Configura le connessioni client

StorageGRID software

NetApp
July 23, 2026

Sommario

Configura le connessioni client

Configura le connessioni client S3 a StorageGRID

Come amministratore della griglia, gestisci le opzioni di configurazione che controllano come le applicazioni client S3 si connettono al tuo sistema StorageGRID per archiviare e recuperare dati.

I dettagli relativi a Swift sono stati rimossi da questa versione del sito della documentazione. Vedi "StorageGRID 11.8: Configura le connessioni client S3 e Swift".

Attività di configurazione

1. Esegui le attività preliminari in StorageGRID, in base a come l'applicazione client si connetterà a StorageGRID.

Compiti richiesti

Devi ottenere:

- indirizzi IP
- ${post_edited_translations.segment}
- Certificato SSL

Attività facoltative

Facoltativamente, configura:

- Federazione di identità
- SSO

1. Utilizza StorageGRID per ottenere i valori necessari all'applicazione per connettersi alla grid. Puoi usare il setup wizard S3 oppure configurare manualmente ogni entità StorageGRID.

Usa setup wizard

${post_edited_translations.segment}

Configura manualmente

1. Crea un gruppo ad alta disponibilità
2. ${post_edited_translations.segment}
3. Crea account tenant
4. ${post_edited_translations.segment}
5. Configura regola e criterio ILM

1. Utilizza l'applicazione S3 per completare la connessione a StorageGRID. Crea voci DNS per associare gli indirizzi IP ai domain name che intendi utilizzare.

Se necessario, esegui ulteriori configurazioni dell'applicazione.

2. Esegui attività ricorrenti nell'applicazione e in StorageGRID per gestire e monitorare lo storage a oggetti nel tempo.

Informazioni necessarie per collegare StorageGRID a un'applicazione client

Prima di poter collegare StorageGRID a un'applicazione client S3, devi eseguire alcuni passaggi di configurazione in StorageGRID e ottenere determinati valori.

Di quali valori hai bisogno?

La tabella seguente mostra i valori che devi configurare in StorageGRID e dove tali valori vengono utilizzati dall'applicazione S3 e dal DNS server.

Valore	Dove configuri il valore	${post_edited_translations.segment}
Indirizzi IP virtuali (VIP)	${post_edited_translations.segment}	Voce DNS
Porta	StorageGRID > Endpoint del bilanciatore di carico	${post_edited_translations.segment}
Certificato SSL	StorageGRID > Endpoint del bilanciatore di carico	${post_edited_translations.segment}
Nome server (FQDN)	StorageGRID > Endpoint del bilanciatore di carico	• ${post_edited_translations.segment} • Voce DNS
ID della chiave di accesso S3 e chiave di accesso segreta	StorageGRID > Tenant e bucket	${post_edited_translations.segment}
${post_edited_translations.segment}	StorageGRID > Tenant e bucket	${post_edited_translations.segment}

Come posso ottenere questi valori?

A seconda delle tue esigenze, puoi fare una delle seguenti cose per ottenere le informazioni di cui hai bisogno:

- **Usa il "setup wizard S3"**. La setup wizard ti aiuta a configurare rapidamente i valori richiesti in StorageGRID e genera uno o due file che puoi usare quando configuri l'applicazione S3. La procedura guidata ti accompagna nei passaggi necessari e ti aiuta a verificare che le impostazioni siano conformi alle best practice di StorageGRID.

> Se stai configurando un'applicazione S3, è consigliato usare il setup wizard a meno che tu non abbia esigenze particolari o che la tua implementazione richieda una personalizzazione significativa.

- **Usa l'"setup wizard di FabricPool"**. Simile alla setup wizard, la FabricPool setup wizard ti aiuta a configurare rapidamente i valori richiesti e genera un file che puoi usare quando configuri un livello cloud FabricPool in ONTAP.

  > Se hai intenzione di utilizzare StorageGRID come sistema di storage a oggetti per un cloud tier FabricPool, si consiglia di utilizzare il setup wizard di FabricPool a meno che tu non sappia di avere requisiti speciali o che la tua implementazione richieda una personalizzazione significativa.

- **Configura gli elementi manualmente**. Se ti stai connettendo a un'applicazione S3 e preferisci non utilizzare la setup wizard, puoi ottenere i valori richiesti eseguendo la configurazione manualmente. Segui questi passaggi:

  a. Configura il gruppo ad alta disponibilità (HA) che desideri utilizzare per l'applicazione S3. Vedi "Configura i gruppi ad alta disponibilità".

  b. Crea l'endpoint del bilanciatore di carico che l'applicazione S3 userà. Vedi "${post_edited_translations.segment}".

  c. Crea l'account tenant che l'applicazione S3 utilizzerà. Vedi "Crea un tenant account".

  d. Per un tenant S3, accedi all'account tenant e genera un ID chiave di accesso e una chiave di accesso segreta per ciascun utente che accederà all'applicazione. Consulta "Crea le tue chiavi di accesso".

  e. Crea uno o più bucket S3 all'interno dell'account tenant. Per S3, consulta "Crea bucket S3".

  f. Per aggiungere istruzioni di posizionamento specifiche per gli oggetti appartenenti al nuovo tenant o bucket/container, crea una nuova regola ILM e attiva una nuova policy ILM per utilizzare tale regola. Vedi "Crea regola ILM" e "Crea criteri ILM".

Sicurezza per i client S3 in StorageGRID

Gli account tenant di StorageGRID utilizzano applicazioni client S3 per salvare i dati degli oggetti in StorageGRID. Dovresti esaminare le misure di sicurezza implementate per le applicazioni client.

Riepilogo

Il seguente elenco riassume come viene implementata la sicurezza per l'API REST di S3:

Sicurezza della connessione

TLS

Autenticazione del server

Certificato server X.509 firmato dalla CA di sistema o certificato server personalizzato fornito dall'amministratore

Autenticazione del client

ID della chiave di accesso dell'account S3 e chiave di accesso segreta

Autorizzazione del client

Proprietà del bucket e tutte le politiche di controllo degli accessi applicabili

Come StorageGRID garantisce la sicurezza delle applicazioni client

Le applicazioni client S3 possono connettersi al servizio Load Balancer sui nodi Gateway, sui nodi Admin o direttamente sui nodi Storage.

- I client che si connettono al servizio Load Balancer possono utilizzare HTTPS o HTTP, in base a come "configura l'endpoint del bilanciatore di carico".

  HTTPS fornisce una comunicazione sicura, crittografata tramite TLS, ed è consigliato. Devi associare un certificato di sicurezza all'endpoint.

  HTTP offre comunicazioni meno sicure e non crittografate e dovrebbe essere utilizzato solo per grid non di produzione o di test.

- ${post_edited_translations.segment}

  ${post_edited_translations.segment}

  HTTP fornisce una comunicazione meno sicura e non crittografata, ma può essere opzionalmente "abilitato" per grid non di produzione o di test.

- ${post_edited_translations.segment}
- Le comunicazioni tra il servizio Load Balancer e i nodi di archiviazione all'interno della griglia sono crittografate sia che l'endpoint del load balancer sia configurato per accettare connessioni HTTP o HTTPS.
- I client devono fornire "intestazioni di autenticazione HTTP" a StorageGRID per eseguire le operazioni REST API.

Certificati di sicurezza e applicazioni client

In tutti i casi, le applicazioni client possono stabilire connessioni TLS utilizzando un certificato server personalizzato caricato dall'amministratore della griglia oppure un certificato generato dal sistema StorageGRID:

- Quando le applicazioni client si connettono al servizio Load Balancer, utilizzano il certificato configurato per l'endpoint del load balancer. Ogni endpoint del load balancer ha il proprio certificato—un certificato server personalizzato caricato dall'amministratore della grid oppure un certificato generato dall'amministratore della grid in StorageGRID durante la configurazione dell'endpoint.

  Vedi "Considerazioni sul bilanciamento del carico".

- Quando le applicazioni client si connettono direttamente a un nodo di archiviazione, utilizzano i certificati server generati dal sistema per i nodi di archiviazione quando il sistema StorageGRID è stato installato (che sono firmati dall'autorità di certificazione del sistema), oppure un singolo certificato server personalizzato fornito per la grid da un amministratore della grid. Vedi "aggiungi un certificato API S3 personalizzato".

Devi configurare i client in modo che considerino attendibile l'autorità di certificazione che ha firmato il certificato utilizzato per stabilire le connessioni TLS.

Algoritmi di hashing e crittografia supportati per le librerie TLS

Il sistema StorageGRID supporta un set di suite di cifratura che le applicazioni client possono utilizzare quando stabiliscono una sessione TLS. Per configurare i cifrari, vai su **Configurazione** > **Sicurezza** > **Impostazioni di sicurezza** e seleziona **Policy TLS e SSH**.

${post_edited_translations.segment}

StorageGRID supporta TLS 1.2 e TLS 1.3.

SSLv3 e TLS 1.1 (o versioni precedenti) non sono più supportati.

Usa setup wizard

Considerazioni e requisiti relativi alla procedura guidata di configurazione S3 di StorageGRID

Puoi usare la setup wizard per configurare StorageGRID come sistema di storage a oggetti per un'applicazione S3.

Quando usare la setup wizard

La setup wizard ti accompagna in ogni fase della configurazione di StorageGRID per l'utilizzo con un'applicazione S3. Come parte del completamento della setup wizard, scarichi file che puoi utilizzare per inserire i valori nell'applicazione S3. Usa la setup wizard per configurare il tuo sistema più rapidamente e per assicurarti che le impostazioni siano conformi alle best practice di StorageGRID.

Se hai il "Permesso di accesso root", puoi completare la setup wizard quando inizi a usare StorageGRID Grid Manager, oppure puoi accedere e completare la wizard in qualsiasi momento successivo. A seconda delle tue esigenze, puoi anche configurare manualmente alcuni o tutti gli elementi richiesti e poi usare la wizard per raccogliere i valori di cui un'applicazione S3 ha bisogno.

Prima di utilizzare la procedura guidata

Prima di utilizzare la procedura guidata, assicurati di aver completato questi prerequisiti.

Ottieni indirizzi IP e configura le interfacce VLAN

Se configurerai un gruppo ad alta disponibilità (HA), sai a quali nodi si connetterà l'applicazione S3 e quale rete StorageGRID verrà utilizzata. Sai anche quali valori inserire per il CIDR della subnet, l'indirizzo IP del gateway e gli indirizzi IP virtuali (VIP).

Se prevedi di utilizzare una LAN virtuale per separare il traffico dall'applicazione S3, hai già configurato l'interfaccia VLAN. Vedi "Configura le interfacce VLAN".

Configura la federazione delle identità e il single sign-on

Se prevedi di utilizzare la federazione delle identità o il single sign-on (SSO) per il tuo sistema StorageGRID, hai abilitato queste funzionalità. Sai anche quale gruppo federato deve avere access root per il tenant account che verrà utilizzato dall'applicazione S3. Vedi "${post_edited_translations.segment}" e "Configura single sign-on".

Ottieni e configura i nomi di dominio

Sai quale fully qualified domain name (FQDN) usare per StorageGRID. Le voci del name server DNS mapperanno questo FQDN agli indirizzi IP virtuali (VIP) del gruppo HA che crei usando la procedura guidata.

Se intendi utilizzare le richieste in stile ospitato virtuale di S3, dovresti avere "nomi di dominio degli endpoint S3 configurati". L'utilizzo delle richieste in stile ospitato virtuale è consigliato.

Esamina i requisiti per il bilanciamento del carico e il certificato di sicurezza

Se intendi utilizzare il load balancer StorageGRID, hai già esaminato le considerazioni generali sul bilanciamento del carico. Hai a disposizione i certificati da caricare o i valori necessari per generare un certificato.

Se vuoi usare un endpoint di bilanciamento del carico esterno (di terze parti), devi avere il fully qualified domain name (FQDN), la porta e il certificato per quel bilanciatore di carico.

${post_edited_translations.segment}

Se vuoi consentire al tenant S3 di clonare i dati dell'account e replicare gli oggetti del bucket in un'altra griglia utilizzando una connessione di federazione di griglia, conferma quanto segue prima di avviare lo wizard:

- Hai "hai configurato la connessione alla federazione di griglia".
- Lo stato della connessione è **Connected**.
- ${post_edited_translations.segment}

Accedere e completare la setup wizard in StorageGRID

Puoi usare la setup wizard per configurare StorageGRID per l'utilizzo con un'applicazione S3. La setup wizard fornisce i valori di cui l'applicazione ha bisogno per accedere a un bucket StorageGRID e per salvare oggetti.

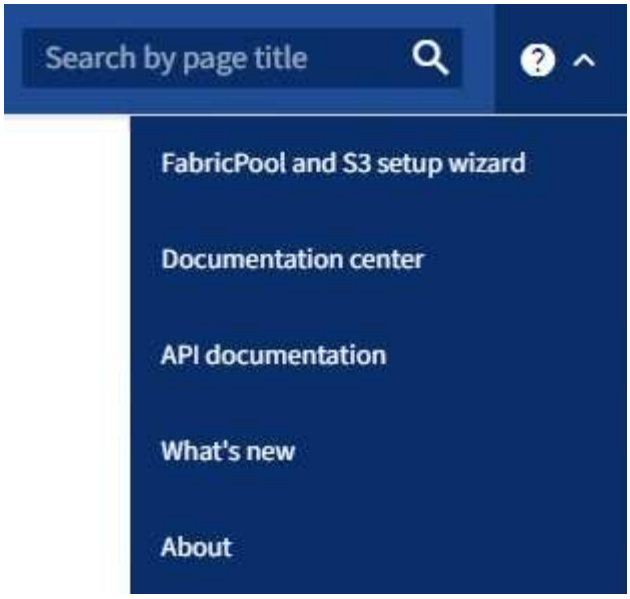
Prima di iniziare

- Hai il "Permesso di accesso root".
- Hai esaminato le "considerazioni e requisiti" per usare la procedura guidata.

Accedi al wizard

Passaggi

1. Accedi al Grid Manager utilizzando un "browser web supportato".
2. Se il banner **FabricPool and S3 setup wizard** appare sulla dashboard, seleziona il link nel banner. Se il banner non appare più, seleziona l'icona di aiuto dalla barra dell'intestazione in Grid Manager e seleziona **FabricPool and S3 setup wizard**.



3. Nella sezione dell'applicazione S3 della pagina FabricPool and S3 setup wizard, seleziona **Configura ora**.

Passaggio 1 di 6: Configura il gruppo HA

Un gruppo HA è una raccolta di nodi che contengono ciascuno il servizio StorageGRID Load Balancer. Un gruppo HA può contenere Gateway Nodes, Admin Nodes o entrambi.

Puoi usare un gruppo HA per mantenere disponibili le connessioni dati S3. Se l'interfaccia attiva nel gruppo HA si guasta, un'interfaccia di backup può gestire il carico di lavoro con un impatto minimo sulle operazioni S3.

Per i dettagli su questa attività, vedi "Gestisci i gruppi ad alta disponibilità".

Passaggi

1. Se intendi utilizzare un bilanciatore di carico esterno, non è necessario creare un gruppo HA. Seleziona **Salta questo passaggio** e vai a Passaggio 2 di 6: Configura l'endpoint del bilanciamento del carico.
2. Per utilizzare il bilanciatore di carico StorageGRID, puoi creare un nuovo gruppo HA o usare un gruppo HA esistente.

Crea gruppo HA

a. Per creare un nuovo gruppo HA, seleziona **Crea gruppo HA**.

b. Per la fase **Inserisci i dettagli**, compila i seguenti campi.

Campo	Descrizione
nome gruppo HA	Un nome visualizzato univoco per questo gruppo HA.
${post_edited_translations.segment}	La descrizione di questo gruppo HA.

c. Nella fase **Aggiungi interfacce**, seleziona le interfacce del nodo che vuoi usare in questo gruppo HA.

   Utilizza le intestazioni di colonna per ordinare le righe o inserisci un termine di ricerca per individuare più rapidamente le interfacce.

   Puoi selezionare uno o più nodi, ma puoi selezionare solo un'interfaccia per ciascun nodo.

d. Per la fase **Assegna priorità alle interfacce**, determina l'interfaccia primaria e le eventuali interfacce di backup per questo gruppo HA.

   Trascina le righe per modificare i valori nella colonna **Ordine di priorità**.

   La prima interfaccia nell'elenco è l'interfaccia primaria. L'interfaccia primaria è l'interfaccia attiva a meno che non si verifichi un errore.

   Se il gruppo HA include più di un'interfaccia e l'interfaccia attiva si guasta, gli indirizzi IP virtuali (VIP) vengono spostati sulla prima interfaccia di backup in ordine di priorità. Se anche quella interfaccia si guasta, gli indirizzi VIP vengono spostati sull'interfaccia di backup successiva e così via. Quando i guasti vengono risolti, gli indirizzi VIP tornano all'interfaccia con la priorità più alta disponibile.

e. Per la fase **Inserisci indirizzi IP**, compila i seguenti campi.

Campo	Descrizione
CIDR della sottorete	L'indirizzo della subnet VIP in notazione CIDR: un indirizzo IPv4 seguito da una barra e dalla lunghezza della subnet (0-32). L'indirizzo di rete non deve avere alcun bit host impostato. Ad esempio, `192.16.0.0/22`.
Indirizzo IP del gateway (facoltativo)	Se gli indirizzi IP S3 utilizzati per accedere a StorageGRID non sono sulla stessa sottorete degli indirizzi VIP di StorageGRID, inserisci l'indirizzo IP del gateway locale VIP di StorageGRID. L'indirizzo IP del gateway locale deve essere all'interno della sottorete VIP.

Campo	Descrizione
Indirizzo IP virtuale	Inserisci almeno uno e non più di dieci indirizzi VIP per l'interfaccia attiva nel gruppo HA. Tutti gli indirizzi VIP devono essere all'interno della subnet VIP. Almeno un indirizzo deve essere IPv4. Facoltativamente, puoi specificare ulteriori indirizzi IPv4 e IPv6.

f. Seleziona **Crea gruppo HA** e poi seleziona **Fine** per tornare alla setup wizard.

g. Seleziona **Continua** per passare alla fase di bilanciamento del carico.

Usa il gruppo HA esistente

a. Per utilizzare un gruppo HA esistente, seleziona il nome del gruppo HA da **Seleziona un gruppo HA**.

b. Seleziona **Continua** per passare alla fase di bilanciamento del carico.

Passaggio 2 di 6: Configura l'endpoint del bilanciamento del carico

StorageGRID utilizza un bilanciatore di carico per gestire il carico di lavoro delle applicazioni client. Il bilanciamento del carico massimizza la velocità e la capacità di connessione su più Storage Nodes.

Puoi usare il servizio StorageGRID Load Balancer, che è presente su tutti i nodi Gateway e Admin, oppure puoi connetterti a un bilanciatore di carico esterno (di terze parti). Si consiglia di utilizzare il bilanciatore di carico StorageGRID.

Per i dettagli su questa attività, vedi "Considerazioni sul bilanciamento del carico".

Per utilizzare il servizio StorageGRID Load Balancer, seleziona la scheda **StorageGRID load balancer** e poi crea o seleziona l'endpoint del load balancer che vuoi usare. Per utilizzare un load balancer esterno, seleziona la scheda **External load balancer** e fornisci i dettagli relativi al sistema che hai già configurato.

Crea endpoint

Passaggi

1. Per creare un endpoint del bilanciatore di carico, seleziona **Crea endpoint**.
2. Per la fase **Inserisci i dettagli dell'endpoint**, compila i seguenti campi.

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint.
Porta	La porta StorageGRID che vuoi usare per il bilanciamento del carico. Questo campo è impostato di default su 10433 per il primo endpoint che crei, ma puoi inserire qualsiasi porta esterna non utilizzata. Se inserisci 80 o 443, l'endpoint viene configurato solo sui Gateway Nodes, perché queste porte sono riservate sugli Admin Nodes. **Nota:** Le porte utilizzate da altri servizi di grid non sono consentite. Vedi "Porte interne di StorageGRID".
${post_edited_translations.segment}	Deve essere **S3**.
Protocollo di rete	Seleziona **HTTPS**. **Nota**: La comunicazione con StorageGRID senza crittografia TLS è supportata ma non consigliata.

3. Nella fase **Seleziona modalità di associazione**, specifica la modalità di associazione. La modalità di associazione controlla come accedi all'endpoint usando qualsiasi indirizzo IP oppure indirizzi IP e interfacce di rete specifici.

Modalità	Descrizione
${post_edited_translations.segment}	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. Utilizza l'impostazione **Globale** (predefinita) a meno che tu non debba limitare l'accessibilità di questo endpoint.
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.

Modalità	Descrizione
Tipo di nodo	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.

4. 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.
${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.

5. Per la fase **Allega certificato**, seleziona una delle seguenti opzioni:

Campo	Descrizione
Carica il certificato (consigliato)	Utilizza questa opzione per caricare un certificato server firmato da una CA, la chiave privata del certificato e, facoltativamente, un CA bundle.
Genera certificato	Utilizza questa opzione per generare un certificato autofirmato. Consulta "${post_edited_translations.segment}" per i dettagli su cosa inserire.
Usa il certificato StorageGRID S3	Utilizza questa opzione solo se hai già caricato o generato una versione personalizzata del certificato globale di StorageGRID. Vedi "Configura i certificati API S3" per i dettagli.

6. Seleziona **Fine** per tornare al setup wizard S3.
7. Seleziona **Continua** per passare alla fase tenant e bucket.

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

Usa l'endpoint del bilanciatore di carico esistente

Passaggi

1. Per utilizzare un endpoint esistente, seleziona il suo nome da **Seleziona un endpoint del bilanciatore di carico**.
2. Seleziona **Continua** per passare alla fase tenant e bucket.

Usa un bilanciatore di carico esterno

Passaggi

1. Per utilizzare un bilanciatore di carico esterno, compila i seguenti campi.

Campo	Descrizione
FQDN	Il fully qualified domain name (FQDN) del bilanciatore di carico esterno.
Porta	Il numero di porta che l'applicazione S3 userà per connettersi al load balancer esterno.
Certificato	Copia il certificato del server per il load balancer esterno e incollalo in questo campo.

2. Seleziona **Continua** per passare alla fase tenant e bucket.

Passaggio 3 di 6: Crea tenant e bucket

Un tenant è un'entità che può utilizzare le applicazioni S3 per archiviare e recuperare oggetti in StorageGRID. Ogni tenant ha i propri utenti, chiavi di accesso, bucket, oggetti e un set specifico di funzionalità.

Un bucket è un container utilizzato per archiviare gli oggetti di un tenant e i metadati degli oggetti. Anche se i tenant possono avere molti bucket, la procedura guidata ti aiuta a creare un tenant e un bucket nel modo più rapido e semplice. Se hai bisogno di aggiungere bucket o impostare opzioni in seguito, puoi usare il Tenant Manager.

Per i dettagli su questa attività, vedi "Crea account tenant" e "Crea bucket S3".

Passaggi

1. Inserisci un nome per il tenant account.

   I nomi dei tenant non devono essere univoci. Quando viene creato l'account del tenant, riceve un ID account univoco e numerico.

2. Definisci access root per il tenant account, in base al fatto che il tuo sistema StorageGRID utilizzi "federazione di identità", "single sign-on (SSO)" o entrambi.

Opzione	${post_edited_translations.segment}
Se la federazione delle identità non è abilitata	Specifica la password da usare quando accedi al tenant come utente root.
Se la federazione delle identità è abilitata	a. Seleziona un gruppo federato esistente per avere "Permesso di accesso root" per il tenant. b. Facoltativamente, specifica la password da usare quando accedi al tenant come utente root.

Opzione	${post_edited_translations.segment}
Se sono abilitati sia la federazione delle identità che il single sign-on (SSO)	Seleziona un gruppo federato esistente da assegnare "Permesso di accesso root" al tenant. Nessun utente locale può accedere.

3. Se vuoi che la procedura guidata crei l'ID della chiave di accesso e la chiave di accesso segreta per l'utente root, seleziona **Crea automaticamente la chiave di accesso S3 per l'utente root**.

   Seleziona questa opzione se l'unico utente del tenant sarà l'utente root. Se altri utenti utilizzeranno questo tenant, "usa Tenant Manager" configura le chiavi e le autorizzazioni.

4. Se vuoi creare un bucket per questo tenant ora, seleziona **Crea bucket per questo tenant**.

   Se S3 Object Lock è abilitato per la grid, il bucket creato in questo passaggio non ha S3 Object Lock abilitato. Se devi usare un bucket S3 Object Lock per questa applicazione S3, non selezionare di creare un bucket ora. Utilizza invece Tenant Manager per "crea il bucket" più tardi.

   a. Inserisci il nome del bucket che l'applicazione S3 utilizzerà. Ad esempio, `s3-bucket`.

      Non puoi cambiare il nome del bucket dopo aver creato il bucket.

   b. Seleziona la **regione** per questo bucket.

      Utilizza la regione predefinita (`us-east-1`) a meno che tu non preveda di utilizzare ILM in futuro per filtrare gli oggetti in base alla regione del bucket.

5. Seleziona **Crea e continua**.

Passaggio 4 di 6: Scarica i dati

Nella fase di download dei dati, puoi scaricare uno o due file per salvare i dettagli di ciò che hai appena configurato.

Passaggi

1. Se hai selezionato **Crea automaticamente la chiave di accesso S3 per l'utente root**, esegui una o entrambe le seguenti operazioni:
   - Seleziona **Scarica le chiavi di accesso** per scaricare un `.csv` file contenente il nome dell'account tenant, l'ID della chiave di accesso e la chiave di accesso segreta.
   - Seleziona l'icona di copia ( ) per copiare l'ID della chiave di accesso e la chiave di accesso segreta negli appunti.
2. Seleziona **Scarica i valori di configurazione** per scaricare un `.txt` file contenente le impostazioni per l'endpoint del bilanciamento del carico, il tenant, il bucket e l'utente root.
3. Salva queste informazioni in un luogo sicuro.

   Non chiudere questa pagina finché non hai copiato entrambe le chiavi di accesso. Le chiavi non saranno disponibili dopo che avrai chiuso questa pagina. Assicurati di salvare queste informazioni in un luogo sicuro perché possono essere utilizzate per ottenere dati dal tuo sistema StorageGRID.

4. Se richiesto, seleziona la casella di controllo per confermare di aver scaricato o copiato le chiavi.
5. Seleziona **Continua** per andare alla fase delle regole e dei criteri ILM.

Passaggio 5 di 6: Esamina la regola ILM e la policy ILM per S3

Le regole di gestione del ciclo di vita delle informazioni (ILM) controllano il posizionamento, la durata e il comportamento di acquisizione di tutti gli oggetti nel tuo sistema StorageGRID. La policy ILM inclusa con StorageGRID crea due copie replicate di tutti gli oggetti. Questa policy è in vigore finché non attivi almeno una nuova policy.

Passaggi

1. Esamina le informazioni fornite nella pagina.
2. Se vuoi aggiungere istruzioni specifiche per gli oggetti appartenenti al nuovo tenant o bucket, crea una nuova regola e una nuova policy. Vedi "Crea regola ILM" e "Usa le policy ILM".
3. Seleziona **Ho letto questi passaggi e ho capito cosa devo fare**.
4. Seleziona la casella di controllo per indicare che hai capito cosa fare dopo.
5. Seleziona **Continua** per andare su **Riepilogo**.

Passaggio 6 di 6: Rivedi il riepilogo

Passaggi

1. Rivedi il riepilogo.
2. Prendi nota dei dettagli nei passaggi successivi, che descrivono la configurazione aggiuntiva che potrebbe essere necessaria prima di connetterti al client S3. Ad esempio, selezionando **Sign in as root** vieni indirizzato al Tenant Manager, dove puoi aggiungere utenti tenant, creare bucket aggiuntivi e aggiornare le impostazioni dei bucket.
3. Seleziona **Fine**.
4. Configura l'applicazione utilizzando il file scaricato da StorageGRID o i valori ottenuti manualmente.

${post_edited_translations.segment}

Scopri i gruppi ad alta disponibilità di StorageGRID

I gruppi ad alta disponibilità (HA) forniscono connessioni dati ad alta disponibilità per i client S3 e connessioni ad alta disponibilità al Grid Manager e al Tenant Manager.

Puoi raggruppare le interfacce di rete di più nodi Admin e Gateway in un gruppo ad alta disponibilità (HA). Se l'interfaccia attiva nel gruppo HA si guasta, un'interfaccia di backup può gestire il carico di lavoro.

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- I gruppi HA che includono solo Admin Node forniscono connessioni ad alta disponibilità al Grid Manager e al Tenant Manager.
- Un gruppo HA che include solo appliance di servizi e nodi software basati su VMware può fornire connessioni ad alta disponibilità per "Tenant S3 che usano S3 Select". I gruppi HA sono consigliati quando si utilizza S3 Select, ma non obbligatori.

${post_edited_translations.segment}

1. Selezioni un'interfaccia di rete per uno o più Admin Node o Gateway Node. Puoi usare un'interfaccia Grid Network (eth0), un'interfaccia Client Network (eth2), un'interfaccia VLAN o un'interfaccia di accesso che hai aggiunto al nodo.

   ${post_edited_translations.segment}

2. Specifica un'interfaccia come interfaccia primaria. L'interfaccia primaria è l'interfaccia attiva a meno che non si verifichi un guasto.
3. ${post_edited_translations.segment}
4. Puoi assegnare da uno a 10 indirizzi IP virtuali (VIP) al gruppo. Le applicazioni client possono utilizzare uno qualsiasi di questi indirizzi VIP per connettersi a StorageGRID.

Per istruzioni, consulta "Configura i gruppi ad alta disponibilità".

Qual è l'interfaccia attiva?

Durante il normale funzionamento, tutti gli indirizzi VIP del gruppo HA vengono aggiunti all'interfaccia primaria, che è la prima interfaccia in ordine di priorità. Finché l'interfaccia primaria rimane disponibile, viene utilizzata quando i client si connettono a qualsiasi indirizzo VIP del gruppo. Cioè, durante il normale funzionamento, l'interfaccia primaria è l'interfaccia "attiva" per il gruppo.

Analogamente, durante il normale funzionamento, le interfacce a priorità inferiore del gruppo HA fungono da interfacce di "backup". Queste interfacce di backup non vengono utilizzate a meno che l'interfaccia primaria (attualmente attiva) non diventi non disponibile.

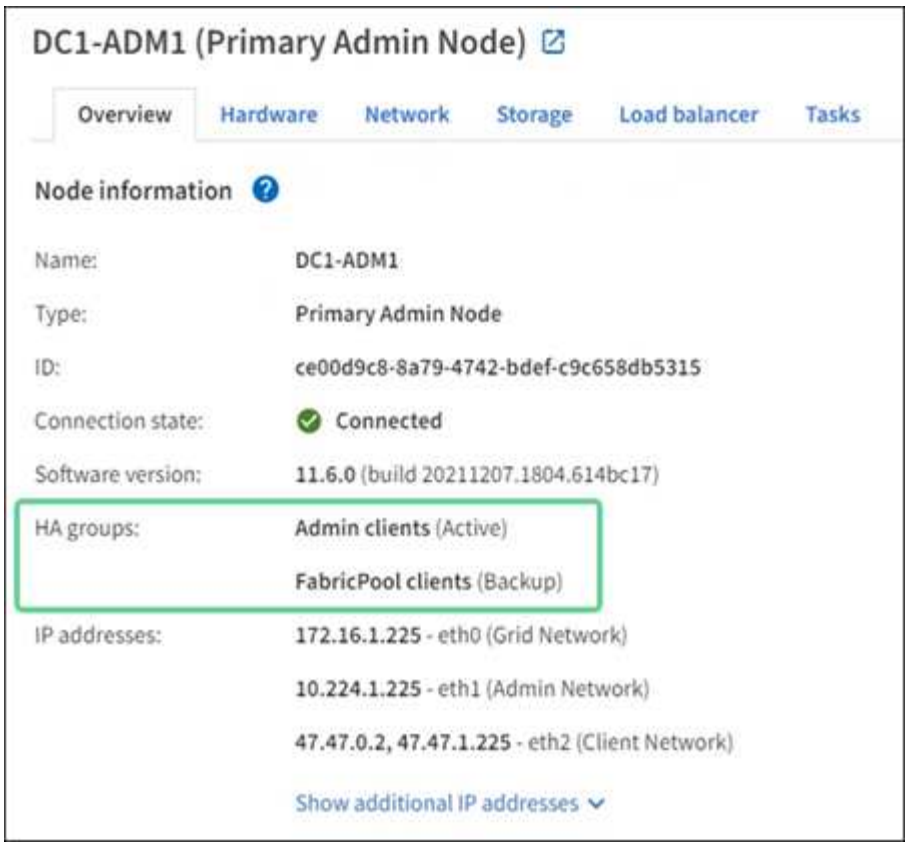
Visualizza lo stato attuale del gruppo HA di un nodo

Per verificare se un nodo è assegnato a un gruppo HA e determinarne lo stato attuale, seleziona **Nodi** > ***nodo***.

Se la scheda **Panoramica** include una voce per i **gruppi HA**, il nodo viene assegnato ai gruppi HA elencati. Il valore che segue il nome del gruppo indica lo stato corrente del nodo nel gruppo HA:

- ${post_edited_translations.segment}
- **Backup**: Il gruppo HA non sta attualmente utilizzando questo nodo; questa è un'interfaccia di backup.
- **Arrestato**: Il gruppo HA non può essere ospitato su questo nodo perché il servizio di High Availability (keepalived) è stato arrestato manualmente.
- **Errore**: Il gruppo HA non può essere ospitato su questo nodo a causa di uno o più dei seguenti motivi:
  - ${post_edited_translations.segment}
  - L'interfaccia eth0 o VIP del nodo è inattiva.
  - ${post_edited_translations.segment}

In questo esempio, il nodo Admin primario è stato aggiunto a due gruppi HA. Attualmente, questo nodo funge da interfaccia attiva per il gruppo di client Admin e da interfaccia di backup per il gruppo di client FabricPool.



Cosa succede quando l'interfaccia attiva si guasta?

L'interfaccia che attualmente ospita gli indirizzi VIP è l'interfaccia attiva. Se il gruppo HA include più di un'interfaccia e l'interfaccia attiva si guasta, gli indirizzi VIP vengono spostati sulla prima interfaccia di backup disponibile, in ordine di priorità. Se anche questa interfaccia si guasta, gli indirizzi VIP vengono spostati sulla successiva interfaccia di backup disponibile e così via.

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- L'interfaccia attiva si disconnette.
- Il servizio Load Balancer si interrompe.
- ${post_edited_translations.segment}

> Il failover potrebbe non essere attivato da guasti di rete esterni al nodo che ospita l'interfaccia attiva. Analogamente, il failover non viene attivato dai servizi del Grid Manager o del Tenant Manager.

Il processo di failover in genere richiede solo pochi secondi ed è sufficientemente rapido da far sì che le applicazioni client risentano minimamente dell'impatto e possano fare affidamento sui normali meccanismi di retry per continuare a funzionare.

Quando il problema viene risolto e un'interfaccia a priorità più elevata torna disponibile, gli indirizzi VIP vengono automaticamente spostati sull'interfaccia a priorità più alta disponibile.

Come i gruppi HA di StorageGRID garantiscono l'alta disponibilità

Puoi usare i gruppi ad alta disponibilità (HA) per offrire connessioni altamente disponibili a StorageGRID per i dati degli oggetti e per uso amministrativo.

- Un gruppo HA può fornire connessioni amministrative ad alta disponibilità al Grid Manager o al Tenant Manager.
- Un gruppo HA può fornire connessioni dati altamente disponibili per i client S3.
- Un gruppo HA che contiene una sola interfaccia ti permette di fornire molti indirizzi VIP e di impostare esplicitamente gli indirizzi IPv6.

Un gruppo HA può garantire l'alta disponibilità solo se tutti i nodi inclusi nel gruppo forniscono gli stessi servizi. Quando crei un gruppo HA, aggiungi interfacce dai tipi di nodi che forniscono i servizi di cui hai bisogno.

- ${post_edited_translations.segment}
- **Nodi gateway**: includono il servizio Load Balancer.

${post_edited_translations.segment}	**${post_edited_translations.segment}**
${post_edited_translations.segment}	• Nodo amministrativo primario (**Primario**) • Nodi amministrativi non primari **Nota:** Il nodo di amministrazione primario deve essere l'interfaccia primaria. Alcune procedure di manutenzione possono essere eseguite solo dal nodo di amministrazione primario.
Accesso solo al Tenant Manager	• Nodi Admin primari o non primari
Accesso client S3—Servizio Load Balancer	• Nodi di amministrazione • ${post_edited_translations.segment}
Accesso client S3 per "S3 Select"	• ${post_edited_translations.segment} • Nodi software basati su VMware **Nota**: i gruppi HA sono consigliati quando usi S3 Select, ma non sono obbligatori.

Limitazioni dell'utilizzo dei gruppi HA con Grid Manager o Tenant Manager

${post_edited_translations.segment}

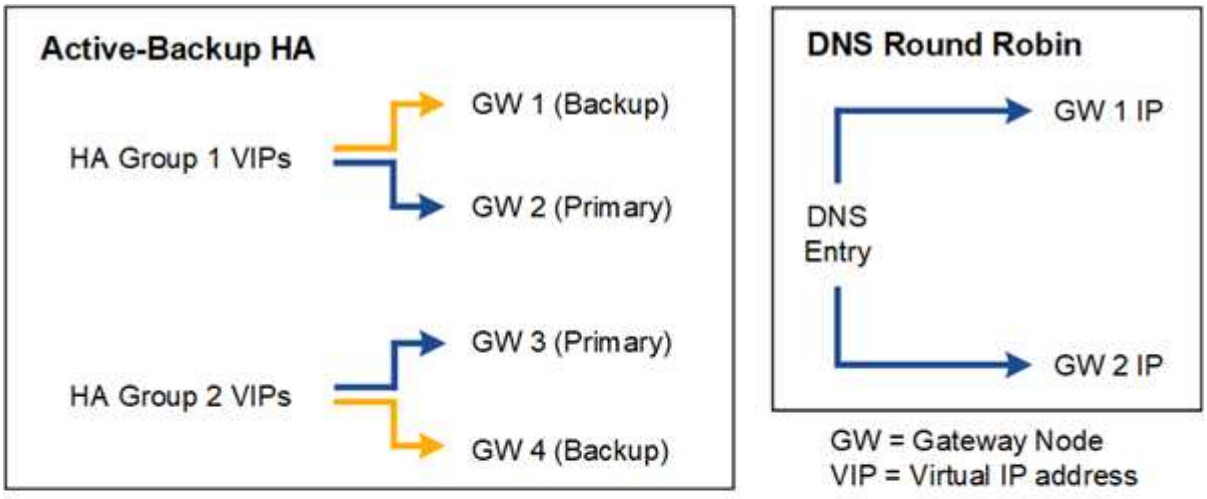
Se al momento del failover hai effettuato l'accesso a Grid Manager o Tenant Manager, verrai disconnesso e dovrai accedere di nuovo per riprendere la tua attività.

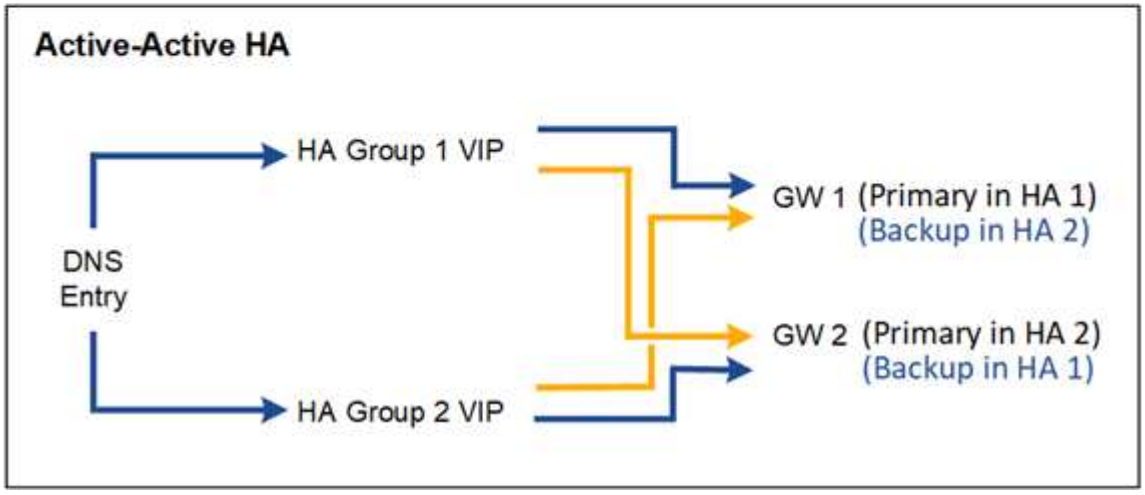
Alcune procedure di manutenzione non possono essere eseguite quando il nodo di amministrazione primario non è disponibile. Durante il failover, puoi usare Grid Manager per monitorare il tuo sistema StorageGRID.

Opzioni di configurazione per i gruppi di alta disponibilità di StorageGRID

I seguenti diagrammi forniscono esempi di diverse modalità in cui è possibile configurare i gruppi ad alta disponibilità (HA). Ogni opzione presenta vantaggi e svantaggi.

${post_edited_translations.segment}





${post_edited_translations.segment}

Configurazione	Vantaggi	Svantaggi
Active-Backup HA	• Gestito da StorageGRID senza dipendenze esterne. • Failover rapido.	• In un gruppo HA è attivo un solo nodo. Almeno un nodo per gruppo HA sarà inattivo.

Configurazione	Vantaggi	Svantaggi
DNS Round Robin	• Aumento del throughput aggregato. • Nessun host inattivo.	• Failover lento, che potrebbe dipendere dal comportamento del client. • Richiede la configurazione dell'hardware al di fuori di StorageGRID. • Necessita di un controllo dello stato di salute implementato dal cliente.
HA active-active	• Il traffico viene distribuito su più gruppi HA. • ${post_edited_translations.segment} • Failover rapido.	• Più complesso da configurare. • Richiede la configurazione dell'hardware al di fuori di StorageGRID. • Necessita di un controllo dello stato di salute implementato dal cliente.

Configura i gruppi ad alta disponibilità in StorageGRID

Puoi configurare gruppi ad alta disponibilità (HA) per garantire un accesso altamente disponibile ai servizi sui nodi di amministrazione o sui nodi gateway.

Un sistema StorageGRID può avere un massimo di 255 gruppi HA.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Permesso di accesso root".
- Se prevedi di utilizzare un'interfaccia VLAN in un gruppo HA, hai creato l'interfaccia VLAN. Vedi "Configura le interfacce VLAN".
- Se prevedi di utilizzare un'interfaccia di accesso per un nodo in un gruppo HA, hai già creato l'interfaccia:
  - **Linux (prima dell'installazione del nodo)**: "Crea i file di configurazione del nodo"
  - **Linux (dopo l'installazione del nodo)**: "${post_edited_translations.segment}"
  - **VMware (dopo l'installazione del nodo)**: "${post_edited_translations.segment}"

"Linux" si riferisce a un'installazione di RHEL, Ubuntu o Debian. Per un elenco delle versioni supportate, vedi "NetApp Interoperability Matrix Tool (IMT)".

Crea un gruppo ad alta disponibilità

Quando crei un gruppo di alta disponibilità, selezioni una o più interfacce e le organizzi in ordine di priorità. Quindi, assegni uno o più indirizzi VIP al gruppo.

Un'interfaccia deve appartenere a un nodo Gateway o a un nodo Admin per essere inclusa in un gruppo HA. Un gruppo HA può utilizzare solo un'interfaccia per un determinato nodo; tuttavia, altre interfacce per lo stesso nodo possono essere utilizzate in altri gruppi HA.

Accedi al wizard

Passaggi

1. ${post_edited_translations.segment}
2. Seleziona **Create**.

${post_edited_translations.segment}

Passaggi

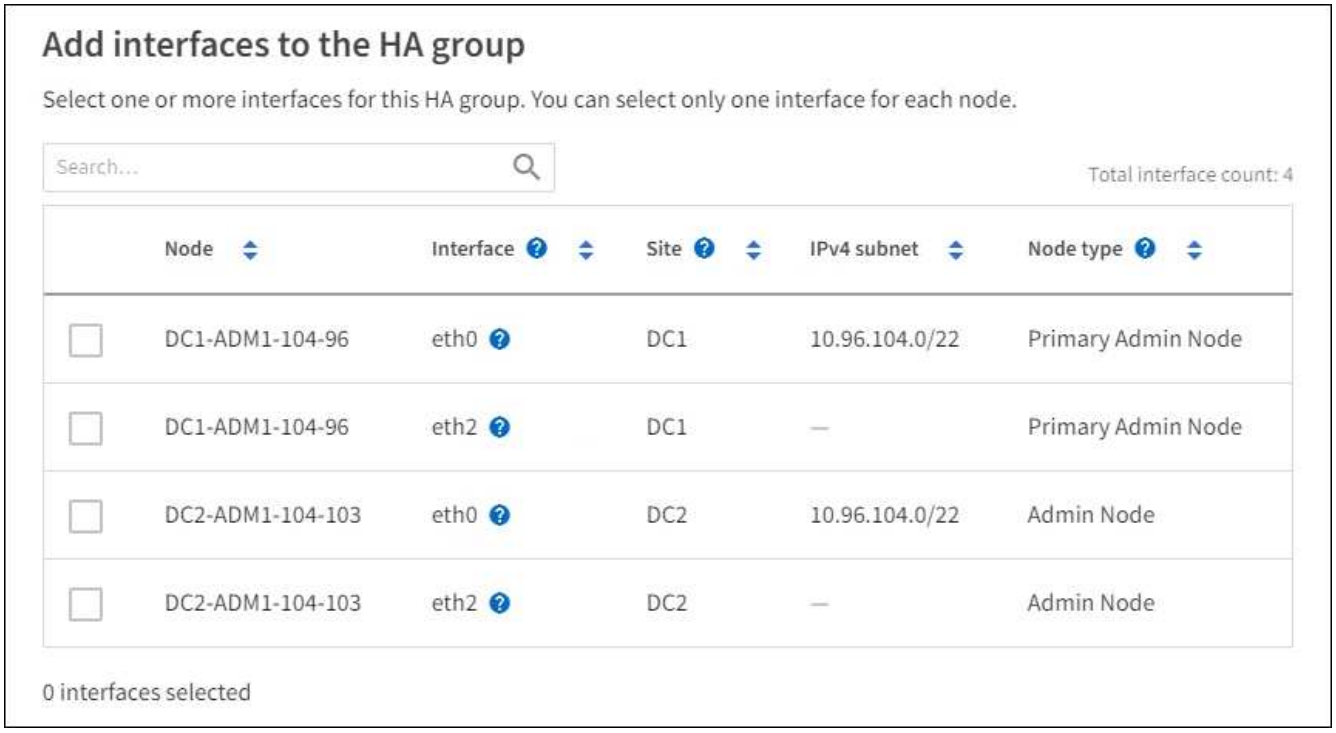
1. ${post_edited_translations.segment}
2. Facoltativamente, inserisci una descrizione per il gruppo HA.
3. Seleziona **Continue**.

Aggiungi interfacce al gruppo HA

Passaggi

1. Seleziona una o più interfacce da aggiungere a questo gruppo HA.

   Utilizza le intestazioni di colonna per ordinare le righe o inserisci un termine di ricerca per individuare più rapidamente le interfacce.

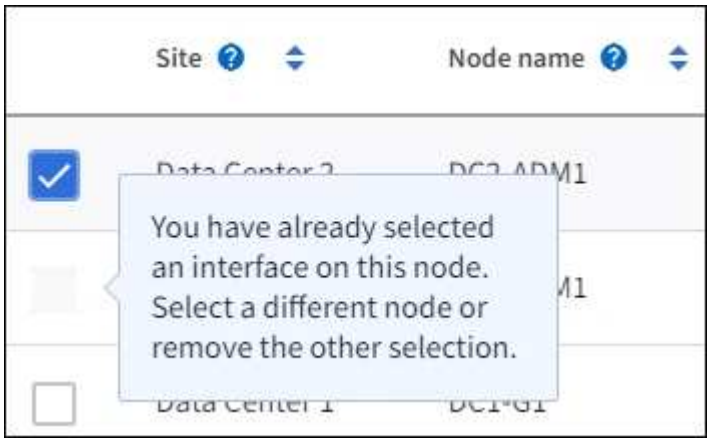


   ${post_edited_translations.segment}

   Linee guida per la selezione delle interfacce

   - Devi selezionare almeno un'interfaccia.
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}

- Se selezioni interfacce su diversi tipi di nodi, viene visualizzata una nota informativa. Ti viene ricordato che, in caso di failover, i servizi forniti dal nodo precedentemente attivo potrebbero non essere disponibili sul nodo appena attivo. Ad esempio, un Gateway Node di backup non può fornire la protezione HA dei servizi dell'Admin Node. Allo stesso modo, un Admin Node di backup non può eseguire tutte le procedure di manutenzione che l'Admin Node primario può fornire.
- Se non riesci a selezionare un'interfaccia, la relativa checkbox è disabilitata. Il tooltip fornisce ulteriori informazioni.



- Non puoi selezionare un'interfaccia se il suo valore di subnet o il suo gateway sono in conflitto con un'altra interfaccia selezionata.
- Non puoi selezionare un'interfaccia configurata se non ha un indirizzo IP statico.

2. Seleziona **Continue**.

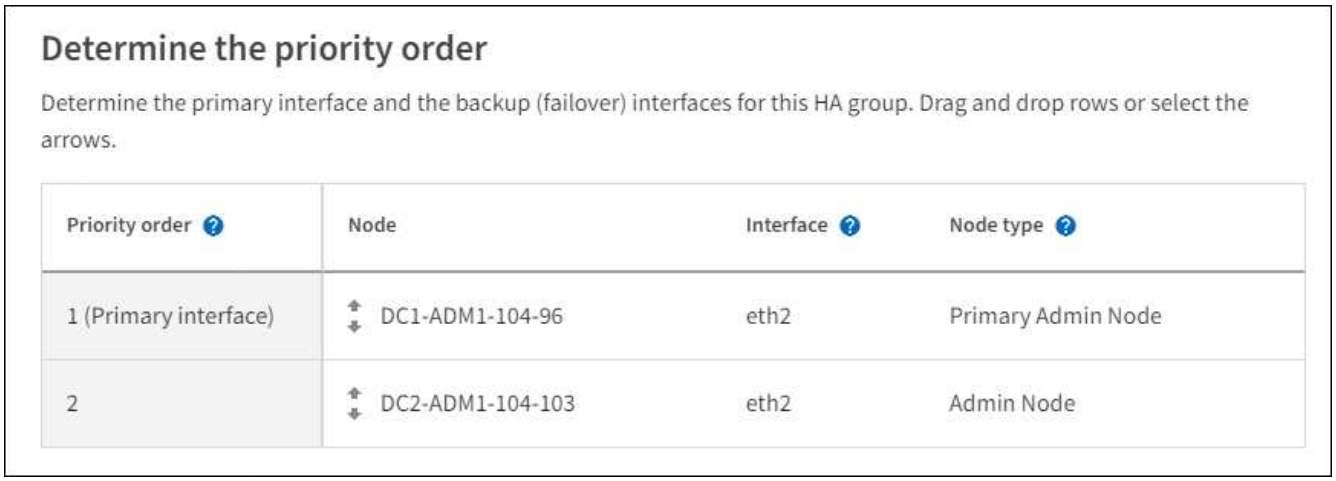
${post_edited_translations.segment}

Se il gruppo HA include più di un'interfaccia, puoi determinare qual è l'interfaccia primaria e quali sono quelle di backup (failover). Se l'interfaccia primaria si guasta, gli indirizzi VIP vengono spostati sull'interfaccia disponibile con la priorità più alta. Se anche quell'interfaccia si guasta, gli indirizzi VIP vengono spostati sull'interfaccia disponibile con la priorità immediatamente inferiore, e così via.

Passaggi

1. ${post_edited_translations.segment}

   La prima interfaccia nell'elenco è l'interfaccia primaria. L'interfaccia primaria è l'interfaccia attiva a meno che non si verifichi un errore.



Se il gruppo HA fornisce accesso al Grid Manager, devi selezionare un'interfaccia sul nodo Admin primario come interfaccia primaria. Alcune procedure di manutenzione possono essere eseguite solo dal nodo Admin primario.

2. Seleziona **Continue**.

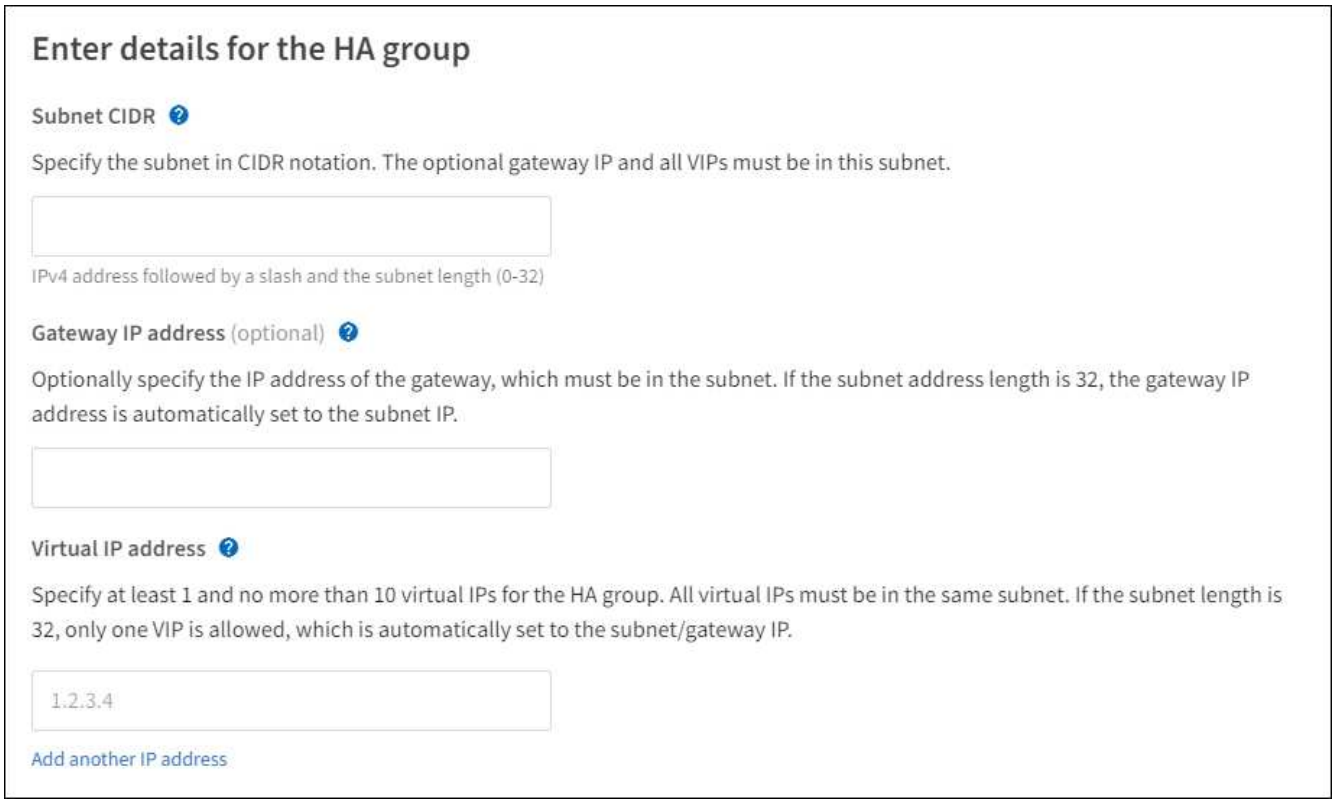
Inserisci gli indirizzi IP

Passaggi

1. Nel campo **Subnet CIDR**, specifica la subnet VIP in notazione CIDR: un indirizzo IPv4 seguito da una barra e dalla lunghezza della subnet (0-32).

   L'indirizzo di rete non deve avere alcun bit host impostato. Ad esempio, `192.16.0.0/22`.

   ${post_edited_translations.segment}



2. Opzionalmente, se client S3 amministrativi o tenant accederanno a questi indirizzi VIP da una subnet diversa, inserisci l'**indirizzo IP del gateway**. L'indirizzo del gateway deve trovarsi all'interno della subnet VIP.

   Gli utenti client e admin utilizzeranno questo gateway per accedere agli indirizzi IP virtuali.

3. Inserisci almeno uno e non più di dieci indirizzi VIP per l'interfaccia attiva nel gruppo HA. Tutti gli indirizzi VIP devono essere all'interno della subnet VIP e saranno tutti attivi contemporaneamente sull'interfaccia attiva.

   Devi fornire almeno un indirizzo IPv4. Facoltativamente, puoi specificare ulteriori indirizzi IPv4 e IPv6.

4. ${post_edited_translations.segment}

   Il gruppo HA è stato creato e ora puoi utilizzare gli indirizzi IP virtuali configurati.

Prossimi passi

Se utilizzerai questo gruppo HA per il bilanciamento del carico, crea un endpoint del bilanciatore del carico per determinare la porta e il protocollo di rete e per allegare i certificati richiesti. Vedi "${post_edited_translations.segment}".

Modifica un gruppo ad alta disponibilità

Puoi modificare un gruppo di alta disponibilità (HA) per cambiarne il nome e la descrizione, aggiungere o rimuovere interfacce, cambiare l'ordine di priorità o aggiungere o aggiornare gli indirizzi IP virtuali.

Ad esempio, potresti dover modificare un gruppo HA se vuoi rimuovere il nodo associato a un'interfaccia selezionata in una procedura di decommission di un sito o di un nodo.

Passaggi

1. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

2. Seleziona la casella di controllo per il gruppo HA che vuoi modificare.
3. Esegui una delle seguenti operazioni, a seconda di cosa vuoi aggiornare:
   - Seleziona **Azioni** > **Modifica indirizzo IP virtuale** per aggiungere o rimuovere indirizzi VIP.
   - Seleziona **Azioni** > **Modifica gruppo HA** per aggiornare il nome o la descrizione del gruppo, aggiungere o rimuovere interfacce, modificare l'ordine di priorità oppure aggiungere o rimuovere indirizzi VIP.
4. Se hai selezionato **Modifica indirizzo IP virtuale**:
   a. Aggiorna gli indirizzi IP virtuali per il gruppo HA.
   b. Seleziona **Salva**.
   c. Seleziona **Fine**.
5. Se hai selezionato **Modifica gruppo HA**:
   a. ${post_edited_translations.segment}
   b. Facoltativamente, seleziona o deseleziona le caselle di controllo per aggiungere o rimuovere interfacce.

      Se il gruppo HA fornisce l'accesso a Grid Manager, devi selezionare un'interfaccia sull'Admin Node primario come interfaccia primaria. Alcune procedure di manutenzione possono essere eseguite solo dall'Admin Node primario

   c. Facoltativamente, trascina le righe per modificare l'ordine di priorità dell'interfaccia primaria e delle eventuali interfacce di backup per questo gruppo HA.
   d. Facoltativamente, aggiorna gli indirizzi IP virtuali.
   e. Seleziona **Salva** e poi seleziona **Fine**.

Rimuovi un gruppo ad alta disponibilità

Puoi rimuovere uno o più gruppi ad alta disponibilità (HA) alla volta.

Non puoi rimuovere un gruppo HA se è associato a un endpoint del bilanciatore di carico. Per eliminare un gruppo HA, devi rimuoverlo da tutti gli endpoint del bilanciatore di carico che lo utilizzano.

Per evitare interruzioni del servizio per i client, aggiorna tutte le applicazioni client S3 interessate prima di rimuovere un gruppo HA. Aggiorna ciascun client in modo che si connetta utilizzando un altro indirizzo IP, ad esempio l'indirizzo IP virtuale di un gruppo HA diverso o l'indirizzo IP configurato per un'interfaccia durante l'installazione.

Passaggi

1. ${post_edited_translations.segment}
2. Esamina la colonna **Endpoint del bilanciatore del carico** per ciascun gruppo HA che desideri rimuovere. Se sono elencati endpoint del bilanciatore del carico:
   a. ${post_edited_translations.segment}

b. Seleziona la casella di controllo per l'endpoint.

c. ${post_edited_translations.segment}

d. Aggiorna la modalità di associazione per rimuovere il gruppo HA.

e. Seleziona **Salva modifiche**.

3. ${post_edited_translations.segment}
4. Seleziona **Azioni** > **Rimuovi gruppo HA**.
5. ${post_edited_translations.segment}

   Tutti i gruppi HA che hai selezionato vengono rimossi. Un banner verde di successo viene visualizzato nella pagina Gruppi di alta disponibilità.

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}

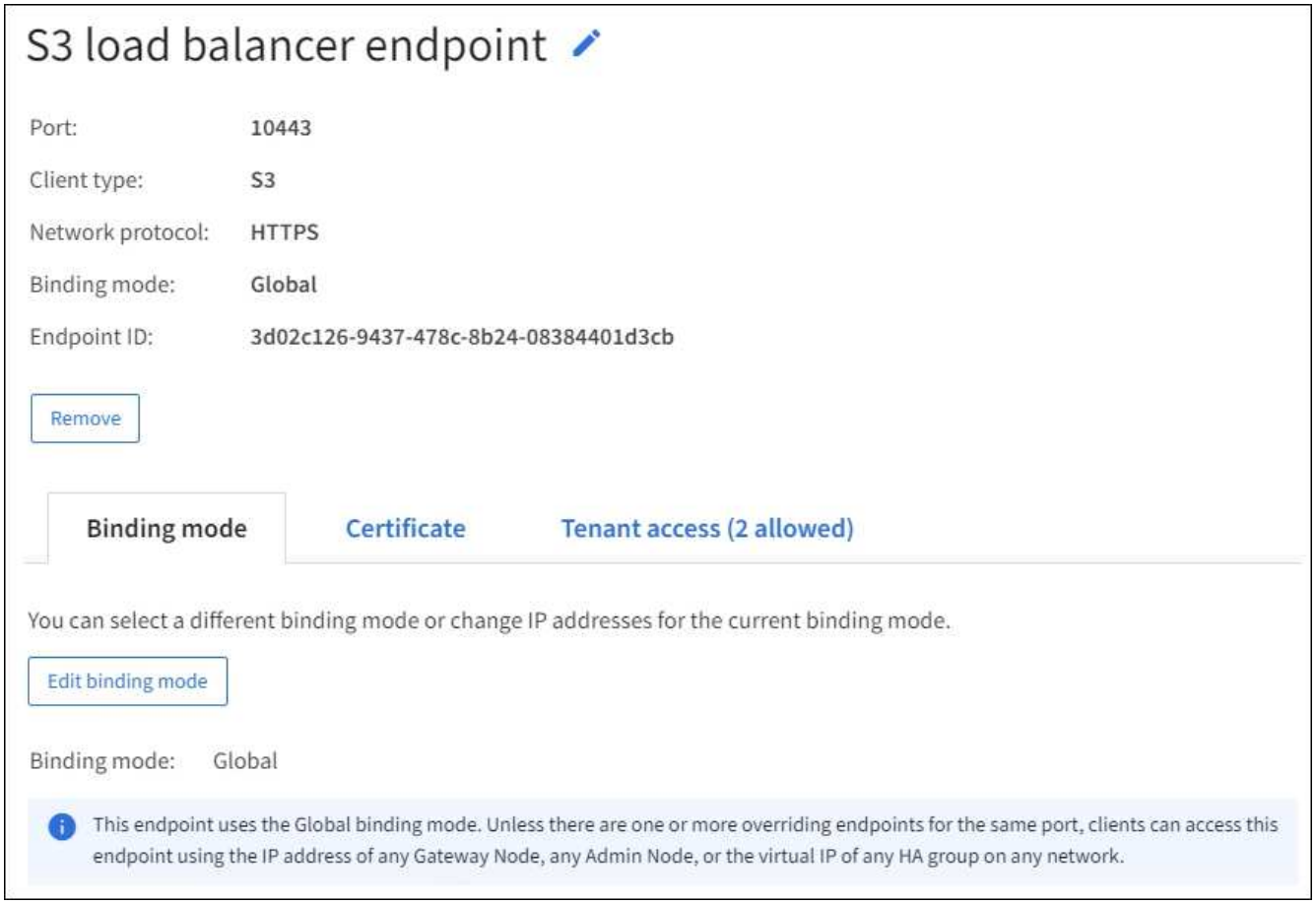
2. ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - fully qualified domain name o indirizzo IP
   - Dettagli relativi ai certificati richiesti

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**.

Attività	Menu azioni	Pagina dei dettagli
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**.

Configura i nomi di dominio degli endpoint S3 in StorageGRID

Per supportare le richieste in stile virtual-hosted di S3, devi usare Grid Manager per configurare l'elenco dei nomi di dominio degli endpoint S3 a cui si connettono i client S3.

L'utilizzo di un indirizzo IP per un domain name dell'endpoint non è supportato. Le versioni future impediranno questa configurazione.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".
- ${post_edited_translations.segment}

Non apportare modifiche alla domain name configuration durante un aggiornamento della griglia.

Informazioni su questa attività

${post_edited_translations.segment}

- Usa Grid Manager per aggiungere i domain name degli endpoint S3 al sistema StorageGRID.
- Assicurati che "${post_edited_translations.segment}" sia firmato per tutti i domain name richiesti dal client.

  Ad esempio, se l'endpoint è `s3.company.com`, devi assicurarti che il certificato utilizzato per le connessioni HTTPS includa l'endpoint `s3.company.com` e il Subject Alternative Name (SAN) wildcard dell'endpoint: `*.s3.company.com`.

- Configura il DNS server utilizzato dal client. Includi i record DNS per gli indirizzi IP che i client utilizzano per stabilire le connessioni e assicurati che i record facciano riferimento a tutti i nomi di dominio degli endpoint S3 richiesti, inclusi eventuali nomi wildcard.

I client possono connettersi a StorageGRID utilizzando l'indirizzo IP di un Gateway Node, di un Admin Node o di un Storage Node, oppure connettendosi all'indirizzo IP virtuale di un high availability group. Dovresti capire come le applicazioni client si connettono alla grid così da includere gli indirizzi IP corretti nei record DNS.

${post_edited_translations.segment}

- I client che si connettono a un endpoint del bilanciatore di carico possono utilizzare un certificato personalizzato per tale endpoint. Ogni endpoint del bilanciatore di carico può essere configurato per riconoscere diversi domain name degli endpoint S3.
- ${post_edited_translations.segment}

Se non aggiungi i nomi di dominio degli endpoint S3 e l'elenco è vuoto, il supporto per le richieste in stile virtual-hosted di S3 è disattivato.

Aggiungi un domain name S3

Passaggi

1. Seleziona **Configuration** > **Network** > **S3 endpoint domain names**.
2. Inserisci il domain name nel campo **Domain name 1**. Seleziona **Add another domain name** per aggiungere altri domain name.
3. Seleziona **Salva**.
4. Assicurati che i certificati server utilizzati dai client corrispondano ai domain name degli endpoint S3 richiesti.
   - Se i client si connettono a un endpoint del bilanciatore di carico che utilizza il proprio certificato, "aggiorna il certificato associato all'endpoint".
   - Se i client si connettono a un endpoint di load balancer che utilizza il certificato API S3 globale o direttamente ai Storage Node, "aggiorna il certificato API S3 globale".
5. ${post_edited_translations.segment}

Risultato

Ora, quando i client utilizzano l'endpoint `bucket.s3.company.com`, il DNS server risolve l'endpoint corretto e il certificato autentica l'endpoint come previsto.

Rinomina un domain name endpoint S3

Se cambi un nome utilizzato dalle applicazioni S3, le richieste in stile virtual-hosted non andranno a buon fine.

Passaggi

1. Seleziona **Configuration** > **Network** > **S3 endpoint domain names**.
2. Seleziona il campo domain name che vuoi modificare ed effettua le modifiche necessarie.
3. Seleziona **Salva**.
4. ${post_edited_translations.segment}

Elimina un domain name endpoint S3

Se rimuovi un nome utilizzato dalle applicazioni S3, le richieste in stile virtual-hosted non andranno a buon fine.

Passaggi

1. Seleziona **Configuration** > **Network** > **S3 endpoint domain names**.
2. Seleziona l'icona di eliminazione ✕ accanto al domain name.
3. ${post_edited_translations.segment}

Informazioni correlate

- "${post_edited_translations.segment}"
- "${post_edited_translations.segment}"
- "Configura i gruppi ad alta disponibilità"

Indirizzi IP e porte per le connessioni client StorageGRID

${post_edited_translations.segment}

Le applicazioni client possono connettersi a StorageGRID utilizzando l'indirizzo IP di un nodo grid e il numero di porta del servizio su quel nodo. In alternativa, puoi creare gruppi di high availability (HA) di nodi di bilanciamento del carico per fornire connessioni ad alta disponibilità che utilizzano indirizzi IP virtuali (VIP). Se desideri connetterti a StorageGRID utilizzando un fully qualified domain name (FQDN) anziché un indirizzo IP o VIP, puoi configurare le voci DNS.

Questa tabella riassume i diversi modi in cui i client possono connettersi a StorageGRID e gli indirizzi IP e le porte utilizzati per ciascun tipo di connessione. Se hai già creato gli endpoint del bilanciatore del carico e i gruppi ad alta disponibilità (HA), consulta Dove trovare gli indirizzi IP per individuare questi valori nel Grid Manager.

${post_edited_translations.segment}	**${post_edited_translations.segment}**	**indirizzo IP**	**Porta**
Gruppo HA	${post_edited_translations.segment}	${post_edited_translations.segment}	${post_edited_translations.segment}
Nodo amministratore	${post_edited_translations.segment}	Indirizzo IP del nodo amministratore	${post_edited_translations.segment}
${post_edited_translations.segment}	${post_edited_translations.segment}	Indirizzo IP del nodo gateway	${post_edited_translations.segment}

${post_edited_translations.segment}	${post_edited_translations.segment}	indirizzo IP	Porta
Nodo di archiviazione	LDR	Indirizzo IP del nodo di archiviazione	Porte S3 predefinite: • ${post_edited_translations.segment} • ${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

`https://VIP-of-HA-group:LB-endpoint-port`

Ad esempio, se l'indirizzo IP virtuale del gruppo HA è 192.0.2.5 e il numero di porta dell'endpoint del bilanciatore di carico è 10443, allora un'applicazione potrebbe utilizzare il seguente URL per connettersi a StorageGRID:

`https://192.0.2.5:10443`

Dove trovare gli indirizzi IP

1. Accedi al Grid Manager utilizzando un "browser web supportato".
2. Per trovare l'indirizzo IP di un nodo della griglia:
   a. Selezionare **Nodi**.
   b. ${post_edited_translations.segment}
   c. Seleziona la scheda **Overview**.
   d. ${post_edited_translations.segment}
   e. ${post_edited_translations.segment}

   Puoi stabilire connessioni dalle applicazioni client a uno qualsiasi degli indirizzi IP presenti nell'elenco:

   - **eth0:** Rete Grid
   - **eth1:** Rete amministrativa (opzionale)
   - **eth2:** Rete client (opzionale)

   > Se stai visualizzando un nodo Admin o un nodo Gateway e questo è il nodo attivo in un gruppo ad alta disponibilità, l'indirizzo IP virtuale del gruppo HA viene mostrato su eth2.

3. ${post_edited_translations.segment}
   a. ${post_edited_translations.segment}
   b. ${post_edited_translations.segment}

4. Per trovare il numero di porta di un endpoint del Load Balancer:
   a. ${post_edited_translations.segment}
   b. Annota il numero di porta dell'endpoint che vuoi usare.

      > Se il numero di porta è 80 o 443, l'endpoint viene configurato solo sui nodi Gateway, perché queste porte sono riservate sui nodi Admin. Tutte le altre porte vengono configurate sia sui nodi Gateway che sui nodi Admin.

   c. Seleziona il nome dell'endpoint dalla tabella.
   d. Conferma che il **tipo di client** (S3) corrisponde all'applicazione client che userà l'endpoint.

Informazioni sul copyright

Informazioni sul marchio commerciale