'applicazione S3. Se sostituisci o rinnovi il certificato utilizzato per un endpoint del bilanciatore di carico, devi sostituire o

rinnovare anche il certificato equivalente utilizzato dall'applicazione S3.

- Utilizza un certificato CA firmato pubblicamente. Se utilizzi un certificato firmato da una CA, puoi sostituire i certificati in scadenza senza interruzioni.
- ${post_edited_translations.segment}

Considerazioni sulla modalità di binding

La modalità di binding ti consente di controllare quali indirizzi IP possono essere utilizzati per accedere a un endpoint del bilanciatore del carico. Se un endpoint utilizza una modalità di binding, le applicazioni client possono accedere all'endpoint solo se utilizzano un indirizzo IP consentito o il corrispondente fully qualified domain name (FQDN). Le applicazioni client che utilizzano qualsiasi altro indirizzo IP o FQDN non possono accedere all'endpoint.

Puoi specificare una delle seguenti modalità di associazione:

- **Global** (predefinito): le applicazioni client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi Gateway Node o Admin Node, l'indirizzo virtual IP (VIP) di qualsiasi gruppo HA su qualsiasi rete o un FQDN corrispondente. Utilizza questa impostazione a meno che tu non debba limitare l'accessibilità di un endpoint.
- **Indirizzi IP virtuali dei gruppi HA**. Le applicazioni client devono utilizzare un indirizzo IP virtuale (o il corrispondente FQDN) di un gruppo HA.
- **Interfacce dei nodi**. I client devono utilizzare gli indirizzi IP (o i corrispondenti FQDN) delle interfacce dei nodi selezionate.
- **Tipo di nodo**. In base al tipo di nodo selezionato, i client devono utilizzare l'indirizzo IP (o il corrispondente FQDN) di un qualsiasi Admin Node oppure l'indirizzo IP (o il corrispondente FQDN) di un qualsiasi Gateway Node.

Considerazioni per l'accesso del tenant

L'accesso dei tenant è una funzionalità di sicurezza opzionale che ti permette di controllare quali StorageGRID tenant account possono usare un endpoint del bilanciatore di carico per accedere ai propri bucket. Puoi consentire a tutti i tenant di accedere a un endpoint (impostazione predefinita), oppure puoi specificare un elenco di tenant autorizzati o bloccati per ciascun endpoint.

Puoi usare questa funzionalità per offrire un migliore isolamento di sicurezza tra i tenant e i loro endpoint. Ad esempio, potresti usarla per assicurarti che i materiali top-secret o altamente classificati di proprietà di un tenant restino completamente inaccessibili agli altri tenant.

> Ai fini del controllo degli accessi, il tenant viene determinato dalle chiavi di accesso utilizzate nella richiesta del client; se non vengono fornite chiavi di accesso come parte della richiesta (come nel caso di accesso anonimo), viene utilizzato il proprietario del bucket per determinare il tenant.

Esempio di accesso tenant

Per capire come funziona questa funzionalità di sicurezza, considera il seguente esempio:

1. Hai creato due endpoint di bilanciamento del carico, come segue:
   - Endpoint **pubblico**: usa la porta 10443 e permette l'accesso a tutti i tenant.
   - Endpoint **Top secret**: utilizza la porta 10444 e consente l'accesso solo al tenant **Top secret**. Tutti gli altri tenant non possono accedere a questo endpoint.

2. Il `top-secret.pdf` si trova in un bucket di proprietà del tenant **Top secret**.

Per accedere a `top-secret.pdf`, un utente nel tenant **Top secret** può inviare una richiesta GET a `https://w.x.y.z:10444/top-secret.pdf`. Poiché a questo tenant è consentito utilizzare l'endpoint 10444, l'utente può accedere all'oggetto. Tuttavia, se un utente appartenente a qualsiasi altro tenant invia la stessa richiesta allo stesso URL, riceve un messaggio immediato di Access Denied. L'accesso viene negato anche se le credenziali e la firma sono valide.

disponibilità CPU

Il servizio Load Balancer su ciascun Admin Node e Gateway Node opera in modo indipendente durante l'inoltro del traffico S3 agli Storage Node. Attraverso un processo di ponderazione, il servizio Load Balancer instrada un maggior numero di richieste agli Storage Node con maggiore disponibilità di CPU. Le informazioni sul carico della CPU dei nodi vengono aggiornate ogni pochi minuti, ma la ponderazione potrebbe essere aggiornata con maggiore frequenza. A tutti gli Storage Node viene assegnato un valore di peso base minimo, anche se un nodo segnala un utilizzo del 100% o non segnala affatto il proprio utilizzo.

${post_edited_translations.segment}

Configurare gli endpoint del bilanciamento del carico StorageGRID

Gli endpoint del bilanciatore di carico determinano le porte e i protocolli di rete che i client S3 possono utilizzare per connettersi al bilanciatore di carico StorageGRID sui nodi Gateway e Admin. Puoi anche usare gli endpoint per accedere a Grid Manager, Tenant Manager o a entrambi.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Permesso di accesso root".
- Hai esaminato il "considerazioni per il bilanciamento del carico".
- Se in precedenza hai rimappato una porta che intendi utilizzare per l'endpoint del bilanciatore di carico, hai "${post_edited_translations.segment}".
- Hai creato tutti i gruppi di alta disponibilità (HA) che intendi utilizzare. I gruppi HA sono consigliati, ma non obbligatori. Vedi "Gestisci i gruppi ad alta disponibilità".
- Se l'endpoint del bilanciatore di carico verrà utilizzato da "${post_edited_translations.segment}", non deve utilizzare gli indirizzi IP o i FQDN di alcun nodo bare-metal. Per gli endpoint del bilanciatore di carico utilizzati per S3 Select sono consentiti solo appliance di servizi e nodi software basati su VMware.
- Hai configurato tutte le interfacce VLAN che intendi utilizzare. Vedi "Configura le interfacce VLAN".
- ${post_edited_translations.segment}

> Le modifiche al certificato di un endpoint possono richiedere fino a 15 minuti per essere applicate a tutti i nodi.

  - Per caricare un certificato, ti servono il certificato del server, la chiave privata del certificato e, facoltativamente, un bundle CA.
  - Per generare un certificato, ti servono tutti i nomi di dominio e gli indirizzi IP che i client S3 useranno

per accedere all'endpoint. Devi anche conoscere il subject (Distinguished Name).

- Se vuoi utilizzare il certificato dell'API S3 di StorageGRID (che può essere utilizzato anche per le connessioni dirette ai Storage Node), hai già sostituito il certificato predefinito con un certificato personalizzato firmato da un'autorità di certificazione esterna. Vedi "Configura i certificati API S3".

Crea un endpoint del bilanciatore di carico

Ciascun endpoint del bilanciatore del carico per client S3 specifica una porta, un tipo di client (S3) e un protocollo di rete (HTTP o HTTPS). Gli endpoint del bilanciatore del carico dell'interfaccia di gestione specificano una porta, un tipo di interfaccia e una Client Network non attendibile.

Accedi al wizard

Passaggi

1. ${post_edited_translations.segment}
2. Per creare un endpoint per un client S3, seleziona la scheda **S3 client**.
3. ${post_edited_translations.segment}
4. Seleziona **Create**.

Inserisci i dettagli dell'endpoint

Passaggi

1. ${post_edited_translations.segment}

${post_edited_translations.segment}

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint, che verrà visualizzato nella tabella nella pagina degli endpoint del bilanciatore di carico.
Porta	La porta StorageGRID che desideri utilizzare per il bilanciamento del carico. Questo campo è impostato per impostazione predefinita su 10433 per il primo endpoint che crei, ma puoi inserire qualsiasi porta esterna non utilizzata da 1 a 65535. Se inserisci **80** o **8443**, l'endpoint viene configurato solo sui nodi Gateway, a meno che tu non abbia liberato la porta 8443. A quel punto puoi usare la porta 8443 come endpoint S3 e la porta verrà configurata sia sui nodi Gateway che sui nodi Admin.
${post_edited_translations.segment}	Deve essere **S3**.
Protocollo di rete	Il protocollo di rete che i client utilizzeranno per connettersi a questo endpoint. • Seleziona **HTTPS** per una comunicazione sicura con crittografia TLS (consigliato). Devi allegare un certificato di sicurezza prima di poter salvare l'endpoint. • Seleziona **HTTP** per una comunicazione meno sicura e non crittografata. Utilizza HTTP solo per una grid non di produzione.
${post_edited_translations.segment}	Abilita o disabilita "memorizzazione nella cache sui nodi Gateway" per questo endpoint del bilanciatore del carico. In caso di problemi con la cache, fai riferimento a "Risolvi i problemi di caching del bilanciatore di carico".

Interfaccia di gestione

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint, che verrà visualizzato nella tabella nella pagina degli endpoint del bilanciatore di carico.
Porta	La porta StorageGRID che vuoi usare per accedere a Grid Manager, Tenant Manager o entrambi. • Grid Manager: **8443** • Tenant Manager: **9443** • Sia Grid Manager che Tenant Manager: **443** **Nota**: Puoi usare queste porte preimpostate o altre porte disponibili.

Campo	Descrizione
Tipo di interfaccia	${post_edited_translations.segment}
Rete client non affidabile	Seleziona **Sì** se questo endpoint deve essere accessibile alle reti client non attendibili. Altrimenti, seleziona **No**. Quando selezioni **Sì**, la porta è aperta su tutte le Client Networks non attendibili. **Nota**: Puoi configurare una porta come aperta o chiusa alle reti client non attendibili solo quando crei l'endpoint del bilanciatore di carico.

1. Seleziona **Continue**.

Seleziona una modalità di associazione

Passaggi

1. Seleziona una modalità di associazione per l'endpoint per controllare come l'endpoint viene accessibile utilizzando qualsiasi indirizzo IP o utilizzando indirizzi IP e interfacce di rete specifici.

   Sono disponibili diverse modalità di binding sia per gli endpoint client che per gli endpoint dell'interfaccia di gestione. Tutte le modalità per entrambi i tipi di endpoint sono elencate qui.

Modalità	Descrizione
Globale (impostazione predefinita per gli endpoint client)	I client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi Gateway Node o Admin Node, l'indirizzo IP virtuale (VIP) di qualsiasi gruppo HA su qualsiasi rete o un FQDN corrispondente. ${post_edited_translations.segment}
Indirizzi IP virtuali dei gruppi HA	I client devono utilizzare un indirizzo IP virtuale (o il corrispondente FQDN) di un gruppo HA per accedere a questo endpoint. Gli endpoint con questa modalità di binding possono utilizzare tutti lo stesso numero di porta, a condizione che i gruppi HA che selezioni per gli endpoint non si sovrappongano.
${post_edited_translations.segment}	I client devono utilizzare gli indirizzi IP (o i corrispondenti FQDN) delle interfacce dei nodi selezionati per accedere a questo endpoint.
Tipo di nodo (solo endpoint client)	In base al tipo di nodo che selezioni, i client devono usare l'indirizzo IP (o il corrispondente FQDN) di qualsiasi Admin Node oppure l'indirizzo IP (o il corrispondente FQDN) di qualsiasi Gateway Node per accedere a questo endpoint.

Modalità	Descrizione
Tutti i nodi amministratori (impostazione predefinita per gli endpoint dell'interfaccia di gestione)	I client devono utilizzare l'indirizzo IP (o il corrispondente FQDN) di qualsiasi Admin Node per accedere a questo endpoint.

Se più di un endpoint utilizza la stessa porta, StorageGRID utilizza il seguente ordine di priorità per decidere quale endpoint usare: **Virtual IPs of HA groups** > **Interfacce nodo** > **Tipo di nodo** > **Globale**.

Se stai creando endpoint per l'interfaccia di gestione, sono consentiti solo gli Admin Node.

2. Se hai selezionato **Indirizzi IP virtuali dei gruppi HA**, seleziona uno o più gruppi HA.

   Se stai creando endpoint per l'interfaccia di gestione, seleziona VIP associati solo ad Admin Nodes.

3. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}

Controlla l'accesso dei tenant

Un endpoint dell'interfaccia di gestione può controllare l'accesso del tenant solo quando l'endpoint ha il ${post_edited_translations.segment}.

Passaggi

1. Per la fase di **accesso del tenant**, seleziona una delle seguenti opzioni:

Campo	Descrizione
Consenti a tutti i tenant (impostazione predefinita)	Tutti gli account tenant possono utilizzare questo endpoint per accedere ai propri bucket. Devi selezionare questa opzione se non hai ancora creato alcun account tenant. Dopo aver aggiunto gli account tenant, puoi modificare l'endpoint del bilanciatore di carico per consentire o bloccare account specifici.
${post_edited_translations.segment}	Solo i tenant account selezionati possono utilizzare questo endpoint per accedere ai propri bucket.
Blocca i tenant selezionati	Gli account tenant selezionati non possono utilizzare questo endpoint per accedere ai propri bucket. Tutti gli altri tenant possono utilizzare questo endpoint.

2. Se stai creando un endpoint **HTTP**, non è necessario associare un certificato. Seleziona **Crea** per aggiungere il nuovo endpoint del load balancer. Quindi, vai a Dopo aver finito. Altrimenti, seleziona **Continua** per associare il certificato.

Allega certificato

Passaggi

1. Se stai creando un endpoint **HTTPS**, seleziona il tipo di certificato di sicurezza che desideri associare all'endpoint.

   Il certificato protegge le connessioni tra i client S3 e il servizio Load Balancer sui nodi Admin o Gateway.

   - **Carica il certificato**. Seleziona questa opzione se hai certificati personalizzati da caricare.
   - **Genera certificato**. Seleziona questa opzione se hai i valori necessari per generare un certificato personalizzato.
   - **Utilizza il certificato S3 di StorageGRID**. Seleziona questa opzione se vuoi usare il certificato API S3 globale, che può essere usato anche per le connessioni dirette ai Storage Node.

     Non puoi selezionare questa opzione a meno che tu non abbia sostituito il certificato API S3 predefinito, firmato dalla CA della grid, con un certificato personalizzato firmato da un'autorità di certificazione esterna. Vedi "Configura i certificati API S3".

   - **Utilizza il certificato dell'interfaccia di gestione**. Seleziona questa opzione se vuoi utilizzare il certificato dell'interfaccia di gestione globale, che può essere usato anche per le connessioni dirette agli Admin Node.
2. Se non stai utilizzando il certificato StorageGRID S3, carica o genera il certificato.

Carica il certificato

a. Seleziona **Carica certificato**.

b. Carica i file del certificato server richiesti:

- **Certificato del server**: Il file del certificato server personalizzato in codifica PEM.
- **Chiave privata del certificato**: Il file della chiave privata del certificato del server personalizzato (`.key`).

> Le chiavi private EC devono essere di almeno 224 bit. Le chiavi private RSA devono essere di almeno 2048 bit.

- **CA bundle**: un singolo file opzionale contenente i certificati di ciascuna autorità di certificazione (CA) emittente intermedia. Il file deve contenere ciascuno dei file di certificato CA codificati in PEM, concatenati nell'ordine della catena di certificati.

c. Espandi **Dettagli del certificato** per vedere i metadati di ogni certificato che hai caricato. Se hai caricato un CA bundle opzionale, ogni certificato viene visualizzato nella sua scheda.

- Seleziona **Scarica certificato** per salvare il file del certificato o seleziona **Scarica pacchetto CA** per salvare il pacchetto di certificati.

  Specifica il nome del file del certificato e la posizione di download. Salva il file con l'estensione `.pem`.

  Ad esempio: `storagegrid_certificate.pem`

- ${post_edited_translations.segment}

d. Seleziona **Crea**. + L'endpoint del load balancer viene creato. Il certificato personalizzato viene utilizzato per tutte le nuove connessioni successive tra i client S3 o l'interfaccia di gestione e l'endpoint.

Genera certificato

a. Seleziona **Genera certificato**.

b. ${post_edited_translations.segment}

Campo	Descrizione
domain name	Uno o più fully qualified domain name da includere nel certificato. Usa un * come carattere jolly per rappresentare più domain name.
IP	Uno o più indirizzi IP da includere nel certificato.
${post_edited_translations.segment}	Soggetto o nome distinto (DN) X.509 del titolare del certificato. ${post_edited_translations.segment}
Giorni di validità	${post_edited_translations.segment}

Campo	Descrizione
Aggiungi estensioni di utilizzo chiave	${post_edited_translations.segment} Queste estensioni definiscono lo scopo della chiave contenuta nel certificato. **Nota**: Lascia questa casella di controllo selezionata, a meno che tu non abbia problemi di connessione con client meno recenti quando i certificati includono queste estensioni.

c. Seleziona **Genera**.

d. Seleziona **Dettagli del certificato** per visualizzare i metadati del certificato generato.

- ${post_edited_translations.segment}

  Specifica il nome del file del certificato e la posizione di download. Salva il file con l'estensione `.pem`.

  Ad esempio: `storagegrid_certificate.pem`

- Seleziona **Copia certificato PEM** per copiare il contenuto del certificato da incollare altrove.

e. Seleziona **Create**.

L'endpoint del bilanciatore di carico è stato creato. Il certificato personalizzato viene utilizzato per tutte le nuove connessioni successive tra i client S3 o l'interfaccia di gestione e questo endpoint.

Dopo aver finito

Passaggi

1. ${post_edited_translations.segment}

   L'indirizzo IP che inserisci nel record DNS dipende dal fatto che tu stia usando un gruppo HA di nodi di bilanciamento del carico:

   - ${post_edited_translations.segment}
   - Se non usi un gruppo HA, i client si connetteranno al servizio StorageGRID Load Balancer utilizzando l'indirizzo IP di un Gateway Node o di un Admin Node.

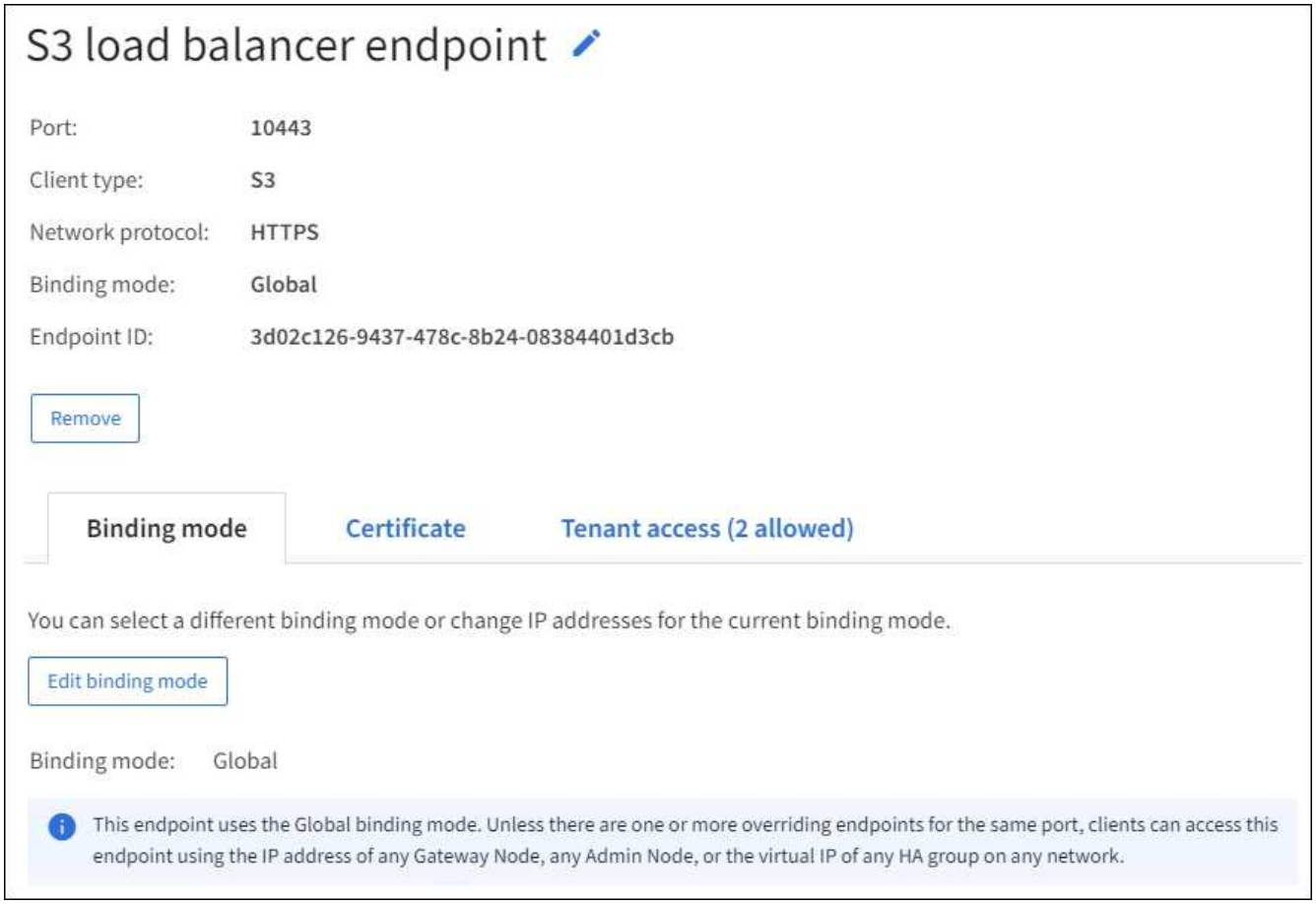
     ${post_edited_translations.segment}

2. ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - fully qualified domain name o indirizzo IP
   - Dettagli relativi ai certificati richiesti

Visualizza e modifica gli endpoint del bilanciatore di carico

Puoi visualizzare i dettagli degli endpoint del bilanciatore di carico esistenti, inclusi i metadati del certificato per un endpoint protetto. Puoi modificare alcune impostazioni per un endpoint.

- Per visualizzare le informazioni di base relative a tutti gli endpoint del bilanciatore di carico, consulta le tabelle nella pagina Endpoint del bilanciatore di carico.
- Per visualizzare tutti i dettagli relativi a uno specifico endpoint, inclusi i metadati del certificato, seleziona il nome dell'endpoint nella tabella. Le informazioni visualizzate variano a seconda del tipo di endpoint e di come è configurato.



- Per modificare un endpoint, usa il menu **Azioni** nella pagina degli endpoint del bilanciatore di carico.

> Se perdi l'accesso a Grid Manager mentre modifichi la porta di un endpoint dell'interfaccia di gestione, aggiorna l'URL e la porta per riottenere l'accesso.

> Dopo aver modificato un endpoint, potresti dover attendere fino a 15 minuti perché le modifiche vengano applicate a tutti i nodi.

Attività	Menu azioni	Pagina dei dettagli
Modifica il nome dell'endpoint	a. Seleziona la casella di controllo per l'endpoint. b. ${post_edited_translations.segment} c. ${post_edited_translations.segment} d. Seleziona **Salva**.	a. ${post_edited_translations.segment} b. Seleziona l'icona di modifica . c. ${post_edited_translations.segment} d. Seleziona **Salva**.
Modifica la porta dell'endpoint	a. Seleziona la casella di controllo per l'endpoint. b. Seleziona **Azioni** > **Modifica porta endpoint** c. Inserisci un numero di porta valido. d. Seleziona **Salva**.	*n/a*
Modifica la modalità di associazione dell'endpoint	a. Seleziona la casella di controllo per l'endpoint. b. ${post_edited_translations.segment} c. Aggiorna la modalità di associazione secondo necessità. d. Seleziona **Salva modifiche**.	a. ${post_edited_translations.segment} b. ${post_edited_translations.segment} c. Aggiorna la modalità di associazione secondo necessità. d. Seleziona **Salva modifiche**.
${post_edited_translations.segment}	a. Seleziona la casella di controllo per l'endpoint. b. ${post_edited_translations.segment} c. Carica o genera un nuovo certificato personalizzato oppure inizia a utilizzare il certificato S3 globale, come richiesto. d. Seleziona **Salva modifiche**.	a. ${post_edited_translations.segment} b. Seleziona la scheda **Certificato**. c. ${post_edited_translations.segment} d. Carica o genera un nuovo certificato personalizzato oppure inizia a utilizzare il certificato S3 globale, come richiesto. e. Seleziona **Salva modifiche**.
${post_edited_translations.segment}	a. Seleziona la casella di controllo per l'endpoint. b. Seleziona **Azioni** > **Modifica tenant access**. c. Scegli un'opzione di accesso diversa, seleziona o rimuovi i tenant dall'elenco, oppure fai entrambe le cose. d. Seleziona **Salva modifiche**.	a. ${post_edited_translations.segment} b. Seleziona la scheda **Accesso tenant**. c. Seleziona **Modifica tenant access**. d. Scegli un'opzione di accesso diversa, seleziona o rimuovi i tenant dall'elenco, oppure fai entrambe le cose. e. Seleziona **Salva modifiche**.

Rimuovi gli endpoint del bilanciatore di carico

Puoi rimuovere uno o più endpoint usando il menu **Azioni** oppure puoi rimuovere un singolo endpoint dalla pagina dei dettagli.

> Per evitare interruzioni per i client, aggiorna tutte le applicazioni client S3 interessate prima di rimuovere un endpoint del bilanciatore di carico. Aggiorna ogni client perché si connetta usando una porta assegnata a un altro endpoint del bilanciatore di carico. Assicurati di aggiornare anche tutte le informazioni richieste sui certificati.

> Se perdi l'accesso a Grid Manager mentre rimuovi un endpoint dell'interfaccia di gestione, aggiorna l'URL.

- Per rimuovere uno o più endpoint:
  a. Dalla pagina del bilanciatore di carico, seleziona la casella di controllo per ogni endpoint che vuoi rimuovere.
  b. Seleziona **Azioni** > **Rimuovi**.
  c. Seleziona **OK**.
- ${post_edited_translations.segment}
  a. ${post_edited_translations.segment}
  b. ${post_edited_translations.segment}
  c. Seleziona **OK**.

Informazioni sul copyright

Copyright © 2026 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.