Configurare le connessioni client

StorageGRID software

NetApp
December 03, 2025

Sommario

Configurare le connessioni client

Configurare le connessioni client S3

In qualità di amministratore della griglia, gestisci le opzioni di configurazione che controllano il modo in cui le applicazioni client S3 si connettono al tuo sistema StorageGRID per archiviare e recuperare i dati.

I dettagli su Swift sono stati rimossi da questa versione del sito di documentazione. Vedere "StorageGRID 11.8: configurazione delle connessioni client S3 e Swift" .

Attività di configurazione

1. Eseguire le attività prerequisite in StorageGRID, in base al modo in cui l'applicazione client si connetterà a StorageGRID.

Compiti richiesti

È necessario ottenere:

- indirizzi IP
- Nomi di dominio
- Certificato SSL

Attività facoltative

Facoltativamente, configurare:

- Federazione delle identità
- SSO

1. Utilizzare StorageGRID per ottenere i valori di cui l'applicazione ha bisogno per connettersi alla griglia. È possibile utilizzare la procedura guidata di configurazione di S3 oppure configurare manualmente ciascuna entità StorageGRID .

Utilizzare la procedura guidata di configurazione S3

Seguire i passaggi della procedura guidata di configurazione S3.

Configurare manualmente

1. Crea un gruppo ad alta disponibilità
2. Crea endpoint del bilanciatore del carico
3. Crea un account inquilino
4. Crea bucket e chiavi di accesso
5. Configurare la regola e la politica ILM

1. Utilizzare l'applicazione S3 per completare la connessione a StorageGRID. Crea voci DNS per associare

gli indirizzi IP a tutti i nomi di dominio che intendi utilizzare.

Se necessario, eseguire ulteriori configurazioni dell'applicazione.

2. Eseguire attività continue nell'applicazione e in StorageGRID per gestire e monitorare l'archiviazione degli oggetti nel tempo.

Informazioni necessarie per collegare StorageGRID a un'applicazione client

Prima di poter collegare StorageGRID a un'applicazione client S3, è necessario eseguire i passaggi di configurazione in StorageGRID e ottenere un determinato valore.

Di quali valori ho bisogno?

Nella tabella seguente vengono mostrati i valori che è necessario configurare in StorageGRID e dove tali valori vengono utilizzati dall'applicazione S3 e dal server DNS.

Valore	Dove è configurato il valore	Dove viene utilizzato il valore
Indirizzi IP virtuali (VIP)	StorageGRID > Gruppo HA	voce DNS
Porta	StorageGRID > Endpoint del bilanciatore del carico	Applicazione client
Certificato SSL	StorageGRID > Endpoint del bilanciatore del carico	Applicazione client
Nome del server (FQDN)	StorageGRID > Endpoint del bilanciatore del carico	• Applicazione client • voce DNS
ID chiave di accesso S3 e chiave di accesso segreta	StorageGRID > Tenant e bucket	Applicazione client
Nome del bucket/contenitore	StorageGRID > Tenant e bucket	Applicazione client

Come posso ottenere questi valori?

A seconda delle tue esigenze, puoi procedere in uno dei seguenti modi per ottenere le informazioni di cui hai bisogno:

- *Usa il"Procedura guidata di configurazione S3" *. La procedura guidata di configurazione di S3 consente di configurare rapidamente i valori richiesti in StorageGRID e genera uno o due file che è possibile utilizzare durante la configurazione dell'applicazione S3. La procedura guidata ti guida attraverso i passaggi necessari e ti aiuta a verificare che le tue impostazioni siano conformi alle best practice StorageGRID .

> Se si sta configurando un'applicazione S3, si consiglia di utilizzare la procedura guidata di configurazione S3, a meno che non si abbiano requisiti particolari o che l'implementazione non richieda una personalizzazione significativa.

- *Usa il"Procedura guidata di configurazione FabricPool" *. Simile alla procedura guidata di configurazione di S3, la procedura guidata di configurazione FabricPool consente di configurare rapidamente i valori richiesti e genera un file che è possibile utilizzare quando si configura un livello cloud FabricPool in ONTAP.

  > Se si prevede di utilizzare StorageGRID come sistema di archiviazione degli oggetti per un livello cloud FabricPool , si consiglia di utilizzare la procedura guidata di configurazione FabricPool , a meno che non si abbiano requisiti speciali o che l'implementazione non richieda una personalizzazione significativa.

- **Configurare gli elementi manualmente**. Se ci si connette a un'applicazione S3 e si preferisce non utilizzare la procedura guidata di configurazione S3, è possibile ottenere i valori richiesti eseguendo manualmente la configurazione. Segui questi passaggi:
  a. Configurare il gruppo ad alta disponibilità (HA) che si desidera utilizzare per l'applicazione S3. Vedere "Configurare gruppi ad alta disponibilità" .
  b. Creare l'endpoint del bilanciatore del carico che verrà utilizzato dall'applicazione S3. Vedere "Configurare gli endpoint del bilanciatore del carico" .
  c. Creare l'account tenant che verrà utilizzato dall'applicazione S3. Vedere "Crea un account inquilino" .
  d. Per un tenant S3, accedi all'account del tenant e genera un ID chiave di accesso e una chiave di accesso segreta per ogni utente che accederà all'applicazione. Vedere "Crea le tue chiavi di accesso" .
  e. Creare uno o più bucket S3 all'interno dell'account tenant. Per S3, vedere"Crea bucket S3" .
  f. Per aggiungere istruzioni di posizionamento specifiche per gli oggetti appartenenti al nuovo tenant o bucket/contenitore, creare una nuova regola ILM e attivare una nuova policy ILM per utilizzare tale regola. Vedere"Crea regola ILM" E"Crea policy ILM" .

Sicurezza per i client S3

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

Riepilogo

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

Sicurezza della connessione
TLS

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

Autenticazione del client
ID chiave di accesso all'account S3 e chiave di accesso segreta

Autorizzazione del cliente
Proprietà del bucket e tutte le policy di controllo degli accessi applicabili

Come StorageGRID fornisce sicurezza per le applicazioni client

Le applicazioni client S3 possono connettersi al servizio Load Balancer sui nodi gateway o sui nodi amministrativi oppure direttamente sui nodi di archiviazione.

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

  HTTPS garantisce una comunicazione sicura e crittografata tramite TLS ed è consigliato. È necessario allegare un certificato di sicurezza all'endpoint.

  HTTP fornisce una comunicazione meno sicura e non crittografata e dovrebbe essere utilizzato solo per griglie non di produzione o di prova.

- I client che si connettono ai nodi di archiviazione possono anche utilizzare HTTPS o HTTP.

  HTTPS è il protocollo predefinito ed è consigliato.

  HTTP fornisce una comunicazione meno sicura e non crittografata, ma può essere facoltativamente"abilitato" per griglie non di produzione o di prova.

- Le comunicazioni tra StorageGRID e il client sono crittografate tramite TLS.
- Le comunicazioni tra il servizio Load Balancer e i nodi di archiviazione all'interno della griglia sono crittografate indipendentemente dal fatto che l'endpoint del load balancer sia configurato per accettare connessioni HTTP o HTTPS.
- I clienti devono fornire"Intestazioni di autenticazione HTTP" a StorageGRID per eseguire operazioni REST API.

Certificati di sicurezza e applicazioni client

In tutti i casi, le applicazioni client possono effettuare connessioni TLS utilizzando un certificato server personalizzato caricato dall'amministratore della griglia o 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 bilanciatore del carico ha il proprio certificato: un certificato server personalizzato caricato dall'amministratore della griglia o un certificato generato dall'amministratore della griglia in StorageGRID durante la configurazione dell'endpoint.

  Vedere "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 al momento dell'installazione del sistema StorageGRID (firmati dall'autorità di certificazione del sistema) oppure un singolo certificato server personalizzato fornito per la griglia da un amministratore della griglia. Vedere "aggiungi un certificato API S3 personalizzato" .

I client devono essere configurati in modo da considerare attendibile l'autorità di certificazione che ha firmato qualsiasi certificato utilizzato per stabilire 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 **Criteri TLS e SSH**.

Versioni supportate di TLS

StorageGRID supporta TLS 1.2 e TLS 1.3.

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

Utilizzare la procedura guidata di configurazione S3

Utilizzare la procedura guidata di configurazione S3: considerazioni e requisiti

È possibile utilizzare la procedura guidata di configurazione S3 per configurare StorageGRID come sistema di archiviazione degli oggetti per un'applicazione S3.

Quando utilizzare la procedura guidata di configurazione S3

La procedura guidata di configurazione di S3 ti guida attraverso ogni fase della configurazione di StorageGRID per l'utilizzo con un'applicazione S3. Durante il completamento della procedura guidata, scaricherai i file che potrai utilizzare per immettere valori nell'applicazione S3. Utilizza la procedura guidata per configurare il sistema più rapidamente e per assicurarti che le impostazioni siano conformi alle best practice StorageGRID .

Se hai il"Permesso di accesso root" , puoi completare la procedura guidata di configurazione di S3 quando inizi a utilizzare StorageGRID Grid Manager oppure puoi accedere e completare la procedura guidata in qualsiasi momento successivo. A seconda delle esigenze, è anche possibile configurare manualmente alcuni o tutti gli elementi richiesti e quindi utilizzare la procedura guidata per assemblare i valori necessari a un'applicazione S3.

Prima di utilizzare la procedura guidata

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

Ottenere indirizzi IP e configurare le interfacce VLAN

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

Se si prevede di utilizzare una LAN virtuale per separare il traffico dall'applicazione S3, è già stata configurata l'interfaccia VLAN. Vedere "Configurare le interfacce VLAN" .

Configurare la federazione delle identità e SSO

Se intendi utilizzare la federazione delle identità o l'accesso singolo (SSO) per il tuo sistema StorageGRID , hai abilitato queste funzionalità. Si sa anche quale gruppo federato deve avere accesso root per l'account tenant che verrà utilizzato dall'applicazione S3. Vedere"Utilizzare la federazione delle identità" E"Configurare l'accesso singolo" .

Ottieni e configura i nomi di dominio

Sai quale nome di dominio completo (FQDN) utilizzare per StorageGRID. Le voci del server dei nomi di dominio (DNS) mapperanno questo FQDN agli indirizzi IP virtuali (VIP) del gruppo HA creato tramite la procedura guidata.

Se si prevede di utilizzare richieste in stile host virtuale S3, è necessario disporre"nomi di dominio endpoint S3 configurati" . Si consiglia di utilizzare richieste in stile virtual hosted.

Esaminare i requisiti del bilanciatore del carico e del certificato di sicurezza

Se si prevede di utilizzare il bilanciatore del carico StorageGRID , è necessario aver esaminato le considerazioni generali sul bilanciamento del carico. Hai i certificati che caricherai o i valori necessari per generare un certificato.

Se si prevede di utilizzare un endpoint di bilanciamento del carico esterno (di terze parti), è necessario disporre del nome di dominio completo (FQDN), della porta e del certificato per tale bilanciatore del carico.

Configurare tutte le connessioni della federazione di griglia

Se si desidera consentire al tenant S3 di clonare i dati dell'account e replicare gli oggetti bucket in un'altra griglia utilizzando una connessione di federazione della griglia, confermare quanto segue prima di avviare la procedura guidata:

- Hai"configurato la connessione della federazione di griglia" .
- Lo stato della connessione è **Connesso**.
- Hai i permessi di accesso Root.

Accedi e completa la procedura guidata di configurazione S3

È possibile utilizzare la procedura guidata di configurazione S3 per configurare StorageGRID per l'utilizzo con un'applicazione S3. La procedura guidata di configurazione fornisce i valori necessari all'applicazione per accedere a un bucket StorageGRID e salvare gli oggetti.

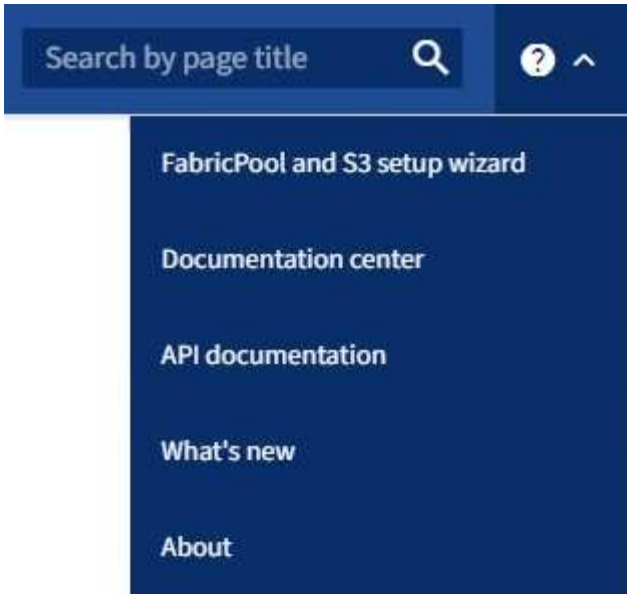
Prima di iniziare

- Tu hai il"Permesso di accesso root" .
- Hai esaminato il"considerazioni e requisiti" per utilizzare la procedura guidata.

Accedi alla procedura guidata

Passi

1. Sign in a Grid Manager utilizzando un"browser web supportato" .
2. Se nella dashboard viene visualizzato il banner **Procedura guidata di configurazione FabricPool e S3**, selezionare il collegamento nel banner. Se il banner non viene più visualizzato, seleziona l'icona della guida dalla barra dell'intestazione in Grid Manager e seleziona **Procedura guidata di configurazione di FabricPool e S3**.



3. Nella sezione Applicazione S3 della pagina della procedura guidata di configurazione FabricPool e S3, seleziona **Configura ora**.

Passaggio 1 di 6: configurare il gruppo HA

Un gruppo HA è una raccolta di nodi, ognuno dei quali contiene il servizio StorageGRID Load Balancer. Un gruppo HA può contenere nodi gateway, nodi amministrativi o entrambi.

È possibile utilizzare un gruppo HA per mantenere disponibili le connessioni dati S3. Se l'interfaccia attiva nel gruppo HA fallisce, un'interfaccia di backup può gestire il carico di lavoro con un impatto minimo sulle operazioni S3.

Per i dettagli su questa attività, vedere"Gestire gruppi ad alta disponibilità" .

Passi

1. Se si prevede di utilizzare un bilanciatore del carico esterno, non è necessario creare un gruppo HA. Seleziona **Salta questo passaggio** e vai aPassaggio 2 di 6: configurare l'endpoint del bilanciatore del carico .
2. Per utilizzare il bilanciatore del carico StorageGRID , è possibile creare un nuovo gruppo HA o utilizzare un gruppo HA esistente.

Crea gruppo HA

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

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

Campo	Descrizione
Nome del gruppo HA	Un nome visualizzato univoco per questo gruppo HA.
Descrizione (facoltativa)	Descrizione di questo gruppo HA.

c. Per il passaggio **Aggiungi interfacce**, seleziona le interfacce del nodo che desideri utilizzare in questo gruppo HA.

   Utilizzare le intestazioni di colonna per ordinare le righe oppure immettere un termine di ricerca per individuare più rapidamente le interfacce.

   È possibile selezionare uno o più nodi, ma è possibile selezionare solo un'interfaccia per ciascun nodo.

d. Per il passaggio **Assegna priorità alle interfacce**, determinare l'interfaccia primaria e tutte le interfacce di backup per questo gruppo HA.

   Trascinare 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 non funziona, gli indirizzi IP virtuali (VIP) vengono spostati sulla prima interfaccia di backup in ordine di priorità. Se tale interfaccia non funziona, gli indirizzi VIP vengono spostati alla successiva interfaccia di backup e così via. Una volta risolti i guasti, gli indirizzi VIP tornano all'interfaccia con la priorità più alta disponibile.

e. Per il passaggio **Inserisci indirizzi IP**, compila i seguenti campi.

Campo	Descrizione
CIDR di 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 si trovano sulla stessa subnet degli indirizzi VIP StorageGRID , immettere l'indirizzo IP del gateway locale VIP StorageGRID . L'indirizzo IP del gateway locale deve essere all'interno della subnet VIP.

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

f. Selezionare **Crea gruppo HA** e quindi **Fine** per tornare alla procedura guidata di configurazione di S3.

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

Utilizzare il gruppo HA esistente

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

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

Passaggio 2 di 6: configurare l'endpoint del bilanciatore del carico

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

È possibile utilizzare il servizio StorageGRID Load Balancer, presente su tutti i nodi gateway e amministrativi, oppure connettersi a un bilanciatore del carico esterno (di terze parti). Si consiglia di utilizzare il bilanciatore del carico StorageGRID .

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

Per utilizzare il servizio StorageGRID Load Balancer, seleziona la scheda * StorageGRID load balancer* e quindi crea o seleziona l'endpoint del load balancer che desideri utilizzare. Per utilizzare un bilanciatore del carico esterno, seleziona la scheda **Bilanciatore del carico esterno** e fornisci i dettagli sul sistema che hai già configurato.

Crea endpoint

Passi

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

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint.
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. Se si immette 80 o 443, l'endpoint viene configurato solo sui nodi gateway, perché queste porte sono riservate sui nodi amministrativi. **Nota:** non sono consentite le porte utilizzate da altri servizi di rete. Vedi il"Riferimento porta di rete" .
Tipo di cliente	Deve essere **S3**.
Protocollo di rete	Selezionare **HTTPS**. **Nota**: la comunicazione con StorageGRID senza crittografia TLS è supportata ma non consigliata.

3. Per il passaggio **Seleziona modalità di associazione**, specificare la modalità di associazione. La modalità di associazione controlla il modo in cui si accede all'endpoint utilizzando qualsiasi indirizzo IP o specifici indirizzi IP e interfacce di rete.

Modalità	Descrizione
Globale (predefinito)	I client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministrativo, l'indirizzo IP virtuale (VIP) di qualsiasi gruppo HA su qualsiasi rete o un FQDN corrispondente. Utilizzare l'impostazione **Globale** (predefinita) 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 il corrispondente FQDN) di un gruppo HA. Gli endpoint con questa modalità di associazione possono utilizzare tutti lo stesso numero di porta, purché i gruppi HA selezionati per gli endpoint non si sovrappongano.
Interfacce dei nodi	Per accedere a questo endpoint, i client devono utilizzare gli indirizzi IP (o i corrispondenti FQDN) delle interfacce dei nodi selezionati.

Modalità	Descrizione
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 oppure l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo gateway per accedere a questo endpoint.

4. Per il passaggio Accesso tenant, seleziona una delle seguenti opzioni:

Campo	Descrizione
Consenti tutti i tenant (predefinito)	Tutti gli account tenant possono utilizzare questo endpoint per accedere ai propri bucket.
Consenti inquilini selezionati	Solo gli account tenant selezionati possono utilizzare questo endpoint per accedere ai propri bucket.
Blocca gli inquilini 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 il passaggio **Allega certificato**, seleziona una delle seguenti opzioni:

Campo	Descrizione
Carica il certificato (consigliato)	Utilizzare questa opzione per caricare un certificato server firmato da una CA, una chiave privata del certificato e un bundle CA facoltativo.
Genera certificato	Utilizzare questa opzione per generare un certificato autofirmato. Vedere"Configurare gli endpoint del bilanciatore del carico" per i dettagli su cosa inserire.
Utilizzare il certificato StorageGRID S3	Utilizzare questa opzione solo se è già stata caricata o generata una versione personalizzata del certificato globale StorageGRID . Vedere"Configurare i certificati API S3" per i dettagli.

6. Selezionare **Fine** per tornare alla procedura guidata di configurazione S3.
7. Selezionare **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.

Utilizzare l'endpoint del bilanciatore del carico esistente

Passi

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

Utilizzare un bilanciatore di carico esterno

Passi

1. Per utilizzare un bilanciatore del carico esterno, compilare i seguenti campi.

Campo	Descrizione
Nome di dominio completo	Nome di dominio completo (FQDN) del bilanciatore del carico esterno.
Porta	Numero di porta che l'applicazione S3 utilizzerà per connettersi al bilanciatore del carico esterno.
Certificato	Copiare il certificato del server per il bilanciatore del carico esterno e incollarlo in questo campo.

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

Passaggio 3 di 6: creare 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 contenitore utilizzato per archiviare gli oggetti e i metadati degli oggetti di un tenant. Anche se i tenant potrebbero avere molti bucket, la procedura guidata ti aiuta a creare un tenant e un bucket nel modo più rapido e semplice. Se in un secondo momento è necessario aggiungere bucket o impostare opzioni, è possibile utilizzare Tenant Manager.

Per i dettagli su questa attività, vedere"Crea un account inquilino" E"Crea bucket S3" .

Passi

1. Inserisci un nome per l'account tenant.

   I nomi degli inquilini non devono essere univoci. Quando viene creato l'account tenant, questo riceve un ID account numerico univoco.

2. Definisci l'accesso root per l'account tenant, in base all'utilizzo o meno da parte del sistema StorageGRID"federazione di identità" ,"accesso unico (SSO)" , o entrambi.

Opzione	Fai questo
Se la federazione delle identità non è abilitata	Specificare la password da utilizzare quando si accede al tenant come utente root locale.
Se la federazione delle identità è abilitata	a. Seleziona un gruppo federato esistente da avere"Permesso di accesso root" per l'inquilino. b. Facoltativamente, specificare la password da utilizzare quando si accede al tenant come utente root locale.

Opzione	Fai questo
Se sono abilitati sia la federazione delle identità che il Single Sign-On (SSO)	Seleziona un gruppo federato esistente da avere"Permesso di accesso root" per l'inquilino. Nessun utente locale può effettuare l'accesso.

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

   Selezionare questa opzione se l'unico utente del tenant sarà l'utente root. Se altri utenti utilizzeranno questo tenant,"utilizzare Tenant Manager" per configurare chiavi e permessi.

4. Se desideri creare subito un bucket per questo tenant, seleziona **Crea bucket per questo tenant**.

   Se il blocco oggetti S3 è abilitato per la griglia, il bucket creato in questo passaggio non ha il blocco oggetti S3 abilitato. Se è necessario utilizzare un bucket S3 Object Lock per questa applicazione S3, non selezionare l'opzione per creare un bucket ora. Invece, usa Tenant Manager per"creare il secchio" Dopo.

   a. Immettere il nome del bucket che verrà utilizzato dall'applicazione S3. Ad esempio, `s3-bucket` .

      Non è possibile modificare il nome del bucket dopo averlo creato.

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

      Utilizza la regione predefinita(`us-east-1`) a meno che non si 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.

Passi

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

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

4. Se richiesto, seleziona la casella di controllo per confermare di aver scaricato o copiato le chiavi.
5. Selezionare **Continua** per passare alla fase relativa alle regole e ai criteri ILM.

Passaggio 5 di 6: rivedere 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 sistema StorageGRID . La policy ILM inclusa in StorageGRID crea due copie replicate di tutti gli oggetti. Questa politica è valida finché non attivi almeno una nuova politica.

Passi

1. Esaminare le informazioni fornite nella pagina.
2. Se si desidera aggiungere istruzioni specifiche per gli oggetti appartenenti al nuovo tenant o bucket, creare una nuova regola e un nuovo criterio. Vedere"Crea regola ILM" E"Utilizzare le policy ILM" .
3. Seleziona **Ho esaminato questi passaggi e ho capito cosa devo fare**.
4. Seleziona la casella di controllo per indicare che hai capito cosa fare dopo.
5. Selezionare **Continua** per andare a **Riepilogo**.

Fase 6 di 6: Riepilogo della revisione

Passi

1. Rivedi il riepilogo.
2. Prendere nota dei dettagli nei passaggi successivi, che descrivono la configurazione aggiuntiva che potrebbe essere necessaria prima di connettersi al client S3. Ad esempio, selezionando * Sign in come root* si accede a Tenant Manager, dove è possibile aggiungere utenti tenant, creare bucket aggiuntivi e aggiornare le impostazioni dei bucket.
3. Selezionare **Fine**.
4. Configurare l'applicazione utilizzando il file scaricato da StorageGRID o i valori ottenuti manualmente.

Gestire i gruppi HA

Cosa sono i gruppi ad alta disponibilità (HA)?

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

È possibile raggruppare le interfacce di rete di più nodi di amministrazione e gateway in un gruppo ad alta disponibilità (HA). Se l'interfaccia attiva nel gruppo HA non funziona, un'interfaccia di backup può gestire il carico di lavoro.

Ogni gruppo HA fornisce l'accesso ai servizi condivisi sui nodi selezionati.

- I gruppi HA che includono nodi gateway, nodi amministrativi o entrambi forniscono connessioni dati ad alta disponibilità per i client S3.
- I gruppi HA che includono solo nodi amministrativi 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 utilizzano S3 Select" . I gruppi HA sono consigliati

quando si utilizza S3 Select, ma non sono obbligatori.

Come si crea un gruppo HA?

1. Selezionare un'interfaccia di rete per uno o più nodi amministrativi o nodi gateway. È possibile utilizzare un'interfaccia Grid Network (eth0), un'interfaccia Client Network (eth2), un'interfaccia VLAN o un'interfaccia di accesso aggiunta al nodo.

   > Non è possibile aggiungere un'interfaccia a un gruppo HA se ha un indirizzo IP assegnato tramite DHCP.

2. Si specifica un'interfaccia come interfaccia primaria. L'interfaccia primaria è l'interfaccia attiva, a meno che non si verifichi un errore.
3. È possibile determinare l'ordine di priorità per tutte le interfacce di backup.
4. Assegna al gruppo da uno a 10 indirizzi IP virtuali (VIP). Le applicazioni client possono utilizzare uno qualsiasi di questi indirizzi VIP per connettersi a StorageGRID.

Per le istruzioni, vedere"Configurare gruppi ad alta disponibilità" .

Qual è l'interfaccia attiva?

Durante il normale funzionamento, tutti gli indirizzi VIP per il 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. Ciò significa che durante il normale funzionamento, l'interfaccia primaria è l'interfaccia "attiva" per il gruppo.

Allo stesso modo, durante il normale funzionamento, tutte le interfacce con priorità inferiore per il gruppo HA fungono da interfacce di "backup". Queste interfacce di backup non vengono utilizzate a meno che l'interfaccia primaria (attualmente attiva) non diventi più disponibile.

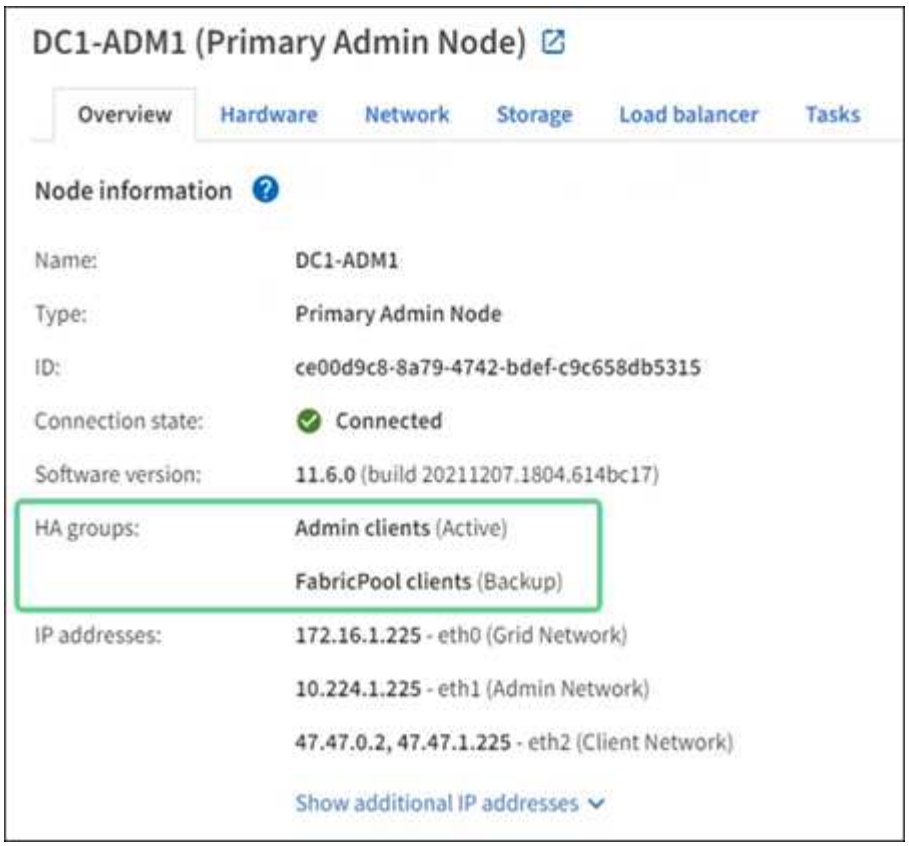
Visualizza lo stato attuale del gruppo HA di un nodo

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

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

- **Attivo**: il gruppo HA è attualmente ospitato su questo nodo.
- **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 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:
  - Il servizio Load Balancer (nginx-gw) non è in esecuzione sul nodo.
  - L'interfaccia eth0 o VIP del nodo è inattiva.
  - Il nodo è inattivo.

In questo esempio, il nodo di amministrazione primario è stato aggiunto a due gruppi HA. Questo nodo è attualmente l'interfaccia attiva per il gruppo di client Admin e un'interfaccia di backup per il gruppo di client FabricPool .



Cosa succede quando l'interfaccia attiva fallisce?

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 non funziona, gli indirizzi VIP vengono spostati sulla prima interfaccia di backup disponibile in ordine di priorità. Se tale interfaccia non funziona, gli indirizzi VIP vengono spostati alla successiva interfaccia di backup disponibile e così via.

Il failover può essere attivato per uno qualsiasi di questi motivi:

- Il nodo su cui è configurata l'interfaccia si interrompe.
- Il nodo su cui è configurata l'interfaccia perde la connettività con tutti gli altri nodi per almeno 2 minuti.
- L'interfaccia attiva si disattiva.
- Il servizio Load Balancer si arresta.
- Il servizio di alta disponibilità si arresta.

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

Il processo di failover richiede in genere solo pochi secondi ed è sufficientemente veloce da non avere un impatto significativo sulle applicazioni client e da consentire loro di continuare a funzionare con i normali comportamenti di ripetizione.

Quando l'errore viene risolto e un'interfaccia con priorità più alta diventa nuovamente disponibile, gli indirizzi VIP vengono automaticamente spostati sull'interfaccia con priorità più alta disponibile.

Come vengono utilizzati i gruppi HA?

È possibile utilizzare gruppi ad alta disponibilità (HA) per fornire connessioni ad alta disponibilità 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 ad alta disponibilità per i client S3.
- Un gruppo HA che contiene una sola interfaccia consente di fornire molti indirizzi VIP e di impostare esplicitamente indirizzi IPv6.

Un gruppo HA può garantire un'elevata disponibilità solo se tutti i nodi inclusi nel gruppo forniscono gli stessi servizi. Quando si crea un gruppo HA, aggiungere le interfacce dai tipi di nodi che forniscono i servizi richiesti.

- **Nodi amministrativi**: includono il servizio Load Balancer e consentono l'accesso al Grid Manager o al Tenant Manager.
- **Nodi gateway**: includono il servizio Load Balancer.

Scopo del gruppo HA	Aggiungi nodi di questo tipo al gruppo HA
Accesso a Grid Manager	• Nodo amministratore 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 amministrativi primari o non primari
Accesso client S3 - Servizio Load Balancer	• Nodi amministrativi • Nodi gateway
Accesso client S3 per"S3 Seleziona"	• Servizi elettrodomestici • Nodi software basati su VMware **Nota**: i gruppi HA sono consigliati quando si utilizza S3 Select, ma non sono obbligatori.

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

Se un servizio Grid Manager o Tenant Manager non funziona, il failover del gruppo HA non viene attivato.

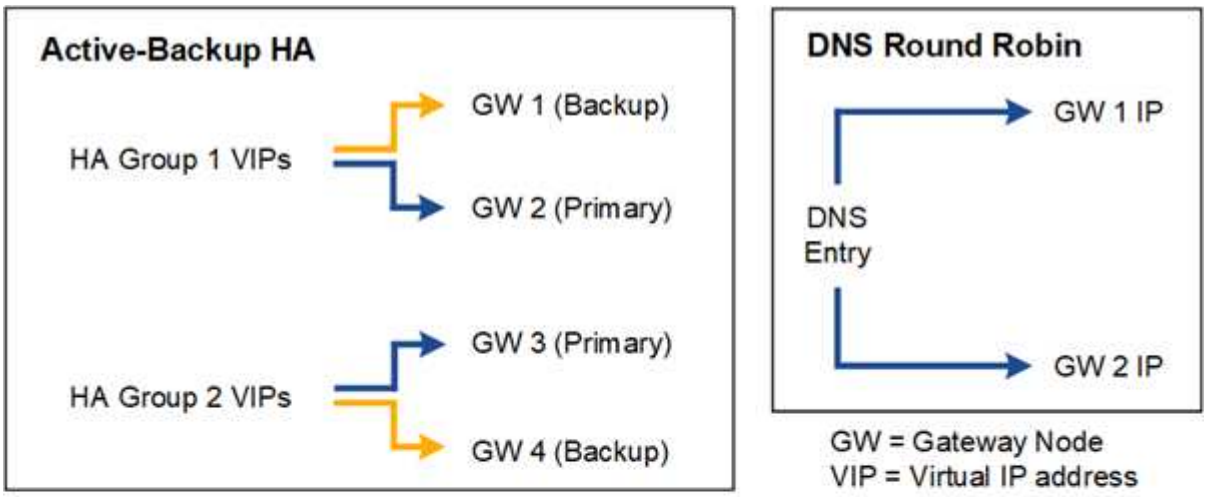
Se hai effettuato l'accesso a Grid Manager o Tenant Manager quando si verifica il failover, verrai disconnesso e dovrai effettuare nuovamente l'accesso per riprendere l'attività.

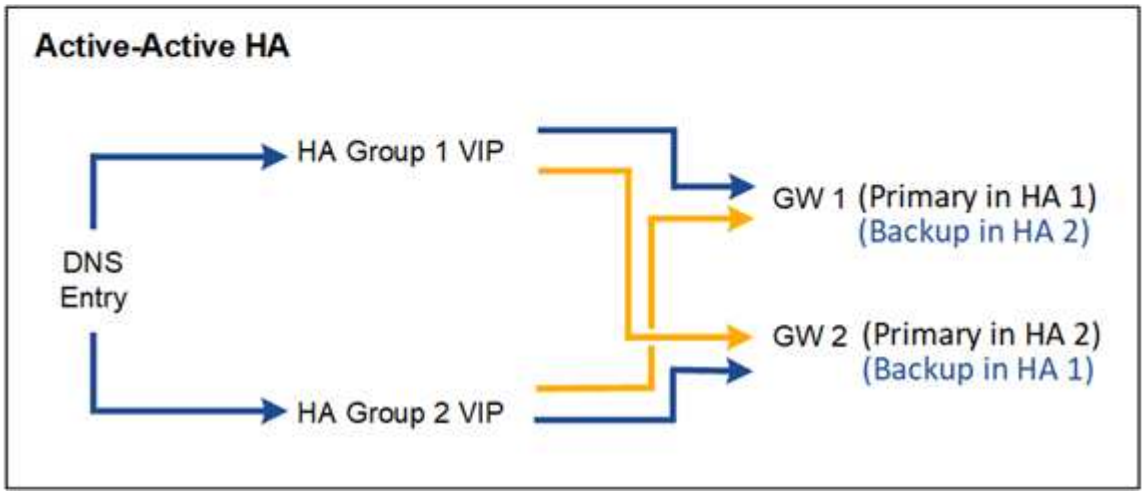
Alcune procedure di manutenzione non possono essere eseguite quando il nodo di amministrazione primario non è disponibile. Durante il failover, è possibile utilizzare Grid Manager per monitorare il sistema StorageGRID .

Opzioni di configurazione per i gruppi HA

I diagrammi seguenti forniscono esempi di diversi modi in cui è possibile configurare i gruppi HA. Ogni opzione presenta vantaggi e svantaggi.

Nei diagrammi, il blu indica l'interfaccia primaria nel gruppo HA e il giallo indica l'interfaccia di backup nel gruppo HA.





La tabella riassume i vantaggi di ciascuna configurazione HA mostrata nel diagramma.

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

Configurazione	Vantaggi	Svantaggi
DNS Round Robin	• Aumento della produttività aggregata. • Nessun host inattivo.	• Failover lento, che potrebbe dipendere dal comportamento del client. • Richiede la configurazione dell'hardware al di fuori di StorageGRID. • Richiede un controllo sanitario implementato dal cliente.
HA attivo-attivo	• Il traffico è distribuito su più gruppi HA. • Elevata produttività aggregata che aumenta con il numero di gruppi HA. • Failover rapido.	• Più complesso da configurare. • Richiede la configurazione dell'hardware al di fuori di StorageGRID. • Richiede un controllo sanitario implementato dal cliente.

Configurare gruppi ad alta disponibilità

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Tu hai il"Permesso di accesso root" .
- Se si prevede di utilizzare un'interfaccia VLAN in un gruppo HA, è stata creata l'interfaccia VLAN. Vedere "Configurare le interfacce VLAN" .
- Se si prevede di utilizzare un'interfaccia di accesso per un nodo in un gruppo HA, è stata creata l'interfaccia:
  - **Red Hat Enterprise Linux (prima di installare il nodo)**:"Creare file di configurazione del nodo"
  - **Ubuntu o Debian (prima di installare il nodo)**:"Creare file di configurazione del nodo"
  - **Linux (dopo aver installato il nodo)**:"Linux: aggiungere interfacce trunk o di accesso a un nodo"
  - **VMware (dopo l'installazione del nodo)**:"VMware: aggiungi trunk o interfacce di accesso a un nodo"

Creare un gruppo ad alta disponibilità

Quando si crea un gruppo ad alta disponibilità, si seleziona una o più interfacce e le si organizza in ordine di priorità. Quindi, assegni uno o più indirizzi VIP al gruppo.

Per includere un nodo gateway o un nodo amministrativo in un gruppo HA, è necessaria un'interfaccia. Un gruppo HA può utilizzare una sola interfaccia per ogni nodo; tuttavia, altre interfacce per lo stesso nodo possono essere utilizzate in altri gruppi HA.

Accedi alla procedura guidata

Passi

1. Selezionare **CONFIGURAZIONE** > **Rete** > **Gruppi ad alta disponibilità**.

2. Seleziona **Crea**.

Inserisci i dettagli per il gruppo HA

Passi

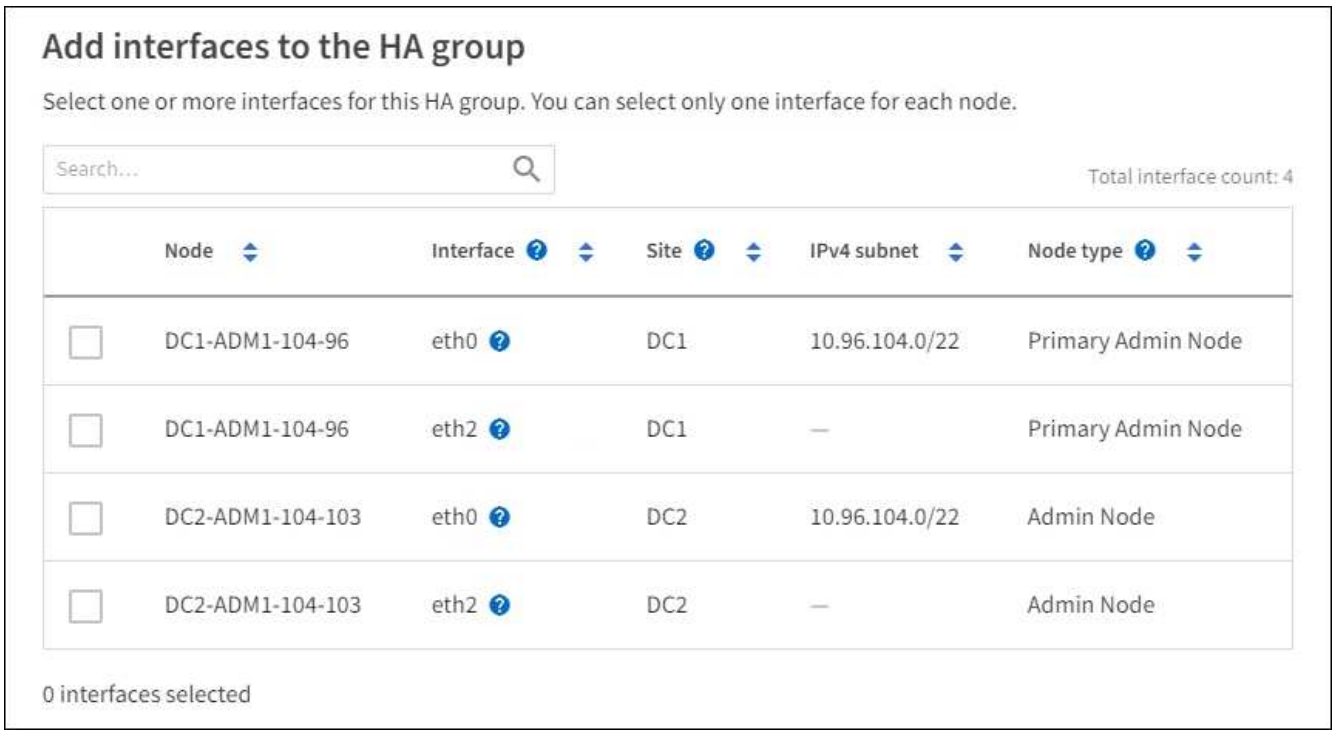
1. Fornire un nome univoco per il gruppo HA.
2. Facoltativamente, immettere una descrizione per il gruppo HA.
3. Selezionare **Continua**.

Aggiungere interfacce al gruppo HA

Passi

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

   Utilizzare le intestazioni di colonna per ordinare le righe oppure immettere un termine di ricerca per individuare più rapidamente le interfacce.



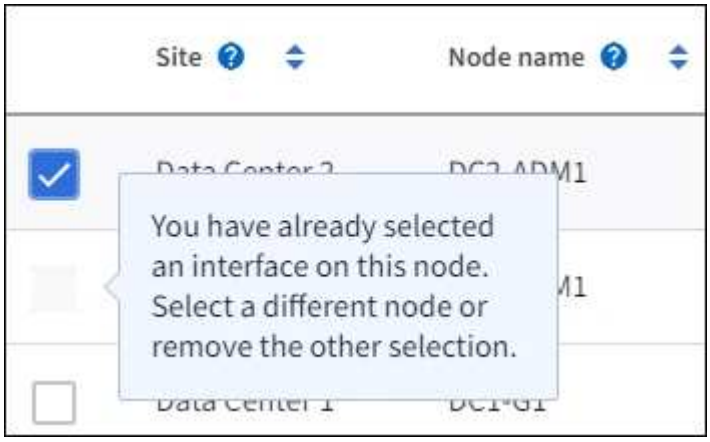
> Dopo aver creato un'interfaccia VLAN, attendere fino a 5 minuti affinché la nuova interfaccia venga visualizzata nella tabella.

Linee guida per la selezione delle interfacce

- È necessario selezionare almeno un'interfaccia.
- È possibile selezionare una sola interfaccia per un nodo.
- Se il gruppo HA è destinato alla protezione HA dei servizi del nodo amministrativo, che includono Grid Manager e Tenant Manager, selezionare le interfacce solo sui nodi amministrativi.
- Se il gruppo HA è destinato alla protezione HA del traffico client S3, selezionare le interfacce sui nodi di amministrazione, sui nodi gateway o su entrambi.
- Se si selezionano interfacce su diversi tipi di nodi, viene visualizzata una nota informativa. Si ricorda che se si verifica un failover, i servizi forniti dal nodo precedentemente attivo potrebbero non essere

disponibili sul nodo nuovamente attivo. Ad esempio, un nodo gateway di backup non può fornire protezione HA dei servizi del nodo amministrativo. Allo stesso modo, un Admin Node di backup non può eseguire tutte le procedure di manutenzione che può fornire il Admin Node primario.

- Se non è possibile selezionare un'interfaccia, la relativa casella di controllo è disattivata. La descrizione comandi fornisce ulteriori informazioni.



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

2. Selezionare **Continua**.

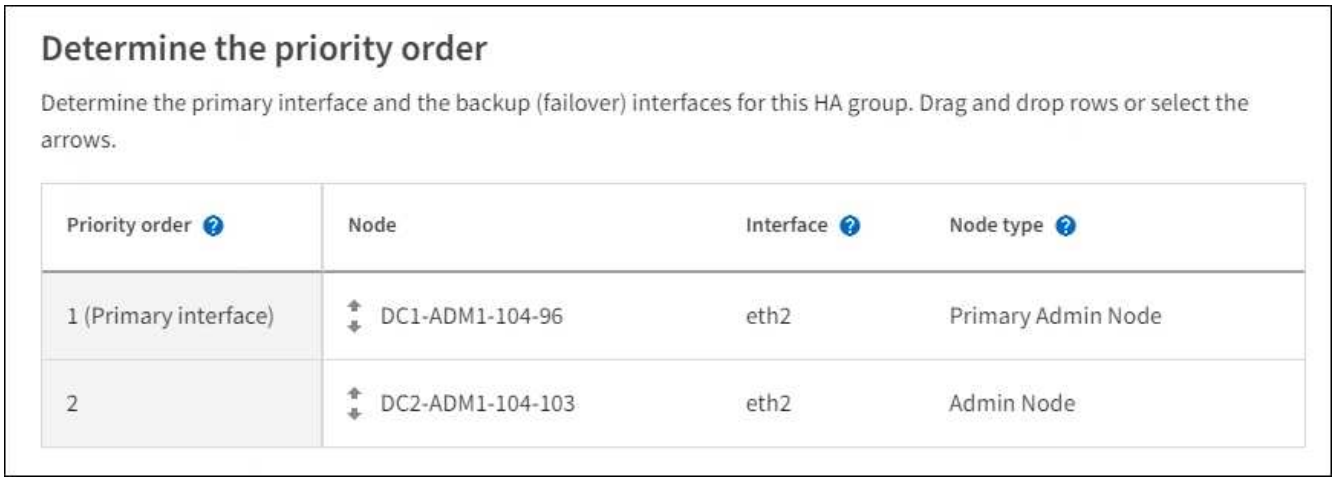
Determinare l'ordine di priorità

Se il gruppo HA include più di un'interfaccia, è possibile determinare quale sia l'interfaccia primaria e quali siano le interfacce di backup (failover). Se l'interfaccia primaria non funziona, gli indirizzi VIP vengono spostati sull'interfaccia con la priorità più alta disponibile. Se tale interfaccia non funziona, gli indirizzi VIP vengono spostati all'interfaccia con priorità più alta disponibile, e così via.

Passi

1. Trascinare le righe nella colonna **Ordine di priorità** per determinare l'interfaccia primaria e le eventuali interfacce di backup.

   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 l'accesso a Grid Manager, è necessario selezionare un'interfaccia sul nodo di amministrazione primario come interfaccia primaria. Alcune procedure di manutenzione possono essere eseguite solo dal nodo di amministrazione primario.

2. Selezionare **Continua**.

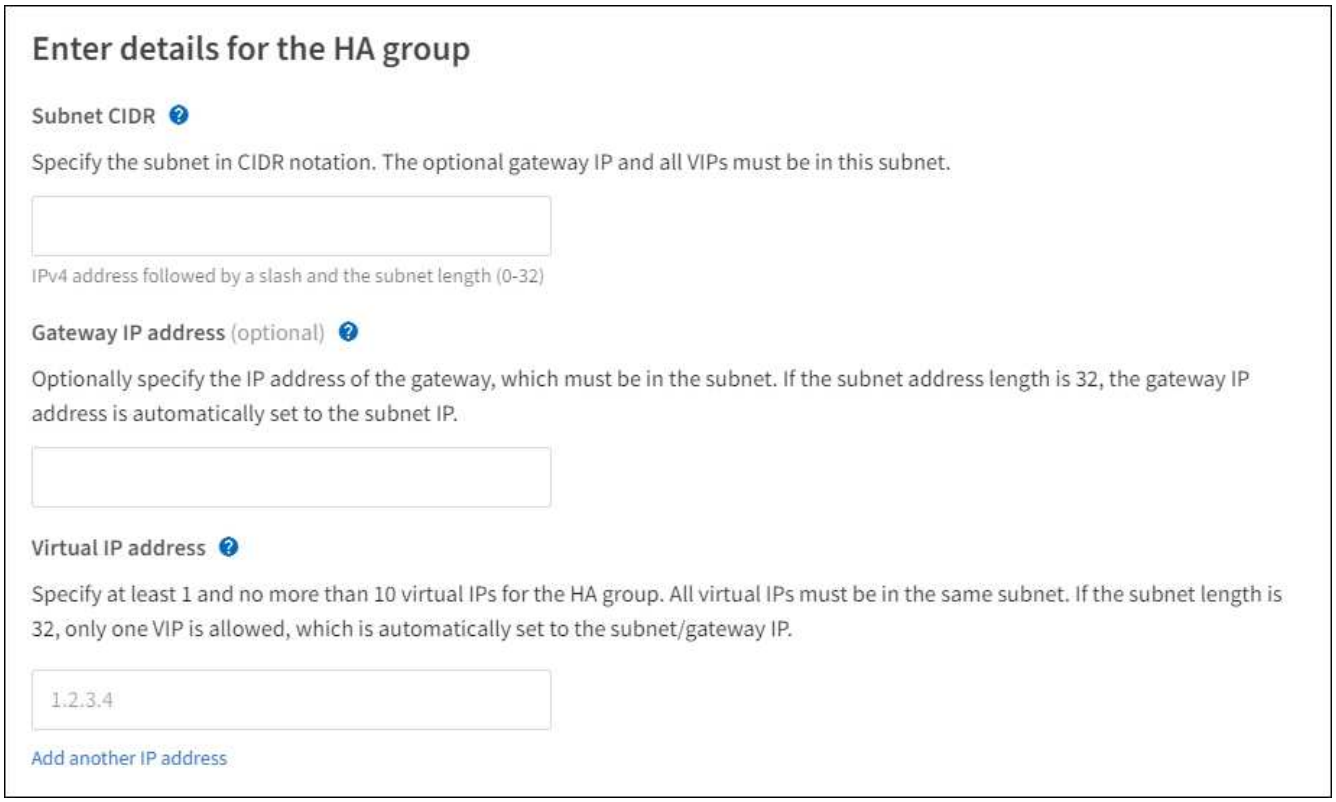
Inserisci gli indirizzi IP

Passi

1. Nel campo **Subnet CIDR**, specificare la subnet VIP in notazione CIDR, ovvero 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`.

   Se si utilizza un prefisso a 32 bit, l'indirizzo di rete VIP funge anche da indirizzo gateway e indirizzo VIP.



2. Facoltativamente, se un client amministrativo o tenant S3 accederà a questi indirizzi VIP da una subnet diversa, immettere l'**indirizzo IP del gateway**. L'indirizzo del gateway deve essere all'interno della subnet VIP.

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

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

   È necessario fornire almeno un indirizzo IPv4. Facoltativamente, è possibile specificare indirizzi IPv4 e IPv6 aggiuntivi.

4. Selezionare **Crea gruppo HA** e selezionare **Fine**.

   Il gruppo HA è stato creato ed è ora possibile utilizzare gli indirizzi IP virtuali configurati.

Prossimi passi

Se si intende utilizzare questo gruppo HA per il bilanciamento del carico, creare un endpoint del bilanciatore del carico per determinare la porta e il protocollo di rete e per allegare eventuali certificati richiesti. Vedere "Configurare gli endpoint del bilanciatore del carico" .

Modifica un gruppo ad alta disponibilità

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

Ad esempio, potrebbe essere necessario modificare un gruppo HA se si desidera rimuovere il nodo associato a un'interfaccia selezionata in una procedura di dismissione di un sito o di un nodo.

Passi

1. Selezionare **CONFIGURAZIONE** > **Rete** > **Gruppi ad alta disponibilità**.

   La pagina Gruppi ad alta disponibilità mostra tutti i gruppi HA esistenti.

2. Selezionare la casella di controllo per il gruppo HA che si desidera modificare.
3. A seconda di cosa vuoi aggiornare, procedi in uno dei seguenti modi:
   - Selezionare **Azioni** > **Modifica indirizzo IP virtuale** per aggiungere o rimuovere indirizzi VIP.
   - Selezionare **Azioni** > **Modifica gruppo HA** per aggiornare il nome o la descrizione del gruppo, aggiungere o rimuovere interfacce, modificare l'ordine di priorità o aggiungere o rimuovere indirizzi VIP.
4. Se hai selezionato **Modifica indirizzo IP virtuale**:
   a. Aggiornare gli indirizzi IP virtuali per il gruppo HA.
   b. Seleziona **Salva**.
   c. Selezionare **Fine**.
5. Se hai selezionato **Modifica gruppo HA**:
   a. Facoltativamente, aggiorna il nome o la descrizione del gruppo.
   b. Facoltativamente, seleziona o deseleziona le caselle di controllo per aggiungere o rimuovere le interfacce.

      > Se il gruppo HA fornisce l'accesso a Grid Manager, è necessario selezionare un'interfaccia sul nodo di amministrazione primario come interfaccia primaria. Alcune procedure di manutenzione possono essere eseguite solo dal nodo di amministrazione primario

   c. Facoltativamente, trascinare le righe per modificare l'ordine di priorità dell'interfaccia primaria e di tutte le interfacce di backup per questo gruppo HA.
   d. Facoltativamente, aggiornare gli indirizzi IP virtuali.
   e. Selezionare **Salva** e poi **Fine**.

Rimuovere un gruppo ad alta disponibilità

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

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

Per evitare interruzioni del client, aggiornare tutte le applicazioni client S3 interessate prima di rimuovere un gruppo HA. Aggiornare 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.

Passi

1. Selezionare **CONFIGURAZIONE** > **Rete** > **Gruppi ad alta disponibilità**.
2. Esaminare la colonna **Endpoint del bilanciatore del carico** per ogni gruppo HA che si desidera rimuovere. Se sono elencati degli endpoint del bilanciatore del carico:
   a. Vai a **CONFIGURAZIONE** > **Rete** > **Endpoint del bilanciatore del carico**.
   b. Selezionare la casella di controllo per l'endpoint.
   c. Selezionare **Azioni** > **Modifica modalità di associazione endpoint**.
   d. Aggiornare la modalità di associazione per rimuovere il gruppo HA.
   e. Seleziona **Salva modifiche**.
3. Se non sono elencati endpoint del bilanciatore del carico, selezionare la casella di controllo per ciascun gruppo HA che si desidera rimuovere.
4. Selezionare **Azioni** > **Rimuovi gruppo HA**.
5. Rivedi il messaggio e seleziona **Elimina gruppo HA** per confermare la selezione.

   Tutti i gruppi HA selezionati verranno rimossi. Nella pagina Gruppi ad alta disponibilità viene visualizzato un banner verde di successo.

Gestire il bilanciamento del carico

Considerazioni sul bilanciamento del carico

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

Che cos'è il bilanciamento del carico?

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 nodi di archiviazione.

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

Il servizio Load Balancer su ciascun nodo funziona in modo indipendente quando inoltra il traffico client ai nodi

di archiviazione. Attraverso un processo di ponderazione, il servizio Load Balancer indirizza più richieste ai nodi di archiviazione con maggiore disponibilità della CPU.

> Sebbene il servizio StorageGRID Load Balancer sia il meccanismo di bilanciamento del carico consigliato, potrebbe essere opportuno integrare un bilanciatore del carico di terze parti. Per informazioni, contattare il rappresentante dell'account NetApp o fare riferimento a "TR-4626: Bilanciatori di carico globali e di terze parti StorageGRID" .

Di quanti nodi di bilanciamento del carico ho bisogno?

Come buona pratica generale, ogni sito nel sistema StorageGRID dovrebbe includere due o più nodi con il servizio Load Balancer. Ad esempio, un sito potrebbe includere due nodi gateway oppure sia un nodo amministrativo che un nodo gateway. Assicurarsi che vi sia un'adeguata infrastruttura di rete, hardware o virtualizzazione per ciascun nodo di bilanciamento del carico, indipendentemente dal fatto che si utilizzino appliance di servizi, nodi bare metal o nodi basati su macchine virtuali (VM).

Che cos'è un endpoint di bilanciamento del carico?

Un endpoint del bilanciatore del carico 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 di bilanciamento del carico. L'endpoint definisce anche il tipo di client (S3), la modalità di associazione e, facoltativamente, un elenco di tenant consentiti o bloccati.

Per creare un endpoint del bilanciatore del carico, seleziona **CONFIGURAZIONE** > **Rete** > **Endpoint del bilanciatore del carico** oppure completa la procedura guidata di configurazione FabricPool e S3. Per istruzioni:

- "Configurare gli endpoint del bilanciatore del carico"
- "Utilizzare la procedura guidata di configurazione S3"
- "Utilizzare la procedura guidata di configurazione FabricPool"

Considerazioni per il porto

Per impostazione predefinita, la porta per un endpoint del bilanciatore del carico è 10433 per il primo endpoint creato, ma è possibile specificare qualsiasi porta esterna non utilizzata 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 amministrativi. Se si utilizza la stessa porta per più endpoint, è necessario specificare una modalità di associazione diversa per ciascun endpoint.

Non sono consentite le porte utilizzate da altri servizi di rete. Vedi il"Riferimento porta di rete" .

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, soprattutto negli ambienti di produzione. Quando si seleziona il protocollo di rete per l'endpoint del bilanciatore del carico StorageGRID , è necessario selezionare **HTTPS**.

Considerazioni sui certificati degli endpoint del bilanciatore del carico

Se selezioni **HTTPS** come protocollo di rete per l'endpoint del bilanciatore del carico, devi fornire un certificato di sicurezza. Quando si crea l'endpoint del bilanciatore del carico, è possibile utilizzare una qualsiasi di queste tre opzioni:

- **Carica un certificato firmato (consigliato)**. Questo certificato può essere firmato da un'autorità di certificazione (CA) pubblica o privata. La procedura consigliata per proteggere la connessione è quella di utilizzare un certificato del server CA pubblicamente attendibile. 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.

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

  - Il file del certificato del server personalizzato.
  - File della chiave privata del certificato del server personalizzato.
  - Facoltativamente, un pacchetto CA dei certificati di ciascuna autorità di certificazione emittente intermedia.
- **Genera un certificato autofirmato**.
- **Utilizzare il certificato globale StorageGRID S3**. È necessario caricare o generare una versione personalizzata di questo certificato prima di poterlo selezionare per l'endpoint del bilanciatore del carico. Vedere "Configurare i certificati API S3" .

Di quali valori ho bisogno?

Per creare il certificato, è necessario 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) per il certificato deve includere il nome di dominio completo che l'applicazione client utilizzerà per StorageGRID. Per esempio:

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

Se necessario, il certificato può utilizzare caratteri jolly per rappresentare i nomi di dominio completi di tutti i nodi amministrativi e dei nodi gateway che eseguono il servizio Load Balancer. Per esempio, `*.storagegrid.example.com` usa il carattere jolly * per rappresentare `adm1.storagegrid.example.com` E `gn1.storagegrid.example.com` .

Se si prevede di utilizzare richieste in stile host virtuale S3, il certificato deve includere anche una voce **Nome alternativo** per ciascuna"Nome di dominio dell'endpoint S3" che hai configurato, inclusi eventuali nomi jolly. Per esempio:

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

> Se si utilizzano caratteri jolly per i nomi di dominio, rivedere il"Linee guida per il rafforzamento dei certificati del server" .

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

Come posso gestire 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 dei certificati, seguire queste best practice:

- Monitorare attentamente tutti gli avvisi che segnalano l'avvicinarsi della data di scadenza dei certificati, come gli avvisi **Scadenza del certificato dell'endpoint del bilanciatore del carico** e **Scadenza del certificato del server globale per l'API S3**.
- Mantenere sempre sincronizzate le versioni del certificato dell'applicazione StorageGRID e S3. Se si sostituisce o si rinnova il certificato utilizzato per un endpoint del bilanciatore del carico, è necessario sostituire o rinnovare il certificato equivalente utilizzato dall'applicazione S3.
- Utilizzare un certificato CA firmato pubblicamente. Se si utilizza un certificato firmato da una CA, è possibile sostituire i certificati prossimi alla scadenza senza interruzioni.
- Se hai generato un certificato StorageGRID autofirmato e tale certificato sta per scadere, devi sostituirlo manualmente sia in StorageGRID che nell'applicazione S3 prima che scada il certificato esistente.

Considerazioni sulla modalità di rilegatura

La modalità di associazione 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 associazione, le applicazioni client possono accedere all'endpoint solo se utilizzano un indirizzo IP consentito o il corrispondente nome di dominio completo (FQDN). Le applicazioni client che utilizzano un altro indirizzo IP o FQDN non possono accedere all'endpoint.

È possibile specificare una qualsiasi delle seguenti modalità di associazione:

- **Globale** (predefinito): le applicazioni client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministrativo, 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 FQDN corrispondente) di un gruppo HA.
- **Interfacce dei nodi**. I client devono utilizzare gli indirizzi IP (o i corrispondenti FQDN) delle interfacce dei nodi selezionati.
- **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 oppure l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo gateway.

Considerazioni sull'accesso degli inquilini

L'accesso tenant è una funzionalità di sicurezza facoltativa che consente di controllare quali account tenant StorageGRID possono utilizzare un endpoint del bilanciatore del carico per accedere ai propri 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 garantire un migliore isolamento di sicurezza tra i tenant e i loro endpoint. Ad esempio, è possibile utilizzare questa funzionalità per garantire che i materiali top secret o altamente classificati di proprietà di un inquilino rimangano completamente inaccessibili agli altri inquilini.

> 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 l'accesso anonimo), per determinare il tenant viene utilizzato il proprietario del bucket.

Esempio di accesso dell'inquilino

Per capire come funziona questa funzione di sicurezza, prendiamo in considerazione il seguente esempio:

1. Hai creato due endpoint del bilanciatore del carico, come segue:
   - Endpoint **pubblico**: 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**. A tutti gli altri tenant è impedito l'accesso a questo endpoint.
2. IL `top-secret.pdf` si trova in un bucket di proprietà del tenant **Top secret**.

Per accedere al `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, riceverà immediatamente un messaggio di accesso negato. L'accesso viene negato anche se le credenziali e la firma sono valide.

disponibilità della CPU

Il servizio Load Balancer su ciascun nodo amministrativo e nodo gateway funziona in modo indipendente quando inoltra il traffico S3 ai nodi di archiviazione. Attraverso un processo di ponderazione, il servizio Load Balancer indirizza più richieste ai nodi di archiviazione con 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 archiviazione viene assegnato un valore di peso di base minimo, anche se un nodo segnala un utilizzo del 100% o non segnala il proprio 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 bilanciatore del carico

Gli endpoint del bilanciatore del carico determinano le porte e i protocolli di rete che i client S3 possono utilizzare quando si connettono al bilanciatore del carico StorageGRID sui nodi gateway e amministrativi. È anche possibile utilizzare gli endpoint per accedere a Grid Manager, Tenant Manager o entrambi.

I dettagli su Swift sono stati rimossi da questa versione del sito di documentazione. Vedere "Configurare le connessioni client S3 e Swift" .

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Tu 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 del carico, hai"rimosso il rimappaggio della porta" .
- Hai creato tutti i gruppi ad alta disponibilità (HA) che intendi utilizzare. I gruppi HA sono consigliati, ma non obbligatori. Vedere "Gestire gruppi ad alta disponibilità" .
- Se l'endpoint del bilanciatore del carico verrà utilizzato da"Tenant S3 per S3 Select" , non deve utilizzare gli indirizzi IP o i nomi di dominio completi di alcun nodo bare-metal. Per gli endpoint del bilanciatore del 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. Vedere "Configurare le interfacce VLAN" .
- Se si sta creando un endpoint HTTPS (consigliato), si dispone delle informazioni per il certificato del server.

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

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

Creare un endpoint del bilanciatore del carico

Ogni endpoint del bilanciatore del carico del 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 rete client non attendibile.

Accedi alla procedura guidata

Passi

1. Selezionare **CONFIGURAZIONE** > **Rete** > **Endpoint del bilanciatore del carico**.
2. Per creare un endpoint per un client S3 o Swift, selezionare la scheda **Client S3 o Swift**.
3. Per creare un endpoint per l'accesso a Grid Manager, Tenant Manager o entrambi, selezionare la scheda **Interfaccia di gestione**.
4. Seleziona **Crea**.

Inserisci i dettagli dell'endpoint

Passi

1. Selezionare le istruzioni appropriate per immettere 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 apparirà nella tabella nella pagina Endpoint del bilanciatore 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 puoi utilizzare la porta 8443 come endpoint S3 e la porta verrà configurata sia sul gateway che sui nodi di amministrazione.
Tipo di cliente	Il tipo di applicazione client che utilizzerà questo endpoint, **S3** o **Swift**.
Protocollo di rete	Protocollo di rete che i client utilizzeranno per connettersi a questo endpoint. • Selezionare **HTTPS** per comunicazioni sicure e crittografate TLS (consigliato). 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 apparirà nella tabella nella pagina Endpoint del bilanciatore del carico.
Porta	La porta StorageGRID che si desidera utilizzare per accedere a Grid Manager, Tenant Manager o entrambi. • Responsabile della griglia: **8443** • Responsabile dell'affitto: **9443** • Sia il gestore della griglia che il gestore dell'inquilino: **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 accederà tramite questo endpoint.

Campo	Descrizione
Rete client non attendibile	Selezionare **Sì** se questo endpoint deve essere accessibile alle reti client non attendibili. Altrimenti, seleziona **No**. Se selezioni **Sì**, la porta è aperta su tutte le reti client non attendibili. **Nota**: è possibile configurare una porta in modo che sia aperta o chiusa per reti client non attendibili solo quando si crea l'endpoint del bilanciatore del carico.

1. Selezionare **Continua**.

Seleziona una modalità di rilegatura

Passi

1. Selezionare una modalità di associazione per l'endpoint per controllare il modo in cui si accede all'endpoint tramite qualsiasi indirizzo IP o tramite indirizzi IP e interfacce di rete specifici.

   Alcune modalità di associazione sono disponibili sia per gli endpoint client che per gli endpoint dell'interfaccia di gestione. Qui sono elencate tutte le modalità per entrambi i tipi di endpoint.

Modalità	Descrizione
Globale (predefinito per gli endpoint client)	I client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministrativo, 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 il corrispondente FQDN) di un gruppo HA. Gli endpoint con questa modalità di associazione possono utilizzare tutti lo stesso numero di porta, purché i gruppi HA selezionati per gli endpoint non si sovrappongano.
Interfacce dei nodi	Per accedere a questo endpoint, i client devono utilizzare gli indirizzi IP (o i corrispondenti FQDN) delle interfacce dei nodi selezionati.
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 oppure l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo gateway per accedere a questo endpoint.
Tutti i nodi amministrativi (predefiniti per gli endpoint dell'interfaccia di gestione)	Per accedere a questo endpoint, i client devono utilizzare l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di amministrazione.

Se più endpoint utilizzano 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 creano endpoint dell'interfaccia di gestione, sono consentiti solo i nodi amministrativi.

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

   Se si creano endpoint dell'interfaccia di gestione, selezionare i VIP associati solo ai nodi di amministrazione.

3. Se hai selezionato **Interfacce nodo**, seleziona una o più interfacce nodo per ogni nodo di amministrazione o nodo gateway che desideri associare a questo endpoint.
4. Se hai selezionato **Tipo di nodo**, seleziona Nodi amministrativi, che include sia il nodo amministrativo primario che eventuali nodi amministrativi non primari, oppure Nodi gateway.

Controlla l'accesso degli inquilini

Un endpoint dell'interfaccia di gestione può controllare l'accesso del tenant solo quando l'endpoint hatipo di interfaccia di Tenant Manager .

Passi

1. Per il passaggio **Accesso tenant**, seleziona una delle seguenti opzioni:

Campo	Descrizione
Consenti tutti i tenant (predefinito)	Tutti gli account tenant possono utilizzare questo endpoint per accedere ai propri bucket. È necessario selezionare questa opzione se non è ancora stato creato alcun account tenant. Dopo aver aggiunto gli account tenant, puoi modificare l'endpoint del bilanciatore del carico per consentire o bloccare account specifici.
Consenti inquilini selezionati	Solo gli account tenant selezionati possono utilizzare questo endpoint per accedere ai propri bucket.
Blocca gli inquilini 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 si crea un endpoint **HTTP**, non è necessario allegare un certificato. Selezionare **Crea** per aggiungere il nuovo endpoint del bilanciatore del carico. Poi vai aDopo aver finito . Altrimenti, seleziona **Continua** per allegare il certificato.

Allega il certificato

Passi

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 il servizio Load Balancer sui nodi di amministrazione o sui nodi gateway.

- **Carica il certificato**. Seleziona questa opzione se hai 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**. Selezionare questa opzione se si desidera utilizzare il certificato API S3 globale, che può essere utilizzato anche per le connessioni dirette ai nodi di archiviazione.

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

- **Utilizzare il certificato dell'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 di amministrazione.

2. Se non si utilizza il certificato StorageGRID S3, caricare o generare il certificato.

Carica il certificato

a. Seleziona **Carica certificato**.

b. Carica i file del certificato del server richiesti:

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

> Le chiavi private EC devono essere di 224 bit o più grandi. Le chiavi private RSA devono essere di 2048 bit o più grandi.

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

c. Espandi **Dettagli certificato** per visualizzare i metadati di ciascun certificato caricato. Se hai caricato un bundle CA facoltativo, ogni certificato verrà visualizzato in una scheda separata.

- Selezionare **Scarica certificato** per salvare il file del certificato oppure selezionare **Scarica bundle CA** per salvare il bundle del certificato.

  Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione `.pem` .

  Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copia certificato PEM** o **Copia pacchetto CA PEM** per copiare il contenuto del certificato e incollarlo altrove.

d. Seleziona **Crea**. + L'endpoint del bilanciatore del 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 l'endpoint.

Genera certificato

a. Seleziona **Genera certificato**.

b. Specificare le informazioni del certificato:

Campo	Descrizione
Nome di dominio	Uno o più nomi di dominio completamente qualificati da includere nel certificato. Utilizzare un * come carattere jolly per rappresentare più nomi di dominio.
Proprietà intellettuale	Uno o più indirizzi IP da includere nel certificato.
Oggetto (facoltativo)	Soggetto X.509 o nome distinto (DN) del proprietario del certificato. Se non viene immesso alcun valore in questo campo, il certificato generato utilizza il primo nome di dominio o indirizzo IP come nome comune (CN) del soggetto.

Campo	Descrizione
Giorni validi	Numero di giorni dopo la creazione in cui scade il certificato.
Aggiungi estensioni di utilizzo delle chiavi	Se selezionata (impostazione predefinita e consigliata), le estensioni per l'utilizzo delle chiavi e per l'utilizzo esteso delle chiavi vengono aggiunte al certificato generato. Queste estensioni definiscono lo scopo della chiave contenuta nel certificato. **Nota**: lasciare selezionata questa casella di controllo a meno che non si riscontrino problemi di connessione con client più vecchi quando i certificati includono queste estensioni.

c. Seleziona **Genera**.

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

- Selezionare **Scarica certificato** per salvare il file del certificato.

  Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione `.pem` .

  Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copia certificato PEM** per copiare il contenuto del certificato e incollarlo altrove.

e. Seleziona **Crea**.

L'endpoint del bilanciatore del 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

Passi

1. Se si utilizza un DNS, assicurarsi che includa un record per associare il nome di dominio completo (FQDN) StorageGRID a ciascun indirizzo IP che i client utilizzeranno per effettuare le connessioni.

   L'indirizzo IP immesso nel record DNS varia a seconda che si utilizzi un gruppo HA di nodi di bilanciamento del carico:

   - Se hai 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 StorageGRID Load Balancer utilizzando l'indirizzo IP di un nodo gateway o di un nodo amministrativo.

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

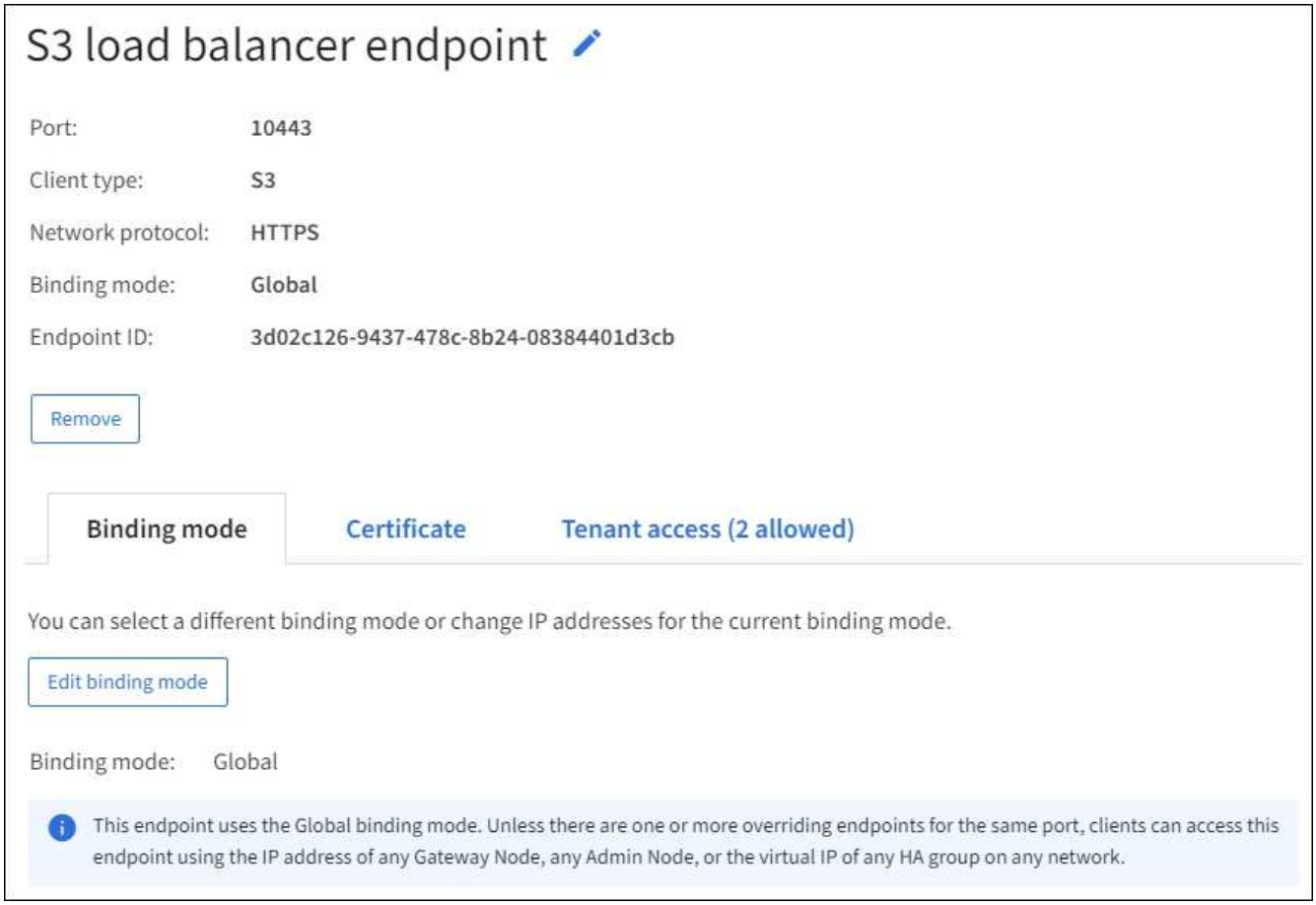
2. Fornire ai client S3 le informazioni necessarie per connettersi all'endpoint:
   - Numero di porta

- Nome di dominio completo o indirizzo IP
- Eventuali dettagli del certificato richiesti

Visualizza e modifica gli endpoint del bilanciatore del carico

È possibile visualizzare i dettagli degli endpoint del bilanciatore 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 bilanciatore del carico, consultare le tabelle nella pagina Endpoint del bilanciatore del carico.
- Per visualizzare tutti i dettagli su 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 Endpoint del bilanciatore 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 affinché le modifiche vengano applicate a tutti i nodi.

Compito	Menu Azioni	Pagina dei dettagli
Modifica il nome dell'endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare **Azioni** > **Modifica nome endpoint**. c. Inserisci il nuovo nome. d. Seleziona **Salva**.	a. Selezionare il nome dell'endpoint per visualizzarne i dettagli. b. Seleziona l'icona di modifica . c. Inserisci il nuovo nome. d. Seleziona **Salva**.
Modifica la porta dell'endpoint	a. Selezionare 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. Selezionare la casella di controllo per l'endpoint. b. Selezionare **Azioni** > **Modifica modalità di associazione endpoint**. c. Aggiornare la modalità di associazione secondo necessità. d. Seleziona **Salva modifiche**.	a. Selezionare il nome dell'endpoint per visualizzarne i dettagli. b. Selezionare **Modifica modalità di rilegatura**. c. Aggiornare la modalità di associazione secondo necessità. d. Seleziona **Salva modifiche**.
Modifica il certificato dell'endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare **Azioni** > **Modifica certificato endpoint**. c. Carica o genera un nuovo certificato personalizzato oppure inizia a utilizzare il certificato S3 globale, a seconda delle necessità. d. Seleziona **Salva modifiche**.	a. Selezionare il nome dell'endpoint per visualizzarne i dettagli. b. Selezionare la scheda **Certificato**. c. Seleziona **Modifica certificato**. d. Carica o genera un nuovo certificato personalizzato oppure inizia a utilizzare il certificato S3 globale, a seconda delle necessità. e. Seleziona **Salva modifiche**.
Modifica l'accesso dell'inquilino	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare **Azioni** > **Modifica accesso tenant**. c. Scegli un'opzione di accesso diversa, seleziona o rimuovi gli inquilini dall'elenco oppure fai entrambe le cose. d. Seleziona **Salva modifiche**.	a. Selezionare il nome dell'endpoint per visualizzarne i dettagli. b. Selezionare la scheda **Accesso inquilino**. c. Seleziona **Modifica accesso tenant**. d. Scegli un'opzione di accesso diversa, seleziona o rimuovi gli inquilini dall'elenco oppure fai entrambe le cose. e. Seleziona **Salva modifiche**.

Rimuovere gli endpoint del bilanciatore del carico

È possibile rimuovere uno o più endpoint utilizzando il menu **Azioni** oppure è possibile rimuovere un singolo endpoint dalla pagina dei dettagli.

> Per evitare interruzioni del client, aggiornare tutte le applicazioni client S3 interessate prima di rimuovere un endpoint del bilanciatore del carico. Aggiornare ciascun client per connettersi tramite una porta assegnata a un altro endpoint del bilanciatore del carico. Assicuratevi di aggiornare anche tutte le informazioni richieste sul certificato.

> 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. Nella pagina Bilanciatore del carico, seleziona la casella di controllo per ogni endpoint che desideri rimuovere.
  b. Selezionare **Azioni** > **Rimuovi**.
  c. Selezionare **OK**.
- Per rimuovere un endpoint dalla pagina dei dettagli:
  a. Dalla pagina Bilanciatore del carico, seleziona il nome dell'endpoint.
  b. Seleziona **Rimuovi** nella pagina dei dettagli.
  c. Selezionare **OK**.

Configurare i nomi di dominio degli endpoint S3

Per supportare le richieste in stile S3 virtual-hosted, è necessario utilizzare 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 nome di dominio endpoint non è supportato. Le versioni future impediranno questa configurazione.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Hai"autorizzazioni di accesso specifiche" .
- Hai confermato che non è in corso alcun aggiornamento della rete.

> Non apportare modifiche alla configurazione del nome di dominio quando è in corso un aggiornamento della griglia.

Informazioni su questo compito

Per consentire ai client di utilizzare i nomi di dominio degli endpoint S3, è necessario eseguire tutte le seguenti operazioni:

- Utilizzare Grid Manager per aggiungere i nomi di dominio degli endpoint S3 al sistema StorageGRID .

- Assicurarsi che il"certificato utilizzato dal client per le connessioni HTTPS a StorageGRID" è firmato per tutti i nomi di dominio richiesti dal cliente.

  Ad esempio, se l'endpoint è `s3.company.com` , è necessario assicurarsi che il certificato utilizzato per le connessioni HTTPS includa `s3.company.com` endpoint e il nome alternativo del soggetto (SAN) jolly dell'endpoint: `*.s3.company.com` .

- Configurare il server DNS utilizzato dal client. Includere i record DNS per gli indirizzi IP utilizzati dai client per effettuare le connessioni e assicurarsi che i record facciano riferimento a tutti i nomi di dominio degli endpoint S3 richiesti, inclusi eventuali nomi jolly.

> ⓘ I client possono connettersi a StorageGRID utilizzando l'indirizzo IP di un nodo gateway, di un nodo di amministrazione o di un nodo di archiviazione oppure connettendosi all'indirizzo IP virtuale di un gruppo ad alta disponibilità. È necessario comprendere come le applicazioni client si connettono alla griglia, in modo da includere gli indirizzi IP corretti nei record DNS.

I client che utilizzano connessioni HTTPS (consigliate) alla griglia possono utilizzare uno di questi certificati:

- I client che si connettono a un endpoint del bilanciatore del carico possono utilizzare un certificato personalizzato per tale endpoint. Ogni endpoint del bilanciatore del carico può essere configurato per riconoscere diversi nomi di dominio degli endpoint S3.
- I client che si connettono a un endpoint del bilanciatore del carico o direttamente a un nodo di archiviazione possono personalizzare il certificato API S3 globale per includere tutti i nomi di dominio dell'endpoint S3 richiesti.

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

Aggiungi un nome di dominio dell'endpoint S3

Passi

1. Selezionare **CONFIGURAZIONE** > **Rete** > **Nomi di dominio endpoint S3**.
2. Inserisci il nome del dominio nel campo **Nome dominio 1**. Seleziona **Aggiungi un altro nome di dominio** per aggiungere altri nomi di dominio.
3. Seleziona **Salva**.
4. Assicurarsi che i certificati del server utilizzati dai client corrispondano ai nomi di dominio dell'endpoint S3 richiesti.
   - Se i client si connettono a un endpoint del bilanciatore del carico che utilizza il proprio certificato,"aggiornare il certificato associato all'endpoint" .
   - Se i client si connettono a un endpoint del bilanciatore del carico che utilizza il certificato API S3 globale o direttamente ai nodi di archiviazione,"aggiornare il certificato API S3 globale" .
5. Aggiungere i record DNS necessari per garantire che le richieste di nomi di dominio degli endpoint possano essere risolte.

Risultato

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

Rinominare un nome di dominio dell'endpoint S3

Se si modifica un nome utilizzato dalle applicazioni S3, le richieste in stile virtual-hosted non riusciranno.

Passi

1. Selezionare **CONFIGURAZIONE** > **Rete** > **Nomi di dominio endpoint S3**.
2. Seleziona il campo del nome di dominio che desideri modificare e apporta le modifiche necessarie.
3. Seleziona **Salva**.
4. Seleziona **Sì** per confermare la modifica.

Elimina un nome di dominio dell'endpoint S3

Se si rimuove un nome utilizzato dalle applicazioni S3, le richieste in stile virtual-hosted non riusciranno.

Passi

1. Selezionare **CONFIGURAZIONE** > **Rete** > **Nomi di dominio endpoint S3**.
2. Seleziona l'icona Elimina accanto al nome di dominio.
3. Selezionare **Sì** per confermare l'eliminazione.

Informazioni correlate

- "Utilizzare l'API REST S3"
- "Visualizza gli indirizzi IP"
- "Configurare gruppi ad alta disponibilità"

Riepilogo: indirizzi IP e porte per le connessioni client

Per archiviare o recuperare oggetti, le applicazioni client S3 si connettono al servizio Load Balancer, incluso in tutti i nodi amministrativi e gateway, oppure al servizio Local Distribution Router (LDR), incluso in tutti i nodi di archiviazione.

Le applicazioni client possono connettersi a StorageGRID utilizzando l'indirizzo IP di un nodo della griglia e il numero di porta del servizio su quel nodo. Facoltativamente, è possibile creare gruppi ad alta disponibilità (HA) di nodi di bilanciamento del carico per fornire connessioni ad alta disponibilità che utilizzano indirizzi IP virtuali (VIP). Se si desidera connettersi a StorageGRID utilizzando un nome di dominio completo (FQDN) anziché un indirizzo IP o VIP, è possibile configurare le voci DNS.

Questa tabella riepiloga 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 endpoint del bilanciatore del carico e gruppi ad alta disponibilità (HA), vediDove trovare gli indirizzi IP per individuare questi valori nel Grid Manager.

Dove avviene la connessione	Servizio a cui il client si connette	indirizzo IP	Porta
gruppo HA	Bilanciatore del carico	Indirizzo IP virtuale di un gruppo HA	Porta assegnata all'endpoint del bilanciatore del carico

Dove avviene la connessione	Servizio a cui il client si connette	indirizzo IP	Porta
Nodo di amministrazione	Bilanciatore del carico	Indirizzo IP del nodo di amministrazione	Porta assegnata all'endpoint del bilanciatore del carico
Nodo Gateway	Bilanciatore del carico	Indirizzo IP del nodo gateway	Porta assegnata all'endpoint del bilanciatore del carico
Nodo di archiviazione	Relazione a distanza	Indirizzo IP del nodo di archiviazione	Porte S3 predefinite: • HTTPS: 18082 • HTTP: 18084

URL di esempio

Per connettere un'applicazione client all'endpoint del Load Balancer di un gruppo HA di nodi gateway, utilizzare un URL strutturato come mostrato di seguito:

`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 del carico è 10443, un'applicazione potrebbe utilizzare il seguente URL per connettersi a StorageGRID:

`https://192.0.2.5:10443`

Dove trovare gli indirizzi IP

1. Sign in a Grid Manager utilizzando un"browser web supportato" .
2. Per trovare l'indirizzo IP di un nodo della griglia:
   a. Selezionare **NODES**.
   b. Selezionare il nodo di amministrazione, il nodo gateway o il nodo di archiviazione a cui si desidera connettersi.
   c. Selezionare la scheda **Panoramica**.
   d. Nella sezione Informazioni sul nodo, annotare gli indirizzi IP del nodo.
   e. Selezionare **Mostra altro** per visualizzare gli indirizzi IPv6 e le mappature delle interfacce.

      È possibile stabilire connessioni dalle applicazioni client a uno qualsiasi degli indirizzi IP nell'elenco:

      - **eth0:** Rete di griglia
      - **eth1:** Rete di amministrazione (facoltativo)
      - **eth2:** Rete client (facoltativo)

Se si visualizza un nodo di amministrazione o un nodo gateway ed è il nodo attivo in un gruppo ad alta disponibilità, l'indirizzo IP virtuale del gruppo HA viene visualizzato su eth2.

3. Per trovare l'indirizzo IP virtuale di un gruppo ad alta disponibilità:
   a. Selezionare **CONFIGURAZIONE** > **Rete** > **Gruppi ad alta disponibilità**.
   b. Nella tabella, annotare l'indirizzo IP virtuale del gruppo HA.
4. Per trovare il numero di porta di un endpoint del Load Balancer:
   a. Selezionare **CONFIGURAZIONE** > **Rete** > **Endpoint del bilanciatore del carico**.
   b. Annotare il numero di porta dell'endpoint che si desidera utilizzare.

      Se il numero di porta è 80 o 443, l'endpoint viene configurato solo sui nodi gateway, perché tali porte sono riservate sui nodi amministrativi. Tutte le altre porte sono configurate sia sui nodi gateway che sui nodi amministrativi.

   c. Selezionare il nome dell'endpoint dalla tabella.
   d. Verificare che il **Tipo di client** (S3) corrisponda all'applicazione client che utilizzerà l'endpoint.

Informazioni sul copyright

Informazioni sul marchio commerciale