Gestire il bilanciamento del carico

StorageGRID 11.8

NetApp
March 19, 2024

Sommario

Gestire il bilanciamento del carico

Considerazioni per il bilanciamento del carico

È possibile utilizzare il bilanciamento del carico per gestire i carichi di lavoro di acquisizione e recupero dai client S3 e Swift.

Cos'è il bilanciamento del carico?

Quando un'applicazione client salva o recupera i dati da un sistema StorageGRID, StorageGRID utilizza un sistema di bilanciamento 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 tra più nodi di storage.

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

Il servizio Load Balancer su ciascun nodo funziona in modo indipendente quando si inoltra il traffico client ai nodi di storage. Attraverso un processo di ponderazione, il servizio Load Balancer indirizza più richieste ai nodi di storage con una maggiore disponibilità della CPU.

> Anche se il servizio bilanciamento del carico di StorageGRID è il meccanismo di bilanciamento del carico consigliato, potrebbe essere necessario integrare un bilanciamento del carico di terze parti. Per informazioni, contattare il rappresentante commerciale NetApp o visitare il sito Web all'indirizzo "TR-4626: Bilanciatori di carico globali e di terze parti StorageGRID".

Quanti nodi per il bilanciamento del carico sono necessari?

Come Best practice generale, ogni sito del sistema StorageGRID deve includere due o più nodi nel servizio bilanciamento del carico. Ad esempio, un sito potrebbe includere due nodi gateway o sia un nodo amministratore che un nodo gateway. Assicurarsi che vi sia un'infrastruttura di rete, hardware o virtualizzazione adeguata per ciascun nodo di bilanciamento del carico, sia che si utilizzino appliance di servizi SG100 o SG1000, nodi bare metal o nodi basati su macchine virtuali (VM).

Che cos'è un endpoint di bilanciamento del carico?

Un endpoint di bilanciamento del carico definisce la porta e il protocollo di rete (HTTPS o HTTP) che le richieste dell'applicazione 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 o Swift), la modalità di binding e, facoltativamente, un elenco di tenant consentiti o bloccati.

Per creare un endpoint di bilanciamento del carico, selezionare **CONFIGURAZIONE** > **rete** > **endpoint di bilanciamento del carico** oppure completare la configurazione guidata di FabricPool e S3. Per istruzioni:

- "Configurare gli endpoint del bilanciamento del carico"
- "Utilizzare l'installazione guidata S3"
- "Utilizzare l'installazione guidata di FabricPool"

Considerazioni per la porta

Per impostazione predefinita, la porta di un endpoint di bilanciamento del carico è 10433 per il primo endpoint creato, ma è possibile specificare qualsiasi porta esterna inutilizzata compresa tra 1 e 65535. Se si utilizza la porta 80 o 443, l'endpoint utilizzerà il servizio Load Balancer solo sui nodi gateway. Queste porte sono riservate sui nodi di amministrazione. Se si utilizza la stessa porta per più di un endpoint, è necessario specificare una modalità di binding diversa per ciascun endpoint.

Le porte utilizzate da altri servizi di rete non sono consentite. Vedere "Riferimento porta di rete".

Considerazioni sul protocollo di rete

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

Considerazioni per i certificati endpoint del bilanciamento del carico

Se si seleziona **HTTPS** come protocollo di rete per l'endpoint del bilanciamento del carico, è necessario fornire un certificato di sicurezza. È possibile utilizzare una di queste tre opzioni quando si crea l'endpoint del bilanciamento del carico:

- **Caricare un certificato firmato (consigliato)**. Il certificato può essere firmato da un'autorità di certificazione pubblica o privata. L'utilizzo di un certificato del server CA pubblicamente attendibile per proteggere la connessione è la procedura consigliata. A differenza dei certificati generati, i certificati firmati da una CA possono essere ruotati senza interruzioni, in modo da evitare problemi di scadenza.

  Prima di creare l'endpoint del bilanciamento del carico, è necessario ottenere i seguenti file:

  - Il file di certificato del server personalizzato.
  - Il file di chiave privata del certificato del server personalizzato.
  - Facoltativamente, un bundle CA dei certificati di ciascuna autorità di certificazione di emissione intermedia.
- **Generare un certificato autofirmato**.
- **Utilizzare il certificato globale StorageGRID S3 e Swift**. È necessario caricare o generare una versione personalizzata del certificato prima di poterla selezionare per l'endpoint del bilanciamento del carico. Vedere "Configurare i certificati API S3 e Swift".

Di quali valori ho bisogno?

Per creare il certificato, è necessario conoscere tutti i nomi di dominio e gli indirizzi IP utilizzati dalle applicazioni client S3 o Swift per accedere all'endpoint.

La voce **Subject DN** (Distinguished Name) per il certificato deve includere il nome di dominio completo che l'applicazione client utilizzerà per StorageGRID. Ad esempio:

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

Se necessario, il certificato può utilizzare i caratteri jolly per rappresentare i nomi di dominio completi di tutti i

nodi Admin e Gateway che eseguono il servizio Load Balancer. Ad esempio, `*.storagegrid.example.com` utilizza il carattere jolly * per rappresentare `adm1.storagegrid.example.com` e. `gn1.storagegrid.example.com`.

Se si prevede di utilizzare richieste in stile host virtuali S3, il certificato deve includere anche una voce **Nome alternativo** per ciascuna "Nome di dominio dell'endpoint S3" sono stati configurati, inclusi i nomi con caratteri jolly. Ad esempio:

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

> Se si utilizzano caratteri jolly per i nomi di dominio, consultare "Linee guida per la protezione avanzata dei certificati server".

È inoltre necessario definire una voce DNS per ciascun nome nel certificato di protezione.

Come si gestiscono i certificati in scadenza?

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

Per evitare problemi di scadenza del certificato, attenersi alle seguenti Best practice:

- Monitorare attentamente gli avvisi che avvisano di avvicinarsi alle date di scadenza del certificato, come ad esempio **scadenza del certificato endpoint del bilanciamento del carico** e **scadenza del certificato server globale per gli avvisi S3 e Swift API**.
- Mantenere sempre sincronizzate le versioni del certificato delle applicazioni StorageGRID e S3. Se si sostituisce o si rinnova il certificato utilizzato per un endpoint di bilanciamento del carico, è necessario sostituire o rinnovare il certificato equivalente utilizzato dall'applicazione S3.
- Utilizzare un certificato CA con firma pubblica. Se si utilizza un certificato firmato da una CA, è possibile sostituire i certificati in scadenza senza interruzioni.
- Se è stato generato un certificato StorageGRID autofirmato e il certificato sta per scadere, è necessario sostituirlo manualmente in StorageGRID e nell'applicazione S3 prima della scadenza del certificato esistente.

Considerazioni per la modalità di binding

La modalità di binding consente di controllare quali indirizzi IP possono essere utilizzati per accedere a un endpoint del bilanciamento 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 FQDN (Fully Qualified Domain Name). Le applicazioni client che utilizzano qualsiasi altro indirizzo IP o FQDN non possono accedere all'endpoint.

È possibile specificare una delle seguenti modalità di binding:

- **Globale** (impostazione predefinita): Le applicazioni client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministratore, l'indirizzo IP virtuale (VIP) di qualsiasi gruppo ha su qualsiasi rete o un FQDN corrispondente. Utilizzare questa impostazione a meno che non sia necessario limitare l'accessibilità di un endpoint.
- **IP virtuali dei gruppi ha**. Le applicazioni client devono utilizzare un indirizzo IP virtuale (o un FQDN corrispondente) di un gruppo ha.

- **Interfacce nodo**. I client devono utilizzare gli indirizzi IP (o gli FQDN corrispondenti) 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 qualsiasi nodo di amministrazione o l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di gateway.

Considerazioni sull'accesso al tenant

L'accesso tenant è una funzionalità di sicurezza opzionale che consente di controllare quali account tenant StorageGRID possono utilizzare un endpoint di bilanciamento del carico per accedere ai bucket. È possibile consentire a tutti i tenant di accedere a un endpoint (impostazione predefinita) oppure specificare un elenco dei tenant consentiti o bloccati per ciascun endpoint.

È possibile utilizzare questa funzionalità per fornire un migliore isolamento della sicurezza tra i tenant e i relativi endpoint. Ad esempio, è possibile utilizzare questa funzione per garantire che i materiali top-secret o altamente classificati di proprietà di un tenant rimangano 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 (ad esempio con accesso anonimo), il proprietario del bucket viene utilizzato per determinare il tenant.

Esempio di accesso al tenant

Per comprendere il funzionamento di questa funzionalità di sicurezza, si consideri il seguente esempio:

1. Sono stati creati due endpoint di bilanciamento del carico, come segue:
   - Endpoint **Public**: Utilizza la porta 10443 e consente 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 un altro tenant invia la stessa richiesta allo stesso URL, riceve un messaggio di accesso immediato negato. L'accesso viene negato anche se le credenziali e la firma sono valide.

Disponibilità della CPU

Il servizio Load Balancer su ciascun nodo Admin e nodo Gateway opera in modo indipendente quando inoltra il traffico S3 o Swift ai nodi Storage. Attraverso un processo di ponderazione, il servizio Load Balancer indirizza più richieste ai nodi di storage con una maggiore disponibilità della CPU. Le informazioni sul carico della CPU del nodo vengono aggiornate ogni pochi minuti, ma la ponderazione potrebbe essere aggiornata più frequentemente. A tutti i nodi di storage viene assegnato un valore minimo di peso di base, anche se un nodo riporta un utilizzo pari al 100% o non ne riporta l'utilizzo.

In alcuni casi, le informazioni sulla disponibilità della CPU sono limitate al sito in cui si trova il servizio Load Balancer.

Configurare gli endpoint del bilanciamento del carico

Gli endpoint del bilanciamento del carico determinano le porte e i protocolli di rete che i client S3 e Swift possono utilizzare per la connessione al bilanciamento del carico StorageGRID sui nodi gateway e di amministrazione. È inoltre possibile utilizzare gli endpoint per accedere a Grid Manager, Tenant Manager o a entrambi.

Il supporto per le applicazioni client Swift è stato obsoleto e verrà rimosso in una release futura.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".
- Hai esaminato il "considerazioni per il bilanciamento del carico".
- Se in precedenza è stata rimappata una porta che si intende utilizzare per l'endpoint del bilanciamento del carico, è possibile "rimosso il remap della porta".
- Hai creato tutti i gruppi ad alta disponibilità (ha) che intendi utilizzare. I gruppi HA sono consigliati, ma non richiesti. Vedere "Gestire i gruppi ad alta disponibilità".
- Se l'endpoint del bilanciamento del carico verrà utilizzato da "S3 tenant per S3 Select", Non deve utilizzare gli indirizzi IP o FQDN di nodi bare-metal. Solo le appliance SG100 o SG1000 e i nodi software basati su VMware sono consentiti per gli endpoint del bilanciamento del carico utilizzati per S3 Select.
- Sono state configurate le interfacce VLAN che si intende utilizzare. Vedere "Configurare le interfacce VLAN".
- Se si crea un endpoint HTTPS (consigliato), si dispone delle informazioni per il certificato del server.

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

  - Per caricare un certificato, è necessario disporre del certificato del server, della chiave privata del certificato e, facoltativamente, di un bundle CA.
  - Per generare un certificato, sono necessari tutti i nomi di dominio e gli indirizzi IP utilizzati dai client S3 o Swift per accedere all'endpoint. Devi anche conoscere l'oggetto (Nome distinto).
  - Se si desidera utilizzare il certificato API StorageGRID S3 e Swift (che può essere utilizzato anche per le connessioni dirette ai nodi di storage), il certificato predefinito è già stato sostituito con un certificato personalizzato firmato da un'autorità di certificazione esterna. Vedere "Configurare i certificati API S3 e Swift".

Creare un endpoint per il bilanciamento del carico

Ogni endpoint del bilanciamento del carico dei client S3 o Swift specifica una porta, un tipo di client (S3 o Swift) e un protocollo di rete (HTTP o HTTPS). Gli endpoint del bilanciamento del carico dell'interfaccia di gestione specificano una porta, un tipo di interfaccia e una rete client non attendibile.

Accedere alla procedura guidata

Fasi

1. Selezionare **CONFIGURATION** > **Network** > **Load Balancer Endpoints**.

2. Per creare un endpoint per un client S3 o Swift, selezionare la scheda **S3 o Swift client**.
3. Per creare un endpoint per l'accesso a Grid Manager, Tenant Manager o entrambi, selezionare la scheda **interfaccia di gestione**.
4. Selezionare **Crea**.

Inserire i dettagli dell'endpoint

Fasi

1. Selezionare le istruzioni appropriate per inserire i dettagli per il tipo di endpoint che si desidera creare.

Client S3 o Swift

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint, che verrà visualizzato nella tabella della pagina endpoint del bilanciamento del carico.
Porta	La porta StorageGRID che si desidera utilizzare per il bilanciamento del carico. Per impostazione predefinita, questo campo è impostato su 10433 per il primo endpoint creato, ma è possibile immettere qualsiasi porta esterna non utilizzata compresa tra 1 e 65535. Se si immette **80** o **8443**, l'endpoint viene configurato solo sui nodi Gateway, a meno che non sia stata liberata la porta 8443. Quindi è possibile utilizzare la porta 8443 come endpoint S3 e la porta verrà configurata su entrambi i nodi Gateway e Admin.
Tipo di client	Il tipo di applicazione client che utilizzerà questo endpoint, **S3** o **Swift**.
Protocollo di rete	Il protocollo di rete che i client utilizzeranno per la connessione a questo endpoint. • Selezionare **HTTPS** per la comunicazione sicura con crittografia TLS (scelta consigliata). È necessario allegare un certificato di sicurezza prima di poter salvare l'endpoint. • Selezionare **HTTP** per comunicazioni meno sicure e non crittografate. Utilizzare HTTP solo per una griglia non di produzione.

Interfaccia di gestione

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint, che verrà visualizzato nella tabella della pagina endpoint del bilanciamento del carico.
Porta	La porta StorageGRID che si desidera utilizzare per accedere a Gestore griglia, Gestore tenant o entrambi. • Gestore griglia: **8443** • Responsabile del tenant: **9443** • Sia Grid Manager che Tenant Manager: **443** **Nota**: È possibile utilizzare queste porte preimpostate o altre porte disponibili.
Tipo di interfaccia	Selezionare il pulsante di opzione per l'interfaccia StorageGRID a cui si accede utilizzando questo endpoint.

Campo	Descrizione
Rete client non attendibile	Selezionare **Sì** se l'endpoint deve essere accessibile alle reti client non attendibili. In caso contrario, selezionare **No**. Quando si seleziona **Sì**, la porta è aperta su tutte le reti client non attendibili. **Nota**: È possibile configurare una porta per essere aperta o chiusa a reti client non attendibili solo quando si crea l'endpoint di bilanciamento del carico.

1. Selezionare **continua**.

Selezionare una modalità di binding

Fasi

1. Selezionare una modalità di associazione per l'endpoint per controllare la modalità di accesso all'endpoint utilizzando qualsiasi indirizzo IP o specifici indirizzi IP e interfacce di rete.

   Alcune modalità di associazione sono disponibili per gli endpoint client o per gli endpoint dell'interfaccia di gestione. Tutte le modalità per entrambi i tipi di endpoint sono elencate di seguito.

Modalità	Descrizione
Globale (impostazione predefinita per gli endpoint client)	I client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministratore, l'indirizzo IP virtuale (VIP) di qualsiasi gruppo ha su qualsiasi rete o un FQDN corrispondente. Utilizzare l'impostazione **Globale** a meno che non sia necessario limitare l'accessibilità di questo endpoint.
IP virtuali dei gruppi ha	Per accedere a questo endpoint, i client devono utilizzare un indirizzo IP virtuale (o un FQDN corrispondente) di un gruppo ha. Gli endpoint con questa modalità di binding possono utilizzare tutti lo stesso numero di porta, purché i gruppi ha selezionati per gli endpoint non si sovrappongano.
Interfacce di nodo	I client devono utilizzare gli indirizzi IP (o gli FQDN corrispondenti) delle interfacce dei nodi selezionate per accedere a questo endpoint.
Tipo di nodo (solo endpoint client)	In base al tipo di nodo selezionato, i client devono utilizzare l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di amministrazione o l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di gateway per accedere a questo endpoint.

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

Se più di un endpoint utilizza la stessa porta, StorageGRID utilizza questo ordine di priorità per decidere quale endpoint utilizzare: **IP virtuali dei gruppi ha** > **interfacce nodo** > **tipo di nodo** > **Globale**.

Se si stanno creando endpoint dell'interfaccia di gestione, sono consentiti solo i nodi Admin.

2. Se si seleziona **IP virtuali dei gruppi ha**, selezionare uno o più gruppi ha.

   Se si stanno creando endpoint dell'interfaccia di gestione, selezionare VIP associati solo ai nodi Admin.

3. Se si seleziona **Node interfaces**, selezionare una o più interfacce di nodo per ciascun nodo Admin o nodo gateway che si desidera associare a questo endpoint.
4. Se si seleziona **Node type** (tipo nodo), selezionare Admin Node (nodi amministratore), che include sia l'Admin Node primario che qualsiasi Admin Node non primario, oppure Gateway Node (nodi gateway).

Controllo dell'accesso al tenant

Un endpoint dell'interfaccia di gestione può controllare l'accesso al tenant solo quando l'endpoint dispone di Tipo di interfaccia di Tenant Manager.

Fasi

1. Per il passaggio **accesso tenant**, selezionare una delle seguenti opzioni:

Campo	Descrizione
Allow all tenant (Consenti tutti i tenant) (impostazione predefinita	Tutti gli account tenant possono utilizzare questo endpoint per accedere ai bucket. Selezionare questa opzione se non sono ancora stati creati account tenant. Dopo aver aggiunto account tenant, è possibile modificare l'endpoint del bilanciamento del carico per consentire o bloccare account specifici.
Consenti tenant selezionati	Solo gli account tenant selezionati possono utilizzare questo endpoint per accedere ai bucket.
Blocca i tenant selezionati	Gli account tenant selezionati non possono utilizzare questo endpoint per accedere ai bucket. Tutti gli altri tenant possono utilizzare questo endpoint.

2. Se si crea un endpoint **HTTP**, non è necessario allegare un certificato. Selezionare **Create** per aggiungere il nuovo endpoint del bilanciamento del carico. Quindi, passare a. Al termine. In caso contrario, selezionare **continua** per allegare il certificato.

Allega certificato

Fasi

1. Se si sta creando un endpoint **HTTPS**, selezionare il tipo di certificato di sicurezza che si desidera allegare all'endpoint.

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

   - **Carica certificato**. Selezionare questa opzione se si dispone di certificati personalizzati da caricare.
   - **Genera certificato**. Selezionare questa opzione se si dispone dei valori necessari per generare un certificato personalizzato.
   - **Utilizzare il certificato StorageGRID S3 e Swift**. Selezionare questa opzione se si desidera utilizzare il certificato globale S3 e Swift API, che può essere utilizzato anche per le connessioni dirette ai nodi di storage.

     Non è possibile selezionare questa opzione a meno che non sia stato sostituito il certificato S3 e Swift API predefinito, firmato dalla CA Grid, con un certificato personalizzato firmato da un'autorità di certificazione esterna. Vedere "Configurare i certificati API S3 e Swift".

   - **Utilizza certificato interfaccia di gestione**. Selezionare questa opzione se si desidera utilizzare il certificato dell'interfaccia di gestione globale, che può essere utilizzato anche per le connessioni dirette ai nodi amministrativi.
2. Se non si utilizza il certificato StorageGRID S3 e Swift, caricare o generare il certificato.

Carica certificato

a. Selezionare **carica certificato**.

b. Caricare i file dei certificati del server richiesti:

- **Server certificate**: Il file di certificato del server personalizzato in codifica PEM.
- **Certificate private key** (chiave privata certificato): Il file di chiave privata del certificato del server personalizzato (`.key`).

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

- **Bundle CA**: Un singolo file opzionale contenente i certificati di ogni autorità di certificazione di emissione intermedia (CA). Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati in ordine di catena del certificato.

c. Espandere **Dettagli certificato** per visualizzare i metadati di ciascun certificato caricato. Se è stato caricato un bundle CA opzionale, ciascun certificato viene visualizzato nella propria scheda.

- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato oppure selezionare **Download CA bundle** (Scarica pacchetto CA) per salvare il bundle del certificato.

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

  Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy certificate PEM** or **Copy CA bundle PEM** per copiare il contenuto del certificato e incollarlo altrove.

d. Selezionare **Crea**.
Viene creato l'endpoint del bilanciamento del carico. Il certificato personalizzato viene utilizzato per tutte le nuove connessioni successive tra i client S3 e Swift o l'interfaccia di gestione e l'endpoint.

Generare un certificato

a. Selezionare **genera certificato**.

b. Specificare le informazioni del certificato:

Campo	Descrizione
Nome di dominio	Uno o più nomi di dominio completi da includere nel certificato. Utilizzare un * come carattere jolly per rappresentare più nomi di dominio.
IP	Uno o più indirizzi IP da includere nel certificato.

Campo	Descrizione
Soggetto (facoltativo)	X.509 nome soggetto o nome distinto (DN) del proprietario del certificato. Se in questo campo non viene immesso alcun valore, il certificato generato utilizza il primo nome di dominio o indirizzo IP come nome comune (CN) del soggetto.
Giorni di validità	Numero di giorni successivi alla creazione della scadenza del certificato.
Aggiungere estensioni di utilizzo chiave	Se selezionata (impostazione predefinita e consigliata), l'utilizzo delle chiavi e le estensioni estese dell'utilizzo delle chiavi vengono aggiunte al certificato generato. Queste estensioni definiscono lo scopo della chiave contenuta nel certificato. **Nota**: Lasciare questa casella di controllo selezionata a meno che non si verifichino problemi di connessione con client meno recenti quando i certificati includono queste estensioni.

c. Selezionare **generate**.

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

   - Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

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

     Ad esempio: `storagegrid_certificate.pem`

   - Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.

e. Selezionare **Crea**.

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

Al termine

Fasi

1. Se si utilizza un DNS, assicurarsi che il DNS includa un record per associare il nome di dominio completo (FQDN, Fully Qualified Domain Name) di StorageGRID a ciascun indirizzo IP utilizzato dai client per effettuare le connessioni.

   L'indirizzo IP inserito nel record DNS dipende dall'utilizzo di un gruppo ha di nodi per il bilanciamento del carico:

- Se è stato configurato un gruppo ha, i client si connetteranno agli indirizzi IP virtuali di quel gruppo ha.
- Se non si utilizza un gruppo ha, i client si connetteranno al servizio bilanciamento del carico StorageGRID utilizzando l'indirizzo IP di un nodo gateway o di un nodo amministratore.

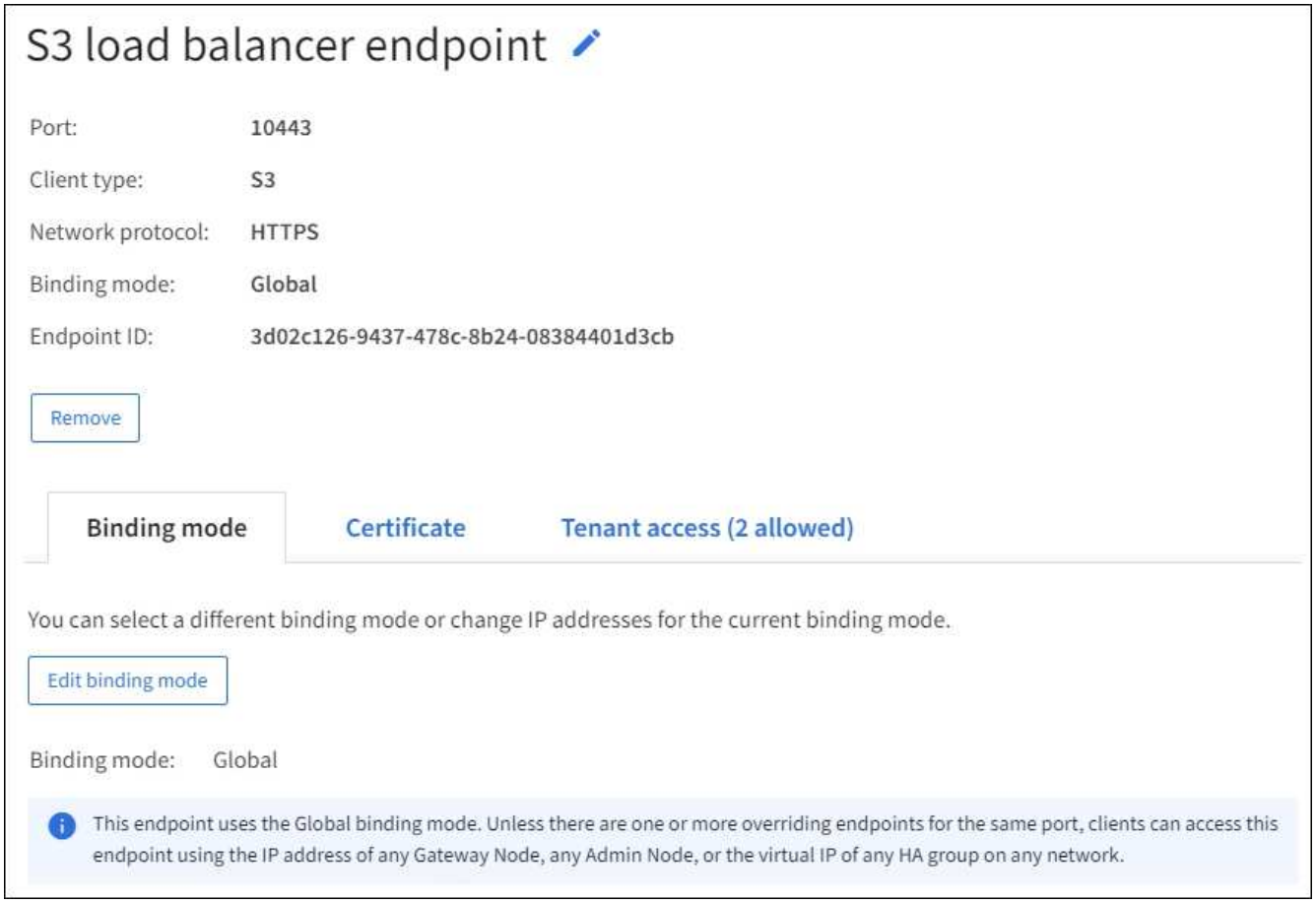
  È inoltre necessario assicurarsi che il record DNS faccia riferimento a tutti i nomi di dominio degli endpoint richiesti, inclusi i nomi con caratteri jolly.

2. Fornire ai client S3 e Swift le informazioni necessarie per connettersi all'endpoint:
   - Numero di porta
   - Nome di dominio completo o indirizzo IP
   - Tutti i dettagli del certificato richiesti

Visualizzare e modificare gli endpoint del bilanciamento del carico

È possibile visualizzare i dettagli degli endpoint del bilanciamento del carico esistenti, inclusi i metadati del certificato per un endpoint protetto. È possibile modificare determinate impostazioni per un endpoint.

- Per visualizzare le informazioni di base per tutti gli endpoint del bilanciamento del carico, esaminare le tabelle nella pagina Endpoints del bilanciamento del carico.
- Per visualizzare tutti i dettagli relativi a un endpoint specifico, inclusi i metadati del certificato, selezionare il nome dell'endpoint nella tabella. Le informazioni visualizzate variano a seconda del tipo di endpoint e della sua configurazione.



- Per modificare un endpoint, utilizzare il menu **azioni** nella pagina Endpoints del bilanciamento del carico.

Se si perde l'accesso a Grid Manager durante la modifica della porta di un endpoint dell'interfaccia di gestione, aggiornare l'URL e la porta per riottenere l'accesso.

Dopo aver modificato un endpoint, potrebbe essere necessario attendere fino a 15 minuti per applicare le modifiche a tutti i nodi.

Attività	Menu delle azioni	Pagina dei dettagli
Modificare il nome dell'endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare **azioni** > **Modifica nome endpoint**. c. Inserire il nuovo nome. d. Selezionare **Salva**.	a. Selezionare il nome dell'endpoint per visualizzare i dettagli. b. Selezionare l'icona di modifica . c. Inserire il nuovo nome. d. Selezionare **Salva**.
Modificare la porta dell'endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare **azioni** > **Modifica porta endpoint** c. Immettere un numero di porta valido. d. Selezionare **Salva**.	*n/a*
Modificare la modalità di associazione degli endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare **azioni** > **Modifica modalità di associazione endpoint**. c. Aggiornare la modalità di binding secondo necessità. d. Selezionare **Save Changes** (Salva modifiche).	a. Selezionare il nome dell'endpoint per visualizzare i dettagli. b. Selezionare **Edit binding mode** (Modifica modalità di associazione). c. Aggiornare la modalità di binding secondo necessità. d. Selezionare **Save Changes** (Salva modifiche).
Modificare il certificato dell'endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare **azioni** > **Modifica certificato endpoint**. c. Caricare o generare un nuovo certificato personalizzato o iniziare a utilizzare il certificato globale S3 e Swift, come richiesto. d. Selezionare **Save Changes** (Salva modifiche).	a. Selezionare il nome dell'endpoint per visualizzare i dettagli. b. Selezionare la scheda **certificato**. c. Selezionare **Modifica certificato**. d. Caricare o generare un nuovo certificato personalizzato o iniziare a utilizzare il certificato globale S3 e Swift, come richiesto. e. Selezionare **Save Changes** (Salva modifiche).

Attività	Menu delle azioni	Pagina dei dettagli
Modificare l'accesso al tenant	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare **azioni** > **Modifica accesso tenant**. c. Scegliere un'opzione di accesso diversa, selezionare o rimuovere i tenant dall'elenco oppure eseguire entrambe le operazioni. d. Selezionare **Save Changes** (Salva modifiche).	a. Selezionare il nome dell'endpoint per visualizzare i dettagli. b. Selezionare la scheda **accesso tenant**. c. Selezionare **Edit tenant access** (Modifica accesso tenant). d. Scegliere un'opzione di accesso diversa, selezionare o rimuovere i tenant dall'elenco oppure eseguire entrambe le operazioni. e. Selezionare **Save Changes** (Salva modifiche).

Rimuovere gli endpoint del bilanciamento del carico

È possibile rimuovere uno o più endpoint dal menu **azioni** oppure rimuovere un singolo endpoint dalla pagina dei dettagli.

> Per evitare interruzioni del client, aggiornare le applicazioni client S3 o Swift interessate prima di rimuovere un endpoint di bilanciamento del carico. Aggiornare ogni client per la connessione utilizzando una porta assegnata a un altro endpoint del bilanciamento del carico. Assicurarsi di aggiornare anche tutte le informazioni di certificato richieste.

> Se si perde l'accesso a Grid Manager durante la rimozione di un endpoint dell'interfaccia di gestione, aggiornare l'URL.

- Per rimuovere uno o più endpoint:
  a. Dalla pagina bilanciamento del carico, selezionare la casella di controllo per ciascun endpoint che si desidera rimuovere.
  b. Selezionare **azioni** > **Rimuovi**.
  c. Selezionare **OK**.
- Per rimuovere un endpoint dalla pagina dei dettagli:
  a. Dalla pagina bilanciamento del carico. selezionare il nome dell'endpoint.
  b. Selezionare **Rimuovi** nella pagina dei dettagli.
  c. Selezionare **OK**.