



Configurare le connessioni client S3 e Swift

StorageGRID

NetApp
October 03, 2025

Sommario

Configurare le connessioni client S3 e Swift	1
Informazioni sulle connessioni client S3 e Swift	1
Riepilogo: Indirizzi IP e porte per le connessioni client	1
Configurare le interfacce VLAN	4
Considerazioni per le interfacce VLAN	4
Creare un'interfaccia VLAN	5
Modificare un'interfaccia VLAN	7
Rimuovere un'interfaccia VLAN	8
Gestire i gruppi ad alta disponibilità	8
Gestire i gruppi ad alta disponibilità (ha): Panoramica	8
Come vengono utilizzati i gruppi ha?	11
Opzioni di configurazione per i gruppi ha	12
Configurare i gruppi ad alta disponibilità	14
Gestire il bilanciamento del carico	20
Gestire il bilanciamento del carico: Panoramica	20
Come funziona il bilanciamento del carico - Servizio di bilanciamento del carico	21
Configurare gli endpoint del bilanciamento del carico	21
Come funziona il bilanciamento del carico - servizio CLB (obsoleto)	30
Configurare i nomi di dominio degli endpoint API S3	31
Abilitare HTTP per le comunicazioni client	33
Controllare quali operazioni client sono consentite	34

Configurare le connessioni client S3 e Swift

Informazioni sulle connessioni client S3 e Swift

In qualità di amministratore di grid, gestisci le opzioni di configurazione che controllano il modo in cui i tenant S3 e Swift possono connettere le applicazioni client al sistema StorageGRID per memorizzare e recuperare i dati. Esistono diverse opzioni per soddisfare i diversi requisiti di client e tenant.

Le applicazioni client possono memorizzare o recuperare oggetti connettendosi a una delle seguenti opzioni:

- Il servizio Load Balancer sui nodi Admin o Gateway o, facoltativamente, l'indirizzo IP virtuale di un gruppo ad alta disponibilità (ha) di nodi Admin o nodi Gateway
- Il servizio CLB sui nodi gateway o, facoltativamente, l'indirizzo IP virtuale di un gruppo ad alta disponibilità di nodi gateway



Il servizio CLB è obsoleto. I client configurati prima della release StorageGRID 11.3 possono continuare a utilizzare il servizio CLB sui nodi gateway. Tutte le altre applicazioni client che dipendono da StorageGRID per fornire il bilanciamento del carico devono connettersi utilizzando il servizio bilanciamento del carico.

- Nodi di storage, con o senza bilanciamento del carico esterno

È possibile configurare le seguenti funzioni sul sistema StorageGRID:

- **Interfacce VLAN:** È possibile creare interfacce LAN virtuali (VLAN) su nodi Admin e nodi Gateway per isolare e partizionare il traffico client e tenant per garantire sicurezza, flessibilità e performance. Dopo aver creato un'interfaccia VLAN, aggiungerla a un gruppo ad alta disponibilità (ha).
- **Gruppi ad alta disponibilità:** È possibile creare un gruppo ha delle interfacce per i nodi gateway o i nodi di amministrazione per creare una configurazione di backup attivo oppure utilizzare un DNS round-robin o un bilanciamento del carico di terze parti e più gruppi ha per ottenere una configurazione Active-Active. Le connessioni client vengono eseguite utilizzando gli indirizzi IP virtuali dei gruppi ha.
- **Servizio Load Balancer:** È possibile consentire ai client di utilizzare il servizio Load Balancer creando endpoint di bilanciamento del carico per le connessioni client. Quando si crea un endpoint di bilanciamento del carico, specificare un numero di porta, se l'endpoint accetta connessioni HTTP o HTTPS, il tipo di client (S3 o Swift) che utilizzerà l'endpoint e il certificato da utilizzare per le connessioni HTTPS (se applicabile).
- **Untrusted Client Network:** È possibile rendere la rete client più sicura configurandola come non attendibile. Quando la rete client non è attendibile, i client possono connettersi solo utilizzando endpoint di bilanciamento del carico.

È inoltre possibile abilitare l'utilizzo di HTTP per i client che si connettono a StorageGRID direttamente ai nodi di storage o utilizzando il servizio CLB (obsoleto) ed è possibile configurare i nomi di dominio degli endpoint API S3 per i client S3.

Riepilogo: Indirizzi IP e porte per le connessioni client

Le applicazioni client possono connettersi a StorageGRID utilizzando l'indirizzo IP di un nodo Grid e il numero di porta di un servizio su tale nodo. Se sono configurati gruppi ad alta disponibilità (ha), le applicazioni client possono connettersi utilizzando l'indirizzo IP

virtuale del gruppo ha.

A proposito di questa attività

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. Le istruzioni descrivono come trovare queste informazioni in Grid Manager se gli endpoint del bilanciamento del carico e i gruppi ad alta disponibilità (ha) sono già configurati.

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	<ul style="list-style-type: none">• Porta endpoint del bilanciamento del carico
Gruppo HA	CLB Nota: il servizio CLB è obsoleto.	Indirizzo IP virtuale di un gruppo ha	Porte S3 predefinite: <ul style="list-style-type: none">• HTTPS: 8082• HTTP: 8084 Porte Swift predefinite: <ul style="list-style-type: none">• HTTPS:8083• HTTP:8085
Nodo Admin	Bilanciamento del carico	Indirizzo IP del nodo di amministrazione	<ul style="list-style-type: none">• Porta endpoint del bilanciamento del carico
Nodo gateway	Bilanciamento del carico	Indirizzo IP del nodo gateway	<ul style="list-style-type: none">• Porta endpoint del bilanciamento del carico
Nodo gateway	CLB Nota: il servizio CLB è obsoleto.	Indirizzo IP del nodo gateway Nota: per impostazione predefinita, le porte HTTP per CLB e LDR non sono attivate.	Porte S3 predefinite: <ul style="list-style-type: none">• HTTPS: 8082• HTTP: 8084 Porte Swift predefinite: <ul style="list-style-type: none">• HTTPS:8083• HTTP:8085

Dove viene stabilita la connessione	Servizio a cui si connette il client	Indirizzo IP	Porta
Nodo di storage	LDR	Indirizzo IP del nodo di storage	Porte S3 predefinite: <ul style="list-style-type: none"> • HTTPS: 18082 • HTTP: 18084 Porte Swift predefinite: <ul style="list-style-type: none"> • HTTPS: 18083 • HTTP: 18085

Esempi

Per connettere un client S3 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 di un endpoint di bilanciamento del carico S3 è 10443, un client S3 potrebbe utilizzare il seguente URL per connettersi a StorageGRID:

- `https://192.0.2.5:10443`

Per connettere un client Swift 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 192.0.2.6 e il numero di porta di un endpoint di bilanciamento del carico di Swift è 10444, un client Swift potrebbe utilizzare il seguente URL per connettersi a StorageGRID:

- `https://192.0.2.6:10444`

È possibile configurare un nome DNS per l'indirizzo IP utilizzato dai client per la connessione a StorageGRID. Contattare l'amministratore di rete locale.

Fasi

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:

- Selezionare **CONFIGURATION > Network > High Availability groups**.
- Nella tabella, annotare l'indirizzo IP virtuale del gruppo ha.

4. Per trovare il numero di porta di un endpoint Load Balancer:

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

Viene visualizzata la pagina Load Balancer Endpoint, che mostra l'elenco degli endpoint già configurati.

- Selezionare un endpoint e selezionare **Modifica endpoint**.

Viene visualizzata la finestra Edit Endpoint (Modifica endpoint) che visualizza ulteriori dettagli sull'endpoint.

- Verificare che l'endpoint selezionato sia configurato per l'utilizzo con il protocollo corretto (S3 o Swift), quindi selezionare **Annulla**.
- Annotare il numero di porta dell'endpoint che si desidera utilizzare per una connessione client.



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.

Configurare le interfacce VLAN

È possibile creare interfacce LAN virtuale (VLAN) su nodi Admin e nodi Gateway e utilizzarle in gruppi ha ed endpoint di bilanciamento del carico per isolare e partizionare il traffico per garantire sicurezza, flessibilità e performance.

Considerazioni per le interfacce VLAN

- Per creare un'interfaccia VLAN, immettere un ID VLAN e scegliere un'interfaccia principale su uno o più nodi.
- Un'interfaccia principale deve essere configurata come interfaccia di linea sullo switch.
- Un'interfaccia padre può essere Grid Network (eth0), Client Network (eth2) o un'interfaccia trunk aggiuntiva per la macchina virtuale o l'host bare-metal (ad esempio, ens256).
- Per ogni interfaccia VLAN, è possibile selezionare solo un'interfaccia principale per un nodo specifico. Ad esempio, non è possibile utilizzare l'interfaccia Grid Network e l'interfaccia Client Network sullo stesso nodo gateway dell'interfaccia principale per la stessa VLAN.

- Se l'interfaccia VLAN è per il traffico Admin Node, che include il traffico correlato a Grid Manager e Tenant Manager, selezionare le interfacce solo sui nodi Admin.
- Se l'interfaccia VLAN è per il traffico client S3 o Swift, selezionare le interfacce sui nodi Admin o Gateway.
- Per ulteriori informazioni sull'aggiunta di interfacce di linea, consultare quanto segue:
 - **VMware (dopo l'installazione del nodo):** [VMware: Aggiunta di interfacce di accesso o trunk a un nodo](#)
 - **RHEL o CentOS (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](#)
 - **RHEL, CentOS, Ubuntu o Debian (dopo aver installato il nodo):** [Linux: Aggiunta di interfacce di accesso o trunk a un nodo](#)

Creare un'interfaccia VLAN

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un [browser web supportato](#).
- Si dispone dell'autorizzazione di accesso root.
- Un'interfaccia di linea è stata configurata nella rete e collegata al nodo VM o Linux. Si conosce il nome dell'interfaccia di linea.
- Si conosce l'ID della VLAN che si sta configurando.

A proposito di questa attività

L'amministratore di rete potrebbe aver configurato una o più interfacce di trunk e una o più VLAN per separare il traffico client o amministrativo che appartiene a diverse applicazioni o tenant. Ogni VLAN è identificata da un ID numerico o da un tag. Ad esempio, la rete potrebbe utilizzare la VLAN 100 per il traffico FabricPool e la VLAN 200 per un'applicazione di archiviazione.

È possibile utilizzare Grid Manager per creare interfacce VLAN che consentono ai client di accedere a StorageGRID su una VLAN specifica. Quando si creano interfacce VLAN, specificare l'ID VLAN e selezionare le interfacce principali (trunk) su uno o più nodi.

Accedere alla procedura guidata

1. Selezionare **CONFIGURAZIONE rete interfacce VLAN**.
2. Selezionare **Crea**.

Inserire i dettagli delle interfacce VLAN


1. Specificare l'ID della VLAN nella rete. È possibile immettere un valore compreso tra 1 e 4094.

Gli ID VLAN non devono essere univoci. Ad esempio, è possibile utilizzare l'ID VLAN 200 per il traffico amministrativo in un sito e lo stesso ID VLAN per il traffico client in un altro sito. È possibile creare interfacce VLAN separate con diversi set di interfacce padre in ogni sito. Tuttavia, due interfacce VLAN con lo stesso ID non possono condividere la stessa interfaccia su un nodo.


Se si specifica un ID già utilizzato, viene visualizzato un messaggio. È possibile continuare a creare un'altra interfaccia VLAN per lo stesso ID VLAN oppure selezionare **Annulla** e modificare l'ID esistente.

2. Facoltativamente, inserire una breve descrizione per l'interfaccia VLAN.

VLAN details

VLAN ID 

203

Description (optional) 

VLAN for S3 tenants. Uses Admin and Gateway Nodes at site 1.

60/64

Cancel **Continue**

3. Selezionare **continua**.

Scegliere le interfacce padre

La tabella elenca le interfacce disponibili per tutti i nodi Admin e Gateway in ogni sito della griglia. Le interfacce Admin Network (eth1) non possono essere utilizzate come interfacce padre e non vengono visualizzate.







1. Selezionare una o più interfacce padre a cui collegare questa VLAN.

Ad esempio, è possibile collegare una VLAN all'interfaccia di rete client (eth2) per un nodo gateway e un nodo amministratore.

Parent interfaces

Select one or more parent interfaces for this VLAN interface. You can only select one parent interface on each node for each VLAN interface.

Search...


	Site 	Node name 	Interface 	Description 	Node type 	Attached VLANs 
<input type="checkbox"/>	Data Center 2	DC2-ADM1	eth0	Grid Network	Non-primary Admin	—
<input checked="" type="checkbox"/>	Data Center 2	DC2-ADM1	eth2	Client Network	Non-primary Admin	—
<input type="checkbox"/>	Data Center 1	DC1-G1	eth0	Grid Network	Gateway	—
<input checked="" type="checkbox"/>	Data Center 1	DC1-G1	eth2	Client Network	Gateway	—
<input type="checkbox"/>	Data Center 1	DC1-ADM1	eth0	Grid Network	Primary Admin	—

2 interfaces are selected.

Previous **Continue**

2. Selezionare **continua**.

Confermare le impostazioni

1. Esaminare la configurazione e apportare eventuali modifiche.
 - Se è necessario modificare l'ID o la descrizione della VLAN, selezionare **Enter VLAN details** (Inserisci dettagli VLAN) nella parte superiore della pagina.
 - Per modificare un'interfaccia padre, selezionare **Choose parent interfaces** (Scegli interfacce padre) nella parte superiore della pagina oppure selezionare **Previous** (precedente).
 - Se è necessario rimuovere un'interfaccia padre, selezionare il cestino .
2. Selezionare **Salva**.
3. Attendere fino a 5 minuti che la nuova interfaccia venga visualizzata come selezione nella pagina High Availability groups (gruppi ad alta disponibilità) e sia elencata nella tabella **Network interfaces** (interfacce di rete) per il nodo (**NODES parent interface node Network**).

Modificare un'interfaccia VLAN

Quando si modifica un'interfaccia VLAN, è possibile apportare i seguenti tipi di modifiche:

- Modificare l'ID o la descrizione della VLAN.
- Aggiungere o rimuovere interfacce padre.

Ad esempio, se si intende decommissionare il nodo associato, è possibile rimuovere un'interfaccia principale da un'interfaccia VLAN.

Tenere presente quanto segue:

- Non è possibile modificare un ID VLAN se l'interfaccia VLAN viene utilizzata in un gruppo ha.
- Non è possibile rimuovere un'interfaccia padre se tale interfaccia padre è utilizzata in un gruppo ha.

Ad esempio, si supponga che la VLAN 200 sia collegata alle interfacce padre sui nodi A e B. Se un gruppo ha utilizza l'interfaccia VLAN 200 per il nodo A e l'interfaccia eth2 per il nodo B, è possibile rimuovere l'interfaccia padre inutilizzata per il nodo B, ma non è possibile rimuovere l'interfaccia padre utilizzata per il nodo A.

Fasi

1. Selezionare **CONFIGURAZIONE rete interfacce VLAN**.
2. Selezionare la casella di controllo dell'interfaccia VLAN che si desidera modificare. Quindi, selezionare **azioni Modifica**.
3. Facoltativamente, aggiornare l'ID VLAN o la descrizione. Quindi, selezionare **continua**.

Non è possibile aggiornare un ID VLAN se la VLAN viene utilizzata in un gruppo ha.

4. Facoltativamente, selezionare o deselezionare le caselle di controllo per aggiungere interfacce padre o rimuovere interfacce inutilizzate. Quindi, selezionare **continua**.
5. Esaminare la configurazione e apportare eventuali modifiche.
6. Selezionare **Salva**.

Rimuovere un'interfaccia VLAN

È possibile rimuovere una o più interfacce VLAN.

Non è possibile rimuovere un'interfaccia VLAN se è attualmente utilizzata in un gruppo ha. È necessario rimuovere l'interfaccia VLAN dal gruppo ha prima di poterla rimuovere.

Per evitare interruzioni del traffico client, è consigliabile eseguire una delle seguenti operazioni:

- Aggiungere una nuova interfaccia VLAN al gruppo ha prima di rimuovere questa interfaccia VLAN.
- Creare un nuovo gruppo ha che non utilizzi questa interfaccia VLAN.
- Se l'interfaccia VLAN che si desidera rimuovere è attualmente attiva, modificare il gruppo ha. Spostare l'interfaccia VLAN che si desidera rimuovere in fondo all'elenco delle priorità. Attendere che la comunicazione venga stabilita sulla nuova interfaccia principale, quindi rimuovere la vecchia interfaccia dal gruppo ha. Infine, eliminare l'interfaccia VLAN su quel nodo.

Fasi

1. Selezionare **CONFIGURAZIONE rete interfacce VLAN**.
2. Selezionare la casella di controllo per ogni interfaccia VLAN che si desidera rimuovere. Quindi, selezionare **azioni Elimina**.
3. Selezionare **Sì** per confermare la selezione.

Tutte le interfacce VLAN selezionate vengono rimosse. Nella pagina delle interfacce VLAN viene visualizzato un banner verde di successo.

Gestire i gruppi ad alta disponibilità

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 principale è l'interfaccia "Active" per il gruppo.

Analogamente, durante il normale funzionamento, tutte le interfacce con priorità inferiore per il gruppo ha agiscono come interfacce "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:	<div>Admin clients (Active)</div> <div>FabricPool clients (Backup)</div>
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 dal guasto del servizio CLB (obsoleto) o dei servizi per Grid Manager o il 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 e il servizio CLB (obsoleto).

Scopo del gruppo ha	Aggiungere nodi di questo tipo al gruppo ha
Accesso a Grid Manager	<ul style="list-style-type: none">• Nodo amministratore primario (primario)• Nodi amministrativi non primari <p>Nota: 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">• Nodi di amministrazione primari o non primari
Accesso client S3 o Swift — Servizio Load Balancer	<ul style="list-style-type: none">• Nodi di amministrazione• Nodi gateway
Accesso al client S3 per S3 Seleziona	<ul style="list-style-type: none">• Appliance SG100 o SG1000• Nodi software basati su VMware <p>Nota: I gruppi HA sono consigliati quando si utilizza S3 Select, ma non sono richiesti.</p>
Accesso client S3 o Swift — Servizio CLB Nota: il servizio CLB è obsoleto.	<ul style="list-style-type: none">• Nodi gateway

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.

Limitazioni dell'utilizzo di gruppi ha con il servizio CLB

Il guasto del servizio CLB non attiva il failover all'interno del gruppo ha.

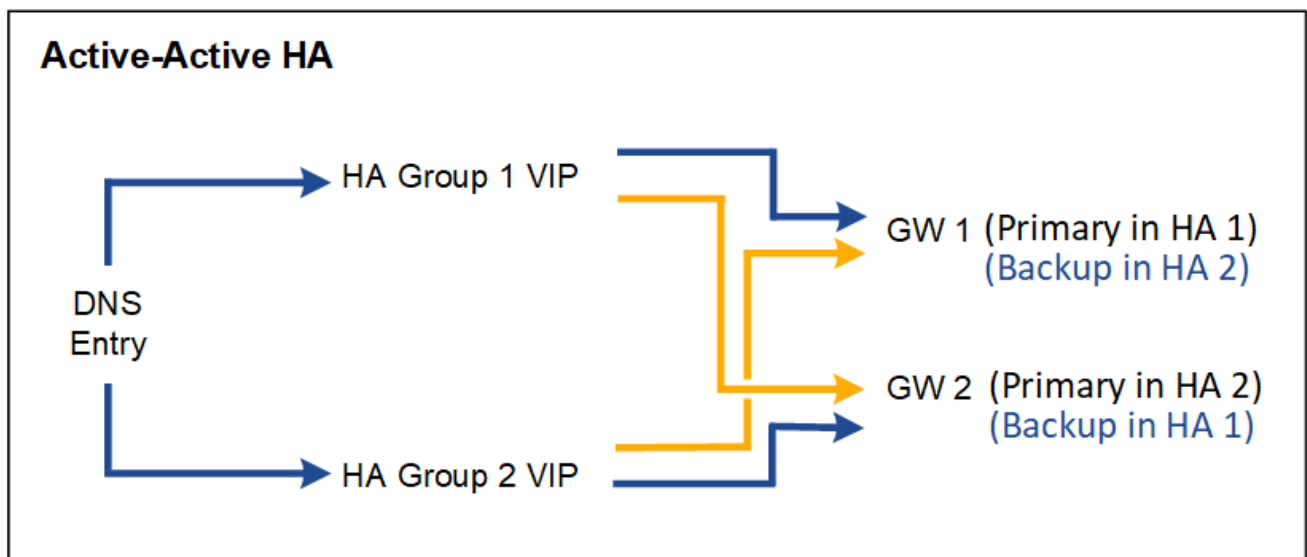
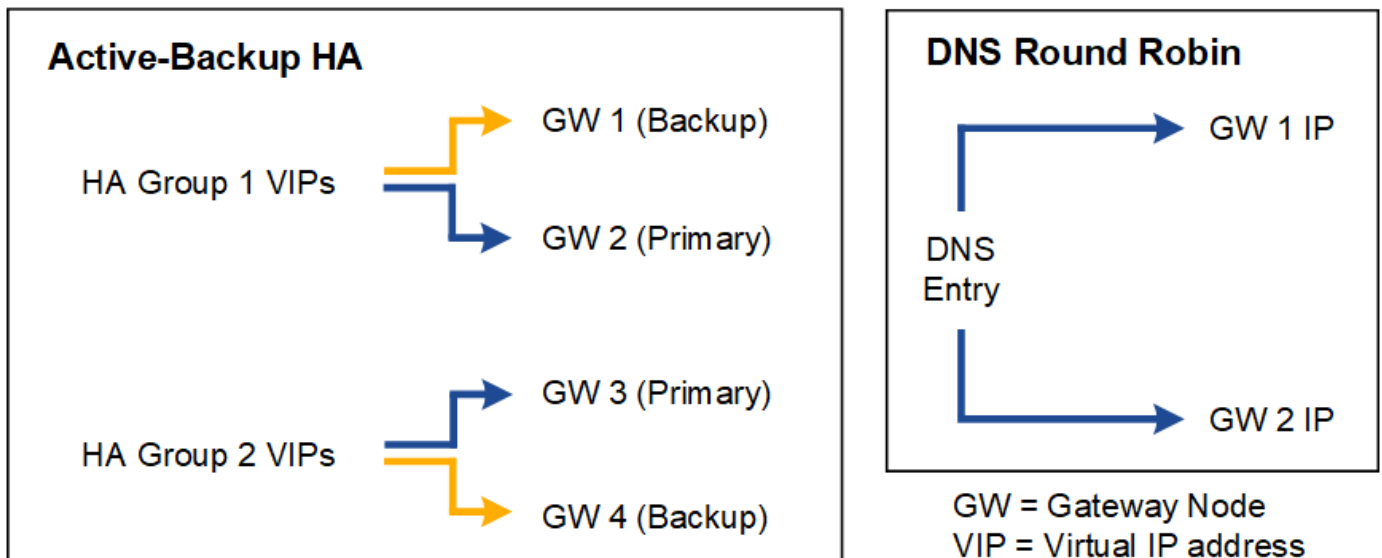


Il servizio CLB è obsoleto.

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

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

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.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un [browser web supportato](#).
- Si dispone dell'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 o CentOS (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

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

Inserire i dettagli del gruppo ha

1. Fornire un nome univoco per il gruppo ha.

×

Create a high availability group

1 Enter details

2 Add interfaces

3 Prioritize interfaces

4 Enter IP addresses

Enter details for the HA group

HA group name

Description (optional)

2. Facoltativamente, inserire una descrizione per il gruppo ha.
3. Selezionare **continua**.

Aggiungere interfacce al gruppo ha

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.

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

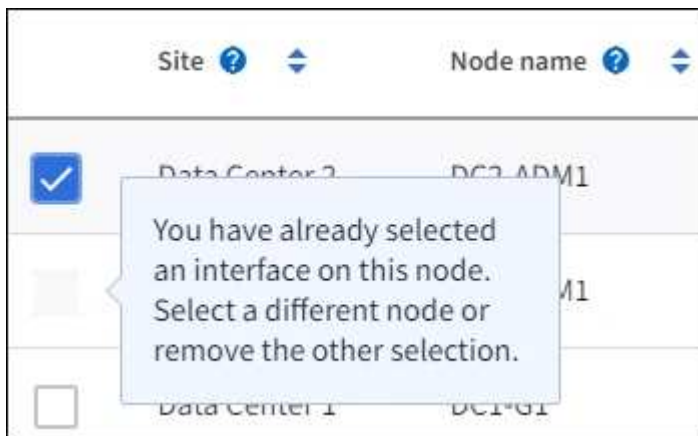
0 interfaces selected



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 il gruppo ha è per la protezione ha del servizio CLB obsoleto, selezionare le interfacce solo sui nodi gateway.
- 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 amministratore di backup non può eseguire tutte le procedure di manutenzione che il nodo amministratore 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

1. Determinare l'interfaccia primaria e le interfacce di backup (failover) per questo gruppo ha.

Trascinare e rilasciare le righe per modificare i valori nella colonna **Ordine di priorità**.

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 ?	Node	Interface ?	Node type ?
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.

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 primaria 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.

2. Selezionare **continua**.

Inserire gli indirizzi IP

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](#)

- 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.

- Inserire uno o più **indirizzi IP virtuali** per il gruppo ha. È possibile aggiungere fino a 10 indirizzi IP. Tutti i VIP devono trovarsi all'interno della subnet VIP.

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

- 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.



Attendere fino a 15 minuti per applicare le modifiche a un gruppo ha a tutti i nodi.

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.


High availability groups

[Learn more about HA groups](#)

You can group the network interfaces of multiple Admin and Gateway Nodes into a high availability (HA) group. If the active interface in the group fails, a backup interface can manage the workload.

Each HA group provides access to the shared services on the selected nodes. Select Gateway Nodes, Admin Nodes, or both for load balancing. Select Admin Nodes for management services. All interfaces in a group must be in the same subnet. You assign one or more virtual IP addresses (VIPs) to each group. Clients use these VIPs to connect to StorageGRID.

 You cannot select an interface if it has a DHCP-assigned IP address.

 Wait up to 15 minutes for changes to an HA group to be applied to all nodes.

Create

Actions ▾

Search...

Q

Total HA groups count: 2

<input type="checkbox"/>	Name ? ▴ ▾	Description ? ▴ ▾	Virtual IP address ? ▴ ▾	Interfaces (in priority order) ? ▴ ▾
<input type="checkbox"/>	FabricPool	Use for FabricPool client access	10.96.104.5 10.96.104.6	DC1-ADM1-104-96:eth2 (active) DC2-ADM1-104-103:eth2
<input type="checkbox"/>	S3 Clients	use for S3 client access	10.96.104.10	DC1-ADM1-104-96:eth0 DC2-ADM1-104-103:eth0

← Previous 1 Next →

2. Selezionare la casella di controllo relativa al 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 e rilasciare le righe per modificare l'ordine di priorità dell'interfaccia primaria e di qualsiasi interfaccia di backup per questo gruppo ha.
- d. Facoltativamente, aggiornare gli indirizzi IP virtuali.
- e. Selezionare **Salva**, quindi **fine**.



Attendere fino a 15 minuti per applicare le modifiche a un gruppo ha a tutti i nodi.

Rimuovere un gruppo ad alta disponibilità

È possibile rimuovere uno o più gruppi ad alta disponibilità (ha) alla volta. Tuttavia, non è possibile rimuovere un gruppo ha se è associato a uno o più endpoint del bilanciamento del carico.

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. Selezionare la casella di controllo per ciascun gruppo ha che si desidera rimuovere. Quindi, selezionare **azioni Rimuovi gruppo ha**.
3. 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

Gestire il bilanciamento del carico: Panoramica

È possibile utilizzare le funzioni di bilanciamento del carico di StorageGRID per gestire i carichi di lavoro di acquisizione e recupero dai client S3 e Swift. Il bilanciamento del carico massimizza la velocità e la capacità di connessione distribuendo i carichi di lavoro e le connessioni tra più nodi di storage.

Puoi bilanciare il carico dei carichi di lavoro dei client nei seguenti modi:

- Utilizzare il servizio Load Balancer, installato nei nodi Admin e nei nodi Gateway. Il servizio Load Balancer fornisce il bilanciamento del carico di livello 7 ed esegue la terminazione TLS delle richieste dei client, ispeziona le richieste e stabilisce nuove connessioni sicure ai nodi di storage. Si tratta del meccanismo di bilanciamento del carico consigliato.

Vedere [Come funziona il bilanciamento del carico - Servizio di bilanciamento del carico](#).

- Utilizzare il servizio di bilanciamento del carico di connessione (CLB) obsoleto, installato solo sui nodi

gateway. Il servizio CLB fornisce il bilanciamento del carico di livello 4 e supporta i costi di collegamento.

Vedere [Come funziona il bilanciamento del carico - servizio CLB \(obsoleto\)](#).

- Integrare un bilanciamento del carico di terze parti. Per ulteriori informazioni, contatta il tuo account rappresentante NetApp.

Come funziona il bilanciamento del carico - Servizio di bilanciamento del carico

Il servizio Load Balancer distribuisce le connessioni di rete in entrata dalle applicazioni client ai nodi di storage. Per abilitare il bilanciamento del carico, è necessario configurare gli endpoint del bilanciamento del carico utilizzando Grid Manager.

È possibile configurare gli endpoint del bilanciamento del carico solo per i nodi Admin o Gateway, poiché questi tipi di nodi contengono il servizio Load Balancer. Non è possibile configurare gli endpoint per i nodi di storage o i nodi di archiviazione.

Ogni endpoint del bilanciamento del carico specifica una porta, un protocollo di rete (HTTP o HTTPS), un tipo di client (S3 o Swift) e una modalità di binding. Gli endpoint HTTPS richiedono un certificato server. Le modalità di binding consentono di limitare l'accessibilità delle porte degli endpoint a:

- Gli indirizzi IP virtuali (VIP) di specifici gruppi ad alta disponibilità (ha)
- Interfacce di rete specifiche di nodi Admin e Gateway specifici

Considerazioni sulle porte

I client possono accedere a qualsiasi endpoint configurato su qualsiasi nodo che esegue il servizio Load Balancer, con due eccezioni: Le porte 80 e 443 sono riservate sui nodi di amministrazione, in modo che gli endpoint configurati su queste porte supportino le operazioni di bilanciamento del carico solo sui nodi gateway.

Se sono state rimappate delle porte, non è possibile utilizzare le stesse porte per configurare gli endpoint del bilanciamento del carico. È possibile creare endpoint utilizzando porte rimappate, ma tali endpoint verranno rimappati alle porte e al servizio CLB originali, non al servizio Load Balancer. Seguire la procedura descritta in [Rimuovere i rimap delle porte](#).



Il servizio CLB è obsoleto.

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.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un [browser web supportato](#).
- Si dispone dell'autorizzazione di accesso root.
- 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](#).

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`. Vedere [Configurare i nomi di dominio degli endpoint API S3](#).

Creare un endpoint per il bilanciamento del carico

Ogni endpoint del bilanciamento del carico specifica una porta, un tipo di client (S3 o Swift) e un protocollo di rete (HTTP o HTTPS).

Accedere alla procedura guidata

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

Inserire i dettagli dell'endpoint

1. Inserire i dettagli per l'endpoint.

×

Create a load balancer endpoint

1 Enter endpoint details

2 Select binding mode

3 Attach certificate

Endpoint details

Name ?

Port ?

Enter an unused port or accept the suggested port.

10443

Client type ?

Select the type of client application that will use this endpoint.

☒ S3
 ☐ Swift

Network protocol ?

Select the network protocol clients will use with this endpoint. If you select HTTPS, attach the security certificate before saving the endpoint.

☐ HTTPS (recommended)
 ☒ HTTP

Cancel

Continue

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint, che verrà visualizzato nella tabella della pagina endpoint del bilanciamento del carico.
Porta	<p>I client delle porte utilizzeranno per connettersi al servizio Load Balancer sui nodi Admin e sui nodi Gateway.</p> <p>Accettare il numero di porta consigliato o inserire una porta esterna non utilizzata da un altro servizio di rete. Inserire un valore compreso tra 1 e 65535.</p> <p>Se si immette 80 o 443, l'endpoint viene configurato solo sui nodi gateway. Queste porte sono riservate sui nodi di amministrazione.</p> <p>Vedere Linee guida per il networking per informazioni sulle porte esterne.</p>
Tipo di client	Il tipo di applicazione client che utilizzerà questo endpoint, S3 o Swift .

Campo	Descrizione
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"> • Selezionare HTTPS per la comunicazione sicura con crittografia TLS (scelta consigliata). È necessario allegare un certificato di sicurezza prima di poter salvare l'endpoint. • Selezionare HTTP per comunicazioni meno sicure e non crittografate. Utilizzare HTTP solo per una griglia non di produzione.

2. Selezionare **continua**.

Selezionare la modalità di binding

1. Selezionare una modalità di binding per l'endpoint per controllare le modalità di accesso all'endpoint.

Opzione	Descrizione
Globale (impostazione predefinita)	<p>I client possono accedere all'endpoint utilizzando un FQDN (Fully Qualified Domain Name), l'indirizzo IP di qualsiasi nodo gateway o nodo amministratore o l'indirizzo IP virtuale di qualsiasi gruppo ha su qualsiasi rete.</p> <p>Utilizzare l'impostazione Global (predefinita) a meno che non sia necessario limitare l'accessibilità di questo endpoint.</p>
Interfacce di nodo	<p>I client devono utilizzare l'indirizzo IP di un nodo e di un'interfaccia di rete selezionati per accedere a questo endpoint.</p>
IP virtuali dei gruppi ha	<p>I client devono utilizzare un indirizzo IP virtuale di un gruppo ha per accedere a questo endpoint.</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> <p>Gli endpoint con questa modalità possono utilizzare tutti lo stesso numero di porta purché le interfacce selezionate per gli endpoint non si sovrappongano.</p>



Se si utilizza la stessa porta per più di un endpoint, un endpoint che utilizza la modalità **Virtual IP of ha groups** sovrascrive un endpoint utilizzando la modalità **Node interfaces**, che sovrascrive un endpoint utilizzando la modalità **Global**.

2. 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.

Binding mode ?

Select a binding mode if you plan to monitor or limit the use of this endpoint with a traffic classification policy.

The binding mode controls how the endpoint is accessed—using any IP address or using specific IP addresses and network interfaces.

☐ Global ☒ Node interfaces ☐ Virtual IPs of HA groups

If you use the same port for more than one endpoint, an endpoint bound to HA groups overrides an endpoint bound to Node interfaces, which overrides a Global endpoint. If this behavior does not meet your requirements, consider using a different port number for each endpoint.

Search...

Total interface count: 3

<input type="checkbox"/>	Node ?	Node interface ?	Site ?	IP address ?	Node type ?
<input type="checkbox"/>	DC1-ADM1	eth0 ?	Data Center 1	172.16.3.246 and 2 more	Primary Admin Node
<input type="checkbox"/>	DC1-ADM1	eth1 ?	Data Center 1	10.224.3.246 and 5 more	Primary Admin Node
<input type="checkbox"/>	DC1-ADM1	eth2 ?	Data Center 1	47.47.3.246 and 3 more	Primary Admin Node

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

Binding mode ?

Select a binding mode if you plan to monitor or limit the use of this endpoint with a traffic classification policy.

The binding mode controls how the endpoint is accessed—using any IP address or using specific IP addresses and network interfaces.

☐ Global ☐ Node interfaces ☒ Virtual IPs of HA groups

If you use the same port for more than one endpoint, an endpoint bound to HA groups overrides an endpoint bound to Node interfaces, which overrides a Global endpoint. If this behavior does not meet your requirements, consider using a different port number for each endpoint.

Search...

Q

Total interface count: 2

<input type="checkbox"/>	Name ?	Description ?	Virtual IP address ?	Interfaces (in priority order) ?
<input type="checkbox"/>	FabricPool	Use for FabricPool client access	10.96.104.5 10.96.104.6	DC1-ADM1-104-96:eth2 (active) DC2-ADM1-104-103:eth2
<input type="checkbox"/>	S3 Clients	use for S3 client access	10.96.104.10	DC1-ADM1-104-96:eth0 DC2-ADM1-104-103:eth0

4. 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

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](#).

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 224 bit o superiori. 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 e l'endpoint.

Generare un certificato

- a. Selezionare **genera certificato**.
- b. Specificare le informazioni del certificato:
 - **Domain name**: 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.
 - **Oggetto**: Nome distinto (DN) o oggetto X.509 del proprietario del certificato.
 - **Giorni validi**: Numero di giorni successivi alla creazione della scadenza del certificato.
- 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 e questo endpoint.

[[dopo la fine]]al termine

1. Se si utilizza un sistema di nomi di dominio (DNS), assicurarsi che il DNS includa un record per associare il nome di dominio completo 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 qualsiasi nodo gateway o 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 inoltre possibile modificare il nome o la modalità di binding di un endpoint e aggiornare eventuali certificati associati.

Non è possibile modificare il tipo di servizio (S3 o Swift), la porta o il protocollo (HTTP o HTTPS).

- Per visualizzare le informazioni di base per tutti gli endpoint del bilanciamento del carico, consultare la tabella nella pagina endpoint del bilanciamento del carico.

Create

Actions ▾

Search...

🔍

Total endpoints count: 1

<input type="checkbox"/>	Name ? ▾	Port ? ▾	Network protocol ? ▾	Binding mode ? ▾	Certificate expiration ? ▾
<input type="checkbox"/>	FabricPool endpoint	10443	HTTPS	Global	Oct 19th, 2022

- Per visualizzare tutti i dettagli relativi a un endpoint specifico, inclusi i metadati del certificato, selezionare il nome dell'endpoint nella tabella.

FabricPool endpoint

Port: 10443
 Client type: S3
 Network protocol: HTTPS
 Binding mode: Global
 Endpoint ID: c2b6feb3-c567-449d-b717-4fed98c4a411

[Remove](#)

Binding Mode

[Certificate](#)

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 endpoint del bilanciamento del carico o nella pagina dei dettagli di un endpoint specifico.



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

Attività	Menu delle azioni	Pagina dei dettagli
Modificare il nome dell'endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare azioni Modifica nome endpoint . c. Inserire il nuovo nome. d. Selezionare Salva .	a. Selezionare il nome dell'endpoint per visualizzare i dettagli. b. Selezionare l'icona di modifica  . c. Inserire il nuovo nome. d. Selezionare Salva .
Modificare la modalità di associazione degli endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare Actions Edit endpoint binding mode . c. Aggiornare la modalità di binding secondo necessità. d. Selezionare Save Changes (Salva modifiche).	a. Selezionare il nome dell'endpoint per visualizzare i dettagli. b. Selezionare Edit binding mode (Modifica modalità di associazione). c. Aggiornare la modalità di binding secondo necessità. d. Selezionare Save Changes (Salva modifiche).

Attività	Menu delle azioni	Pagina dei dettagli
Modificare il certificato dell'endpoint	<ul style="list-style-type: none"> a. Selezionare la casella di controllo per l'endpoint. b. Selezionare azioni Modifica certificato endpoint. c. Caricare o generare un nuovo certificato personalizzato o iniziare a utilizzare il certificato globale S3 e Swift, come richiesto. d. Selezionare Save Changes (Salva modifiche). 	<ul style="list-style-type: none"> a. Selezionare il nome dell'endpoint per visualizzare i dettagli. b. Selezionare la scheda certificato. c. Selezionare Modifica certificato. d. Caricare o generare un nuovo certificato personalizzato o iniziare a utilizzare il certificato globale S3 e Swift, come richiesto. e. Selezionare Save Changes (Salva modifiche).

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.

- 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**.

Come funziona il bilanciamento del carico - servizio CLB (obsoleto)

Il servizio di bilanciamento del carico di connessione (CLB) sui nodi gateway è obsoleto. Il servizio Load Balancer è ora il meccanismo di bilanciamento del carico consigliato.

Il servizio CLB utilizza il bilanciamento del carico di livello 4 per distribuire le connessioni di rete TCP in entrata dalle applicazioni client al nodo di storage ottimale in base alla disponibilità, al carico di sistema e al costo del collegamento configurato dall'amministratore. Quando si sceglie il nodo di storage ottimale, il servizio CLB stabilisce una connessione di rete bidirezionale e inoltra il traffico da e verso il nodo selezionato. La CLB non prende in considerazione la configurazione Grid Network quando indirizza le connessioni di rete in entrata.

Per visualizzare le informazioni sul servizio CLB, selezionare **SUPPORT Tools Grid topology**, quindi espandere un nodo gateway fino a quando non è possibile selezionare **CLB** e le opzioni sottostanti.

Storage Capacity		
Storage Nodes Installed:	N/A	
Storage Nodes Readable:	N/A	
Storage Nodes Writable:	N/A	
Installed Storage Capacity:	N/A	
Used Storage Capacity:	N/A	
Used Storage Capacity for Data:	N/A	
Used Storage Capacity for Metadata:	N/A	
Usable Storage Capacity:	N/A	

Se si sceglie di utilizzare il servizio CLB, si consiglia di configurare i costi di collegamento per il sistema StorageGRID.

- [Quali sono i costi di collegamento](#)
- [Aggiornare i costi dei collegamenti](#)

Configurare i nomi di dominio degli endpoint API S3

Per supportare le richieste in stile host virtuale S3, è necessario utilizzare Grid Manager per configurare l'elenco dei nomi di dominio degli endpoint a cui si connettono i client S3.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un [browser web supportato](#).
- Si dispone di 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 sia 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 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 in modo da riconoscere nomi di dominio degli endpoint diversi.
- I client che si connettono a un endpoint di bilanciamento del carico, direttamente a un nodo di storage o direttamente al servizio CLB obsoleto su un nodo gateway possono personalizzare il certificato globale S3 e Swift API per includere tutti i nomi di dominio degli endpoint richiesti.

Fasi

1. Selezionare **CONFIGURAZIONE rete nomi di dominio**.

Viene visualizzata la pagina Endpoint Domain Names (nomi dominio endpoint).

Endpoint Domain Names

Virtual Hosted-Style Requests

Enable support of S3 virtual hosted-style requests by specifying API endpoint domain names. Support is disabled if this list is empty. Examples: s3.example.com, s3.example.co.uk, s3-east.example.com

Endpoint 1	<input type="text" value="s3.example.com"/>	✕
Endpoint 2	<input type="text"/>	+ ✕

2. Immettere l'elenco dei nomi di dominio degli endpoint API S3 nei campi **Endpoint**. Utilizzare **+** per aggiungere altri campi.

Se l'elenco è vuoto, il supporto per le richieste di tipo host virtuale S3 viene disattivato.

3. Selezionare **Salva**.

4. Assicurarsi che i certificati server utilizzati dai client corrispondano ai nomi di dominio degli endpoint 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 API globale S3 e Swift, direttamente ai nodi di storage o al servizio CLB sui nodi gateway, aggiornare il certificato API globale S3 e Swift.

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.

Informazioni correlate

- [Utilizzare S3](#)
- [Visualizzare gli indirizzi IP](#)
- [Configurare i gruppi ad alta disponibilità](#)
- [Configurare i certificati API S3 e Swift](#)
- [Configurare gli endpoint del bilanciamento del carico](#)

Abilitare HTTP per le comunicazioni client

Per impostazione predefinita, le applicazioni client utilizzano il protocollo di rete HTTPS per tutte le connessioni ai nodi di storage o al servizio CLB obsoleto sui nodi gateway. È possibile attivare il protocollo HTTP per queste connessioni, ad esempio durante il test di un grid non di produzione.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un [browser web supportato](#).
- Si dispone di autorizzazioni di accesso specifiche.

A proposito di questa attività

Completare questa attività solo se i client S3 e Swift devono stabilire connessioni HTTP direttamente ai nodi di storage o al servizio CLB obsoleto sui nodi gateway.

Non è necessario completare questa attività per i client che utilizzano solo connessioni HTTPS o per i client che si connettono al servizio Load Balancer (poiché è possibile configurare ciascun endpoint Load Balancer in modo che utilizzi HTTP o HTTPS). Per ulteriori informazioni, vedere le informazioni sulla configurazione degli endpoint del bilanciamento del carico.

Vedere [Riepilogo: Indirizzi IP e porte per le connessioni client](#) Per sapere quali porte S3 e i client Swift utilizzano per la connessione ai nodi di storage o al servizio CLB obsoleto utilizzando HTTP o HTTPS



Prestare attenzione quando si attiva HTTP per una griglia di produzione perché le richieste verranno inviate senza crittografia.

Fasi

1. Selezionare **CONFIGURAZIONE sistema Opzioni griglia**.
2. Nella sezione Opzioni di rete, selezionare la casella di controllo **attiva connessione HTTP**.

Network Options

Prevent Client Modification ?



Enable HTTP Connection ?



Network Transfer Encryption ?



AES128-SHA



AES256-SHA

3. Selezionare **Salva**.

Informazioni correlate

- [Configurare gli endpoint del bilanciamento del carico](#)
- [Utilizzare S3](#)
- [USA Swift](#)

Controllare quali operazioni client sono consentite

È possibile selezionare l'opzione Impedisci modifica client per negare specifiche operazioni del client HTTP.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un [browser web supportato](#).
- Si dispone di autorizzazioni di accesso specifiche.

A proposito di questa attività

Impedisci modifica client è un'impostazione a livello di sistema. Quando si seleziona l'opzione Impedisci modifica client, le seguenti richieste vengono rifiutate:

- **S3 REST API**

- Elimina richieste bucket
- Qualsiasi richiesta di modifica dei dati di un oggetto esistente, dei metadati definiti dall'utente o del tagging degli oggetti S3



Questa impostazione non si applica ai bucket con versione attivata. Il controllo delle versioni impedisce già le modifiche ai dati degli oggetti, ai metadati definiti dall'utente e all'etichettatura degli oggetti.

- **API REST Swift**

- Eliminare le richieste di container
- Richiede di modificare qualsiasi oggetto esistente. Ad esempio, le seguenti operazioni sono negate: Put Overwrite (Inserisci sovrascrittura), Delete (Elimina), Metadata Update (aggiornamento metadati) e così via.

Fasi

1. Selezionare **CONFIGURAZIONE sistema Opzioni griglia**.
2. Nella sezione Opzioni di rete, selezionare la casella di controllo **Impedisci modifica client**.

Network Options

Prevent Client Modification



Enable HTTP Connection



Network Transfer Encryption



☐ AES128-SHA

☒ AES256-SHA

3. Selezionare **Salva**.

Informazioni sul copyright

Copyright © 2025 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.