



# **Configurare le connessioni client**

## **StorageGRID 11.8**

NetApp  
March 19, 2024

# Sommario

- Configurare le connessioni client ..... 1
  - Configurazione delle connessioni client S3 e Swift: Panoramica ..... 1
  - Sicurezza per client S3 o Swift ..... 4
  - Utilizzare l'installazione guidata S3 ..... 6
  - Gestire i gruppi ha ..... 16
  - Gestire il bilanciamento del carico ..... 27
  - Configurare i nomi di dominio degli endpoint S3 ..... 41
  - Riepilogo: Indirizzi IP e porte per le connessioni client ..... 43

# Configurare le connessioni client

## Configurazione delle connessioni client S3 e Swift: Panoramica

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

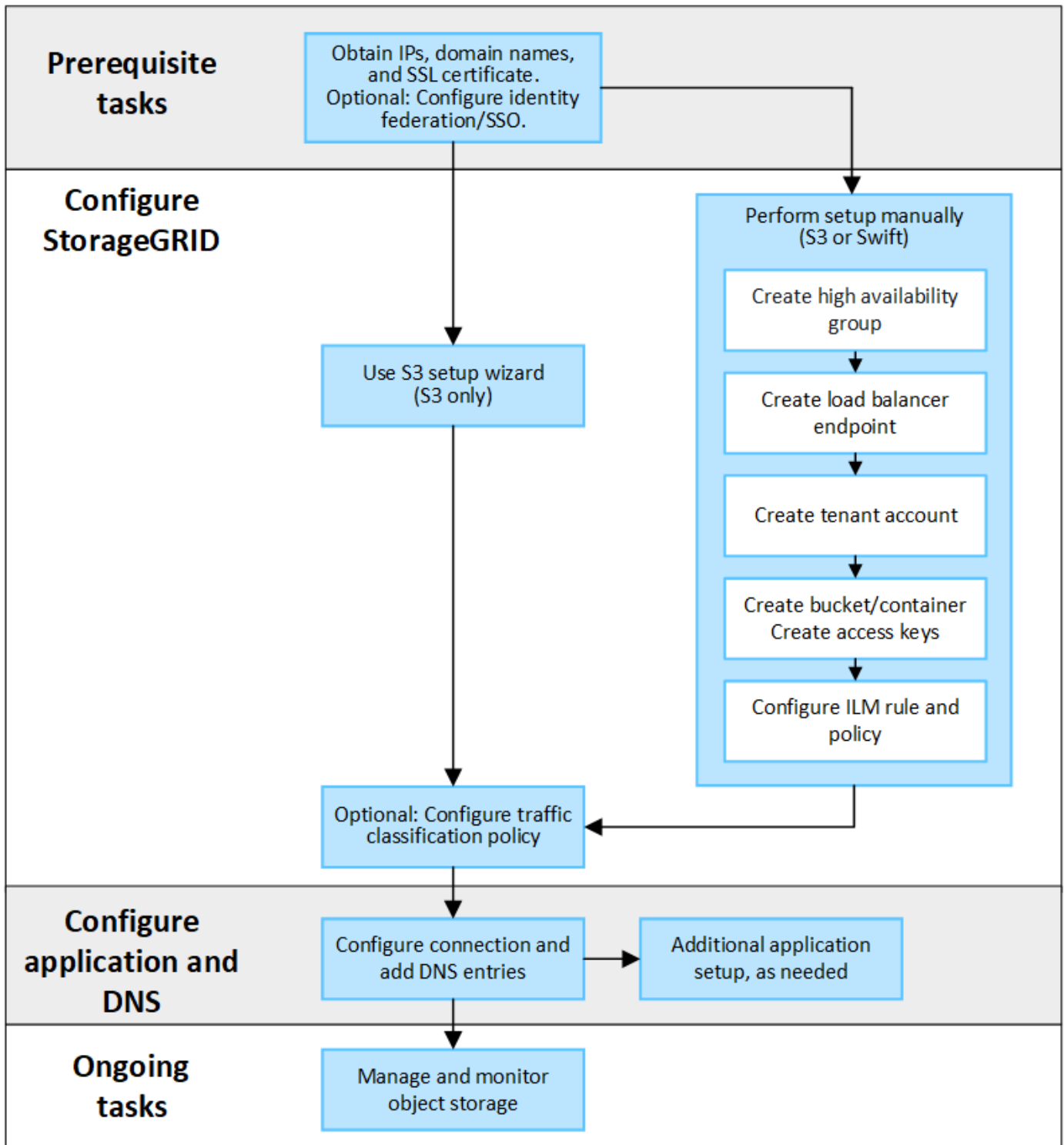


Il supporto per le applicazioni client Swift è stato obsoleto e verrà rimosso in una release futura.

### Workflow di configurazione

Come illustrato nel diagramma del flusso di lavoro, sono disponibili quattro passaggi principali per la connessione di StorageGRID a qualsiasi applicazione S3 o Swift:

1. Eseguire attività preliminari in StorageGRID, in base al modo in cui l'applicazione client si conetterà a StorageGRID.
2. Utilizzare StorageGRID per ottenere i valori necessari all'applicazione per connettersi alla griglia. È possibile utilizzare l'installazione guidata S3 o configurare manualmente ogni entità StorageGRID.
3. Utilizzare l'applicazione S3 o Swift per completare la connessione a StorageGRID. Creare voci DNS per associare gli indirizzi IP ai nomi di dominio che si intende utilizzare.
4. Eseguire attività in corso nell'applicazione e in StorageGRID per gestire e monitorare lo storage a oggetti nel tempo.



## Informazioni necessarie per collegare StorageGRID a un'applicazione client

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

### Di quali valori ho bisogno?

La seguente tabella mostra i valori da configurare in StorageGRID e i valori utilizzati dall'applicazione S3 o Swift 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 bilanciamento del carico	Applicazione client
Certificato SSL	StorageGRID > endpoint del bilanciamento del carico	Applicazione client
Nome server (FQDN)	StorageGRID > endpoint del bilanciamento del carico	<ul style="list-style-type: none"> <li>• Applicazione client</li> <li>• Voce DNS</li> </ul>
ID chiave di accesso S3 e chiave di accesso segreta	StorageGRID > tenant e bucket	Applicazione client
Nome bucket/container	StorageGRID > tenant e bucket	Applicazione client

### Come si ottengono questi valori?

In base alle proprie esigenze, è possibile effettuare una delle seguenti operazioni per ottenere le informazioni necessarie:

- **Utilizzare il "Installazione guidata S3"**. L'installazione guidata S3 consente di configurare rapidamente i valori richiesti in StorageGRID e di creare uno o due file da utilizzare per la configurazione dell'applicazione S3. La procedura guidata guida l'utente attraverso i passaggi richiesti e aiuta a verificare che le impostazioni siano conformi alle Best practice di StorageGRID.



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

- **Utilizzare il "Installazione guidata di FabricPool"**. Analogamente all'installazione guidata di S3, l'installazione guidata di FabricPool consente di configurare rapidamente i valori richiesti e di creare un file da utilizzare quando si configura un livello cloud FabricPool in ONTAP.



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

- **Configurare gli elementi manualmente**. Se si sta effettuando la connessione a un'applicazione Swift (o si sta effettuando la connessione a un'applicazione S3 e si preferisce non utilizzare l'installazione guidata S3), è possibile ottenere i valori richiesti eseguendo la configurazione manualmente. Attenersi alla seguente procedura:
  - a. Configurare il gruppo ad alta disponibilità (ha) che si desidera utilizzare per l'applicazione S3 o Swift. Vedere ["Configurare i gruppi ad alta disponibilità"](#).
  - b. Creare l'endpoint del bilanciamento del carico che verrà utilizzato dall'applicazione S3 o Swift. Vedere ["Configurare gli endpoint del bilanciamento del carico"](#).

- c. Creare l'account tenant utilizzato dall'applicazione S3 o Swift. Vedere ["Creare un account tenant"](#).
- d. Per un tenant S3, accedere all'account tenant e generare un ID della chiave di accesso e una chiave di accesso segreta per ogni utente che accede all'applicazione. Vedere ["Creare le proprie chiavi di accesso"](#).
- e. Creare uno o più bucket S3 o container Swift all'interno dell'account tenant. Per S3, vedere ["Creare un bucket S3"](#). Per Swift, utilizzare ["INSERIRE la richiesta di container"](#).
- f. Per aggiungere istruzioni di posizionamento specifiche per gli oggetti appartenenti al nuovo tenant o bucket/container, creare una nuova regola ILM e attivare un nuovo criterio ILM per utilizzare tale regola. Vedere ["Creare una regola ILM"](#) e ["Creare un criterio ILM"](#).

## Sicurezza per client S3 o Swift

Gli account tenant di StorageGRID utilizzano applicazioni client S3 o Swift per salvare i dati degli oggetti in StorageGRID. È necessario esaminare le misure di protezione implementate per le applicazioni client.

### Riepilogo

La tabella seguente riassume il modo in cui viene implementata la sicurezza per le API REST S3 e Swift:

Problema di sicurezza	Implementazione per API REST
Sicurezza della connessione	TLS
Autenticazione del server	Certificato server X.509 firmato dalla CA di sistema o certificato server personalizzato fornito dall'amministratore
Autenticazione del client	<p><b>S3</b></p> <p>Account S3 (ID chiave di accesso e chiave di accesso segreta)</p> <p><b>Rapido</b></p> <p>Account Swift (nome utente e password)</p>
Autorizzazione del client	<p><b>S3</b></p> <p>Proprietà dei bucket e tutte le policy di controllo degli accessi applicabili</p> <p><b>Rapido</b></p> <p>Accesso al ruolo di amministratore</p>

### In che modo StorageGRID fornisce la protezione per le applicazioni client

Le applicazioni client S3 e Swift possono connettersi al servizio Load Balancer su nodi gateway o nodi amministrativi o direttamente ai nodi storage.

- I client che si connettono al servizio Load Balancer possono utilizzare HTTPS o HTTP, in base alla modalità di utilizzo ["configurare l'endpoint del bilanciamento del carico"](#).

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

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

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

HTTPS è l'impostazione predefinita ed è consigliata.

HTTP fornisce una comunicazione meno sicura e non crittografata, ma può essere opzionale **"attivato"** per reti non di produzione o di prova.

- Le comunicazioni tra StorageGRID e il client vengono crittografate mediante TLS.
- Le comunicazioni tra il servizio Load Balancer e i nodi di storage all'interno della griglia vengono crittografate indipendentemente dal fatto che l'endpoint del bilanciamento del carico sia configurato per accettare connessioni HTTP o HTTPS.
- I client devono fornire le intestazioni di autenticazione HTTP a StorageGRID per eseguire operazioni REST API. Vedere **"Autenticare le richieste"** e **"Endpoint API Swift supportati"**.

## Certificati di sicurezza e applicazioni client

In tutti i casi, le applicazioni client possono stabilire connessioni TLS utilizzando un certificato server personalizzato caricato dall'amministratore della griglia 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 bilanciamento del carico. Ogni endpoint del bilanciamento di carico dispone di un 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 per il bilanciamento del carico"**.

- Quando le applicazioni client si connettono direttamente a un nodo di storage, utilizzano i certificati server generati dal sistema e generati per i nodi di storage 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 **"Aggiunta di un certificato API S3 o Swift personalizzato"**.

I client devono essere configurati in modo da considerare attendibile l'autorità di certificazione che ha firmato il certificato utilizzato per stabilire connessioni TLS.

## Algoritmi di hashing e crittografia supportati per le librerie TLS

Il sistema StorageGRID supporta un insieme di pacchetti di crittografia che le applicazioni client possono utilizzare quando stabiliscono una sessione TLS. Per configurare la crittografia, andare a **CONFIGURATION > Security > Security settings** e selezionare **TLS and SSH policy**.

### 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 l'installazione guidata S3

## Utilizzare l'installazione guidata S3: Considerazioni e requisiti

È possibile utilizzare l'installazione guidata S3 per configurare StorageGRID come sistema di storage a oggetti per un'applicazione S3.

### Quando utilizzare l'installazione guidata S3

L'installazione guidata S3 guida l'utente attraverso ogni fase della configurazione di StorageGRID per l'utilizzo con un'applicazione S3. Durante il completamento della procedura guidata, è possibile scaricare i file da utilizzare per immettere i valori nell'applicazione S3. Utilizzare la procedura guidata per configurare il sistema più rapidamente e per assicurarsi che le impostazioni siano conformi alle Best practice StorageGRID.

Se si dispone di ["Autorizzazione di accesso root"](#), È possibile completare l'installazione guidata di S3 quando si inizia a utilizzare il Gestore griglie di StorageGRID oppure è possibile accedere e completare la procedura guidata in qualsiasi momento. A seconda dei requisiti, è possibile configurare manualmente alcuni o tutti gli elementi richiesti e utilizzare la procedura guidata per assemblare i valori richiesti da un'applicazione S3.

### Prima di utilizzare la procedura guidata

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

### Ottenere gli indirizzi IP e configurare le interfacce VLAN

Se si configura un gruppo ad alta disponibilità (ha), si conoscono i nodi a cui si conetterà l'applicazione S3 e la rete StorageGRID da utilizzare. Si conoscono anche i valori da inserire per la subnet CIDR, l'indirizzo IP del gateway e gli indirizzi IP virtuali (VIP).

Se si intende utilizzare una LAN virtuale per separare il traffico dall'applicazione S3, l'interfaccia VLAN è già stata configurata. Vedere ["Configurare le interfacce VLAN"](#).

### Configurare la federazione di identità e SSO

Se si prevede di utilizzare la federazione di identità o il Single Sign-on (SSO) per il sistema StorageGRID, queste funzionalità sono state attivate. Si sa anche quale gruppo federato deve disporre dell'accesso root per l'account tenant utilizzato dall'applicazione S3. Vedere ["USA la federazione delle identità"](#) e ["Configurare il single sign-on"](#).

### Ottenere e configurare i nomi di dominio

Si conosce il nome di dominio completo (FQDN) da utilizzare per StorageGRID. Le voci DNS (Domain Name Server) associano questo FQDN agli indirizzi IP virtuali (VIP) del gruppo ha creato utilizzando la procedura guidata.

Se si prevede di utilizzare le richieste in stile host virtuale S3, è necessario ["Nomi di dominio degli endpoint S3 configurati"](#). Si consiglia di utilizzare richieste virtuali in stile host.

### Esaminare i requisiti del bilanciamento del carico e del certificato di sicurezza

Se si intende utilizzare il bilanciamento del carico StorageGRID, sono state esaminate le considerazioni generali sul bilanciamento del carico. Si dispone dei certificati da caricare o dei valori necessari per generare un certificato.

Se si intende utilizzare un endpoint esterno (di terze parti) per il bilanciamento del carico, si dispone del nome di dominio completo (FQDN), della porta e del certificato per il bilanciamento del carico.



## Configurare le connessioni di federazione di griglie

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 a federazione di griglie, prima di avviare la procedura guidata, confermare quanto segue:

- Lo hai fatto "[configurazione della connessione a federazione di griglie](#)".
- Lo stato della connessione è **connesso**.
- Si dispone dell'autorizzazione di accesso root.

## Accedere e completare l'installazione guidata di S3

È possibile utilizzare l'installazione guidata S3 per configurare StorageGRID per l'utilizzo con un'applicazione S3. L'installazione guidata fornisce i valori necessari all'applicazione per accedere a un bucket StorageGRID e per salvare gli oggetti.

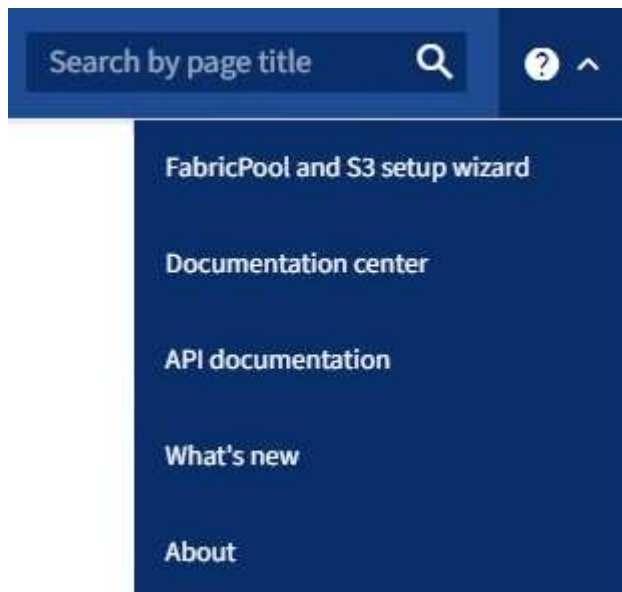
### Prima di iniziare

- Hai il "[Autorizzazione di accesso root](#)".
- Hai esaminato il "[considerazioni e requisiti](#)" per utilizzare la procedura guidata.

### Accedere alla procedura guidata

#### Fasi

1. Accedere a Grid Manager utilizzando un "[browser web supportato](#)".
2. Se nella dashboard viene visualizzato il banner **FabricPool and S3 setup wizard**, selezionare il link nel banner. Se il banner non viene più visualizzato, selezionare l'icona della guida dalla barra di intestazione in Gestione griglia e selezionare **Installazione guidata FabricPool and S3**.



3. Nella sezione dell'applicazione S3 della pagina di installazione guidata di FabricPool e S3, selezionare **Configura ora**.

## Fase 1 di 6: Configurare il gruppo ha

Un gruppo ha è un insieme di nodi che contengono ciascuno il servizio bilanciamento del carico StorageGRID. Un gruppo ha può contenere nodi gateway, nodi di amministrazione o entrambi.

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

Per ulteriori informazioni su questa attività, vedere ["Gestire i gruppi ad alta disponibilità"](#).

### Fasi

1. Se si prevede di utilizzare un bilanciamento del carico esterno, non è necessario creare un gruppo ha. Selezionare **Ignora questo passaggio** e passare a [Fase 2 di 6: Configurare l'endpoint del bilanciamento del carico](#).
2. Per utilizzare il bilanciamento del carico StorageGRID, è possibile creare un nuovo gruppo ha o utilizzare un gruppo ha esistente.

## Creare un gruppo ha

- a. Per creare un nuovo gruppo ha, selezionare **Crea gruppo ha**.
- b. Per la fase **inserire i dettagli**, completare i seguenti campi.

Campo	Descrizione
Nome del gruppo HA	Un nome di visualizzazione univoco per questo gruppo ha.
Descrizione (opzionale)	La descrizione di questo gruppo ha.

- c. Per il passo **Add interfaces**, selezionare le interfacce di nodo che si desidera utilizzare in questo gruppo ha.

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

È possibile selezionare uno o più nodi, ma è possibile selezionare una sola interfaccia per ciascun nodo.

- d. Per la fase **prioritize interfaces**, determinare l'interfaccia primaria e 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 principale 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 riesce, gli indirizzi IP virtuali (VIP) si spostano nella prima interfaccia di backup nell'ordine di priorità. Se l'interfaccia non funziona, gli indirizzi VIP passano all'interfaccia di backup successiva e così via. Quando i guasti vengono risolti, gli indirizzi VIP tornano all'interfaccia con la priorità più alta disponibile.

- e. Per il passo **inserire gli indirizzi IP**, completare i seguenti campi.

Campo	Descrizione
Subnet CIDR	L'indirizzo della subnet VIP nella notazione CIDR e n. 8212; un indirizzo IPv4 seguito da una barra e dalla lunghezza della subnet (0-32).  L'indirizzo di rete non deve avere bit host impostati. Ad esempio, 192.16.0.0/22.
Indirizzo IP del gateway (opzionale)	Se gli indirizzi IP S3 utilizzati per accedere a StorageGRID non si trovano sulla stessa sottorete degli indirizzi VIP StorageGRID, inserire l'indirizzo IP del gateway locale VIP StorageGRID. L'indirizzo IP del gateway locale deve trovarsi all'interno della subnet VIP.

Campo	Descrizione
Virtual IP address (Indirizzo IP virtuale)	<p>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.</p> <p>Almeno un indirizzo deve essere IPv4. In alternativa, è possibile specificare ulteriori indirizzi IPv4 e IPv6.</p>

f. Selezionare **Create ha group** (Crea gruppo ha), quindi selezionare **Finish** (fine) per tornare all'installazione guidata 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 dal menu **Select an ha group** (Seleziona un gruppo ha).

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

## Fase 2 di 6: Configurare l'endpoint del bilanciamento del carico

StorageGRID utilizza un bilanciamento del carico per gestire il carico di lavoro dalle applicazioni client. Il bilanciamento del carico massimizza la velocità e la capacità di connessione tra più nodi di storage.

È possibile utilizzare il servizio bilanciamento del carico StorageGRID, disponibile su tutti i nodi gateway e di amministrazione, oppure connettersi a un bilanciamento del carico esterno (di terze parti). Si consiglia di utilizzare il bilanciamento del carico StorageGRID.

Per ulteriori informazioni su questa attività, vedere ["Considerazioni per il bilanciamento del carico"](#).

Per utilizzare il servizio bilanciamento del carico di StorageGRID, selezionare la scheda **StorageGRID load balancer**, quindi creare o selezionare l'endpoint di bilanciamento del carico che si desidera utilizzare. Per utilizzare un bilanciamento del carico esterno, selezionare la scheda **bilanciamento del carico esterno** e fornire i dettagli sul sistema già configurato.

## Creare l'endpoint

### Fasi

1. Per creare un endpoint di bilanciamento del carico, selezionare **Crea endpoint**.
2. Per il passo **inserire i dettagli dell'endpoint**, completare i seguenti campi.

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint.
Porta	<p>La porta StorageGRID che si desidera utilizzare per il bilanciamento del carico. Per impostazione predefinita, questo campo è 10433 per il primo endpoint creato, ma è possibile inserire qualsiasi porta esterna non utilizzata. Se si immette 80 o 443, l'endpoint viene configurato solo sui nodi gateway, poiché queste porte sono riservate sui nodi Admin.</p> <p><b>Nota:</b> le porte utilizzate da altri servizi di rete non sono consentite. Vedere "<a href="#">Riferimento porta di rete</a>".</p>
Tipo di client	Deve essere <b>S3</b> .
Protocollo di rete	<p>Selezionare <b>HTTPS</b>.</p> <p><b>Nota:</b> La comunicazione con StorageGRID senza crittografia TLS è supportata ma non consigliata.</p>

3. Per il passo **Select binding mode**, specificare la modalità di binding. La modalità di associazione controlla l'accesso all'endpoint utilizzando qualsiasi indirizzo IP o specifici indirizzi IP e interfacce di rete.

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

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

4. Per la fase di accesso del tenant, selezionare una delle seguenti opzioni:

Campo	Descrizione
Allow all tenant (Consenti tutti i tenant) (impostazione predefinita)	Tutti gli account tenant possono utilizzare questo endpoint per accedere ai bucket.
Consenti tenant selezionati	Solo gli account tenant selezionati possono utilizzare questo endpoint per accedere ai bucket.
Blocca i tenant selezionati	Gli account tenant selezionati non possono utilizzare questo endpoint per accedere ai bucket. Tutti gli altri tenant possono utilizzare questo endpoint.

5. Per il passo **Allega certificato**, selezionare una delle seguenti opzioni:

Campo	Descrizione
Carica certificato (consigliato)	Utilizzare questa opzione per caricare un certificato server firmato dalla CA, una chiave privata del certificato e un bundle CA opzionale.
Generare un certificato	Utilizzare questa opzione per generare un certificato autofirmato. Vedere " <a href="#">Configurare gli endpoint del bilanciamento del carico</a> " per informazioni dettagliate su cosa inserire.
Utilizza il certificato StorageGRID S3 e Swift	Utilizzare questa opzione solo se è già stata caricata o generata una versione personalizzata del certificato globale StorageGRID. Vedere " <a href="#">Configurare i certificati API S3 e Swift</a> " per ulteriori informazioni.

6. Selezionare **fine** per tornare all'installazione guidata S3.

7. Selezionare **continua** per passare al punto tenant e bucket.



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

### Utilizzare l'endpoint del bilanciamento del carico esistente

#### Fasi

1. Per utilizzare un endpoint esistente, selezionarne il nome dal campo **Select a load balancer endpoint**.

2. Selezionare **continua** per passare al punto tenant e bucket.

### Utilizzare un bilanciamento del carico esterno

#### Fasi

1. Per utilizzare un bilanciamento del carico esterno, completare i seguenti campi.

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

2. Selezionare **continua** per passare al punto tenant e bucket.

### Fase 3 di 6: Creazione di tenant e bucket

Un tenant è un'entità che può utilizzare le applicazioni S3 per memorizzare e recuperare oggetti in StorageGRID. Ogni tenant dispone di utenti, chiavi di accesso, bucket, oggetti e un set specifico di funzionalità. È necessario creare il tenant prima di poter creare il bucket che l'applicazione S3 utilizzerà per memorizzare i propri oggetti.

Un bucket è un container utilizzato per memorizzare gli oggetti e i metadati degli oggetti di un tenant. Anche se alcuni tenant potrebbero avere molti bucket, la procedura guidata consente di creare un tenant e un bucket nel modo più rapido e semplice. Puoi utilizzare il tenant Manager in un secondo momento per aggiungere altri bucket necessari.

È possibile creare un nuovo tenant da utilizzare per questa applicazione S3. In alternativa, è anche possibile creare un bucket per il nuovo tenant. Infine, è possibile consentire alla procedura guidata di creare le chiavi di accesso S3 per l'utente root del tenant.

Per ulteriori informazioni su questa attività, vedere ["Creare un account tenant"](#) e ["Creare un bucket S3"](#).

#### Fasi

1. Selezionare **Crea tenant**.
2. Per la procedura di inserimento dei dettagli, immettere le seguenti informazioni.

Campo	Descrizione
Nome	Un nome per l'account tenant. I nomi dei tenant non devono essere univoci. Una volta creato, l'account tenant riceve un ID account numerico univoco.
Descrizione (opzionale)	Una descrizione che aiuta a identificare il tenant.

Campo	Descrizione
Tipo di client	Il tipo di protocollo client utilizzato dal tenant. Per l'installazione guidata S3, è selezionato <b>S3</b> e il campo è disattivato.
Quota di storage (opzionale)	Se si desidera che il tenant disponga di una quota di storage, un valore numerico per la quota e le unità.

3. Selezionare **continua**.

4. Se si desidera, selezionare le autorizzazioni desiderate per il tenant.



Alcune di queste autorizzazioni hanno requisiti aggiuntivi. Per ulteriori informazioni, selezionare l'icona della guida per ciascuna autorizzazione.

Permesso	Se selezionato...
Consentire i servizi della piattaforma	Il tenant può utilizzare servizi della piattaforma S3 come CloudMirror. Vedere <a href="#">"Gestire i servizi della piattaforma per gli account tenant S3"</a> .
Utilizza la propria origine di identità	Il tenant può configurare e gestire la propria origine di identità per gruppi e utenti federati. Questa opzione è disattivata se si dispone di <a href="#">"SSO configurato"</a> Per il tuo sistema StorageGRID.
Consenti selezione S3	Il tenant può emettere richieste API S3 SelectObjectContent per filtrare e recuperare i dati degli oggetti. Vedere <a href="#">"Manage S3 (Gestisci S3): Selezionare per gli account tenant"</a> .  <b>Importante:</b> Le richieste SelectObjectContent possono ridurre le performance di bilanciamento del carico per tutti i client S3 e per tutti i tenant. Attivare questa funzione solo quando richiesto e solo per tenant attendibili.
USA connessione a federazione di griglie	Il tenant può utilizzare una connessione a federazione di grid.  Selezionando questa opzione: <ul style="list-style-type: none"> <li>• Consente di clonare questo tenant e tutti i gruppi tenant e gli utenti aggiunti all'account da questa griglia (la <i>griglia di origine</i>) all'altra griglia della connessione selezionata (la <i>griglia di destinazione</i>).</li> <li>• Consente a questo tenant di configurare la replica cross-grid tra i bucket corrispondenti su ogni grid.</li> </ul> Vedere <a href="#">"Gestire i tenant consentiti per la federazione di grid"</a> .

5. Se si seleziona **Usa connessione federazione griglia**, selezionare una delle connessioni federazione griglia disponibili.

6. Definire l'accesso root per l'account tenant, in base all'utilizzo o meno da parte del sistema StorageGRID ["federazione delle identità"](#), ["SSO \(Single Sign-on\)"](#), o entrambi.



Opzione	Eseguire questa operazione
Se la federazione delle identità non è attivata	Specificare la password da utilizzare quando si effettua l'accesso al tenant come utente root locale.
Se è attivata la federazione delle identità	<ul style="list-style-type: none"> <li>a. Selezionare un gruppo federated esistente per disporre dell'autorizzazione di accesso root per il tenant.</li> <li>b. Facoltativamente, specificare la password da utilizzare quando si effettua l'accesso al tenant come utente root locale.</li> </ul>
Se sono attivate sia la federazione di identità che il single sign-on (SSO)	Selezionare un gruppo federated esistente per disporre dell'autorizzazione di accesso root per il tenant. Nessun utente locale può accedere.

7. 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 per il tenant sarà l'utente root. Se altri utenti utilizzeranno questo tenant, utilizzare Tenant Manager per configurare le chiavi e le autorizzazioni.

8. Selezionare **continua**.

9. Per il passo Create bucket, è possibile creare un bucket per gli oggetti del tenant. Altrimenti, selezionare **Create tenant without bucket** (Crea tenant senza bucket) per accedere a [fase di download dei dati](#).



Se S3 Object Lock è attivato per la griglia, il bucket creato in questa fase non ha S3 Object Lock abilitato. Se è necessario utilizzare un bucket S3 Object Lock per questa applicazione S3, selezionare **Create tenant without bucket** (Crea tenant senza bucket). Quindi, utilizzare Tenant Manager per ["creare il bucket"](#) invece.

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



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

- b. Selezionare **Region** per questo bucket.

Utilizzare la regione predefinita (`us-east-1`) A meno che non si preveda di utilizzare ILM in futuro per filtrare gli oggetti in base all'area del bucket.


- c. Selezionare **Enable object versioning** (attiva versione oggetto) se si desidera memorizzare ogni versione di ciascun oggetto in questo bucket.

- d. Selezionare **Create tenant and bucket** (Crea tenant e bucket) e passare alla fase di download dei dati.

#### fase 4 di 6: Download dei dati

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

#### Fasi

1. Se è stato selezionato **Create root user S3 access key automatically** (Crea chiave di accesso S3 utente root automaticamente), eseguire una o entrambe le operazioni seguenti:
  - Selezionare **Download access key** (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 **Download Configuration Values** (Scarica valori di configurazione) per scaricare un `.txt` file contenente le impostazioni per l'endpoint del bilanciamento del carico, il tenant, il bucket e l'utente root.
3. Salvare queste informazioni in una posizione sicura.



Non chiudere questa pagina prima di aver copiato entrambi i tasti di accesso. I tasti non saranno disponibili dopo la chiusura di questa pagina. Assicurarsi di salvare queste informazioni in una posizione sicura perché possono essere utilizzate per ottenere dati dal sistema StorageGRID.

4. Se richiesto, selezionare la casella di controllo per confermare che le chiavi sono state scaricate o copiate.
5. Selezionare **continua** per passare alla regola ILM e al passaggio del criterio.

### Fase 5 di 6: Esaminare la regola ILM e il criterio ILM per S3

Le regole ILM (Information Lifecycle Management) controllano il posizionamento, la durata e il comportamento di acquisizione di tutti gli oggetti nel sistema StorageGRID. Il criterio ILM incluso in StorageGRID crea due copie replicate di tutti gli oggetti. Questo criterio è attivo fino a quando non si attiva almeno un nuovo criterio.

#### Fasi

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 una nuova policy. Vedere "[Creare una regola ILM](#)" e "[Criteri ILM: Panoramica](#)".
3. Selezionare **ho esaminato questi passaggi e ho compreso cosa devo fare**.
4. Selezionare la casella di controllo per indicare che si comprende cosa fare in seguito.
5. Selezionare **continua** per accedere a **Riepilogo**.

### Fase 6 di 6: Riepilogo

#### Fasi

1. Esaminare 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 **Accedi come root** si passa a Tenant Manager, dove è possibile aggiungere utenti tenant, creare bucket aggiuntivi e aggiornare le impostazioni del bucket.
3. Selezionare **fine**.
4. Configurare l'applicazione utilizzando il file scaricato da StorageGRID o i valori ottenuti manualmente.

## Gestire i gruppi ha

## Gestire i gruppi ad alta disponibilità (ha): Panoramica

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

### Che cos'è un gruppo ha?

È possibile utilizzare i gruppi ad alta disponibilità (ha) per fornire connessioni dati altamente disponibili per i client S3 e Swift o per fornire connessioni altamente disponibili a Grid Manager e Tenant Manager.

Ciascun gruppo ha fornisce l'accesso ai servizi condivisi sui nodi selezionati.

- I gruppi HA che includono nodi gateway, nodi di amministrazione o entrambi forniscono connessioni dati altamente disponibili per i client S3 e Swift.
- I gruppi HA che includono solo nodi Admin forniscono connessioni altamente disponibili al Grid Manager e al Tenant Manager.
- Un gruppo ha che include solo appliance SG100 o SG1000 e nodi software basati su VMware può fornire connessioni altamente disponibili per "[S3 tenant che utilizzano S3 Select](#)". I gruppi HA sono consigliati quando si utilizza S3 Select, ma non sono richiesti.

### Come crei un gruppo ha?

1. Selezionare un'interfaccia di rete per uno o più nodi Admin o 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 dispone di un indirizzo IP assegnato da DHCP.

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

Per istruzioni, vedere "[Configurare i gruppi ad alta disponibilità](#)".

### Che cos'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 nell'ordine di priorità. Finché l'interfaccia primaria rimane disponibile, viene utilizzata quando i client si connettono a qualsiasi indirizzo VIP del gruppo. Cioè, durante il normale funzionamento, l'interfaccia primaria è l'interfaccia "attiva" per il gruppo.

Analogamente, durante il normale funzionamento, qualsiasi interfaccia a priorità inferiore per il gruppo ha agisce come interfacce di "backup". Queste interfacce di backup non vengono utilizzate a meno che l'interfaccia primaria (attualmente attiva) non diventi disponibile.

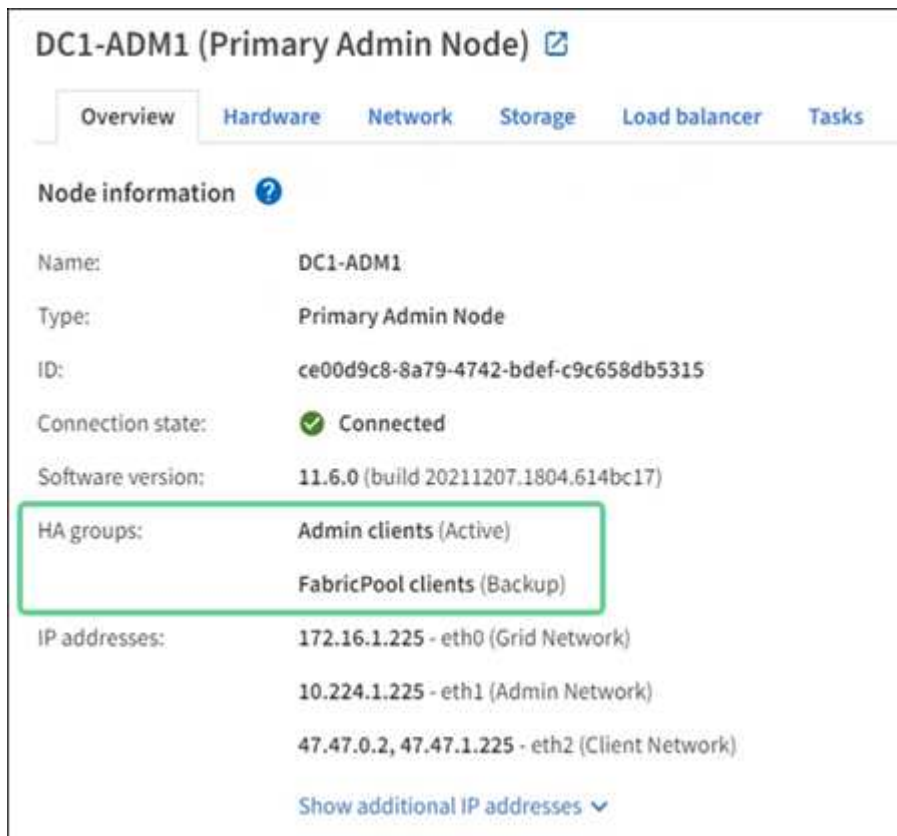
## Visualizzare lo stato corrente del gruppo ha di un nodo

Per verificare se un nodo è assegnato a un gruppo ha e determinarne lo stato corrente, selezionare **NODES > Node**.

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 corrisponde allo 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; si tratta di un'interfaccia di backup.
- **Arrestato:** Il gruppo ha non può essere ospitato su questo nodo perché il servizio ad alta disponibilità (keepalived) è stato arrestato manualmente.
- **Fault:** Il gruppo ha non può essere ospitato su questo nodo a causa di uno o più dei seguenti fattori:
  - Il servizio Load Balancer (nginx-gw) non è in esecuzione sul nodo.
  - L'interfaccia eth0 o VIP del nodo non è disponibile.
  - Il nodo non è attivo.

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 di amministrazione e un'interfaccia di backup per il gruppo di client FabricPool.



**DC1-ADM1 (Primary Admin Node)** [🔗](#)

Overview Hardware Network Storage Load balancer Tasks

**Node information** [?](#)

Name: DC1-ADM1

Type: Primary Admin Node

ID: ce00d9c8-8a79-4742-bdef-c9c658db5315

Connection state: ✔ Connected

Software version: 11.6.0 (build 20211207.1804.614bc17)

HA groups: Admin clients (Active)  
FabricPool clients (Backup)

IP addresses: 172.16.1.225 - eth0 (Grid Network)  
10.224.1.225 - eth1 (Admin Network)  
47.47.0.2, 47.47.1.225 - eth2 (Client Network)

[Show additional IP addresses](#) ▼

## Cosa succede quando l'interfaccia attiva non funziona?

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 riesce, gli indirizzi VIP si spostano sulla prima interfaccia di backup disponibile nell'ordine di priorità. Se l'interfaccia non funziona, gli indirizzi VIP passano alla successiva interfaccia di backup disponibile e così via.

Il failover può essere attivato per uno dei seguenti motivi:

- Il nodo su cui è configurata l'interfaccia non funziona.
- Il nodo su cui è configurata l'interfaccia perde la connettività con tutti gli altri nodi per almeno 2 minuti.
- L'interfaccia attiva non funziona.
- Il servizio Load Balancer si arresta.
- Il servizio High Availability si interrompe.



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 abbastanza rapido da consentire alle applicazioni client di avere un impatto minimo e può fare affidamento sui normali comportamenti di ripetizione per continuare a funzionare.

Quando il guasto viene risolto e un'interfaccia con priorità più alta diventa nuovamente disponibile, gli indirizzi VIP vengono automaticamente spostati nell'interfaccia con priorità più alta disponibile.

## Come vengono utilizzati i gruppi ha?

È possibile utilizzare gruppi ad alta disponibilità (ha) per fornire connessioni altamente disponibili a StorageGRID per i dati a oggetti e per l'utilizzo amministrativo.

- Un gruppo ha può fornire connessioni amministrative altamente disponibili al Grid Manager o al tenant Manager.
- Un gruppo ha può fornire connessioni dati altamente disponibili per i client S3 e Swift.
- Un gruppo ha che contiene una sola interfaccia consente di fornire molti indirizzi VIP e di impostare esplicitamente gli indirizzi IPv6.

Un gruppo ha può fornire alta disponibilità solo se tutti i nodi inclusi nel gruppo forniscono gli stessi servizi. Quando si crea un gruppo ha, aggiungere interfacce dai tipi di nodi che forniscono i servizi richiesti.

- **Admin Node:** Include il servizio Load Balancer e abilita l'accesso al Grid Manager o al Tenant Manager.
- **Gateway Node:** Include il servizio Load Balancer.

Scopo del gruppo ha	Aggiungere nodi di questo tipo al gruppo ha
Accesso a Grid Manager	<ul style="list-style-type: none"><li>• Nodo amministratore primario (<b>primario</b>)</li><li>• Nodi amministrativi non primari</li></ul> <p><b>Nota:</b> l'Admin Node primario deve essere l'interfaccia primaria. Alcune procedure di manutenzione possono essere eseguite solo dal nodo di amministrazione primario.</p>
Accesso solo al tenant manager	<ul style="list-style-type: none"><li>• Nodi di amministrazione primari o non primari</li></ul>

Scopo del gruppo ha	Aggiungere nodi di questo tipo al gruppo ha
Accesso client S3 o Swift — Servizio Load Balancer	<ul style="list-style-type: none"> <li>• Nodi di amministrazione</li> <li>• Nodi gateway</li> </ul>
Accesso al client S3 per "S3 Seleziona"	<ul style="list-style-type: none"> <li>• Appliance SG100 o SG1000</li> <li>• Nodi software basati su VMware</li> </ul> <p><b>Nota:</b> I gruppi HA sono consigliati quando si utilizza S3 Select, ma non sono richiesti.</p>

### 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.

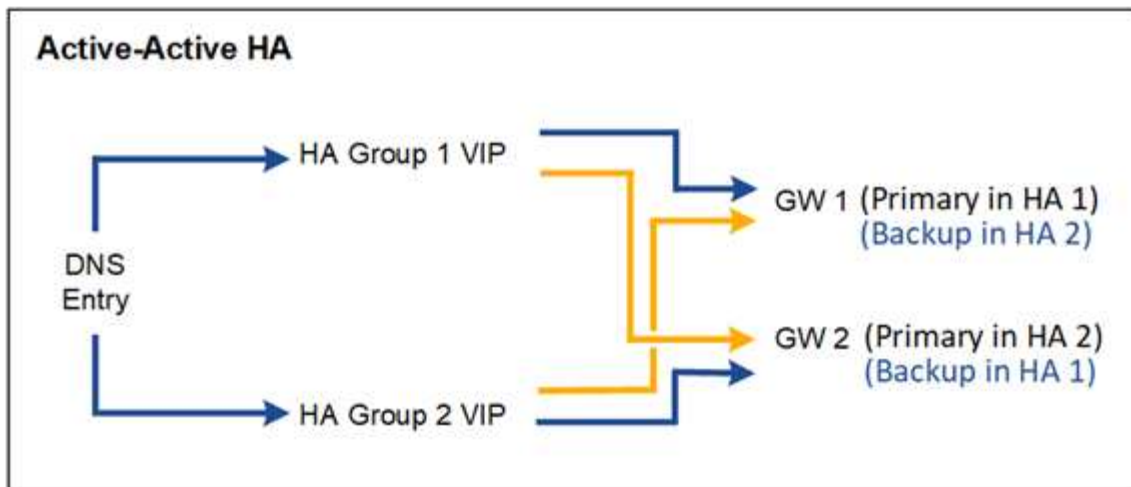
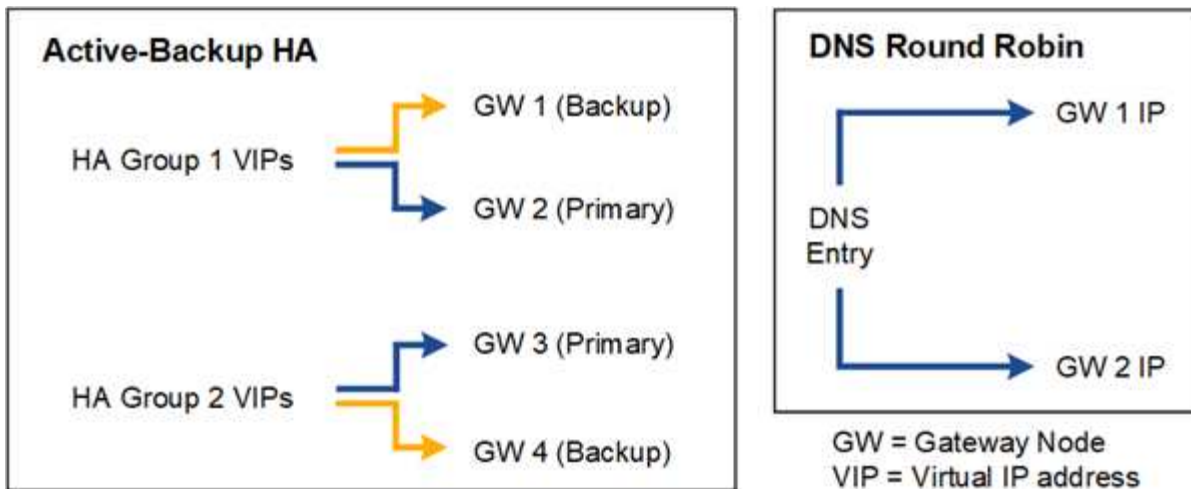
Se hai effettuato l'accesso a Grid Manager o a Tenant Manager quando si verifica il failover, sei disconnesso e devi effettuare nuovamente l'accesso per riprendere l'attività.

Non è possibile eseguire alcune procedure di manutenzione 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 seguenti diagrammi forniscono esempi di diversi modi per configurare i gruppi ha. Ogni opzione presenta vantaggi e svantaggi.

Nei diagrammi, il blu indica l'interfaccia principale 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 Active-Backup	<ul style="list-style-type: none"> <li>Gestito da StorageGRID senza dipendenze esterne.</li> <li>Failover rapido.</li> </ul>	<ul style="list-style-type: none"> <li>Solo un nodo in un gruppo ha è attivo. Almeno un nodo per gruppo ha sarà inattivo.</li> </ul>
DNS Round Robin	<ul style="list-style-type: none"> <li>Maggiore throughput aggregato.</li> <li>Nessun host inattivo.</li> </ul>	<ul style="list-style-type: none"> <li>Failover lento, che potrebbe dipendere dal comportamento del client.</li> <li>Richiede la configurazione dell'hardware al di fuori di StorageGRID.</li> <li>Ha bisogno di un controllo dello stato di salute implementato dal cliente.</li> </ul>

Configurazione	Vantaggi	Svantaggi
Ha Active-Active	<ul style="list-style-type: none"> <li>• Il traffico viene distribuito tra più gruppi ha.</li> <li>• Throughput aggregato elevato che si adatta al numero di gruppi ha.</li> <li>• Failover rapido.</li> </ul>	<ul style="list-style-type: none"> <li>• Più complesso da configurare.</li> <li>• Richiede la configurazione dell'hardware al di fuori di StorageGRID.</li> <li>• Ha bisogno di un controllo dello stato di salute implementato dal cliente.</li> </ul>

## Configurare i gruppi ad alta disponibilità

È possibile configurare i gruppi ad alta disponibilità (ha) per fornire l'accesso altamente disponibile ai servizi sui nodi Admin o Gateway.

### Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai il ["Autorizzazione di accesso root"](#).
- Se si intende utilizzare un'interfaccia VLAN in un gruppo ha, l'interfaccia VLAN è stata creata. Vedere ["Configurare le interfacce VLAN"](#).
- Se si intende utilizzare un'interfaccia di accesso per un nodo in un gruppo ha, l'interfaccia è stata creata:
  - **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 l'installazione del nodo):** ["Linux: Aggiunta di interfacce di accesso o trunk a un nodo"](#)
  - **VMware (dopo l'installazione del nodo):** ["VMware: Aggiunta di interfacce di accesso o trunk a un nodo"](#)

### Creare un gruppo ad alta disponibilità

Quando si crea un gruppo ad alta disponibilità, selezionare una o più interfacce e organizzarle in ordine di priorità. Quindi, assegnare uno o più indirizzi VIP al gruppo.

Un'interfaccia deve essere un nodo gateway o un nodo amministratore per essere incluso in un gruppo ha. Un gruppo ha può utilizzare solo un'interfaccia per un dato nodo; tuttavia, altre interfacce per lo stesso nodo possono essere utilizzate in altri gruppi ha.

### Accedere alla procedura guidata

#### Fasi

1. Selezionare **CONFIGURATION > Network > High Availability groups**.
2. Selezionare **Crea**.

### Inserire i dettagli del gruppo ha

#### Fasi

1. Fornire un nome univoco per il gruppo ha.
2. Facoltativamente, inserire una descrizione per il gruppo ha.



### 3. Selezionare **continua**.

#### Aggiungere interfacce al gruppo ha

##### Fasi

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

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

### Add interfaces to the HA group

Select one or more interfaces for this HA group. You can select only one interface for each node.

Search... Total interface count: 4

Node	Interface	Site	IPv4 subnet	Node type
<input type="checkbox"/> DC1-ADM1-104-96	eth0	DC1	10.96.104.0/22	Primary Admin Node
<input type="checkbox"/> DC1-ADM1-104-96	eth2	DC1	—	Primary Admin Node
<input type="checkbox"/> DC2-ADM1-104-103	eth0	DC2	10.96.104.0/22	Admin Node
<input type="checkbox"/> DC2-ADM1-104-103	eth2	DC2	—	Admin Node

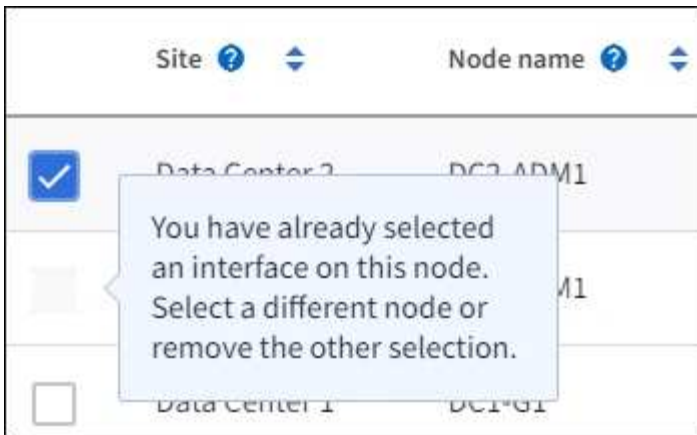
0 interfaces selected



Dopo aver creato un'interfaccia VLAN, attendere fino a 5 minuti per visualizzare la nuova interfaccia nella tabella.

#### Linee guida per la selezione delle interfacce

- Selezionare almeno un'interfaccia.
- È possibile selezionare una sola interfaccia per un nodo.
- Se il gruppo ha è per la protezione ha dei servizi Admin Node, che includono Grid Manager e Tenant Manager, selezionare le interfacce solo sui nodi Admin.
- Se il gruppo ha è per la protezione ha del traffico client S3 o Swift, 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, in caso di failover, i servizi forniti dal nodo precedentemente attivo potrebbero non essere disponibili sul nodo appena attivo. Ad esempio, un nodo gateway di backup non può fornire la protezione ha dei servizi del nodo amministratore. Analogamente, un nodo Admin di backup non può eseguire tutte le procedure di manutenzione che il nodo Admin primario può fornire.
- Se non è possibile selezionare un'interfaccia, la relativa casella di controllo è disattivata. Il suggerimento fornisce ulteriori informazioni.



- Non è possibile selezionare un'interfaccia se il relativo valore di sottorete o il 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 principale non funziona, gli indirizzi VIP passano all'interfaccia con la priorità più alta disponibile. Se l'interfaccia non funziona, gli indirizzi VIP passano alla successiva interfaccia con la priorità più alta disponibile e così via.

### Fasi

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

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

### Determine the priority order

Determine the primary interface and the backup (failover) interfaces for this HA group. Drag and drop rows or select the arrows.

Priority order <span>?</span>	Node	Interface <span>?</span>	Node type <span>?</span>
1 (Primary interface)	↕ DC1-ADM1-104-96	eth2	Primary Admin Node
2	↕ DC2-ADM1-104-103	eth2	Admin Node



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**.

## Inserire gli indirizzi IP

### Fasi

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

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



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

### Enter details for the HA group

**Subnet CIDR**

Specify the subnet in CIDR notation. The optional gateway IP and all VIPs must be in this subnet.

IPv4 address followed by a slash and the subnet length (0-32)

**Gateway IP address (optional)**

Optionally specify the IP address of the gateway, which must be in the subnet. If the subnet address length is 32, the gateway IP address is automatically set to the subnet IP.

**Virtual IP address**

Specify at least 1 and no more than 10 virtual IPs for the HA group. All virtual IPs must be in the same subnet. If the subnet length is 32, only one VIP is allowed, which is automatically set to the subnet/gateway IP.

[Add another IP address](#)

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

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

3. 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 tutti saranno attivi contemporaneamente sull'interfaccia attiva.

Specificare almeno un indirizzo IPv4. In alternativa, è possibile specificare ulteriori indirizzi IPv4 e IPv6.

4. Selezionare **Create ha group** (Crea gruppo ha) e selezionare **Finish** (fine).

Viene creato il gruppo ha ed è ora possibile utilizzare gli indirizzi IP virtuali configurati.

### Passi successivi

Se si utilizza questo gruppo ha per il bilanciamento del carico, creare un endpoint per il bilanciamento del

carico per determinare il protocollo di porta e di rete e per allegare eventuali certificati richiesti. Vedere ["Configurare gli endpoint del bilanciamento del carico"](#).

## Modificare un gruppo ad alta disponibilità

È possibile modificare un gruppo ad alta disponibilità (ha) per modificarne nome e descrizione, aggiungere o rimuovere interfacce, modificare 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 decommissionamento del sito o del nodo.

### Fasi

1. Selezionare **CONFIGURATION > Network > High Availability groups**.

La pagina High Availability groups (gruppi ad alta disponibilità) mostra tutti i gruppi ha esistenti.

2. Selezionare la casella di controllo del gruppo ha che si desidera modificare.
3. Eseguire una delle seguenti operazioni in base a quanto si desidera aggiornare:
  - 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 si seleziona **Modifica indirizzo IP virtuale**:
  - a. Aggiornare gli indirizzi IP virtuali per il gruppo ha.
  - b. Selezionare **Salva**.
  - c. Selezionare **fine**.
5. Se si seleziona **Edit ha group** (Modifica gruppo ha):
  - a. Facoltativamente, aggiornare il nome o la descrizione del gruppo.
  - b. Facoltativamente, selezionare o deselezionare le caselle di controllo per aggiungere o rimuovere 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 delle interfacce di backup per questo gruppo ha.
- d. Facoltativamente, aggiornare gli indirizzi IP virtuali.
- e. Selezionare **Salva**, quindi **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 di bilanciamento del carico. Per eliminare un gruppo ha, è necessario rimuoverlo da tutti gli endpoint del bilanciamento del carico che lo utilizzano.

Per evitare interruzioni del client, aggiornare le applicazioni client S3 o Swift prima di rimuovere un gruppo ha. Aggiornare ciascun client per la connessione 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.

## Fasi

1. Selezionare **CONFIGURATION > Network > High Availability groups**.
2. Esaminare la colonna **endpoint del bilanciamento del carico** per ciascun gruppo ha che si desidera rimuovere. Se sono elencati endpoint del bilanciamento del carico:
  - a. Andare a **CONFIGURATION > Network > Load Balancer Endpoints**.
  - b. Selezionare la casella di controllo per l'endpoint.
  - c. Selezionare **azioni > Modifica modalità di associazione endpoint**.
  - d. Aggiornare la modalità di binding per rimuovere il gruppo ha.
  - e. Selezionare **Save Changes** (Salva modifiche).
3. Se non sono elencati endpoint del bilanciamento del carico, selezionare la casella di controllo per ciascun gruppo ha che si desidera rimuovere.
4. Selezionare **azioni > Rimuovi gruppo ha**.
5. Esaminare il messaggio e selezionare **Delete ha group** (Elimina gruppo ha) per confermare la selezione.

Tutti i gruppi ha selezionati vengono rimossi. Nella pagina dei gruppi ad alta disponibilità viene visualizzato un banner verde di successo.

# Gestire il bilanciamento del carico

## Considerazioni per il bilanciamento del carico

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

### Cos'è il bilanciamento del carico?

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

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

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



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

## Quanti nodi per il bilanciamento del carico sono necessari?

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

## Che cos'è un endpoint di bilanciamento del carico?

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

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

- ["Configurare gli endpoint del bilanciamento del carico"](#)
- ["Utilizzare l'installazione guidata S3"](#)
- ["Utilizzare l'installazione guidata di FabricPool"](#)

### Considerazioni per la porta

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

Le porte utilizzate da altri servizi di rete non sono consentite. Vedere ["Riferimento porta di rete"](#).

### Considerazioni sul protocollo di rete

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

### Considerazioni per i certificati endpoint del bilanciamento del carico

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

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

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

- Il file di certificato del server personalizzato.
- Il file di chiave privata del certificato del server personalizzato.

- Facoltativamente, un bundle CA dei certificati di ciascuna autorità di certificazione di emissione intermedia.

- **Generare un certificato autofirmato.**
- **Utilizzare il certificato globale StorageGRID S3 e Swift.** È necessario caricare o generare una versione personalizzata del certificato prima di poterla selezionare per l'endpoint del bilanciamento del carico. Vedere "[Configurare i certificati API S3 e Swift](#)".

## Di quali valori ho bisogno?

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

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

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

Se necessario, il certificato può utilizzare i caratteri jolly per rappresentare i nomi di dominio completi di tutti i nodi Admin e Gateway che eseguono il servizio Load Balancer. Ad esempio, `*.storagegrid.example.com` utilizza il carattere jolly `*` per rappresentare `adm1.storagegrid.example.com` e `gn1.storagegrid.example.com`.

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

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



Se si utilizzano caratteri jolly per i nomi di dominio, consultare "[Linee guida per la protezione avanzata dei certificati server](#)".

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

## Come si gestiscono i certificati in scadenza?



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

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

- Monitorare attentamente gli avvisi che avvisano di avvicinarsi alle date di scadenza del certificato, come ad esempio **scadenza del certificato endpoint del bilanciamento del carico** e **scadenza del certificato server globale per gli avvisi S3 e Swift API**.
- Mantenere sempre sincronizzate le versioni del certificato delle applicazioni StorageGRID e S3. Se si sostituisce o si rinnova il certificato utilizzato per un endpoint di bilanciamento del carico, è necessario sostituire o rinnovare il certificato equivalente utilizzato dall'applicazione S3.



- Utilizzare un certificato CA con firma pubblica. Se si utilizza un certificato firmato da una CA, è possibile sostituire i certificati in scadenza senza interruzioni.
- Se è stato generato un certificato StorageGRID autofirmato e il certificato sta per scadere, è necessario sostituirlo manualmente in StorageGRID e nell'applicazione S3 prima della scadenza del certificato esistente.

### Considerazioni per la modalità di binding

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

È possibile specificare una delle seguenti modalità di binding:

- **Globale** (impostazione predefinita): Le applicazioni client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministratore, l'indirizzo IP virtuale (VIP) di qualsiasi gruppo ha su qualsiasi rete o un FQDN corrispondente. Utilizzare questa impostazione a meno che non sia necessario limitare l'accessibilità di un endpoint.
- **IP virtuali dei gruppi ha.** Le applicazioni client devono utilizzare un indirizzo IP virtuale (o un FQDN corrispondente) di un gruppo ha.
- **Interfacce nodo.** I client devono utilizzare gli indirizzi IP (o gli FQDN corrispondenti) delle interfacce dei nodi selezionate.
- **Tipo di nodo.** In base al tipo di nodo selezionato, i client devono utilizzare l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di amministrazione o l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di gateway.

### Considerazioni sull'accesso al tenant

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

È possibile utilizzare questa funzionalità per fornire un migliore isolamento della sicurezza tra i tenant e i relativi endpoint. Ad esempio, è possibile utilizzare questa funzione per garantire che i materiali top-secret o altamente classificati di proprietà di un tenant rimangano completamente inaccessibili agli altri tenant.



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

### Esempio di accesso al tenant

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

1. Sono stati creati due endpoint di bilanciamento del carico, come segue:
  - Endpoint **Public**: Utilizza la porta 10443 e consente l'accesso a tutti i tenant.
  - Endpoint **Top secret**: Utilizza la porta 10444 e consente l'accesso solo al tenant **Top secret**. Tutti gli altri tenant non possono accedere a questo endpoint.



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

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

## Disponibilità della CPU

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

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

## Configurare gli endpoint del bilanciamento del carico

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



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

### Prima di iniziare

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



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

- Per caricare un certificato, è necessario disporre del certificato del server, della chiave privata del certificato e, facoltativamente, di un bundle CA.

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

## Creare un endpoint per il bilanciamento del carico

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

### Accedere alla procedura guidata

#### Fasi

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

### Inserire i dettagli dell'endpoint

#### Fasi

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

## Client S3 o Swift

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint, che verrà visualizzato nella tabella della pagina endpoint del bilanciamento del carico.
Porta	<p>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.</p> <p>Se si immette <b>80</b> o <b>8443</b>, l'endpoint viene configurato solo sui nodi Gateway, a meno che non sia stata liberata la porta 8443. Quindi è possibile utilizzare la porta 8443 come endpoint S3 e la porta verrà configurata su entrambi i nodi Gateway e Admin.</p>
Tipo di client	Il tipo di applicazione client che utilizzerà questo endpoint, <b>S3</b> o <b>Swift</b> .
Protocollo di rete	<p>Il protocollo di rete che i client utilizzeranno per la connessione a questo endpoint.</p> <ul style="list-style-type: none"><li>• Selezionare <b>HTTPS</b> per la comunicazione sicura con crittografia TLS (scelta consigliata). È necessario allegare un certificato di sicurezza prima di poter salvare l'endpoint.</li><li>• Selezionare <b>HTTP</b> per comunicazioni meno sicure e non crittografate. Utilizzare HTTP solo per una griglia non di produzione.</li></ul>

## Interfaccia di gestione

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint, che verrà visualizzato nella tabella della pagina endpoint del bilanciamento del carico.
Porta	<p>La porta StorageGRID che si desidera utilizzare per accedere a Gestore griglia, Gestore tenant o entrambi.</p> <ul style="list-style-type: none"><li>• Gestore griglia: <b>8443</b></li><li>• Responsabile del tenant: <b>9443</b></li><li>• Sia Grid Manager che Tenant Manager: <b>443</b></li></ul> <p><b>Nota:</b> È possibile utilizzare queste porte preimpostate o altre porte disponibili.</p>
Tipo di interfaccia	Selezionare il pulsante di opzione per l'interfaccia StorageGRID a cui si accede utilizzando questo endpoint.

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

#### 1. Selezionare **continua**.

#### Selezionare una modalità di binding

##### Fasi

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

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

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

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

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

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

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

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

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

#### Controllo dell'accesso al tenant



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

#### Fasi

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

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

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

## Allega certificato

### Fasi

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

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

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

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

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

## Carica certificato

- a. Selezionare **carica certificato**.
- b. Caricare i file dei certificati del server richiesti:
  - **Server certificate**: Il file di certificato del server personalizzato in codifica PEM.
  - **Certificate private key** (chiave privata certificato): Il file di chiave privata del certificato del server personalizzato (.key).



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

- **Bundle CA**: Un singolo file opzionale contenente i certificati di ogni autorità di certificazione di emissione intermedia (CA). Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati in ordine di catena del certificato.
- c. Espandere **Dettagli certificato** per visualizzare i metadati di ciascun certificato caricato. Se è stato caricato un bundle CA opzionale, ciascun certificato viene visualizzato nella propria scheda.
    - Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato oppure selezionare **Download CA bundle** (Scarica pacchetto CA) per salvare il bundle del certificato.

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

Ad esempio: storagegrid\_certificate.pem

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

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

## Generare un certificato

- a. Selezionare **genera certificato**.
- b. Specificare le informazioni del certificato:

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

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

c. Selezionare **generate**.

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

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

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

Ad esempio: `storagegrid_certificate.pem`

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

e. Selezionare **Crea**.

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

## Al termine

### Fasi

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

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



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

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

2. Fornire ai client S3 e Swift le informazioni necessarie per connettersi all'endpoint:

- Numero di porta
- Nome di dominio completo o indirizzo IP
- Tutti i dettagli del certificato richiesti

### Visualizzare e modificare gli endpoint del bilanciamento del carico

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

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

## S3 load balancer endpoint

Port:	10443
Client type:	S3
Network protocol:	HTTPS
Binding mode:	Global
Endpoint ID:	3d02c126-9437-478c-8b24-08384401d3cb


Remove

Binding mode
Certificate
Tenant access (2 allowed)

You can select a different binding mode or change IP addresses for the current binding mode.

Edit binding mode

Binding mode: Global

 This endpoint uses the Global binding mode. Unless there are one or more overriding endpoints for the same port, clients can access this endpoint using the IP address of any Gateway Node, any Admin Node, or the virtual IP of any HA group on any network.


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



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



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

Attività	Menu delle azioni	Pagina dei dettagli
Modificare il nome dell'endpoint	<ul style="list-style-type: none"> <li>a. Selezionare la casella di controllo per l'endpoint.</li> <li>b. Selezionare <b>azioni &gt; Modifica nome endpoint</b>.</li> <li>c. Inserire il nuovo nome.</li> <li>d. Selezionare <b>Salva</b>.</li> </ul>	<ul style="list-style-type: none"> <li>a. Selezionare il nome dell'endpoint per visualizzare i dettagli.</li> <li>b. Selezionare l'icona di modifica .</li> <li>c. Inserire il nuovo nome.</li> <li>d. Selezionare <b>Salva</b>.</li> </ul>
Modificare la porta dell'endpoint	<ul style="list-style-type: none"> <li>a. Selezionare la casella di controllo per l'endpoint.</li> <li>b. Selezionare <b>azioni &gt; Modifica porta endpoint</b></li> <li>c. Immettere un numero di porta valido.</li> <li>d. Selezionare <b>Salva</b>.</li> </ul>	n/a
Modificare la modalità di associazione degli endpoint	<ul style="list-style-type: none"> <li>a. Selezionare la casella di controllo per l'endpoint.</li> <li>b. Selezionare <b>azioni &gt; Modifica modalità di associazione endpoint</b>.</li> <li>c. Aggiornare la modalità di binding secondo necessità.</li> <li>d. Selezionare <b>Save Changes</b> (Salva modifiche).</li> </ul>	<ul style="list-style-type: none"> <li>a. Selezionare il nome dell'endpoint per visualizzare i dettagli.</li> <li>b. Selezionare <b>Edit binding mode</b> (Modifica modalità di associazione).</li> <li>c. Aggiornare la modalità di binding secondo necessità.</li> <li>d. Selezionare <b>Save Changes</b> (Salva modifiche).</li> </ul>
Modificare il certificato dell'endpoint	<ul style="list-style-type: none"> <li>a. Selezionare la casella di controllo per l'endpoint.</li> <li>b. Selezionare <b>azioni &gt; Modifica certificato endpoint</b>.</li> <li>c. Caricare o generare un nuovo certificato personalizzato o iniziare a utilizzare il certificato globale S3 e Swift, come richiesto.</li> <li>d. Selezionare <b>Save Changes</b> (Salva modifiche).</li> </ul>	<ul style="list-style-type: none"> <li>a. Selezionare il nome dell'endpoint per visualizzare i dettagli.</li> <li>b. Selezionare la scheda <b>certificato</b>.</li> <li>c. Selezionare <b>Modifica certificato</b>.</li> <li>d. Caricare o generare un nuovo certificato personalizzato o iniziare a utilizzare il certificato globale S3 e Swift, come richiesto.</li> <li>e. Selezionare <b>Save Changes</b> (Salva modifiche).</li> </ul>

Attività	Menu delle azioni	Pagina dei dettagli
Modificare l'accesso al tenant	<ul style="list-style-type: none"> <li>a. Selezionare la casella di controllo per l'endpoint.</li> <li>b. Selezionare <b>azioni &gt; Modifica accesso tenant</b>.</li> <li>c. Scegliere un'opzione di accesso diversa, selezionare o rimuovere i tenant dall'elenco oppure eseguire entrambe le operazioni.</li> <li>d. Selezionare <b>Save Changes</b> (Salva modifiche).</li> </ul>	<ul style="list-style-type: none"> <li>a. Selezionare il nome dell'endpoint per visualizzare i dettagli.</li> <li>b. Selezionare la scheda <b>accesso tenant</b>.</li> <li>c. Selezionare <b>Edit tenant access</b> (Modifica accesso tenant).</li> <li>d. Scegliere un'opzione di accesso diversa, selezionare o rimuovere i tenant dall'elenco oppure eseguire entrambe le operazioni.</li> <li>e. Selezionare <b>Save Changes</b> (Salva modifiche).</li> </ul>

### Rimuovere gli endpoint del bilanciamento del carico

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



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



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

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

## Configurare i nomi di dominio degli endpoint S3

Per supportare le richieste in stile virtual-hosted S3, 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"](#).
- Lo hai fatto ["autorizzazioni di accesso specifiche"](#).
- Hai confermato che non è in corso un aggiornamento della griglia.



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

### A proposito di questa attività

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 client.

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 SAN (Subject alternative Name) con caratteri 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 riferiscano a tutti i nomi di dominio degli endpoint S3 richiesti, inclusi i nomi con caratteri jolly.



I client possono connettersi a StorageGRID utilizzando l'indirizzo IP di un nodo gateway, di un nodo amministratore o di un nodo di storage oppure connettendosi all'indirizzo IP virtuale di un gruppo ad alta disponibilità. È necessario comprendere il modo in cui 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 dei seguenti certificati:

- I client che si connettono a un endpoint di bilanciamento del carico possono utilizzare un certificato personalizzato per tale endpoint. Ogni endpoint del bilanciamento del carico può essere configurato per riconoscere diversi nomi di dominio degli endpoint S3.
- I client che si connettono a un endpoint di bilanciamento del carico o direttamente a un nodo di storage possono personalizzare il certificato globale S3 e Swift API per includere tutti i nomi di dominio degli 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 virtual-hosted S3 viene disattivato.

## Aggiungere un nome di dominio dell'endpoint S3

### Fasi

1. Selezionare **CONFIGURATION > Network > S3 endpoint domain name**.
2. Inserire il nome di dominio nel campo **Domain name** 1. Selezionare **Aggiungi un altro nome di dominio** per aggiungere altri nomi di dominio.
3. Selezionare **Salva**.
4. Assicurarsi che i certificati server utilizzati dai client corrispondano ai nomi di dominio degli endpoint S3 richiesti.
  - Se i client si connettono a un endpoint di bilanciamento del carico che utilizza il proprio certificato, "[aggiornare il certificato associato all'endpoint](#)".
  - Se i client si connettono a un endpoint di bilanciamento del carico che utilizza il certificato globale S3 e Swift API o direttamente ai nodi di storage, "[Aggiornare il certificato globale S3 e Swift API](#)".
5. Aggiungere i record DNS necessari per garantire che le richieste dei 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 endpoint S3

Se si modifica un nome utilizzato dalle applicazioni S3, le richieste di tipo virtual-hosted non avranno esito positivo.


### Fasi

1. Selezionare **CONFIGURATION > Network > S3 endpoint domain name**.
2. Selezionare il campo del nome di dominio che si desidera modificare e apportare le modifiche necessarie.
3. Selezionare **Salva**.
4. Selezionare **Sì** per confermare la modifica.

## Eliminare un nome di dominio dell'endpoint S3

Se si rimuove un nome utilizzato dalle applicazioni S3, le richieste di tipo virtual-hosted non avranno esito positivo.

### Fasi

1. Selezionare **CONFIGURATION > Network > S3 endpoint domain name**.
2. Selezionare l'icona di eliminazione  accanto al nome di dominio.
3. Selezionare **Sì** per confermare l'eliminazione.

### Informazioni correlate

- ["UTILIZZARE L'API REST S3"](#)
- ["Visualizzare gli indirizzi IP"](#)
- ["Configurare i gruppi ad alta disponibilità"](#)

## Riepilogo: Indirizzi IP e porte per le connessioni client

Per memorizzare o recuperare oggetti, le applicazioni client S3 e Swift si connettono al

servizio Load Balancer, incluso in tutti i nodi Admin e Gateway, o al servizio Local Distribution Router (LDR), incluso in tutti i nodi Storage.

Le applicazioni client possono connettersi a StorageGRID utilizzando l'indirizzo IP di un nodo Grid e il numero di porta del servizio su tale 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) invece di un indirizzo IP o VIP, è possibile configurare le voci DNS.

Questa tabella riassume i diversi modi in cui i client possono connettersi a StorageGRID e gli indirizzi IP e le porte utilizzati per ciascun tipo di connessione. Se sono già stati creati endpoint di bilanciamento del carico e gruppi ad alta disponibilità (ha), vedere [Dove trovare gli indirizzi IP](#) Per individuare questi valori in Grid Manager.

Dove viene stabilita la connessione	Servizio a cui si connette il client	Indirizzo IP	Porta
Gruppo HA	Bilanciamento del carico	Indirizzo IP virtuale di un gruppo ha	Porta assegnata all'endpoint del bilanciamento del carico
Nodo Admin	Bilanciamento del carico	Indirizzo IP del nodo di amministrazione	Porta assegnata all'endpoint del bilanciamento del carico
Nodo gateway	Bilanciamento del carico	Indirizzo IP del nodo gateway	Porta assegnata all'endpoint del bilanciamento del carico
Nodo di storage	LDR	Indirizzo IP del nodo di storage	Porte S3 predefinite: <ul style="list-style-type: none"><li>• HTTPS: 18082</li><li>• HTTP: 18084</li></ul> Porte Swift predefinite: <ul style="list-style-type: none"><li>• HTTPS: 18083</li><li>• HTTP:18085</li></ul>

## URL di esempio

Per connettere un'applicazione client all'endpoint 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 bilanciamento 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. Accedere a Grid Manager utilizzando un "[browser web supportato](#)".
2. Per trovare l'indirizzo IP di un nodo Grid:
  - a. Selezionare **NODI**.
  - b. Selezionare il nodo Admin, il nodo gateway o il nodo di storage a cui si desidera connettersi.
  - c. Selezionare la scheda **Panoramica**.
  - d. Nella sezione Node Information (informazioni sul nodo), annotare gli indirizzi IP del nodo.
  - e. Selezionare **Mostra altro** per visualizzare gli indirizzi IPv6 e le mappature dell'interfaccia.

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

- **Eth0:** Grid Network
- **Eth1:** Admin Network (opzionale)
- **Eth2:** rete client (opzionale)



Se si sta visualizzando un nodo Admin o un nodo Gateway e si tratta del nodo attivo di 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 **CONFIGURATION > Network > High Availability groups**.
  - b. Nella tabella, annotare l'indirizzo IP virtuale del gruppo ha.
4. Per trovare il numero di porta di un endpoint Load Balancer:
  - a. Selezionare **CONFIGURATION > Network > Load Balancer Endpoints**.
  - 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, poiché tali porte sono riservate sui nodi Admin. Tutte le altre porte sono configurate sia sui nodi Gateway che sui nodi Admin.

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

## Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.