



Configurare e gestire

StorageGRID software

NetApp
December 03, 2025

Sommario

Configurare e gestire un sistema StorageGRID	1
Amministra StorageGRID	1
Amministra StorageGRID	1
Inizia con Grid Manager	1
Controlla l'accesso a StorageGRID	32
Utilizzare la federazione di griglia	80
Gestire la sicurezza	117
Gestire gli inquilini	184
Configurare le connessioni client	204
Gestire reti e connessioni	245
Utilizzare AutoSupport	264
Gestisci nodi di archiviazione	279
Gestisci nodi amministrativi	293
Gestire gli oggetti con ILM	296
Gestire gli oggetti con ILM	296
ILM e ciclo di vita degli oggetti	297
Creare e assegnare gradi di archiviazione	319
Utilizzare pool di archiviazione	322
Utilizzare i pool di archiviazione cloud	330
Gestisci i profili di codifica di cancellazione	350
Configurare le regioni (facoltativo e solo S3)	354
Crea regola ILM	355
Gestire le policy ILM	372
Lavorare con le policy e le regole ILM	388
Utilizzare il blocco oggetto S3	392
Esempio di regole e policy ILM	400
Rafforzamento del sistema	421
Considerazioni generali per il rafforzamento del sistema	421
Linee guida per il rafforzamento degli aggiornamenti software	422
Linee guida per il rafforzamento delle reti StorageGRID	423
Linee guida per il rafforzamento dei nodi StorageGRID	424
Linee guida per il rafforzamento di TLS e SSH	427
Altre linee guida per il rafforzamento	428
Configurare StorageGRID per FabricPool	429
Configurare StorageGRID per FabricPool	429
Informazioni necessarie per collegare StorageGRID come livello cloud	431
Utilizzare la procedura guidata di configurazione FabricPool	432
Configurare StorageGRID manualmente	446
Configurare ONTAP System Manager	456
Configurare il server DNS	458
Le migliori pratiche StorageGRID per FabricPool	459
Rimuovere i dati FabricPool da StorageGRID	463

Configurare e gestire un sistema StorageGRID

Amministra StorageGRID

Amministra StorageGRID

Utilizzare queste istruzioni per configurare e amministrare un sistema StorageGRID .

Informazioni su queste istruzioni

Le attività principali per la configurazione e l'amministrazione StorageGRID consentono di:

- Utilizzare Grid Manager per impostare gruppi e utenti
- Creare account tenant per consentire alle applicazioni client S3 di archiviare e recuperare oggetti
- Configurare e gestire le reti StorageGRID
- Configura AutoSupport
- Gestisci le impostazioni del nodo

Prima di iniziare

- Hai una conoscenza generale del sistema StorageGRID .
- Hai una conoscenza abbastanza approfondita delle shell dei comandi Linux, delle reti e della configurazione e installazione dell'hardware del server.

Inizia con Grid Manager

Requisiti del browser web

È necessario utilizzare un browser web supportato.

browser web	Versione minima supportata
Google Chrome	119
Microsoft Edge	119
Mozilla Firefox	119

Dovresti impostare la larghezza consigliata per la finestra del browser.

Larghezza del browser	Pixel
Minimo	1024
Ottimale	1280

Sign in a Grid Manager

Per accedere alla pagina di accesso di Grid Manager, è necessario immettere il nome di dominio completo (FQDN) o l'indirizzo IP di un nodo di amministrazione nella barra degli indirizzi di un browser Web supportato.

Ogni sistema StorageGRID include un nodo amministrativo primario e un numero qualsiasi di nodi amministrativi non primari. È possibile accedere a Grid Manager su qualsiasi nodo di amministrazione per gestire il sistema StorageGRID. Tuttavia, alcune procedure di manutenzione possono essere eseguite solo dal nodo di amministrazione primario.

Connettiti al gruppo HA

Se i nodi amministrativi sono inclusi in un gruppo ad alta disponibilità (HA), la connessione avviene tramite l'indirizzo IP virtuale del gruppo HA o un nome di dominio completo mappato all'indirizzo IP virtuale. Il nodo di amministrazione primario dovrebbe essere selezionato come interfaccia primaria del gruppo, in modo che quando si accede a Grid Manager, si acceda al nodo di amministrazione primario, a meno che il nodo di amministrazione primario non sia disponibile. Vedere ["Gestire gruppi ad alta disponibilità"](#).

Utilizzare SSO

I passaggi di accesso sono leggermente diversi se ["è stato configurato l'accesso singolo \(SSO\)"](#).

Sign in a Grid Manager sul primo nodo di amministrazione

Prima di iniziare

- Hai le tue credenziali di accesso.
- Stai utilizzando un ["browser web supportato"](#).
- I cookie sono abilitati nel tuo browser web.
- Appartieni a un gruppo di utenti che ha almeno un'autorizzazione.
- Hai l'URL per Grid Manager:

```
https://FQDN_or_Admin_Node_IP/
```

È possibile utilizzare il nome di dominio completo, l'indirizzo IP di un nodo di amministrazione o l'indirizzo IP virtuale di un gruppo HA di nodi di amministrazione.

Per accedere a Grid Manager su una porta diversa da quella predefinita per HTTPS (443), includere il numero di porta nell'URL:

```
https://FQDN_or_Admin_Node_IP:port/
```



SSO non è disponibile sulla porta riservata di Grid Manager. È necessario utilizzare la porta 443.

Passi

1. Avviare un browser web supportato.
2. Nella barra degli indirizzi del browser, inserisci l'URL di Grid Manager.
3. Se viene visualizzato un avviso di sicurezza, installare il certificato utilizzando la procedura guidata di installazione del browser. Vedere ["Gestire i certificati di sicurezza"](#).

4. Sign in a Grid Manager.

La schermata di accesso visualizzata dipende dalla configurazione dell'accesso singolo (SSO) per StorageGRID.

Non si utilizza SSO

- a. Inserisci il tuo nome utente e la password per Grid Manager.
- b. Seleziona **Accedi**.



The screenshot shows the login interface for NetApp StorageGRID Grid Manager. At the top, the logo "NetApp StorageGRID®" is displayed, followed by the title "Grid Manager". Below the title, there are two input fields: "Username" and "Password". The "Username" field is currently empty with a cursor at the start. Below the "Password" field is a blue "Sign in" button. At the bottom of the form, there are three links: "Tenant sign in", "NetApp support", and "NetApp.com".

Utilizzo di SSO

- Se StorageGRID utilizza SSO e questa è la prima volta che accedi all'URL su questo browser:
 - i. Seleziona * Sign in*. Puoi lasciare lo 0 nel campo Account.



Sign in

Account

Sign in

[NetApp support](#) | [NetApp.com](#)

- ii. Inserisci le tue credenziali SSO standard nella pagina di accesso SSO della tua organizzazione. Per esempio:

Sign in with your organizational account

Sign in

- Se StorageGRID utilizza SSO e in precedenza hai effettuato l'accesso a Grid Manager o a un account tenant:
 - i. Inserisci **0** (ID account per Grid Manager) oppure seleziona **Grid Manager** se compare nell'elenco degli account recenti.

The image shows a web interface for NetApp StorageGRID. At the top, there is a logo consisting of a square icon followed by the text "NetApp StorageGRID®". Below the logo is the heading "Sign in". Underneath the heading, there is a section labeled "Recent" which contains a dropdown menu with the text "Grid Manager" and a downward arrow. Below this is a section labeled "Account" which contains a text input field with the number "0". At the bottom of the form is a blue button with the text "Sign in". Below the button, there is a link that says "NetApp support | NetApp.com".

NetApp StorageGRID®

Sign in

Recent

Grid Manager ▼

Account

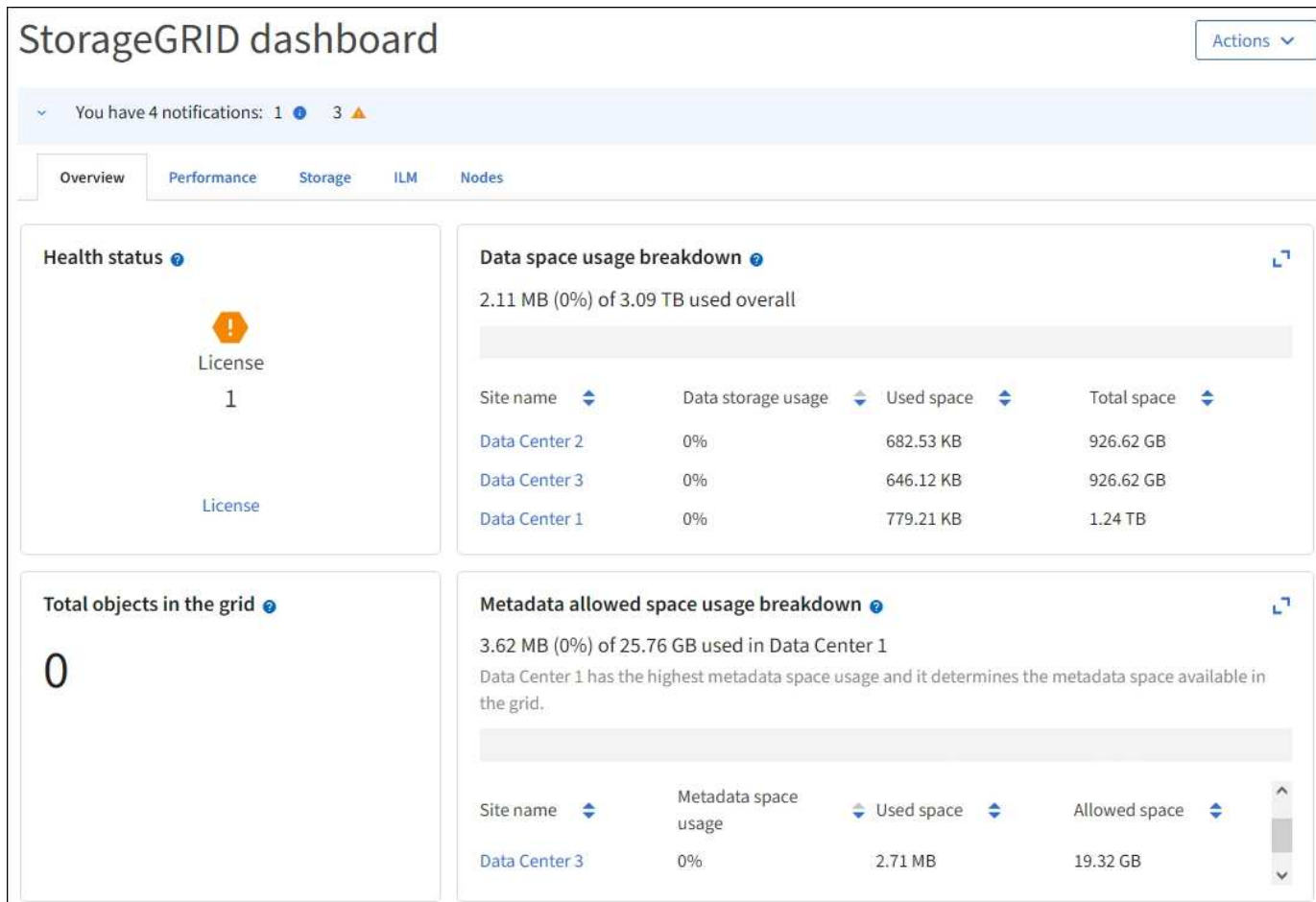
0

Sign in

[NetApp support](#) | [NetApp.com](#)

- ii. Seleziona * Sign in*.
- iii. Sign in con le tue credenziali SSO standard alla pagina di accesso SSO della tua organizzazione.

Dopo aver effettuato l'accesso, viene visualizzata la home page di Grid Manager, che include la dashboard. Per sapere quali informazioni sono fornite, vedere ["Visualizza e gestisci la dashboard"](#) .



Accedi a un altro nodo di amministrazione

Per accedere a un altro nodo di amministrazione, seguire questi passaggi.

Non si utilizza SSO

Passi

1. Nella barra degli indirizzi del browser, inserisci il nome di dominio completo o l'indirizzo IP dell'altro nodo di amministrazione. Includere il numero di porta, se necessario.
2. Inserisci il tuo nome utente e la password per Grid Manager.
3. Seleziona **Accedi**.

Utilizzo di SSO

Se StorageGRID utilizza SSO e hai effettuato l'accesso a un nodo amministrativo, puoi accedere ad altri nodi amministrativi senza dover effettuare nuovamente l'accesso.

Passi

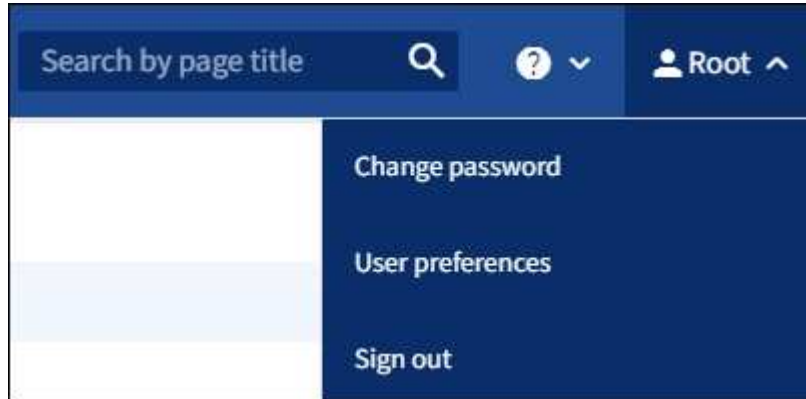
1. Inserisci il nome di dominio completo o l'indirizzo IP dell'altro nodo di amministrazione nella barra degli indirizzi del browser.
2. Se la sessione SSO è scaduta, inserisci nuovamente le tue credenziali.

Esci da Grid Manager

Una volta terminato di lavorare con Grid Manager, è necessario disconnettersi per impedire agli utenti non autorizzati di accedere al sistema StorageGRID . In base alle impostazioni dei cookie del browser, la chiusura del browser potrebbe non comportare la disconnessione dal sistema.

Passi

1. Seleziona il tuo nome utente nell'angolo in alto a destra.



2. Seleziona **Esci**.

Opzione	Descrizione
SSO non in uso	Hai effettuato la disconnessione dal nodo di amministrazione. Viene visualizzata la pagina di accesso di Grid Manager. Nota: se hai effettuato l'accesso a più di un nodo di amministrazione, devi disconnetterti da ciascun nodo.
SSO abilitato	Hai effettuato l'uscita da tutti i nodi amministrativi a cui stavi accedendo. Viene visualizzata la pagina di accesso a StorageGRID . Grid Manager è elencato come predefinito nel menu a discesa Account recenti e il campo ID account mostra 0. Nota: se l'SSO è abilitato e hai effettuato l'accesso anche a Tenant Manager, devi anche "uscire dall'account dell'inquilino" A "uscire da SSO" .

Cambia la tua password

Se sei un utente locale di Grid Manager, puoi modificare la tua password.

Prima di iniziare

Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .

Informazioni su questo compito

Se accedi a StorageGRID come utente federato o se è abilitato l'accesso singolo (SSO), non puoi modificare

la password in Grid Manager. In alternativa, è necessario modificare la password nella fonte di identità esterna, ad esempio Active Directory o OpenLDAP.

Passi

1. Dall'interfaccia Grid Manager, seleziona **il tuo nome** > **Cambia password**.
2. Inserisci la tua password attuale.
3. Digita una nuova password.

La password deve contenere almeno 8 e non più di 32 caratteri. Le password sono sensibili alle maiuscole e alle minuscole.

4. Reinserisci la nuova password.
5. Seleziona **Salva**.

Visualizza le informazioni sulla licenza StorageGRID

Ogni volta che è necessario, è possibile visualizzare le informazioni sulla licenza del sistema StorageGRID , ad esempio la capacità di archiviazione massima della griglia.

Prima di iniziare

Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .

Informazioni su questo compito

Se si verifica un problema con la licenza software per questo sistema StorageGRID , la scheda Stato di integrità nella dashboard include un'icona Stato licenza e un collegamento **Licenza**. Il numero indica il numero di problemi relativi alla licenza.



Passi

1. Accedi alla pagina Licenza eseguendo una delle seguenti operazioni:
 - Selezionare **MANUTENZIONE** > **Sistema** > **Licenza**.
 - Dalla scheda Stato di integrità nella dashboard, seleziona l'icona Stato licenza o il collegamento **Licenza**.

Questo collegamento appare solo se c'è un problema con la licenza.

2. Visualizza i dettagli di sola lettura per la licenza corrente:

- ID di sistema StorageGRID , ovvero il numero di identificazione univoco per questa installazione StorageGRID
- Numero di serie della licenza
- Tipo di licenza, **Perpetua** o **Abbonamento**
- Capacità di stoccaggio autorizzata della rete
- Capacità di archiviazione supportata
- Data di scadenza della licenza. **N/D** appare per una licenza perpetua.
- Data di fine del supporto

Questa data viene letta dal file di licenza corrente e potrebbe non essere aggiornata se hai esteso o rinnovato il contratto di assistenza dopo aver ottenuto il file di licenza. Per aggiornare questo valore, vedere ["Aggiorna le informazioni sulla licenza StorageGRID"](#) . È anche possibile visualizzare la data di fine effettiva del contratto utilizzando Active IQ.

- Contenuto del file di testo della licenza

Aggiorna le informazioni sulla licenza StorageGRID

È necessario aggiornare le informazioni sulla licenza del sistema StorageGRID ogni volta che cambiano i termini della licenza. Ad esempio, è necessario aggiornare le informazioni sulla licenza se si acquista capacità di archiviazione aggiuntiva per la propria rete.

Prima di iniziare

- Hai un nuovo file di licenza da applicare al tuo sistema StorageGRID .
- Hai ["autorizzazioni di accesso specifiche"](#) .
- Hai la passphrase di provisioning.

Passi

1. Selezionare **MANUTENZIONE > Sistema > Licenza**.
2. Nella sezione Aggiorna licenza, seleziona **Sfoglia**.
3. Individuare e selezionare il nuovo file di licenza(.txt).

Il nuovo file di licenza viene convalidato e visualizzato.

4. Immettere la passphrase di provisioning.
5. Seleziona **Salva**.

Utilizzare la API

Utilizzare l'API di gestione della griglia

È possibile eseguire attività di gestione del sistema utilizzando l'API REST di Grid Management anziché l'interfaccia utente di Grid Manager. Ad esempio, potresti voler utilizzare l'API per automatizzare le operazioni o per creare più entità, come gli utenti, più rapidamente.

Risorse di alto livello

L'API di gestione della griglia fornisce le seguenti risorse di primo livello:

- `/grid`: L'accesso è limitato agli utenti di Grid Manager e si basa sulle autorizzazioni di gruppo configurate.
- `/org`: L'accesso è limitato agli utenti che appartengono a un gruppo LDAP locale o federato per un account tenant. Per maggiori dettagli, vedere ["Utilizzare un account tenant"](#).
- `/private`: L'accesso è limitato agli utenti di Grid Manager e si basa sulle autorizzazioni di gruppo configurate. Le API private sono soggette a modifiche senza preavviso. Anche gli endpoint privati StorageGRID ignorano la versione API della richiesta.

Inviare richieste API

L'API Grid Management utilizza la piattaforma API open source Swagger. Swagger fornisce un'interfaccia utente intuitiva che consente agli sviluppatori e ai non sviluppatori di eseguire operazioni in tempo reale in StorageGRID tramite l'API.

L'interfaccia utente di Swagger fornisce dettagli e documentazione completi per ogni operazione API.

Prima di iniziare

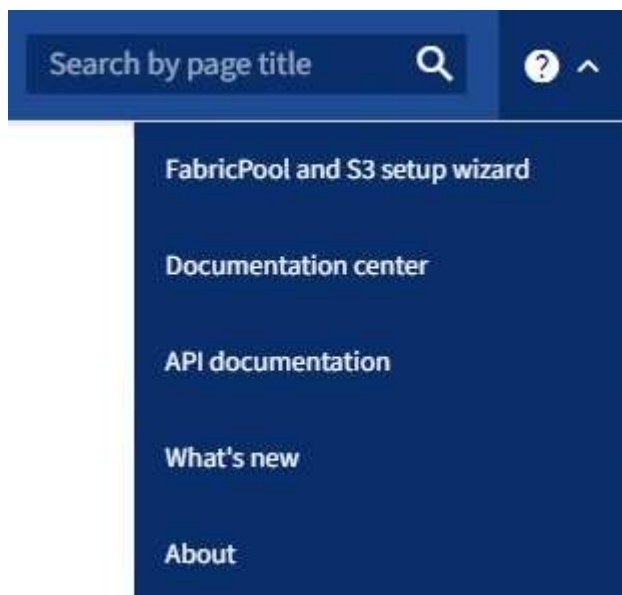
- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai ["autorizzazioni di accesso specifiche"](#).



Tutte le operazioni API eseguite tramite la pagina web Documentazione API sono operazioni live. Fare attenzione a non creare, aggiornare o eliminare per errore dati di configurazione o altri dati.

Passi

1. Dall'interfaccia di Grid Manager, seleziona l'icona della guida e seleziona **Documentazione API**.



2. Per eseguire un'operazione con l'API privata, seleziona **Vai alla documentazione dell'API privata** nella pagina dell'API di gestione StorageGRID.

Le API private sono soggette a modifiche senza preavviso. Anche gli endpoint privati StorageGRID

ignorano la versione API della richiesta.

3. Selezionare l'operazione desiderata.

Quando si espande un'operazione API, è possibile visualizzare le azioni HTTP disponibili, come GET, PUT, UPDATE e DELETE.

4. Selezionare un'azione HTTP per visualizzare i dettagli della richiesta, tra cui l'URL dell'endpoint, un elenco di eventuali parametri obbligatori o facoltativi, un esempio del corpo della richiesta (se necessario) e le possibili risposte.

groups Operations on groups

GET /grid/groups Lists Grid Administrator Groups

Parameters Try it out

Name	Description
type string (query)	filter by group type Available values : local, federated --
limit integer (query)	maximum number of results Default value : 25 25
marker string (query)	marker-style pagination offset (value is Group's URN) marker - marker-style pagination offset (value
includeMarker boolean (query)	If set, the marker element is also returned --
order string (query)	pagination order (desc requires marker) Available values : asc, desc --

Responses Response content type application/json

Code	Description
200	successfully retrieved Example Value Model <pre>{ "responseTime": "2021-03-29T14:22:19.673Z", "status": "success", "apiVersion": "3.3", "deprecated": false, "data": [{ "displayName": "Developers", </pre>

5. Determina se la richiesta richiede parametri aggiuntivi, come un gruppo o un ID utente. Quindi, ottieni questi valori. Potrebbe essere necessario inviare prima una richiesta API diversa per ottenere le

informazioni necessarie.

6. Determina se è necessario modificare il corpo della richiesta di esempio. In tal caso, puoi selezionare **Modello** per conoscere i requisiti per ciascun campo.
7. Seleziona **Provalo**.
8. Fornire tutti i parametri richiesti o modificare il corpo della richiesta come richiesto.
9. Selezionare **Esegui**.
10. Esaminare il codice di risposta per determinare se la richiesta è andata a buon fine.

Operazioni dell'API di gestione della griglia

L'API di gestione della griglia organizza le operazioni disponibili nelle seguenti sezioni.



Questo elenco include solo le operazioni disponibili nell'API pubblica.

- **account**: operazioni per gestire gli account dei tenant di archiviazione, tra cui la creazione di nuovi account e il recupero dell'utilizzo dello spazio di archiviazione per un determinato account.
- **alert-history**: Operazioni sugli avvisi risolti.
- **alert-receivers**: Operazioni sui destinatari delle notifiche di avviso (e-mail).
- **alert-rules**: Operazioni sulle regole di avviso.
- **alert-silences**: Operazioni sui silenzi degli avvisi.
- **avvisi**: Operazioni sugli avvisi.
- **audit**: Operazioni per elencare e aggiornare la configurazione di audit.
- **auth**: Operazioni per eseguire l'autenticazione della sessione utente.

L'API di gestione della griglia supporta lo schema di autenticazione Bearer Token. Per effettuare l'accesso, è necessario fornire un nome utente e una password nel corpo JSON della richiesta di autenticazione (ovvero, `POST /api/v3/authorize`). Se l'utente viene autenticato correttamente, viene restituito un token di sicurezza. Questo token deve essere fornito nell'intestazione delle successive richieste API ("`Authorization: Bearer token`"). Il token scade dopo 16 ore.



Se per il sistema StorageGRID è abilitato l'accesso Single Sign-On, è necessario eseguire diversi passaggi per l'autenticazione. Vedere "Autenticazione all'API se è abilitato l'accesso singolo".

Per informazioni su come migliorare la sicurezza dell'autenticazione, vedere "Protezione contro la falsificazione delle richieste tra siti".

- **client-certificates**: Operazioni per configurare i certificati client in modo che StorageGRID sia accessibile in modo sicuro tramite strumenti di monitoraggio esterni.
- **config**: Operazioni relative alla versione del prodotto e alle versioni dell'API di gestione della griglia. È possibile elencare la versione di rilascio del prodotto e le versioni principali dell'API Grid Management supportate da tale versione, nonché disabilitare le versioni obsolete dell'API.
- **deactivated-features**: Operazioni per visualizzare le funzionalità che potrebbero essere state disattivate.
- **dns-servers**: Operazioni per elencare e modificare i server DNS esterni configurati.
- **drive-details**: Operazioni sulle unità per modelli specifici di dispositivi di archiviazione.

- **endpoint-domain-names**: Operazioni per elencare e modificare i nomi di dominio degli endpoint S3.
- **erasure-coding**: Operazioni sui profili di codifica di cancellazione.
- **espansione**: Operazioni di espansione (a livello di procedura).
- **expansion-nodes**: Operazioni di espansione (a livello di nodo).
- **expansion-sites**: Operazioni di espansione (a livello di sito).
- **grid-networks**: Operazioni per elencare e modificare l'elenco delle reti di griglia.
- **grid-passwords**: Operazioni per la gestione delle password della griglia.
- **gruppi**: operazioni per gestire i gruppi di amministratori di griglia locali e per recuperare i gruppi di amministratori di griglia federati da un server LDAP esterno.
- **identity-source**: Operazioni per configurare una fonte di identità esterna e per sincronizzare manualmente le informazioni sui gruppi federati e sugli utenti.
- **ilm**: Operazioni sulla gestione del ciclo di vita delle informazioni (ILM).
- **in-progress-procedures**: Recupera le procedure di manutenzione attualmente in corso.
- **licenza**: Operazioni per recuperare e aggiornare la licenza StorageGRID .
- **logs**: Operazioni per la raccolta e il download dei file di registro.
- **metriche**: operazioni sulle metriche StorageGRID , tra cui query di metriche istantanee in un singolo punto nel tempo e query di metriche di intervallo in un intervallo di tempo. L'API di gestione della griglia utilizza lo strumento di monitoraggio dei sistemi Prometheus come fonte di dati backend. Per informazioni sulla creazione di query Prometheus, consultare il sito web di Prometheus.



Metriche che includono *private* nei loro nomi sono destinati esclusivamente all'uso interno. Queste metriche sono soggette a modifiche tra le versioni StorageGRID senza preavviso.

- **node-details**: Operazioni sui dettagli del nodo.
- **node-health**: Operazioni sullo stato di integrità del nodo.
- **node-storage-state**: Operazioni sullo stato di archiviazione del nodo.
- **nntp-servers**: operazioni per elencare o aggiornare i server NTP (Network Time Protocol) esterni.
- **oggetti**: Operazioni sugli oggetti e sui metadati degli oggetti.
- **recovery**: Operazioni per la procedura di recupero.
- **recovery-package**: Operazioni per scaricare il pacchetto di ripristino.
- **regioni**: Operazioni per visualizzare e creare regioni.
- **s3-object-lock**: Operazioni sulle impostazioni globali di S3 Object Lock.
- **server-certificate**: Operazioni per visualizzare e aggiornare i certificati del server Grid Manager.
- **snmp**: Operazioni sulla configurazione SNMP corrente.
- **storage-watermarks**: Filigrane del nodo di archiviazione.
- **traffic-classes**: Operazioni per le policy di classificazione del traffico.
- **untrusted-client-network**: Operazioni sulla configurazione della rete client non attendibile.
- **utenti**: operazioni per visualizzare e gestire gli utenti di Grid Manager.

Controllo delle versioni dell'API di gestione della griglia

L'API di gestione della griglia utilizza il controllo delle versioni per supportare aggiornamenti senza interruzioni.

Ad esempio, questo URL di richiesta specifica la versione 4 dell'API.

```
https://hostname_or_ip_address/api/v4/authorize
```

La versione principale dell'API viene aggiornata quando vengono apportate modifiche che non sono compatibili con le versioni precedenti. La versione secondaria dell'API viene aggiornata quando vengono apportate modifiche *compatibili* con le versioni precedenti. Le modifiche compatibili includono l'aggiunta di nuovi endpoint o nuove proprietà.

L'esempio seguente illustra come la versione dell'API viene aumentata in base al tipo di modifiche apportate.

Tipo di modifica all'API	Vecchia versione	Nuova versione
Compatibile con le versioni precedenti	2,1	2,2
Non compatibile con le versioni precedenti	2,1	3,0

Quando si installa il software StorageGRID per la prima volta, viene abilitata solo la versione più recente dell'API. Tuttavia, quando si esegue l'aggiornamento a una nuova versione delle funzionalità di StorageGRID, si continua ad avere accesso alla versione API precedente per almeno una versione delle funzionalità StorageGRID.



È possibile configurare le versioni supportate. Consultare la sezione **config** della documentazione dell'API Swagger per "[API di gestione della griglia](#)" per maggiori informazioni. Dopo aver aggiornato tutti i client API per utilizzare la versione più recente, è necessario disattivare il supporto per la versione precedente.

Le richieste obsolete vengono contrassegnate come obsolete nei seguenti modi:

- L'intestazione della risposta è "Obsoleto: vero"
- Il corpo della risposta JSON include "deprecated": true
- Un avviso obsoleto è stato aggiunto a nms.log. Per esempio:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Determina quali versioni API sono supportate nella versione corrente

Utilizzare il GET `/versions` Richiesta API per restituire un elenco delle principali versioni API supportate. Questa richiesta si trova nella sezione **config** della documentazione dell'API Swagger.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Specificare una versione API per una richiesta

È possibile specificare la versione API utilizzando un parametro di percorso(/api/v4) o un'intestazione(Api-Version: 4). Se si specificano entrambi i valori, il valore dell'intestazione sovrascrive il valore del percorso.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Protezione contro la falsificazione delle richieste tra siti (CSRF)

È possibile contribuire a proteggersi dagli attacchi CSRF (Cross-Site Request Forgery) contro StorageGRID utilizzando i token CSRF per migliorare l'autenticazione che utilizza i cookie. Grid Manager e Tenant Manager abilitano automaticamente questa funzionalità di sicurezza; altri client API possono scegliere se abilitarla o meno al momento dell'accesso.

Un aggressore in grado di attivare una richiesta a un sito diverso (ad esempio con un modulo HTTP POST) può far sì che determinate richieste vengano effettuate utilizzando i cookie dell'utente che ha effettuato l'accesso.

StorageGRID aiuta a proteggersi dagli attacchi CSRF utilizzando i token CSRF. Se abilitato, il contenuto di un cookie specifico deve corrispondere al contenuto di un'intestazione specifica o di un parametro del corpo POST specifico.

Per abilitare la funzione, impostare `csrfToken` parametro a `true` durante l'autenticazione. L'impostazione predefinita è `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept: application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Quando è vero, un `GridCsrfToken` il cookie è impostato con un valore casuale per gli accessi a Grid Manager e `AccountCsrfToken` il cookie viene impostato con un valore casuale per gli accessi al Tenant Manager.

Se il cookie è presente, tutte le richieste che possono modificare lo stato del sistema (POST, PUT, PATCH, DELETE) devono includere uno dei seguenti elementi:

- IL `X-Csrf-Token` intestazione, con il valore dell'intestazione impostato sul valore del cookie token CSRF.
- Per gli endpoint che accettano un corpo codificato in formato: A `csrfToken` parametro del corpo della richiesta codificato nel modulo.

Per ulteriori esempi e dettagli, consultare la documentazione API online.



Le richieste che hanno impostato un cookie token CSRF applicheranno anche l'intestazione "Content-Type: application/json" per qualsiasi richiesta che prevede un corpo di richiesta JSON come protezione aggiuntiva contro gli attacchi CSRF.

Utilizzare l'API se è abilitato l'accesso singolo

Utilizzare l'API se è abilitato l'accesso singolo (Active Directory)

Se hai ["configurato e abilitato l'accesso singolo \(SSO\)"](#) e si utilizza Active Directory come provider SSO, è necessario inviare una serie di richieste API per ottenere un token di autenticazione valido per l'API Grid Management o l'API Tenant Management.

Sign in all'API se è abilitato l'accesso singolo

Queste istruzioni sono valide se si utilizza Active Directory come provider di identità SSO.

Prima di iniziare

- Conosci il nome utente e la password SSO di un utente federato che appartiene a un gruppo di utenti StorageGRID .
- Se vuoi accedere all'API di gestione tenant, devi conoscere l'ID dell'account tenant.

Informazioni su questo compito

Per ottenere un token di autenticazione, puoi utilizzare uno dei seguenti esempi:

- IL `storagegrid-ssoauth.py` Script Python, che si trova nella directory dei file di installazione StorageGRID(`./rpms` per Red Hat Enterprise Linux, `./debs` per Ubuntu o Debian, e `./vsphere` per VMware).

- Un esempio di flusso di lavoro delle richieste curl.

Il flusso di lavoro curl potrebbe interrompersi se eseguito troppo lentamente. Potresti visualizzare l'errore: `A valid SubjectConfirmation was not found on this Response`.



Il flusso di lavoro curl di esempio non protegge la password dalla visualizzazione da parte di altri utenti.

Se riscontri un problema di codifica URL, potresti visualizzare l'errore: `Unsupported SAML version`.

Passi

1. Selezionare uno dei seguenti metodi per ottenere un token di autenticazione:
 - Utilizzare il `storagegrid-ssoauth.py` Script Python. Vai al passaggio 2.
 - Utilizzare le richieste curl. Vai al passaggio 3.
2. Se vuoi usare il `storagegrid-ssoauth.py` script, passa lo script all'interprete Python ed esegui lo script.

Quando richiesto, immettere i valori per i seguenti argomenti:

- Il metodo SSO. Inserisci ADFS o adfs.
- Il nome utente SSO
- Il dominio in cui è installato StorageGRID
- L'indirizzo per StorageGRID
- ID dell'account tenant, se si desidera accedere all'API di gestione tenant.

```
python3 storagegrid-ssoauth.py
sso_method: adfs
saml_user: my-sso-username
saml_domain: my-domain
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
*****

*****
StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
```

Il token di autorizzazione StorageGRID viene fornito nell'output. Ora puoi utilizzare il token per altre richieste, in modo simile a come utilizzeresti l'API se non utilizzassi l'SSO.

3. Se si desidera utilizzare le richieste curl, attenersi alla seguente procedura.
 - a. Dichiarare le variabili necessarie per effettuare l'accesso.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export SAMLDOMAIN='my-domain'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
export AD_FS_ADDRESS='adfs.example.com'
```



Per accedere all'API di gestione della griglia, utilizzare 0 come TENANTACCOUNTID.

- b. Per ricevere un URL di autenticazione firmato, inviare una richiesta POST a `/api/v3/authorize-saml` e rimuovere la codifica JSON aggiuntiva dalla risposta.

Questo esempio mostra una richiesta POST per un URL di autenticazione firmato per TENANTACCOUNTID. I risultati saranno trasmessi a `python -m json.tool` per rimuovere la codifica JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H "Content-Type: application/json" \
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

La risposta per questo esempio include un URL firmato codificato in URL, ma non include il livello di codifica JSON aggiuntivo.

```
{
  "apiVersion": "3.0",
  "data":
  "https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
  "responseTime": "2018-11-06T16:30:23.355Z",
  "status": "success"
}
```

- c. Salva il SAMLRequest dalla risposta per utilizzarla nei comandi successivi.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

- d. Ottieni un URL completo che includa l'ID della richiesta client da AD FS.

Un'opzione è quella di richiedere il modulo di accesso utilizzando l'URL della risposta precedente.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID" | grep 'form method="post" id="loginForm"'
```

La risposta include l'ID della richiesta del client:

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRTOMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. Salva l'ID della richiesta del client dalla risposta.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. Invia le tue credenziali all'azione del modulo dalla risposta precedente.

```
curl -X POST "https://$AD_FS_ADDRESS
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \
--data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=$SAMPLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS restituisce un reindirizzamento 302, con informazioni aggiuntive nelle intestazioni.



Se l'autenticazione a più fattori (MFA) è abilitata per il tuo sistema SSO, il post del modulo conterrà anche la seconda password o altre credenziali.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRTOMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs; HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. Salva il MSISAuth cookie dalla risposta.

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. Invia una richiesta GET alla posizione specificata con i cookie dal POST di autenticazione.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \
--cookie "MSISAuth=$MSISAuth" --include
```

Le intestazioni della risposta conterranno informazioni sulla sessione AD FS per un successivo utilizzo in caso di disconnessione, mentre il corpo della risposta conterrà SAMLResponse in un campo modulo nascosto.

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmrMfsc2Umcng4NnJDZmFKV
XfXVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThtMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMj01OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3Bvb3NlscDpsZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. Salva il SAMLResponse dal campo nascosto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

- j. Utilizzando il salvato `SAMLResponse`, crea uno `StorageGRID/api/saml-response` richiesta di generazione di un token di autenticazione `StorageGRID`.

Per `RelayState`, utilizzare l'ID dell'account tenant oppure utilizzare 0 se si desidera accedere all'API di gestione della griglia.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
-H "accept: application/json" \
--data-urlencode "SAMLResponse=$SAMLResponse" \
--data-urlencode "RelayState=$TENANTACCOUNTID" \
| python -m json.tool
```

La risposta include il token di autenticazione.

```
{
  "apiVersion": "3.0",
  "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
  "responseTime": "2018-11-07T21:32:53.486Z",
  "status": "success"
}
```

- a. Salva il token di autenticazione nella risposta come `MYTOKEN`.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Ora puoi usare `MYTOKEN` per altre richieste, in modo simile a come utilizzeresti l'API se non si utilizzasse l'SSO.

Disconnettersi dall'API se è abilitato l'accesso singolo

Se è stato abilitato l'accesso singolo (SSO), è necessario inviare una serie di richieste API per disconnettersi dall'API di gestione della griglia o dall'API di gestione dei tenant. Queste istruzioni si applicano se si utilizza Active Directory come provider di identità SSO

Informazioni su questo compito

Se necessario, puoi disconnetterti dall'API `StorageGRID` effettuando il logout dalla pagina di disconnessione singola della tua organizzazione. In alternativa, è possibile attivare il single logout (SLO) da `StorageGRID`, che richiede un token portatore `StorageGRID` valido.

Passi

1. Per generare una richiesta di disconnessione firmata, passare `cookie "sso=true" all'API SLO:


```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Viene restituito un URL di disconnessione:

```
{
  "apiVersion": "3.0",
  "data":
    "https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
  "responseTime": "2018-11-20T22:20:30.839Z",
  "status": "success"
}
```

2. Salva l'URL di disconnessione.

```
export LOGOUT_REQUEST
='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. Inviare una richiesta all'URL di disconnessione per attivare SLO e reindirizzare a StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

Viene restituita la risposta 302. La posizione di reindirizzamento non è applicabile alla disconnessione solo tramite API.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018 22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. Eliminare il token portatore StorageGRID .

L'eliminazione del token portatore StorageGRID funziona allo stesso modo dell'eliminazione senza SSO. Se non viene specificato `cookie "sso=true"`, l'utente viene disconnesso da StorageGRID senza che ciò influisca sullo stato SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

UN 204 No Content la risposta indica che l'utente è ora disconnesso.

```
HTTP/1.1 204 No Content
```

Utilizzare l'API se è abilitato l'accesso Single Sign-On (Azure)

Se hai [configurato e abilitato l'accesso singolo \(SSO\)](#) e si utilizza Azure come provider SSO, è possibile utilizzare due script di esempio per ottenere un token di autenticazione valido per l'API Grid Management o l'API Tenant Management.

Sign in all'API se è abilitato l'accesso Single Sign-On di Azure

Queste istruzioni si applicano se si utilizza Azure come provider di identità SSO

Prima di iniziare

- Conosci l'indirizzo email e la password SSO di un utente federato che appartiene a un gruppo di utenti StorageGRID .
- Se vuoi accedere all'API di gestione tenant, devi conoscere l'ID dell'account tenant.

Informazioni su questo compito

Per ottenere un token di autenticazione, è possibile utilizzare i seguenti script di esempio:

- IL `storagegrid-ssoauth-azure.py` Script Python
- IL `storagegrid-ssoauth-azure.js` Script Node.js

Entrambi gli script si trovano nella directory dei file di installazione StorageGRID(`./rpms` per Red Hat Enterprise Linux, `./debs` per Ubuntu o Debian, e `./vsphere` per VMware).

Per scrivere la tua integrazione API con Azure, consulta `storagegrid-ssoauth-azure.py` sceneggiatura. Lo script Python invia direttamente due richieste a StorageGRID (prima per ottenere SAMLRequest e poi per ottenere il token di autorizzazione) e chiama anche lo script Node.js per interagire con Azure ed eseguire le operazioni SSO.

Le operazioni SSO possono essere eseguite utilizzando una serie di richieste API, ma non è un'operazione semplice. Il modulo Puppeteer Node.js viene utilizzato per eseguire lo scraping dell'interfaccia Azure SSO.

Se riscontri un problema di codifica URL, potresti visualizzare l'errore: `Unsupported SAML version`.

Passi

1. Installare le dipendenze richieste, come segue:
 - a. Installa Node.js (vedi ["https://nodejs.org/en/download/"](https://nodejs.org/en/download/)).

b. Installa i moduli Node.js richiesti (puppeteer e jsdom):

```
npm install -g <module>
```

2. Passare lo script Python all'interprete Python per eseguirlo.

Lo script Python chiamerà quindi lo script Node.js corrispondente per eseguire le interazioni SSO di Azure.

3. Quando richiesto, immettere i valori per i seguenti argomenti (o passarli utilizzando i parametri):

- L'indirizzo e-mail SSO utilizzato per accedere ad Azure
- L'indirizzo per StorageGRID
- ID dell'account tenant, se si desidera accedere all'API di gestione tenant

4. Quando richiesto, immettere la password e prepararsi a fornire un'autorizzazione MFA ad Azure, se richiesto.

```
c:\Users\user\Documents\azure_sso>py storagegrid-azure-ssoauth.py --sso-email-address user@my-domain.com
--sg-address storagegrid.examp.e.com --tenant-account-id 0
Enter the user's SSO password:
*****

Watch for and approve a 2FA authorization request
*****
StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion':
'3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```



Lo script presuppone che l'autenticazione MFA venga eseguita tramite Microsoft Authenticator. Potrebbe essere necessario modificare lo script per supportare altre forme di MFA (ad esempio l'inserimento di un codice ricevuto in un messaggio di testo).

Il token di autorizzazione StorageGRID viene fornito nell'output. Ora puoi utilizzare il token per altre richieste, in modo simile a come utilizzeresti l'API se non utilizzassi l'SSO.

Utilizzare l'API se è abilitato l'accesso singolo (PingFederate)

Se hai [configurato e abilitato l'accesso singolo \(SSO\)](#) e utilizzi PingFederate come provider SSO, devi inviare una serie di richieste API per ottenere un token di autenticazione valido per l'API Grid Management o l'API Tenant Management.

Sign in all'API se è abilitato l'accesso singolo

Queste istruzioni si applicano se si utilizza PingFederate come provider di identità SSO

Prima di iniziare

- Conosci il nome utente e la password SSO di un utente federato che appartiene a un gruppo di utenti StorageGRID .
- Se vuoi accedere all'API di gestione tenant, devi conoscere l'ID dell'account tenant.

Informazioni su questo compito

Per ottenere un token di autenticazione, puoi utilizzare uno dei seguenti esempi:

- IL `storagegrid-ssoauth.py` Script Python, che si trova nella directory dei file di installazione StorageGRID(`./rpms` per Red Hat Enterprise Linux, `./debs` per Ubuntu o Debian, e `./vsphere` per

VMware).

- Un esempio di flusso di lavoro delle richieste curl.

Il flusso di lavoro curl potrebbe interrompersi se eseguito troppo lentamente. Potresti visualizzare l'errore: `A valid SubjectConfirmation was not found on this Response.`



Il flusso di lavoro curl di esempio non protegge la password dalla visualizzazione da parte di altri utenti.

Se riscontri un problema di codifica URL, potresti visualizzare l'errore: `Unsupported SAML version.`

Passi

1. Selezionare uno dei seguenti metodi per ottenere un token di autenticazione:
 - Utilizzare il `storagegrid-ssoauth.py` Script Python. Vai al passaggio 2.
 - Utilizzare le richieste curl. Vai al passaggio 3.
2. Se vuoi usare il `storagegrid-ssoauth.py` script, passa lo script all'interprete Python ed esegui lo script.

Quando richiesto, immettere i valori per i seguenti argomenti:

- Il metodo SSO. È possibile immettere qualsiasi variante di "pingfederate" (PINGFEDERATE, pingfederate e così via).
- Il nome utente SSO
- Il dominio in cui è installato StorageGRID . Questo campo non è utilizzato per PingFederate. Puoi lasciarlo vuoto o inserire qualsiasi valore.
- L'indirizzo per StorageGRID
- ID dell'account tenant, se si desidera accedere all'API di gestione tenant.

```
python3 storagegrid-ssoauth.py
sso_method: pingfederate
saml_user: my-sso-username
saml_domain:
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
*****

*****
StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
```

Il token di autorizzazione StorageGRID viene fornito nell'output. Ora puoi utilizzare il token per altre richieste, in modo simile a come utilizzeresti l'API se non utilizzassi l'SSO.

3. Se si desidera utilizzare le richieste curl, attenersi alla seguente procedura.
 - a. Dichiarare le variabili necessarie per effettuare l'accesso.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
```



Per accedere all'API di gestione della griglia, utilizzare 0 come TENANTACCOUNTID.

- b. Per ricevere un URL di autenticazione firmato, inviare una richiesta POST a `/api/v3/authorize-saml` e rimuovere la codifica JSON aggiuntiva dalla risposta.

Questo esempio mostra una richiesta POST per un URL di autenticazione firmato per TENANTACCOUNTID. I risultati verranno passati a `python -m json.tool` per rimuovere la codifica JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
-H "accept: application/json" -H "Content-Type: application/json" \
--data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

La risposta per questo esempio include un URL firmato codificato in URL, ma non include il livello di codifica JSON aggiuntivo.

```
{
  "apiVersion": "3.0",
  "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
  "responseTime": "2018-11-06T16:30:23.355Z",
  "status": "success"
}
```

- c. Salva il SAMLRequest dalla risposta per utilizzarla nei comandi successivi.

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

- d. Esporta la risposta e il cookie e ripeti la risposta:

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. Esporta il valore 'pf.adapterId' e riproduci la risposta:

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. Esporta il valore 'href' (rimuovi la barra finale /) e riproduci la risposta:

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. Esporta il valore 'azione':

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. Invia i cookie insieme alle credenziali:

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=$SAMPLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. Salva il SAMLResponse dal campo nascosto:

```
export SAMLResponse='PHNhbwXwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Utilizzando il salvato SAMLResponse , crea uno StorageGRID/api/saml-response richiesta di generazione di un token di autenticazione StorageGRID .

Per RelayState , utilizzare l'ID dell'account tenant oppure utilizzare 0 se si desidera accedere all'API di gestione della griglia.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
-H "accept: application/json" \
--data-urlencode "SAMLResponse=$SAMLResponse" \
--data-urlencode "RelayState=$TENANTACCOUNTID" \
| python -m json.tool
```

La risposta include il token di autenticazione.

```
{
  "apiVersion": "3.0",
  "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
  "responseTime": "2018-11-07T21:32:53.486Z",
  "status": "success"
}
```

a. Salva il token di autenticazione nella risposta come MYTOKEN .

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Ora puoi usare MYTOKEN per altre richieste, in modo simile a come utilizzeresti l'API se non si utilizzasse l'SSO.

Disconnettersi dall'API se è abilitato l'accesso singolo

Se è stato abilitato l'accesso singolo (SSO), è necessario inviare una serie di richieste API per disconnettersi dall'API di gestione della griglia o dall'API di gestione dei tenant. Queste istruzioni si applicano se si utilizza PingFederate come provider di identità SSO

Informazioni su questo compito

Se necessario, puoi disconnetterti dall'API StorageGRID effettuando il logout dalla pagina di disconnessione singola della tua organizzazione. In alternativa, è possibile attivare il single logout (SLO) da StorageGRID, che richiede un token portatore StorageGRID valido.

Passi

1. Per generare una richiesta di disconnessione firmata, passare `cookie "sso=true" all'API SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Viene restituito un URL di disconnessione:

```
{
  "apiVersion": "3.0",
  "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
  "responseTime": "2021-10-12T22:20:30.839Z",
  "status": "success"
}
```

2. Salva l'URL di disconnessione.

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. Inviare una richiesta all'URL di disconnessione per attivare SLO e reindirizzare a StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

Viene restituita la risposta 302. La posizione di reindirizzamento non è applicabile alla disconnessione solo tramite API.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. Eliminare il token portatore StorageGRID .

L'eliminazione del token portatore StorageGRID funziona allo stesso modo dell'eliminazione senza SSO. Se non viene specificato `cookie "sso=true", l'utente viene disconnesso da StorageGRID senza che ciò influisca sullo stato SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

UN 204 No Content la risposta indica che l'utente è ora disconnesso.

```
HTTP/1.1 204 No Content
```


Disattivare le funzionalità con l'API

È possibile utilizzare l'API Grid Management per disattivare completamente determinate funzionalità nel sistema StorageGRID . Quando una funzionalità viene disattivata, a nessuno può essere assegnata l'autorizzazione per eseguire le attività correlate a tale funzionalità.

Informazioni su questo compito

Il sistema Funzionalità disattivate consente di impedire l'accesso a determinate funzionalità del sistema StorageGRID . La disattivazione di una funzionalità è l'unico modo per impedire all'utente root o agli utenti che appartengono a gruppi di amministratori con autorizzazione di **accesso root** di utilizzare tale funzionalità.

Per capire come questa funzionalità potrebbe essere utile, consideriamo il seguente scenario:

_La società A è un fornitore di servizi che affitta la capacità di archiviazione del proprio sistema StorageGRID creando account tenant. Per proteggere la sicurezza degli oggetti dei propri locatari, la Società A desidera garantire che i propri dipendenti non possano mai accedere all'account di un locatario dopo che l'account è stato distribuito.

_L'azienda A può raggiungere questo obiettivo utilizzando il sistema Disattiva funzionalità nell'API di gestione della griglia. Disattivando completamente la funzionalità **Modifica password root del tenant** in Grid Manager (sia nell'interfaccia utente che nell'API), la Società A garantisce che gli utenti amministratori, inclusi l'utente root e gli utenti appartenenti a gruppi con autorizzazione di **Accesso root**, non possano modificare la password per l'utente root di alcun account tenant.

Passi

1. Accedi alla documentazione Swagger per l'API Grid Management. Vedere ["Utilizzare l'API di gestione della griglia"](#) .
2. Individuare l'endpoint Disattiva funzionalità.
3. Per disattivare una funzionalità, ad esempio Modifica password root del tenant, invia un corpo all'API in questo modo:

```
{ "grid": { "changeTenantRootPassword": true } }
```

Una volta completata la richiesta, la funzionalità Modifica password root del tenant viene disabilitata. L'autorizzazione di gestione **Modifica password root del tenant** non viene più visualizzata nell'interfaccia utente e qualsiasi richiesta API che tenti di modificare la password root per un tenant fallirà con "403 Forbidden".

Riattiva le funzionalità disattivate

Per impostazione predefinita, è possibile utilizzare l'API Grid Management per riattivare una funzionalità che è stata disattivata. Tuttavia, se si desidera impedire che le funzionalità disattivate vengano riattivate, è possibile disattivare la funzionalità **activateFeatures** stessa.



La funzione **activateFeatures** non può essere riattivata. Se decidi di disattivare questa funzione, tieni presente che perderai definitivamente la possibilità di riattivare qualsiasi altra funzione disattivata. Per ripristinare eventuali funzionalità perse è necessario contattare l'assistenza tecnica.

Passi

1. Accedi alla documentazione Swagger per l'API Grid Management.
2. Individuare l'endpoint Disattiva funzionalità.
3. Per riattivare tutte le funzionalità, invia un corpo all'API in questo modo:

```
{ "grid": null }
```

Una volta completata questa richiesta, tutte le funzionalità, inclusa la funzionalità Modifica password root del tenant, vengono riattivate. L'autorizzazione di gestione **Modifica password root del tenant** ora viene visualizzata nell'interfaccia utente e qualsiasi richiesta API che tenti di modificare la password root per un tenant avrà esito positivo, a condizione che l'utente disponga dell'autorizzazione di gestione **Accesso root** o **Modifica password root del tenant**.



L'esempio precedente fa sì che tutte le funzionalità disattivate vengano riattivate. Se sono state disattivate altre funzionalità che devono rimanere disattivate, è necessario specificarle esplicitamente nella richiesta PUT. Ad esempio, per riattivare la funzionalità Modifica password root del tenant e continuare a disattivare l'autorizzazione di gestione storageAdmin, inviare questa richiesta PUT:

```
{ "grid": {"storageAdmin": true} }
```

Controlla l'accesso a StorageGRID

Controllo dell'accesso a StorageGRID

È possibile controllare chi può accedere a StorageGRID e quali attività gli utenti possono eseguire creando o importando gruppi e utenti e assegnando autorizzazioni a ciascun gruppo. Facoltativamente, è possibile abilitare l'accesso singolo (SSO), creare certificati client e modificare le password della griglia.

Controlla l'accesso al Grid Manager

È possibile determinare chi può accedere a Grid Manager e all'API Grid Management importando gruppi e utenti da un servizio di federazione delle identità o impostando gruppi e utenti locali.

Utilizzando ["federazione di identità"](#) rende l'impostazione ["gruppi"](#) E ["utenti"](#) più veloce e consente agli utenti di accedere a StorageGRID utilizzando credenziali familiari. È possibile configurare la federazione delle identità se si utilizza Active Directory, OpenLDAP o Oracle Directory Server.



Se si desidera utilizzare un altro servizio LDAP v3, contattare l'assistenza tecnica.

Si determinano le attività che ciascun utente può svolgere assegnando diverse ["permessi"](#) a ciascun gruppo. Ad esempio, potresti voler consentire agli utenti di un gruppo di gestire le regole ILM e agli utenti di un altro gruppo di eseguire attività di manutenzione. Per accedere al sistema, un utente deve appartenere ad almeno un gruppo.

Facoltativamente, è possibile configurare un gruppo in sola lettura. Gli utenti di un gruppo di sola lettura possono visualizzare solo impostazioni e funzionalità. Non possono apportare modifiche o eseguire operazioni in Grid Manager o nell'API Grid Management.

Abilita l'accesso singolo

Il sistema StorageGRID supporta l'accesso Single Sign-On (SSO) utilizzando lo standard Security Assertion Markup Language 2.0 (SAML 2.0). Dopo di te ["configurare e abilitare SSO"](#), tutti gli utenti devono essere autenticati da un provider di identità esterno prima di poter accedere a Grid Manager, Tenant Manager, Grid Management API o Tenant Management API. Gli utenti locali non possono accedere a StorageGRID.

Cambia la passphrase di provisioning

La passphrase di provisioning è necessaria per numerose procedure di installazione e manutenzione e per scaricare il pacchetto di ripristino StorageGRID. La passphrase è necessaria anche per scaricare i backup delle informazioni sulla topologia della griglia e le chiavi di crittografia per il sistema StorageGRID. Puoi ["cambiare la passphrase"](#) come richiesto.

Cambiare le password della console del nodo

Ogni nodo nella griglia ha una password univoca per la console del nodo, che è necessaria per accedere al nodo come "admin" tramite SSH oppure come utente root su una connessione alla console fisica/VM. Se necessario, puoi ["cambiare la password della console del nodo"](#) per ogni nodo.

Cambia la passphrase di provisioning

Utilizzare questa procedura per modificare la passphrase di provisioning StorageGRID. La passphrase è necessaria per le procedure di recupero, espansione e manutenzione. La passphrase è necessaria anche per scaricare i backup del pacchetto di ripristino che includono le informazioni sulla topologia della griglia, le password della console del nodo della griglia e le chiavi di crittografia per il sistema StorageGRID.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai i permessi di accesso di Manutenzione o Root.
- Hai la passphrase di provisioning corrente.

Informazioni su questo compito

La passphrase di provisioning è richiesta per molte procedure di installazione e manutenzione e per ["scaricando il pacchetto di ripristino"](#). La passphrase di provisioning non è elencata in `Passwords.txt` file. Assicuratevi di documentare la passphrase di provisioning e di conservarla in un luogo sicuro e protetto.

Passi

1. Selezionare **CONFIGURAZIONE > Controllo accessi > Password griglia**.
2. In **Modifica passphrase di provisioning**, seleziona **Apporta una modifica**
3. Inserisci la tua passphrase di provisioning attuale.
4. Inserisci la nuova passphrase. La passphrase deve contenere almeno 8 e non più di 32 caratteri. Le passphrase sono sensibili alle maiuscole e alle minuscole.
5. Conservare la nuova passphrase di provisioning in un luogo sicuro. È necessario per le procedure di installazione, ampliamento e manutenzione.
6. Reinserisci la nuova passphrase e seleziona **Salva**.

Una volta completata la modifica della passphrase di provisioning, il sistema visualizza un banner verde di successo.



Provisioning passphrase successfully changed. Go to the [Recovery Package](#) to download a new Recovery Package.

7. Selezionare **Pacchetto di ripristino**.

8. Immettere la nuova passphrase di provisioning per scaricare il nuovo pacchetto di ripristino.



Dopo aver modificato la passphrase di provisioning, è necessario scaricare immediatamente un nuovo pacchetto di ripristino. Il file Recovery Package consente di ripristinare il sistema in caso di errore.

Cambiare le password della console del nodo

Ogni nodo della griglia ha una password univoca per la console del nodo, necessaria per accedere al nodo. Segui questi passaggi per modificare ogni password univoca della console del nodo per ogni nodo nella tua griglia.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["Autorizzazione di accesso alla manutenzione o alla root"](#).
- Hai la passphrase di provisioning corrente.

Informazioni su questo compito

Utilizzare la password della console del nodo per accedere a un nodo come "admin" tramite SSH oppure come utente root su una connessione VM/console fisica. Il processo di modifica della password della console del nodo crea nuove password per ogni nodo nella griglia e memorizza le password in un file aggiornato `Passwords.txt` file nel pacchetto di ripristino. Le password sono elencate nella colonna Password del file `Passwords.txt`.



Esistono password di accesso SSH separate per le chiavi SSH utilizzate per la comunicazione tra i nodi. Questa procedura non modifica le password di accesso SSH.

Accedi alla procedura guidata

Passi

1. Selezionare **CONFIGURAZIONE > Controllo accessi > Password griglia**.
2. In **Modifica password console nodo**, seleziona **Apporta una modifica**.

Inserisci la passphrase di provisioning

Passi

1. Inserisci la passphrase di provisioning per la tua griglia.
2. Selezionare **Continua**.

Scarica il pacchetto di ripristino corrente

Prima di modificare le password della console del nodo, scaricare il pacchetto di ripristino corrente. È possibile utilizzare le password contenute in questo file se il processo di modifica della password non riesce per un nodo.

Passi

1. Seleziona **Scarica pacchetto di ripristino**.
2. Copia il file del pacchetto di ripristino(. zip) in due luoghi sicuri, protetti e separati.



Il file del pacchetto di ripristino deve essere protetto perché contiene chiavi di crittografia e password che possono essere utilizzate per ottenere dati dal sistema StorageGRID .

3. Selezionare **Continua**.
4. Quando viene visualizzata la finestra di dialogo di conferma, seleziona **Sì** se sei pronto a iniziare a modificare le password della console del nodo.

Non è possibile annullare questo processo una volta avviato.

Cambiare le password della console del nodo

Quando si avvia il processo di inserimento della password della console del nodo, viene generato un nuovo pacchetto di ripristino che include le nuove password. Quindi, le password vengono aggiornate su ciascun nodo.

Passi

1. Attendi che venga generato il nuovo pacchetto di ripristino, operazione che potrebbe richiedere alcuni minuti.
2. Seleziona **Scarica nuovo pacchetto di ripristino**.
3. Al termine del download:
 - a. Apri il . zip file.
 - b. Conferma di poter accedere ai contenuti, incluso il `Passwords.txt` file, che contiene le nuove password della console del nodo.
 - c. Copia il nuovo file del pacchetto di ripristino(. zip) in due luoghi sicuri, protetti e separati.



Non sovrascrivere il vecchio Recovery Package.

Il file del pacchetto di ripristino deve essere protetto perché contiene chiavi di crittografia e password che possono essere utilizzate per ottenere dati dal sistema StorageGRID .

4. Seleziona la casella di controllo per indicare che hai scaricato il nuovo pacchetto di ripristino e ne hai verificato il contenuto.
5. Selezionare **Modifica password console nodo** e attendere che tutti i nodi vengano aggiornati con le nuove password. Potrebbero volerci alcuni minuti.

Se le password vengono modificate per tutti i nodi, viene visualizzato un banner verde di operazione riuscita. Vai al passaggio successivo.

Se si verifica un errore durante il processo di aggiornamento, un messaggio banner elenca il numero di nodi le cui password non sono state modificate. Il sistema riproverà automaticamente il processo su qualsiasi nodo la cui password non è riuscita a cambiare. Se il processo termina con alcuni nodi che non hanno ancora modificato la password, viene visualizzato il pulsante **Riprova**.

Se l'aggiornamento della password non è riuscito per uno o più nodi:

- a. Esaminare i messaggi di errore elencati nella tabella.
- b. Risolvere i problemi.
- c. Seleziona **Riprova**.



Il nuovo tentativo modifica solo le password della console dei nodi che non sono riusciti nei precedenti tentativi di modifica della password.

6. Dopo aver modificato le password della console del nodo per tutti i nodi, eliminare il [primo pacchetto di ripristino scaricato](#).
7. Facoltativamente, utilizzare il collegamento **Pacchetto di ripristino** per scaricare una copia aggiuntiva del nuovo Pacchetto di ripristino.

Modificare le password di accesso SSH per i nodi amministrativi

La modifica delle password di accesso SSH per i nodi amministrativi aggiorna anche i set univoci di chiavi SSH interne per ciascun nodo nella griglia. Il nodo di amministrazione primario utilizza queste chiavi SSH per accedere ai nodi tramite autenticazione sicura e senza password.

Utilizzare una chiave SSH per accedere a un nodo come `admin` o all'utente `root` su una macchina virtuale o su una connessione alla console fisica.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["Autorizzazione di accesso alla manutenzione o alla root"](#).
- Hai la passphrase di provisioning corrente.

Informazioni su questo compito

Le nuove password di accesso per i nodi di amministrazione e le nuove chiavi interne per ciascun nodo sono memorizzate nel `Passwords.txt` file nel pacchetto di ripristino. Le chiavi sono elencate nella colonna Password di quel file.

Esistono password di accesso SSH separate per le chiavi SSH utilizzate per la comunicazione tra i nodi. Questa procedura non li modifica.

Accedi alla procedura guidata

Passi

1. Selezionare **CONFIGURAZIONE > Controllo accessi > Password griglia**.
2. In **Modifica chiavi SSH**, seleziona **Apporta una modifica**.

Scarica il pacchetto di ripristino corrente

Prima di modificare le chiavi di accesso SSH, scaricare il pacchetto di ripristino corrente. È possibile utilizzare le chiavi contenute in questo file se il processo di modifica delle chiavi non riesce per un nodo.

Passi

1. Inserisci la passphrase di provisioning per la tua griglia.
2. Seleziona **Scarica pacchetto di ripristino**.

3. Copia il file del pacchetto di ripristino(.zip) in due luoghi sicuri, protetti e separati.



Il file del pacchetto di ripristino deve essere protetto perché contiene chiavi di crittografia e password che possono essere utilizzate per ottenere dati dal sistema StorageGRID .

4. Selezionare **Continua**.
5. Quando viene visualizzata la finestra di dialogo di conferma, seleziona **Sì** se sei pronto a iniziare a modificare le chiavi di accesso SSH.



Non è possibile annullare questo processo una volta avviato.

Cambia le chiavi di accesso SSH

Quando viene avviato il processo di modifica delle chiavi di accesso SSH, viene generato un nuovo pacchetto di ripristino che include le nuove chiavi. Quindi, le chiavi vengono aggiornate su ciascun nodo.

Passi

1. Attendi che venga generato il nuovo pacchetto di ripristino, operazione che potrebbe richiedere alcuni minuti.
2. Quando il pulsante Scarica nuovo pacchetto di ripristino è abilitato, seleziona **Scarica nuovo pacchetto di ripristino** e salva il nuovo file del pacchetto di ripristino(.zip) in due luoghi sicuri, protetti e separati.
3. Al termine del download:
 - a. Apri il .zip file.
 - b. Conferma di poter accedere ai contenuti, incluso il Passwords.txt file, che contiene le nuove chiavi di accesso SSH.
 - c. Copia il nuovo file del pacchetto di ripristino(.zip) in due luoghi sicuri, protetti e separati.



Non sovrascrivere il vecchio Recovery Package.

Il file del pacchetto di ripristino deve essere protetto perché contiene chiavi di crittografia e password che possono essere utilizzate per ottenere dati dal sistema StorageGRID .

4. Attendi che le chiavi vengano aggiornate su ciascun nodo, operazione che potrebbe richiedere alcuni minuti.

Se le chiavi vengono modificate per tutti i nodi, viene visualizzato un banner verde di successo.

Se si verifica un errore durante il processo di aggiornamento, un messaggio banner elenca il numero di nodi le cui chiavi non sono state modificate. Il sistema riproverà automaticamente il processo su qualsiasi nodo la cui chiave non è riuscita a cambiare. Se il processo termina con alcuni nodi che non hanno ancora una chiave modificata, viene visualizzato il pulsante **Riprova**.

Se l'aggiornamento della chiave non è riuscito per uno o più nodi:

- a. Esaminare i messaggi di errore elencati nella tabella.
- b. Risolvere i problemi.
- c. Seleziona **Riprova**.

Il nuovo tentativo modifica solo le chiavi di accesso SSH sui nodi che non sono riusciti durante i precedenti tentativi di modifica delle chiavi.

5. Dopo aver modificato le chiavi di accesso SSH per tutti i nodi, eliminare [primo pacchetto di ripristino scaricato](#).
6. Facoltativamente, selezionare **MANUTENZIONE > Sistema > Pacchetto di ripristino** per scaricare una copia aggiuntiva del nuovo Pacchetto di ripristino.

Utilizzare la federazione delle identità

L'utilizzo della federazione delle identità velocizza la configurazione di gruppi e utenti e consente agli utenti di accedere a StorageGRID utilizzando credenziali familiari.

Configurare la federazione delle identità per Grid Manager

È possibile configurare la federazione delle identità in Grid Manager se si desidera che i gruppi di amministratori e gli utenti vengano gestiti in un altro sistema, ad esempio Active Directory, Azure Active Directory (Azure AD), OpenLDAP o Oracle Directory Server.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai ["autorizzazioni di accesso specifiche"](#).
- Stai utilizzando Active Directory, Azure AD, OpenLDAP o Oracle Directory Server come provider di identità.



Se si desidera utilizzare un servizio LDAP v3 non presente nell'elenco, contattare l'assistenza tecnica.

- Se si prevede di utilizzare OpenLDAP, è necessario configurare il server OpenLDAP. Vedere [Linee guida per la configurazione di un server OpenLDAP](#).
- Se si prevede di abilitare l'accesso singolo (SSO), è necessario aver esaminato il ["requisiti e considerazioni per l'accesso unico"](#).
- Se si prevede di utilizzare Transport Layer Security (TLS) per le comunicazioni con il server LDAP, il provider di identità utilizza TLS 1.2 o 1.3. Vedere ["Cifature supportate per le connessioni TLS in uscita"](#).

Informazioni su questo compito

È possibile configurare un'origine identità per Grid Manager se si desidera importare gruppi da un altro sistema, ad esempio Active Directory, Azure AD, OpenLDAP o Oracle Directory Server. È possibile importare i seguenti tipi di gruppi:

- Gruppi di amministrazione. Gli utenti nei gruppi di amministrazione possono accedere a Grid Manager ed eseguire attività in base alle autorizzazioni di gestione assegnate al gruppo.
- Gruppi di utenti tenant per tenant che non utilizzano una propria fonte di identità. Gli utenti nei gruppi di tenant possono accedere a Tenant Manager ed eseguire attività in base alle autorizzazioni assegnate al gruppo in Tenant Manager. Vedere ["Crea un account inquilino"](#) E ["Utilizzare un account tenant"](#) per i dettagli.

Inserisci la configurazione

Passi

1. Selezionare **CONFIGURAZIONE > Controllo accessi > Federazione identità**.
2. Selezionare **Abilita federazione delle identità**.

3. Nella sezione Tipo di servizio LDAP, seleziona il tipo di servizio LDAP che desideri configurare.

Ldap service type

Select the type of LDAP service you want to configure.

Active Directory	Azure	OpenLDAP	Other

Selezionare **Altro** per configurare i valori per un server LDAP che utilizza Oracle Directory Server.

4. Se hai selezionato **Altro**, compila i campi nella sezione Attributi LDAP. procedere al passaggio successivo.

- **Nome univoco utente:** il nome dell'attributo che contiene l'identificatore univoco di un utente LDAP. Questo attributo è equivalente a `sAMAccountName` per Active Directory e `uid` per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `uid`.
- **UUID utente:** il nome dell'attributo che contiene l'identificatore univoco permanente di un utente LDAP. Questo attributo è equivalente a `objectGUID` per Active Directory e `entryUUID` per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `nsuniqueid`. Il valore di ciascun utente per l'attributo specificato deve essere un numero esadecimale di 32 cifre in formato stringa o a 16 byte, in cui i trattini vengono ignorati.
- **Nome univoco del gruppo:** il nome dell'attributo che contiene l'identificatore univoco di un gruppo LDAP. Questo attributo è equivalente a `sAMAccountName` per Active Directory e `cn` per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `cn`.
- **UUID gruppo:** il nome dell'attributo che contiene l'identificatore univoco permanente di un gruppo LDAP. Questo attributo è equivalente a `objectGUID` per Active Directory e `entryUUID` per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `nsuniqueid`. Il valore di ciascun gruppo per l'attributo specificato deve essere un numero esadecimale di 32 cifre in formato stringa o a 16 byte, in cui i trattini vengono ignorati.

5. Per tutti i tipi di servizio LDAP, immettere le informazioni richieste sul server LDAP e sulla connessione di rete nella sezione Configura server LDAP.

- **Nome host:** nome di dominio completo (FQDN) o indirizzo IP del server LDAP.
- **Porta:** la porta utilizzata per connettersi al server LDAP.



La porta predefinita per STARTTLS è 389, mentre la porta predefinita per LDAPS è 636. Tuttavia, puoi utilizzare qualsiasi porta, a patto che il firewall sia configurato correttamente.

- **Nome utente:** percorso completo del nome distinto (DN) dell'utente che si conatterà al server LDAP.

Per Active Directory, è anche possibile specificare il nome di accesso di livello inferiore o il nome dell'entità utente.

L'utente specificato deve avere l'autorizzazione per elencare gruppi e utenti e per accedere ai seguenti attributi:

- `sAMAccountName`O`uid`

- `objectGUID, entryUUID, O nsuniqueid`
 - `cn`
 - `memberOf`O `isMemberOf`
 - **Directory attiva:** `objectSid, primaryGroupID, userAccountControl, E userPrincipalName`
 - **Azzurro:** `accountEnabled E userPrincipalName`
- **Password:** la password associata al nome utente.



Se in futuro dovessi cambiare la password, dovrai aggiornarla in questa pagina.

- **DN base gruppo:** percorso completo del nome distinto (DN) per un sottoalbero LDAP in cui si desidera cercare i gruppi. Nell'esempio di Active Directory (sotto), tutti i gruppi il cui nome distinto è relativo al DN di base (`DC=storagegrid,DC=example,DC=com`) possono essere utilizzati come gruppi federati.



I valori **Nome univoco del gruppo** devono essere univoci all'interno del **DN di base del gruppo** a cui appartengono.

- **DN base utente:** percorso completo del nome distinto (DN) di un sottoalbero LDAP in cui si desidera cercare gli utenti.



I valori **Nome univoco utente** devono essere univoci all'interno del **Nome base utente** a cui appartengono.

- **Formato nome utente associato** (facoltativo): il modello di nome utente predefinito che StorageGRID dovrebbe utilizzare se il modello non può essere determinato automaticamente.

Si consiglia di fornire il **formato nome utente di associazione** perché può consentire agli utenti di accedere se StorageGRID non è in grado di associarsi all'account di servizio.

Inserisci uno di questi modelli:

- **Modello UserPrincipalName (Active Directory e Azure):** `[USERNAME]@example.com`
- **Modello di nome di accesso di livello inferiore (Active Directory e Azure):**
`example\[USERNAME]`
- **Modello di nome distinto:** `CN=[USERNAME], CN=Users, DC=example, DC=com`

Includi **[USERNAME]** esattamente come scritto.

6. Nella sezione Transport Layer Security (TLS), seleziona un'impostazione di sicurezza.

- **Usa STARTTLS:** usa STARTTLS per proteggere le comunicazioni con il server LDAP. Questa è l'opzione consigliata per Active Directory, OpenLDAP o Altro, ma non è supportata per Azure.
- **Usa LDAPS:** l'opzione LDAPS (LDAP su SSL) utilizza TLS per stabilire una connessione al server LDAP. È necessario selezionare questa opzione per Azure.
- **Non utilizzare TLS:** il traffico di rete tra il sistema StorageGRID e il server LDAP non sarà protetto. Questa opzione non è supportata per Azure.



L'utilizzo dell'opzione **Non utilizzare TLS** non è supportato se il server Active Directory impone la firma LDAP. È necessario utilizzare STARTTLS o LDAPS.

7. Se hai selezionato STARTTLS o LDAPS, scegli il certificato utilizzato per proteggere la connessione.
 - **Utilizza il certificato CA del sistema operativo:** utilizza il certificato Grid CA predefinito installato sul sistema operativo per proteggere le connessioni.
 - **Utilizza certificato CA personalizzato:** utilizza un certificato di sicurezza personalizzato.

Se selezioni questa impostazione, copia e incolla il certificato di sicurezza personalizzato nella casella di testo Certificato CA.

Testare la connessione e salvare la configurazione

Dopo aver immesso tutti i valori, è necessario testare la connessione prima di poter salvare la configurazione. StorageGRID verifica le impostazioni di connessione per il server LDAP e il formato del nome utente associato, se ne è stato fornito uno.

Passi

1. Selezionare **Test connessione**.
2. Se non hai fornito un formato di nome utente di associazione:
 - Se le impostazioni di connessione sono valide, viene visualizzato il messaggio "Test di connessione riuscito". Selezionare **Salva** per salvare la configurazione.
 - Se le impostazioni di connessione non sono valide, viene visualizzato il messaggio "Impossibile stabilire la connessione di prova". Selezionare **Chiudi**. Quindi, risolvi eventuali problemi e verifica nuovamente la connessione.
3. Se hai fornito un formato di nome utente vincolato, inserisci il nome utente e la password di un utente federato valido.

Ad esempio, inserisci il tuo nome utente e la tua password. Non includere caratteri speciali nel nome utente, come @ o /.

Test Connection

To test the connection and the bind username format, enter the username and password of a federated user. For example, enter your own federated username and password. The test values are not saved.

Test username

The username of a federated user.

Test password

[Cancel](#) [Test Connection](#)

- Se le impostazioni di connessione sono valide, viene visualizzato il messaggio "Test di connessione riuscito". Selezionare **Salva** per salvare la configurazione.

- Se le impostazioni di connessione, il formato del nome utente associato o il nome utente e la password di prova non sono validi, viene visualizzato un messaggio di errore. Risolvi eventuali problemi e verifica nuovamente la connessione.

Forza la sincronizzazione con la fonte dell'identità

Il sistema StorageGRID sincronizza periodicamente i gruppi federati e gli utenti dalla fonte di identità. È possibile forzare l'avvio della sincronizzazione se si desidera abilitare o limitare le autorizzazioni utente il più rapidamente possibile.

Passi

1. Vai alla pagina Federazione delle identità.
2. Seleziona **Sincronizza server** nella parte superiore della pagina.

Il processo di sincronizzazione potrebbe richiedere del tempo, a seconda dell'ambiente.



L'avviso **Errore di sincronizzazione della federazione delle identità** viene attivato se si verifica un problema durante la sincronizzazione di gruppi e utenti federati dall'origine dell'identità.

Disabilitare la federazione delle identità

È possibile disattivare temporaneamente o permanentemente la federazione delle identità per gruppi e utenti. Quando la federazione delle identità è disabilitata, non c'è comunicazione tra StorageGRID e l'origine dell'identità. Tuttavia, tutte le impostazioni configurate vengono mantenute, consentendoti di riattivare facilmente la federazione delle identità in futuro.

Informazioni su questo compito

Prima di disattivare la federazione delle identità, è necessario tenere presente quanto segue:

- Gli utenti federati non potranno effettuare l'accesso.
- Gli utenti federati attualmente connessi manterranno l'accesso al sistema StorageGRID fino alla scadenza della sessione, ma non potranno effettuare l'accesso dopo la scadenza della sessione.
- La sincronizzazione tra il sistema StorageGRID e l'origine dell'identità non verrà eseguita e non verranno generati avvisi per gli account che non sono stati sincronizzati.
- La casella di controllo **Abilita federazione delle identità** è disabilitata se l'accesso Single Sign-On (SSO) è impostato su **Abilitato** o **Modalità Sandbox**. Lo stato SSO nella pagina Single Sign-on deve essere **Disabilitato** prima di poter disabilitare la federazione delle identità. Vedere "[Disabilitare l'accesso singolo](#)".

Passi

1. Vai alla pagina Federazione delle identità.
2. Deseleziona la casella di controllo **Abilita federazione delle identità**.

Linee guida per la configurazione di un server OpenLDAP

Se si desidera utilizzare un server OpenLDAP per la federazione delle identità, è necessario configurare impostazioni specifiche sul server OpenLDAP.



Per le origini identità diverse da ActiveDirectory o Azure, StorageGRID non bloccherà automaticamente l'accesso S3 agli utenti disabilitati esternamente. Per bloccare l'accesso S3, eliminare tutte le chiavi S3 dell'utente o rimuovere l'utente da tutti i gruppi.

Sovrapposizioni di membri e raffinazione

Le sovrapposizioni memberof e refint dovrebbero essere abilitate. Per ulteriori informazioni, consultare le istruzioni per la manutenzione inversa dell'appartenenza al gruppo in <http://www.openldap.org/doc/admin24/index.html> ["Documentazione OpenLDAP: Guida dell'amministratore versione 2.4"] .

Indicizzazione

È necessario configurare i seguenti attributi OpenLDAP con le parole chiave di indice specificate:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

Inoltre, assicurati che i campi menzionati nella guida per Nome utente siano indicizzati per prestazioni ottimali.

Consultare le informazioni sul mantenimento dell'appartenenza al gruppo inverso in <http://www.openldap.org/doc/admin24/index.html> ["Documentazione OpenLDAP: Guida dell'amministratore versione 2.4"] .

Gestisci gruppi di amministratori

È possibile creare gruppi di amministratori per gestire le autorizzazioni di sicurezza per uno o più utenti amministratori. Per poter accedere al sistema StorageGRID , gli utenti devono appartenere a un gruppo.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Hai "[autorizzazioni di accesso specifiche](#)" .
- Se si prevede di importare un gruppo federato, è necessario aver configurato la federazione delle identità e il gruppo federato esiste già nell'origine identità configurata.

Crea un gruppo di amministratori

I gruppi di amministratori consentono di stabilire quali utenti possono accedere a quali funzionalità e operazioni in Grid Manager e nell'API Grid Management.

Accedi alla procedura guidata

Passi

1. Selezionare **CONFIGURAZIONE > Controllo accessi > Gruppi amministratori**.
2. Seleziona **Crea gruppo**.

Scegli un tipo di gruppo

È possibile creare un gruppo locale o importare un gruppo federato.

- Crea un gruppo locale se vuoi assegnare autorizzazioni agli utenti locali.
- Crea un gruppo federato per importare gli utenti dall'origine dell'identità.

Gruppo locale

Passi

1. Seleziona **Gruppo locale**.
2. Inserisci un nome visualizzato per il gruppo, che potrai aggiornare in seguito se necessario. Ad esempio, "Utenti addetti alla manutenzione" o "Amministratori ILM".
3. Inserisci un nome univoco per il gruppo, che non potrai aggiornare in seguito.
4. Selezionare **Continua**.

Gruppo federato

Passi

1. Seleziona **Gruppo federato**.
2. Inserisci il nome del gruppo che desideri importare, esattamente come appare nell'origine identità configurata.
 - Per Active Directory e Azure, utilizzare sAMAccountName.
 - Per OpenLDAP, utilizzare il CN (nome comune).
 - Per un altro LDAP, utilizzare il nome univoco appropriato per il server LDAP.
3. Selezionare **Continua**.

Gestisci i permessi del gruppo

Passi

1. Per la **Modalità di accesso**, seleziona se gli utenti del gruppo possono modificare le impostazioni ed eseguire operazioni in Grid Manager e nell'API di gestione della griglia oppure se possono solo visualizzare impostazioni e funzionalità.
 - **Lettura-scrittura** (predefinito): gli utenti possono modificare le impostazioni ed eseguire le operazioni consentite dalle loro autorizzazioni di gestione.
 - **Sola lettura**: gli utenti possono solo visualizzare impostazioni e funzionalità. Non possono apportare modifiche o eseguire operazioni in Grid Manager o nell'API Grid Management. Gli utenti locali con privilegi di sola lettura possono modificare le proprie password.



Se un utente appartiene a più gruppi e uno qualsiasi di essi è impostato su **Sola lettura**, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzionalità selezionate.

2. Seleziona uno o più ["autorizzazioni del gruppo amministratore"](#).

È necessario assegnare almeno un'autorizzazione a ciascun gruppo; in caso contrario, gli utenti appartenenti al gruppo non potranno accedere a StorageGRID.

3. Se stai creando un gruppo locale, seleziona **Continua**. Se stai creando un gruppo federato, seleziona

Crea gruppo e Fine.

Aggiungi utenti (solo gruppi locali)

Passi

1. Facoltativamente, seleziona uno o più utenti locali per questo gruppo.

Se non hai ancora creato utenti locali, puoi salvare il gruppo senza aggiungere utenti. Puoi aggiungere questo gruppo all'utente nella pagina Utenti. Vedere "[Gestisci utenti](#)" per i dettagli.

2. Seleziona **Crea gruppo e Fine**.

Visualizza e modifica i gruppi di amministrazione

È possibile visualizzare i dettagli dei gruppi esistenti, modificare un gruppo o duplicare un gruppo.

- Per visualizzare le informazioni di base per tutti i gruppi, consultare la tabella nella pagina Gruppi.
- Per visualizzare tutti i dettagli di un gruppo specifico o per modificare un gruppo, utilizzare il menu **Azioni** o la pagina dei dettagli.

Compito	Menu Azioni	Pagina dei dettagli
Visualizza i dettagli del gruppo	a. Selezionare la casella di controllo per il gruppo. b. Seleziona Azioni > Visualizza dettagli gruppo.	Selezionare il nome del gruppo nella tabella.
Modifica il nome visualizzato (solo gruppi locali)	a. Selezionare la casella di controllo per il gruppo. b. Seleziona Azioni > Modifica nome gruppo. c. Inserisci il nuovo nome. d. Seleziona Salva modifiche.	a. Selezionare il nome del gruppo per visualizzarne i dettagli. b. Seleziona l'icona di modifica . c. Inserisci il nuovo nome. d. Seleziona Salva modifiche.
Modifica la modalità di accesso o le autorizzazioni	a. Selezionare la casella di controllo per il gruppo. b. Seleziona Azioni > Visualizza dettagli gruppo. c. Facoltativamente, modifica la modalità di accesso del gruppo. d. Facoltativamente, seleziona o deseleziona "autorizzazioni del gruppo amministratore". e. Seleziona Salva modifiche.	a. Selezionare il nome del gruppo per visualizzarne i dettagli. b. Facoltativamente, modifica la modalità di accesso del gruppo. c. Facoltativamente, seleziona o deseleziona "autorizzazioni del gruppo amministratore". d. Seleziona Salva modifiche.

Duplica un gruppo

Passi

1. Selezionare la casella di controllo per il gruppo.
2. Selezionare **Azioni > Duplica gruppo**.
3. Completa la procedura guidata Duplica gruppo.

Elimina un gruppo

È possibile eliminare un gruppo di amministratori quando si desidera rimuovere il gruppo dal sistema e rimuovere tutte le autorizzazioni ad esso associate. L'eliminazione di un gruppo di amministratori rimuove tutti gli utenti dal gruppo, ma non elimina gli utenti stessi.

Passi

1. Nella pagina Gruppi, seleziona la casella di controllo per ogni gruppo che desideri rimuovere.
2. Selezionare **Azioni > Elimina gruppo**.
3. Seleziona **Elimina gruppi**.

Autorizzazioni del gruppo amministratore

Quando si creano gruppi di utenti amministratori, si selezionano una o più autorizzazioni per controllare l'accesso a funzionalità specifiche di Grid Manager. È quindi possibile assegnare ciascun utente a uno o più di questi gruppi di amministratori per determinare quali attività può eseguire quell'utente.

È necessario assegnare almeno un'autorizzazione a ciascun gruppo; in caso contrario, gli utenti appartenenti a quel gruppo non potranno accedere a Grid Manager o all'API Grid Management.

Per impostazione predefinita, qualsiasi utente appartenente a un gruppo che dispone di almeno un'autorizzazione può eseguire le seguenti attività:

- Sign in a Grid Manager
- Visualizza la dashboard
- Visualizza le pagine dei nodi
- Visualizza gli avvisi correnti e risolti
- Cambiare la propria password (solo utenti locali)
- Visualizzare alcune informazioni fornite nelle pagine Configurazione e Manutenzione

Interazione tra permessi e modalità di accesso

Per tutte le autorizzazioni, l'impostazione **Modalità di accesso** del gruppo determina se gli utenti possono modificare le impostazioni ed eseguire operazioni oppure se possono solo visualizzare le impostazioni e le funzionalità correlate. Se un utente appartiene a più gruppi e uno qualsiasi di essi è impostato su **Sola lettura**, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzionalità selezionate.

Nelle sezioni seguenti vengono descritte le autorizzazioni che è possibile assegnare durante la creazione o la modifica di un gruppo di amministratori. Per qualsiasi funzionalità non esplicitamente menzionata è necessario il permesso di **accesso root**.

Accesso root

Questa autorizzazione fornisce l'accesso a tutte le funzionalità di amministrazione della griglia.

Cambia la password di root del tenant

Questa autorizzazione fornisce l'accesso all'opzione **Cambia password di root** nella pagina Tenant, consentendo di controllare chi può modificare la password per l'utente root locale del tenant. Questa autorizzazione viene utilizzata anche per la migrazione delle chiavi S3 quando è abilitata la funzionalità di importazione delle chiavi S3. Gli utenti che non dispongono di questa autorizzazione non possono visualizzare l'opzione **Cambia password di root**.



Per concedere l'accesso alla pagina Tenant, che contiene l'opzione **Cambia password di root**, assegnare anche l'autorizzazione **Account tenant**.

Configurazione della pagina della topologia della griglia

Questa autorizzazione consente di accedere alle schede Configurazione nella pagina **SUPPORTO > Strumenti > Topologia griglia**.



La pagina Topologia griglia è stata deprecata e verrà rimossa in una versione futura.

ILM

Questa autorizzazione fornisce l'accesso alle seguenti opzioni del menu **ILM**:

- Regole
- Politiche
- Tag di policy
- Pool di stoccaggio
- Gradi di stoccaggio
- Regioni
- Ricerca metadati oggetto



Per gestire i gradi di archiviazione, gli utenti devono disporre delle autorizzazioni **Altra configurazione della griglia** e **Configurazione della pagina della topologia della griglia**.

Manutenzione

Per utilizzare queste opzioni, gli utenti devono disporre dell'autorizzazione di manutenzione:

- **CONFIGURAZIONE > Controllo accessi:**
 - Password di griglia
- **CONFIGURAZIONE > Rete:**
 - Nomi di dominio endpoint S3
- **MANUTENZIONE > Attività:**
 - Dismissione
 - Espansione
 - Controllo dell'esistenza dell'oggetto
 - Recupero

- **MANUTENZIONE > Sistema:**

- Pacchetto di recupero
- Aggiornamento software

- **SUPPORTO > Strumenti:**

- Registri

Gli utenti che non dispongono dell'autorizzazione di manutenzione possono visualizzare, ma non modificare, queste pagine:

- **MANUTENZIONE > Rete:**

- server DNS
- Rete a griglia
- server NTP

- **MANUTENZIONE > Sistema:**

- Licenza

- **CONFIGURAZIONE > Rete:**

- Nomi di dominio endpoint S3

- **CONFIGURAZIONE > Sicurezza:**

- Certificati

- **CONFIGURAZIONE > Monitoraggio:**

- Server di audit e syslog

Gestisci gli avvisi

Questa autorizzazione fornisce l'accesso alle opzioni per la gestione degli avvisi. Gli utenti devono disporre di questa autorizzazione per gestire silenzi, notifiche di avviso e regole di avviso.

Query sulle metriche

Questa autorizzazione fornisce l'accesso a:

- Pagina **SUPPORTO > Strumenti > Metriche**
- Query personalizzate sulle metriche Prometheus utilizzando la sezione **Metriche** dell'API di gestione della griglia
- Schede della dashboard di Grid Manager che contengono metriche

Ricerca metadati oggetto

Questa autorizzazione fornisce l'accesso alla pagina **ILM > Ricerca metadati oggetto**.

Altra configurazione della griglia

Questa autorizzazione fornisce l'accesso ad ulteriori opzioni di configurazione della griglia.



Per visualizzare queste opzioni aggiuntive, gli utenti devono disporre anche dell'autorizzazione **Configurazione della pagina topologia griglia**.

- **ILM:**
 - Gradi di stoccaggio
- **CONFIGURAZIONE > Sistema:**
- **SUPPORTO > Altro:**
 - Costo del collegamento

Amministratore dell'appliance di archiviazione

Questa autorizzazione prevede:

- Accesso a E-Series SANtricity System Manager su dispositivi di storage tramite Grid Manager.
- Possibilità di eseguire attività di risoluzione dei problemi e manutenzione nella scheda Gestisci unità per gli apparecchi che supportano queste operazioni.

Conti degli inquilini

Questa autorizzazione fornisce la possibilità di:

- Accedi alla pagina Inquilini, dove puoi creare, modificare e rimuovere gli account degli inquilini
- Visualizza le policy di classificazione del traffico esistenti
- Visualizza le schede della dashboard di Grid Manager che contengono i dettagli del tenant

Gestisci utenti

È possibile visualizzare gli utenti locali e federati. È anche possibile creare utenti locali e assegnarli a gruppi di amministratori locali per determinare a quali funzionalità di Grid Manager possono accedere questi utenti.

Prima di iniziare

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

Crea un utente locale

È possibile creare uno o più utenti locali e assegnare ciascun utente a uno o più gruppi locali. Le autorizzazioni del gruppo controllano a quali funzionalità di Grid Manager e Grid Management API l'utente può accedere.

È possibile creare solo utenti locali. Utilizzare la fonte di identità esterna per gestire utenti e gruppi federati.

Grid Manager include un utente locale predefinito, denominato "root". Non è possibile rimuovere l'utente root.



Se è abilitato l'accesso Single Sign-On (SSO), gli utenti locali non possono accedere a StorageGRID.

Accedi alla procedura guidata

Passi

1. Selezionare **CONFIGURAZIONE > Controllo accessi > Utenti amministratori**.
2. Seleziona **Crea utente**.

Inserisci le credenziali utente

Passi

1. Inserisci il nome completo dell'utente, un nome utente univoco e una password.
2. Facoltativamente, seleziona **Sì** se questo utente non deve avere accesso a Grid Manager o all'API Grid Management.
3. Selezionare **Continua**.

Assegna ai gruppi

Passi

1. Facoltativamente, assegnare l'utente a uno o più gruppi per determinare le autorizzazioni dell'utente.

Se non hai ancora creato gruppi, puoi salvare l'utente senza selezionare i gruppi. Puoi aggiungere questo utente a un gruppo nella pagina Gruppi.

Se un utente appartiene a più gruppi, le autorizzazioni sono cumulative. Vedere ["Gestisci gruppi di amministratori"](#) per i dettagli.

2. Selezionare **Crea utente** e poi **Fine**.

Visualizza e modifica gli utenti locali

È possibile visualizzare i dettagli degli utenti locali e federati esistenti. È possibile modificare un utente locale per cambiarne il nome completo, la password o l'appartenenza al gruppo. È anche possibile impedire temporaneamente a un utente di accedere a Grid Manager e all'API Grid Management.

È possibile modificare solo gli utenti locali. Utilizzare la fonte di identità esterna per gestire gli utenti federati.

- Per visualizzare le informazioni di base per tutti gli utenti locali e federati, consultare la tabella nella pagina Utenti.
- Per visualizzare tutti i dettagli di un utente specifico, modificare un utente locale o cambiare la password di un utente locale, utilizzare il menu **Azioni** o la pagina dei dettagli.

Tutte le modifiche verranno applicate la volta successiva che l'utente si disconnette e accede nuovamente a Grid Manager.



Gli utenti locali possono modificare le proprie password utilizzando l'opzione **Cambia password** nel banner di Grid Manager.

Compito	Menu Azioni	Pagina dei dettagli
Visualizza i dettagli dell'utente	a. Selezionare la casella di controllo per l'utente. b. Seleziona Azioni > Visualizza dettagli utente .	Selezionare il nome dell'utente nella tabella.

Compito	Menu Azioni	Pagina dei dettagli
Modifica il nome completo (solo utenti locali)	a. Selezionare la casella di controllo per l'utente. b. Seleziona Azioni > Modifica nome completo. c. Inserisci il nuovo nome. d. Seleziona Salva modifiche.	a. Selezionare il nome dell'utente per visualizzarne i dettagli. b. Seleziona l'icona di modifica  . c. Inserisci il nuovo nome. d. Seleziona Salva modifiche.
Nega o consenti l'accesso a StorageGRID	a. Selezionare la casella di controllo per l'utente. b. Seleziona Azioni > Visualizza dettagli utente. c. Selezionare la scheda Accesso. d. Selezionare Sì per impedire all'utente di accedere a Grid Manager o all'API di gestione della griglia, oppure selezionare No per consentire all'utente di accedere. e. Seleziona Salva modifiche.	a. Selezionare il nome dell'utente per visualizzarne i dettagli. b. Selezionare la scheda Accesso. c. Selezionare Sì per impedire all'utente di accedere a Grid Manager o all'API di gestione della griglia, oppure selezionare No per consentire all'utente di accedere. d. Seleziona Salva modifiche.
Cambia password (solo utenti locali)	a. Selezionare la casella di controllo per l'utente. b. Seleziona Azioni > Visualizza dettagli utente. c. Selezionare la scheda Password. d. Inserisci una nuova password. e. Seleziona Cambia password.	a. Selezionare il nome dell'utente per visualizzarne i dettagli. b. Selezionare la scheda Password. c. Inserisci una nuova password. d. Seleziona Cambia password.
Cambia gruppi (solo utenti locali)	a. Selezionare la casella di controllo per l'utente. b. Seleziona Azioni > Visualizza dettagli utente. c. Selezionare la scheda Gruppi. d. Facoltativamente, seleziona il collegamento dopo il nome di un gruppo per visualizzare i dettagli del gruppo in una nuova scheda del browser. e. Selezionare Modifica gruppi per selezionare gruppi diversi. f. Seleziona Salva modifiche.	a. Selezionare il nome dell'utente per visualizzarne i dettagli. b. Selezionare la scheda Gruppi. c. Facoltativamente, seleziona il collegamento dopo il nome di un gruppo per visualizzare i dettagli del gruppo in una nuova scheda del browser. d. Selezionare Modifica gruppi per selezionare gruppi diversi. e. Seleziona Salva modifiche.

Duplica un utente

È possibile duplicare un utente esistente per crearne uno nuovo con le stesse autorizzazioni.

Passi

1. Selezionare la casella di controllo per l'utente.
2. Selezionare **Azioni > Duplica utente**.
3. Completa la procedura guidata Duplica utente.

Elimina un utente

È possibile eliminare un utente locale per rimuoverlo definitivamente dal sistema.



Non è possibile eliminare l'utente root.

Passi

1. Nella pagina Utenti, seleziona la casella di controllo per ogni utente che desideri rimuovere.
2. Selezionare **Azioni > Elimina utente**.
3. Seleziona **Elimina utente**.

Utilizzare l'accesso singolo (SSO)

Configurare l'accesso singolo

Quando è abilitato l'accesso Single Sign-On (SSO), gli utenti possono accedere a Grid Manager, Tenant Manager, Grid Management API o Tenant Management API solo se le loro credenziali sono autorizzate tramite il processo di accesso SSO implementato dalla tua organizzazione. Gli utenti locali non possono accedere a StorageGRID.

Come funziona l'accesso singolo

Il sistema StorageGRID supporta l'accesso Single Sign-On (SSO) utilizzando lo standard Security Assertion Markup Language 2.0 (SAML 2.0).

Prima di abilitare l'accesso Single Sign-On (SSO), esaminare in che modo i processi di accesso e disconnessione StorageGRID vengono influenzati dall'abilitazione dell'SSO.

Sign in quando SSO è abilitato

Quando l'SSO è abilitato e accedi a StorageGRID, verrai reindirizzato alla pagina SSO della tua organizzazione per convalidare le tue credenziali.

Passi

1. Immettere il nome di dominio completo o l'indirizzo IP di qualsiasi nodo di amministrazione StorageGRID in un browser Web.

Viene visualizzata la pagina Sign in a StorageGRID .

- Se è la prima volta che accedi all'URL su questo browser, ti verrà richiesto un ID account:



Sign in

Account

Sign in

[NetApp support](#) | [NetApp.com](#)

- Se hai già effettuato l'accesso a Grid Manager o Tenant Manager, ti verrà chiesto di selezionare un account recente o di immettere un ID account:



Tenant Manager

Recent

Account

Sign in

[NetApp support](#) | [NetApp.com](#)



La pagina Sign in StorageGRID non viene visualizzata quando si immette l'URL completo per un account tenant (ovvero un nome di dominio completo o un indirizzo IP seguito da `/?accountId=20-digit-account-id`). Invece, verrai immediatamente reindirizzato alla pagina di accesso SSO della tua organizzazione, dove potrai [accedi con le tue credenziali SSO](#).

2. Indica se desideri accedere al Grid Manager o al Tenant Manager:

- Per accedere a Grid Manager, lasciare vuoto il campo **ID account**, immettere **0** come ID account oppure selezionare **Grid Manager** se compare nell'elenco degli account recenti.
- Per accedere a Tenant Manager, immettere l'ID account del tenant a 20 cifre oppure selezionare un tenant per nome se compare nell'elenco degli account recenti.

3. Seleziona * Sign in*

StorageGRID ti reindirizza alla pagina di accesso SSO della tua organizzazione. Per esempio:

Sign in with your organizational account

someone@example.com

Password

Sign in

4. Sign in con le tue credenziali SSO.

Se le tue credenziali SSO sono corrette:

- Il provider di identità (IdP) fornisce una risposta di autenticazione a StorageGRID.
- StorageGRID convalida la risposta di autenticazione.
- Se la risposta è valida e si appartiene a un gruppo federato con autorizzazioni di accesso StorageGRID, si accede a Grid Manager o Tenant Manager, a seconda dell'account selezionato.



Se l'account di servizio non è accessibile, puoi comunque effettuare l'accesso, a patto che tu sia un utente esistente appartenente a un gruppo federato con autorizzazioni di accesso StorageGRID.

5. Facoltativamente, accedi ad altri nodi amministrativi oppure a Grid Manager o Tenant Manager, se disponi delle autorizzazioni adeguate.

Non è necessario reinserire le credenziali SSO.

Disconnettersi quando SSO è abilitato

Quando SSO è abilitato per StorageGRID, ciò che accade quando ci si disconnette dipende dall'account a cui si è effettuato l'accesso e da dove ci si disconnette.

Passi

1. Individua il link **Esci** nell'angolo in alto a destra dell'interfaccia utente.
2. Seleziona **Esci**.

Viene visualizzata la pagina Sign in a StorageGRID . Il menu a discesa **Account recenti** è stato aggiornato per includere **Grid Manager** o il nome del tenant, in modo da poter accedere più rapidamente a queste interfacce utente in futuro.

Se hai effettuato l'accesso a...	E ti disconnetti da...	Hai effettuato la disconnessione da...
Grid Manager su uno o più nodi amministrativi	Grid Manager su qualsiasi nodo di amministrazione	Grid Manager su tutti i nodi amministrativi Nota: se si utilizza Azure per SSO, potrebbero essere necessari alcuni minuti per uscire da tutti i nodi amministrativi.
Tenant Manager su uno o più nodi amministrativi	Tenant Manager su qualsiasi nodo amministrativo	Tenant Manager su tutti i nodi amministrativi
Sia Grid Manager che Tenant Manager	Responsabile della griglia	Solo il Grid Manager. Per uscire dall'SSO è necessario anche disconnettersi da Tenant Manager.



La tabella riassume cosa succede quando ci si disconnette se si utilizza una singola sessione del browser. Se hai effettuato l'accesso a StorageGRID in più sessioni del browser, devi disconnetterti da tutte le sessioni del browser separatamente.

Requisiti e considerazioni per l'accesso singolo

Prima di abilitare l'accesso Single Sign-On (SSO) per un sistema StorageGRID , esaminare i requisiti e le considerazioni.

Requisiti del fornitore di identità

StorageGRID supporta i seguenti provider di identità SSO (IdP):

- Servizio federativo di Active Directory (AD FS)
- Azure Active Directory (Azure AD)
- PingFederate

È necessario configurare la federazione delle identità per il sistema StorageGRID prima di poter configurare un provider di identità SSO. Il tipo di servizio LDAP utilizzato per la federazione delle identità determina il tipo di SSO che è possibile implementare.

Tipo di servizio LDAP configurato	Opzioni per il provider di identità SSO
Directory attiva	• Directory attiva • Azzurro • PingFederate
Azzurro	Azzurro

Requisiti AD FS

È possibile utilizzare una qualsiasi delle seguenti versioni di AD FS:

- Windows Server 2022 ADFS
- Windows Server 2019 ADFS
- Windows Server 2016 ADFS



Windows Server 2016 dovrebbe utilizzare ["Aggiornamento KB3201845"](#) , o superiore.

Requisiti aggiuntivi

- Sicurezza del livello di trasporto (TLS) 1.2 o 1.3
- Microsoft .NET Framework, versione 3.5.1 o successiva

Considerazioni per Azure

Se si utilizza Azure come tipo di SSO e gli utenti hanno nomi di entità utente che non utilizzano sAMAccountName come prefisso, potrebbero verificarsi problemi di accesso se StorageGRID perde la connessione con il server LDAP. Per consentire agli utenti di accedere, è necessario ripristinare la connessione al server LDAP.

Requisiti del certificato del server

Per impostazione predefinita, StorageGRID utilizza un certificato di interfaccia di gestione su ciascun nodo di amministrazione per proteggere l'accesso a Grid Manager, Tenant Manager, Grid Management API e Tenant Management API. Quando si configurano trust di relying party (AD FS), applicazioni aziendali (Azure) o connessioni del provider di servizi (PingFederate) per StorageGRID, si utilizza il certificato del server come certificato di firma per le richieste StorageGRID .

Se non l'hai già fatto ["configurato un certificato personalizzato per l'interfaccia di gestione"](#) , dovresti farlo ora. Quando si installa un certificato server personalizzato, questo viene utilizzato per tutti i nodi amministrativi e può essere utilizzato in tutti i trust relying party StorageGRID , nelle applicazioni aziendali o nelle connessioni SP .



Non è consigliabile utilizzare il certificato server predefinito di un nodo di amministrazione in un trust di relying party, in un'applicazione aziendale o in una connessione SP . Se il nodo fallisce e lo si ripristina, viene generato un nuovo certificato server predefinito. Prima di poter accedere al nodo recuperato, è necessario aggiornare il trust della relying party, l'applicazione aziendale o la connessione SP con il nuovo certificato.

È possibile accedere al certificato del server di un nodo di amministrazione effettuando l'accesso alla shell dei

comandi del nodo e andando su `/var/local/mgmt-api` elenco. Un certificato server personalizzato è denominato `custom-server.crt`. Il certificato del server predefinito del nodo è denominato `server.crt`.

Requisiti portuali

L'accesso Single Sign-On (SSO) non è disponibile sulle porte riservate di Grid Manager o Tenant Manager. Se si desidera che gli utenti eseguano l'autenticazione tramite Single Sign-On, è necessario utilizzare la porta HTTPS predefinita (443). Vedere ["Controllare l'accesso al firewall esterno"](#).

Conferma che gli utenti federati possono accedere

Prima di abilitare l'accesso Single Sign-On (SSO), è necessario confermare che almeno un utente federato possa accedere a Grid Manager e a Tenant Manager per tutti gli account tenant esistenti.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai ["autorizzazioni di accesso specifiche"](#).
- Hai già configurato la federazione delle identità.

Passi

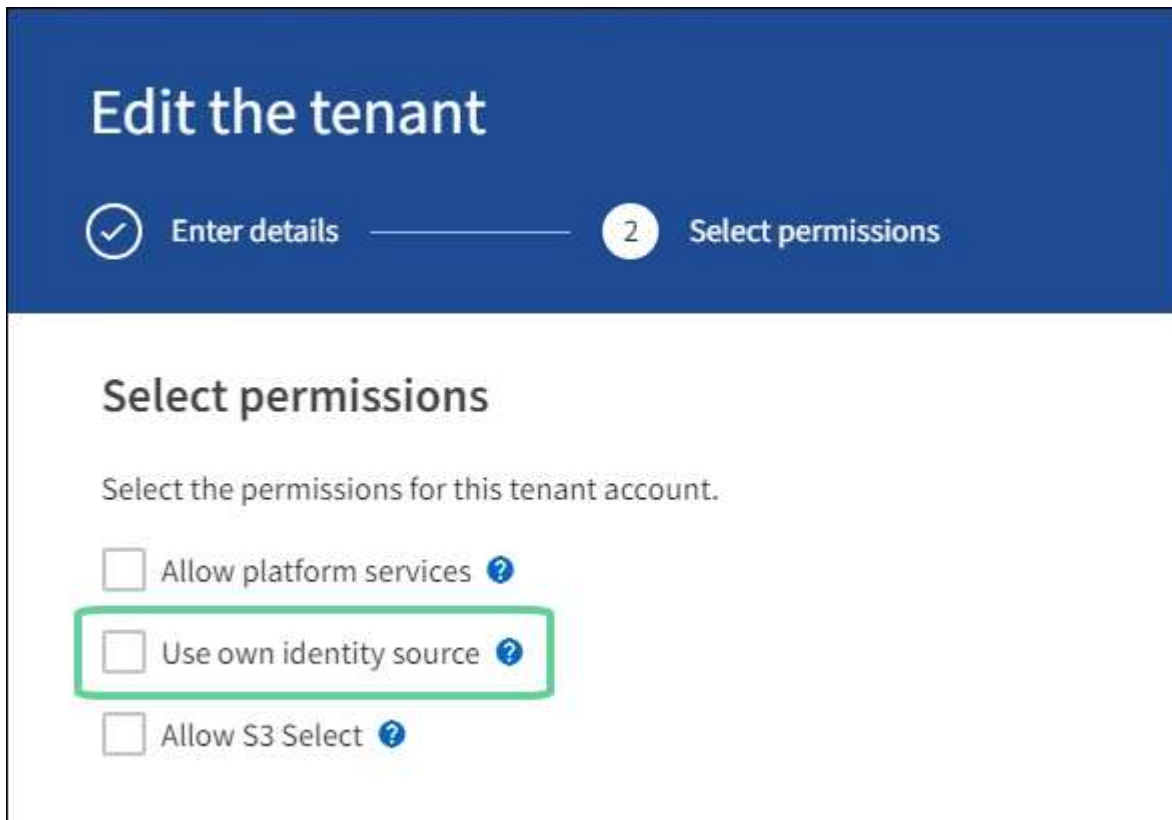
1. Se sono già presenti account tenant, verificare che nessuno dei tenant utilizzi la propria fonte di identità.



Quando si abilita SSO, un'origine identità configurata in Tenant Manager viene sostituita dall'origine identità configurata in Grid Manager. Gli utenti appartenenti all'origine identità del tenant non potranno più effettuare l'accesso a meno che non dispongano di un account con l'origine identità di Grid Manager.

- a. Sign in al Tenant Manager per ogni account tenant.
 - b. Selezionare **GESTIONE ACCESSI > Federazione identità**.
 - c. Verificare che la casella di controllo **Abilita federazione delle identità** non sia selezionata.
 - d. In tal caso, verificare che tutti i gruppi federati eventualmente utilizzati per questo account tenant non siano più necessari, deselezionare la casella di controllo e selezionare **Salva**.
2. Verificare che un utente federato possa accedere a Grid Manager:
 - a. Da Grid Manager, seleziona **CONFIGURAZIONE > Controllo accessi > Gruppi amministratori**.
 - b. Assicurarsi che almeno un gruppo federato sia stato importato dall'origine identità di Active Directory e che gli sia stata assegnata l'autorizzazione di accesso Root.
 - c. Disconnessione.
 - d. Conferma di poter accedere nuovamente a Grid Manager come utente del gruppo federato.
 3. Se sono presenti account tenant, verificare che un utente federato con autorizzazione di accesso Root possa accedere:
 - a. Da Grid Manager, seleziona **TENANTS**.
 - b. Selezionare l'account tenant e selezionare **Azioni > Modifica**.
 - c. Nella scheda Inserisci dettagli, seleziona **Continua**.
 - d. Se è selezionata la casella di controllo **Usa la propria fonte di identità**, deselezionarla e selezionare

Salva.



Viene visualizzata la pagina Inquilino.

- Selezionare l'account tenant, selezionare * Sign in* e accedere all'account tenant come utente root locale.
- Da Tenant Manager, seleziona **GESTIONE ACCESSI > Gruppi**.
- Assicurarsi che almeno a un gruppo federato di Grid Manager sia stata assegnata l'autorizzazione di accesso Root per questo tenant.
- Disconnessione.
- Conferma di poter accedere nuovamente al tenant come utente nel gruppo federato.

Informazioni correlate

- ["Requisiti e considerazioni per l'accesso singolo"](#)
- ["Gestisci gruppi di amministratori"](#)
- ["Utilizzare un account tenant"](#)

Utilizza la modalità sandbox

È possibile utilizzare la modalità sandbox per configurare e testare l'accesso singolo (SSO) prima di abilitarlo per tutti gli utenti StorageGRID . Dopo aver abilitato l'SSO, puoi tornare alla modalità sandbox ogni volta che hai bisogno di modificare o testare nuovamente la configurazione.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .

- Tu hai il "[Permesso di accesso root](#)".
- Hai configurato la federazione delle identità per il tuo sistema StorageGRID.
- Per il tipo di servizio LDAP di federazione delle identità, hai selezionato Active Directory o Azure, in base al provider di identità SSO che intendi utilizzare.

Tipo di servizio LDAP configurato	Opzioni per il provider di identità SSO
Directory attiva	• Directory attiva • Azzurro • PingFederate
Azzurro	Azzurro

Informazioni su questo compito

Quando l'SSO è abilitato e un utente tenta di accedere a un nodo di amministrazione, StorageGRID invia una richiesta di autenticazione al provider di identità SSO. A sua volta, il provider di identità SSO invia una risposta di autenticazione a StorageGRID, indicando se la richiesta di autenticazione è andata a buon fine. Per richieste andate a buon fine:

- La risposta da Active Directory o PingFederate include un identificatore univoco universale (UUID) per l'utente.
- La risposta di Azure include un nome dell'entità utente (UPN).

Per consentire a StorageGRID (il fornitore del servizio) e al provider di identità SSO di comunicare in modo sicuro sulle richieste di autenticazione degli utenti, è necessario configurare determinate impostazioni in StorageGRID. Successivamente, è necessario utilizzare il software del provider di identità SSO per creare un trust della relying party (AD FS), un'applicazione aziendale (Azure) o un provider di servizi (PingFederate) per ciascun nodo di amministrazione. Infine, è necessario tornare a StorageGRID per abilitare SSO.

La modalità sandbox semplifica l'esecuzione di questa configurazione avanti e indietro e il test di tutte le impostazioni prima di abilitare l'SSO. Quando si utilizza la modalità sandbox, gli utenti non possono accedere tramite SSO.

Accedi alla modalità sandbox

Passi

1. Selezionare **CONFIGURAZIONE > Controllo accessi > Single sign-on**.

Viene visualizzata la pagina Single Sign-on, con l'opzione **Disabilitato** selezionata.

Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO status ⓘ ☒ Disabled ☐ Sandbox Mode ☐ Enabled

Save



Se le opzioni di stato SSO non vengono visualizzate, verificare di aver configurato il provider di identità come origine dell'identità federata. Vedere ["Requisiti e considerazioni per l'accesso singolo"](#).

2. Selezionare **Modalità Sandbox**.

Viene visualizzata la sezione Provider di identità.

Inserisci i dettagli del provider di identità

Passi

1. Selezionare il **tipo SSO** dall'elenco a discesa.
2. Compila i campi nella sezione Identity Provider in base al tipo di SSO selezionato.

Directory attiva

- a. Immettere il **Nome del servizio federativo** per il provider di identità, esattamente come appare in Active Directory Federation Service (AD FS).



Per individuare il nome del servizio federativo, accedere a Windows Server Manager. Selezionare **Strumenti > Gestione AD FS**. Dal menu Azione, seleziona **Modifica proprietà del servizio federativo**. Nel secondo campo viene visualizzato il nome del servizio federativo.

- b. Specificare quale certificato TLS verrà utilizzato per proteggere la connessione quando il provider di identità invia informazioni di configurazione SSO in risposta alle richieste StorageGRID .

- **Utilizza il certificato CA del sistema operativo:** utilizza il certificato CA predefinito installato sul sistema operativo per proteggere la connessione.
- **Utilizza certificato CA personalizzato:** utilizza un certificato CA personalizzato per proteggere la connessione.

Se selezioni questa impostazione, copia il testo del certificato personalizzato e incollalo nella casella di testo **Certificato CA**.

- **Non utilizzare TLS:** non utilizzare un certificato TLS per proteggere la connessione.



Se si modifica il certificato CA, immediatamente ["riavviare il servizio mgmt-api sui nodi amministrativi"](#) e testare un SSO riuscito nel Grid Manager.

- c. Nella sezione Relying Party, specificare l'**identificatore del relying party** per StorageGRID. Questo valore controlla il nome utilizzato per ogni trust della relying party in AD FS.

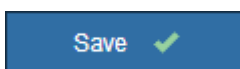
- Ad esempio, se la tua griglia ha un solo nodo amministrativo e non prevedi di aggiungerne altri in futuro, inserisci `SG O StorageGRID` .
- Se la griglia include più di un nodo di amministrazione, includi la stringa `[HOSTNAME]` nell'identificatore. Ad esempio, `SG- [HOSTNAME]` . Viene generata una tabella che mostra l'identificatore della parte affidabile per ciascun nodo di amministrazione nel sistema, in base al nome host del nodo.



È necessario creare un trust della relying party per ciascun nodo amministrativo nel sistema StorageGRID . La presenza di un trust di parte affidabile per ogni nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

- d. Seleziona **Salva**.

Per alcuni secondi sul pulsante **Salva** apparirà un segno di spunta verde.



Azzurro

- a. Specificare quale certificato TLS verrà utilizzato per proteggere la connessione quando il provider di identità invia informazioni di configurazione SSO in risposta alle richieste StorageGRID .

- **Utilizza il certificato CA del sistema operativo:** utilizza il certificato CA predefinito installato sul sistema operativo per proteggere la connessione.
- **Utilizza certificato CA personalizzato:** utilizza un certificato CA personalizzato per proteggere la connessione.

Se selezioni questa impostazione, copia il testo del certificato personalizzato e incollalo nella casella di testo **Certificato CA**.

- **Non utilizzare TLS:** non utilizzare un certificato TLS per proteggere la connessione.



Se si modifica il certificato CA, immediatamente ["riavviare il servizio mgmt-api sui nodi amministrativi"](#) e testare un SSO riuscito nel Grid Manager.

b. Nella sezione Applicazione aziendale, specificare il **Nome dell'applicazione aziendale** per StorageGRID. Questo valore controlla il nome utilizzato per ogni applicazione aziendale in Azure AD.

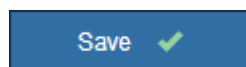
- Ad esempio, se la tua griglia ha un solo nodo amministrativo e non prevedi di aggiungerne altri in futuro, inserisci `SG O StorageGRID`.
- Se la griglia include più di un nodo di amministrazione, includi la stringa `[HOSTNAME]` nell'identificatore. Ad esempio, `SG- [HOSTNAME]`. Viene generata una tabella che mostra il nome dell'applicazione aziendale per ciascun nodo di amministrazione nel sistema, in base al nome host del nodo.



È necessario creare un'applicazione aziendale per ciascun nodo amministrativo nel sistema StorageGRID. Disporre di un'applicazione aziendale per ciascun nodo amministrativo garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo amministrativo.

- Segui i passaggi in ["Crea applicazioni aziendali in Azure AD"](#) per creare un'applicazione aziendale per ogni nodo amministrativo elencato nella tabella.
- Da Azure AD, copiare l'URL dei metadati della federazione per ogni applicazione aziendale. Quindi, incolla questo URL nel campo **URL metadati federazione** corrispondente in StorageGRID.
- Dopo aver copiato e incollato un URL dei metadati di federazione per tutti i nodi amministrativi, seleziona **Salva**.

Per alcuni secondi sul pulsante **Salva** apparirà un segno di spunta verde.



PingFederate

- Specificare quale certificato TLS verrà utilizzato per proteggere la connessione quando il provider di identità invia informazioni di configurazione SSO in risposta alle richieste StorageGRID.
 - **Utilizza il certificato CA del sistema operativo:** utilizza il certificato CA predefinito installato sul sistema operativo per proteggere la connessione.
 - **Utilizza certificato CA personalizzato:** utilizza un certificato CA personalizzato per proteggere la connessione.

Se selezioni questa impostazione, copia il testo del certificato personalizzato e incollalo nella casella di testo **Certificato CA**.

- **Non utilizzare TLS:** non utilizzare un certificato TLS per proteggere la connessione.



Se si modifica il certificato CA, immediatamente **"riavviare il servizio mgmt-api sui nodi amministrativi"** e testare un SSO riuscito nel Grid Manager.

- b. Nella sezione Fornitore di servizi (SP), specificare l'ID di connessione SP per StorageGRID. Questo valore controlla il nome utilizzato per ogni connessione SP in PingFederate.

- Ad esempio, se la tua griglia ha un solo nodo amministrativo e non prevedi di aggiungerne altri in futuro, inserisci `SG O StorageGRID`.
- Se la griglia include più di un nodo di amministrazione, includi la stringa `[HOSTNAME]` nell'identificatore. Ad esempio, `SG-[HOSTNAME]`. Viene generata una tabella che mostra l'ID di connessione SP per ciascun nodo di amministrazione nel sistema, in base al nome host del nodo.



È necessario creare una connessione SP per ciascun nodo amministrativo nel sistema StorageGRID. Disporre di una connessione SP per ciascun nodo amministrativo garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo amministrativo.

- c. Specificare l'URL dei metadati della federazione per ciascun nodo di amministrazione nel campo **URL dei metadati della federazione**.

Utilizzare il seguente formato:

```
https://<Federation Service  
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP  
Connection ID>
```

- d. Seleziona **Salva**.

Per alcuni secondi sul pulsante **Salva** apparirà un segno di spunta verde.

Save ✓

Configurare trust di relying party, applicazioni aziendali o connessioni SP

Una volta salvata la configurazione, viene visualizzato l'avviso di conferma della modalità Sandbox. Questa nota conferma che la modalità sandbox è ora abilitata e fornisce istruzioni generali.

StorageGRID può rimanere in modalità sandbox per tutto il tempo necessario. Tuttavia, quando nella pagina Single Sign-on è selezionata la **Modalità Sandbox**, l'SSO è disabilitato per tutti gli utenti StorageGRID. Possono effettuare l'accesso solo gli utenti locali.

Seguire questi passaggi per configurare trust di relying party (Active Directory), completare applicazioni

aziendali (Azure) o configurare connessioni SP (PingFederate).

Directory attiva

Passi

1. Vai ad Active Directory Federation Services (AD FS).
2. Creare uno o più trust di relying party per StorageGRID, utilizzando ciascun identificatore di relying party mostrato nella tabella nella pagina Single Sign-on StorageGRID .

È necessario creare un trust per ogni nodo amministrativo mostrato nella tabella.

Per le istruzioni, vai a ["Creare trust di relying party in AD FS"](#) .

Azzurro

Passi

1. Dalla pagina Single Sign-On per il nodo di amministrazione a cui hai effettuato l'accesso, seleziona il pulsante per scaricare e salvare i metadati SAML.
2. Quindi, per tutti gli altri nodi amministrativi nella griglia, ripeti questi passaggi:
 - a. Sign in al nodo.
 - b. Selezionare **CONFIGURAZIONE > Controllo accessi > Single sign-on**.
 - c. Scarica e salva i metadati SAML per quel nodo.
3. Vai al portale di Azure.
4. Segui i passaggi in ["Crea applicazioni aziendali in Azure AD"](#) per caricare il file di metadati SAML per ciascun nodo di amministrazione nella corrispondente applicazione aziendale di Azure.

PingFederate

Passi

1. Dalla pagina Single Sign-On per il nodo di amministrazione a cui hai effettuato l'accesso, seleziona il pulsante per scaricare e salvare i metadati SAML.
2. Quindi, per tutti gli altri nodi amministrativi nella griglia, ripeti questi passaggi:
 - a. Sign in al nodo.
 - b. Selezionare **CONFIGURAZIONE > Controllo accessi > Single sign-on**.
 - c. Scarica e salva i metadati SAML per quel nodo.
3. Vai su PingFederate.
4. ["Creare una o più connessioni al fornitore di servizi \(SP\) per StorageGRID"](#) . Utilizzare l'ID di connessione SP per ciascun nodo amministrativo (mostrato nella tabella nella pagina StorageGRID Single Sign-on) e i metadati SAML scaricati per tale nodo amministrativo.

È necessario creare una connessione SP per ogni nodo amministrativo mostrato nella tabella.

Test delle connessioni SSO

Prima di imporre l'uso dell'accesso singolo per l'intero sistema StorageGRID , è necessario verificare che l'accesso singolo e la disconnessione singola siano configurati correttamente per ciascun nodo di amministrazione.

Directory attiva

Passi

1. Nella pagina StorageGRID Single Sign-on, individuare il collegamento nel messaggio della modalità Sandbox.

L'URL deriva dal valore immesso nel campo **Nome del servizio federativo**.

Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

2. Seleziona il collegamento oppure copia e incolla l'URL in un browser per accedere alla pagina di accesso del tuo provider di identità.
3. Per confermare di poter utilizzare SSO per accedere a StorageGRID, seleziona * Sign in a uno dei seguenti siti*, seleziona l'identificativo della parte affidabile per il tuo nodo di amministrazione primario e seleziona * Sign in*.

You are not signed in.

☐ Sign in to this site.

☒ Sign in to one of the following sites:

SG-DC1-ADM1

Sign in

4. Inserisci il tuo nome utente e la tua password federati.
 - Se le operazioni di accesso e disconnessione SSO vanno a buon fine, viene visualizzato un messaggio di conferma.

✓ Single sign-on authentication and logout test completed successfully.

- Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risolvi il problema, cancella i cookie del browser e riprova.
5. Ripetere questi passaggi per verificare la connessione SSO per ciascun nodo amministrativo nella

griglia.

Azzurro

Passi

1. Vai alla pagina Single Sign-On nel portale di Azure.
2. Seleziona **Prova questa applicazione**.
3. Inserisci le credenziali di un utente federato.
 - Se le operazioni di accesso e disconnessione SSO vanno a buon fine, viene visualizzato un messaggio di conferma.

✓ Single sign-on authentication and logout test completed successfully.

- Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risolvi il problema, cancella i cookie del browser e riprova.
4. Ripetere questi passaggi per verificare la connessione SSO per ciascun nodo amministrativo nella griglia.

PingFederate

Passi

1. Dalla pagina StorageGRID Single Sign-on, selezionare il primo collegamento nel messaggio della modalità Sandbox.

Seleziona e testa un collegamento alla volta.

Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure service provider (SP) connections and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Ping Federate to create SP connections for StorageGRID. Create one SP connection for each Admin Node, using the relying party identifier(s) shown below.
2. Test SSO and SLO by selecting the link for each Admin Node:
 - [https://\[redacted\]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69](https://[redacted]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69)
 - [https://\[redacted\]/idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73](https://[redacted]/idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73)
3. StorageGRID displays a success or error message for each test.

When you have confirmed SSO for each SP connection and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and select **Save**.

2. Inserisci le credenziali di un utente federato.
 - Se le operazioni di accesso e disconnessione SSO vanno a buon fine, viene visualizzato un messaggio di conferma.

✓ Single sign-on authentication and logout test completed successfully.

- Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risolvi il problema, cancella i cookie del browser e riprova.
3. Seleziona il collegamento successivo per verificare la connessione SSO per ciascun nodo di amministrazione nella tua griglia.

Se vedi un messaggio di pagina scaduta, seleziona il pulsante **Indietro** nel tuo browser e invia nuovamente le tue credenziali.

Abilita l'accesso singolo

Dopo aver confermato di poter utilizzare SSO per accedere a ciascun nodo di amministrazione, puoi abilitare SSO per l'intero sistema StorageGRID .



Quando SSO è abilitato, tutti gli utenti devono utilizzare SSO per accedere a Grid Manager, Tenant Manager, Grid Management API e Tenant Management API. Gli utenti locali non possono più accedere a StorageGRID.

Passi

1. Selezionare **CONFIGURAZIONE > Controllo accessi > Single sign-on**.
2. Modificare lo stato SSO in **Abilitato**.
3. Seleziona **Salva**.
4. Rivedere il messaggio di avviso e selezionare **OK**.

Ora è abilitato l'accesso singolo.



Se si utilizza il portale di Azure e si accede a StorageGRID dallo stesso computer utilizzato per accedere ad Azure, assicurarsi che l'utente del portale di Azure sia anche un utente StorageGRID autorizzato (un utente in un gruppo federato importato in StorageGRID) oppure disconnettersi dal portale di Azure prima di tentare di accedere a StorageGRID.

Creare trust di relying party in AD FS

È necessario utilizzare Active Directory Federation Services (AD FS) per creare un trust della relying party per ogni nodo amministrativo nel sistema. È possibile creare trust di relying party utilizzando i comandi di PowerShell, importando metadati SAML da StorageGRID o immettendo i dati manualmente.

Prima di iniziare

- Hai configurato l'accesso Single Sign-On per StorageGRID e hai selezionato **AD FS** come tipo di SSO.
- La **modalità sandbox** è selezionata nella pagina Single sign-on in Grid Manager. Vedere ["Utilizza la modalità sandbox"](#).
- Conosci il nome di dominio completo (o l'indirizzo IP) e l'identificativo della parte affidabile per ciascun nodo di amministrazione nel tuo sistema. È possibile trovare questi valori nella tabella dei dettagli dei nodi di amministrazione nella pagina StorageGRID Single Sign-on.



È necessario creare un trust della relying party per ciascun nodo amministrativo nel sistema StorageGRID . La presenza di un trust di parte affidabile per ogni nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

- Hai esperienza nella creazione di trust relying party in AD FS oppure hai accesso alla documentazione di Microsoft AD FS.

- Stai utilizzando lo snap-in Gestione AD FS e appartieni al gruppo Amministratori.
- Se si crea manualmente il trust della relying party, si dispone del certificato personalizzato caricato per l'interfaccia di gestione StorageGRID oppure si sa come accedere a un nodo di amministrazione dalla shell dei comandi.

Informazioni su questo compito

Queste istruzioni si applicano a Windows Server 2016 AD FS. Se si utilizza una versione diversa di AD FS, si noteranno lievi differenze nella procedura. Per qualsiasi domanda, consultare la documentazione di Microsoft AD FS.

Creare un trust della relying party utilizzando Windows PowerShell

È possibile utilizzare Windows PowerShell per creare rapidamente uno o più trust relying party.

Passi

1. Dal menu Start di Windows, seleziona con il pulsante destro del mouse l'icona di PowerShell e seleziona **Esegui come amministratore**.
2. Al prompt dei comandi di PowerShell, immettere il seguente comando:

```
Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL
"https://Admin_Node_FQDN/api/saml-metadata"
```

- Per *Admin_Node_Identifier*, immettere l'identificatore della parte affidabile per il nodo di amministrazione, esattamente come appare nella pagina Single Sign-on. Ad esempio, SG-DC1-ADM1 .
- Per *Admin_Node_FQDN*, immettere il nome di dominio completo per lo stesso nodo di amministrazione. (Se necessario, è possibile utilizzare l'indirizzo IP del nodo. Tuttavia, se si immette un indirizzo IP, tenere presente che sarà necessario aggiornare o ricreare questo trust della relying party se l'indirizzo IP dovesse cambiare.)

3. Da Windows Server Manager, selezionare **Strumenti > Gestione AD FS**.

Viene visualizzato lo strumento di gestione AD FS.

4. Selezionare **AD FS > Trust delle parti affidabili**.

Viene visualizzato l'elenco dei trust delle parti affidanti.

5. Aggiungere una policy di controllo degli accessi al trust della relying party appena creato:
 - a. Individua il trust della parte affidabile che hai appena creato.
 - b. Fare clic con il pulsante destro del mouse sul trust e selezionare **Modifica criterio di controllo degli accessi**.
 - c. Selezionare una politica di controllo degli accessi.
 - d. Selezionare **Applica** e selezionare **OK**
6. Aggiungere una politica di emissione dei reclami al trust della parte affidabile appena creato:
 - a. Individua il trust della parte affidabile che hai appena creato.
 - b. Fare clic con il pulsante destro del mouse sul trust e selezionare **Modifica policy di emissione reclami**.
 - c. Seleziona **Aggiungi regola**.
 - d. Nella pagina Seleziona modello di regola, seleziona **Invia attributi LDAP come claim** dall'elenco e

seleziona **Avanti**.

e. Nella pagina Configura regola, immettere un nome visualizzato per questa regola.

Ad esempio, **ObjectGUID in Name ID** o **UPN in Name ID**.

f. Per l'Attribute Store, selezionare **Active Directory**.

g. Nella colonna Attributo LDAP della tabella Mapping, digitare **objectGUID** oppure selezionare **User-Principal-Name**.

h. Nella colonna Tipo di richiesta in uscita della tabella Mapping, selezionare **ID nome** dall'elenco a discesa.

i. Selezionare **Fine** e quindi **OK**.

7. Verificare che i metadati siano stati importati correttamente.

a. Fare clic con il pulsante destro del mouse sul trust della relying party per aprirne le proprietà.

b. Verificare che i campi nelle schede **Endpoint**, **Identificatori** e **Firma** siano compilati.

Se i metadati sono mancanti, verificare che l'indirizzo dei metadati della Federazione sia corretto oppure immettere i valori manualmente.

8. Ripetere questi passaggi per configurare un trust della relying party per tutti i nodi amministrativi nel sistema StorageGRID .

9. Al termine, torna a StorageGRID e verifica tutti i trust delle relying party per confermare che siano configurati correttamente. Vedere "[Utilizzare la modalità Sandbox](#)" per istruzioni.

Creare un trust della parte affidabile importando i metadati della federazione

È possibile importare i valori per ciascun trust della relying party accedendo ai metadati SAML per ciascun nodo di amministrazione.

Passi

1. In Windows Server Manager, seleziona **Strumenti**, quindi seleziona **Gestione AD FS**.

2. In Azioni, seleziona **Aggiungi trust della parte affidabile**.

3. Nella pagina di benvenuto, seleziona **Richiedi informazioni** e seleziona **Avvia**.

4. Selezionare **Importa dati sulla parte affidabile pubblicati online o su una rete locale**.

5. In **Indirizzo metadati federazione (nome host o URL)**, digitare la posizione dei metadati SAML per questo nodo di amministrazione:

```
https://Admin_Node_FQDN/api/saml-metadata
```

Per *Admin_Node_FQDN*, immettere il nome di dominio completo per lo stesso nodo di amministrazione. (Se necessario, è possibile utilizzare l'indirizzo IP del nodo. Tuttavia, se si immette un indirizzo IP, tenere presente che sarà necessario aggiornare o ricreare questo trust della relying party se l'indirizzo IP dovesse cambiare.)

6. Completare la procedura guidata Trust della parte affidabile, salvare il trust della parte affidabile e chiudere la procedura guidata.



Quando si immette il nome visualizzato, utilizzare l'identificatore della parte affidabile per il nodo di amministrazione, esattamente come appare nella pagina Single Sign-on in Grid Manager. Ad esempio, SG-DC1-ADM1 .

7. Aggiungi una regola di rivendicazione:

- a. Fare clic con il pulsante destro del mouse sul trust e selezionare **Modifica policy di emissione reclami**.
- b. Seleziona **Aggiungi regola**:
- c. Nella pagina Seleziona modello di regola, seleziona **Invia attributi LDAP come claim** dall'elenco e seleziona **Avanti**.
- d. Nella pagina Configura regola, immettere un nome visualizzato per questa regola.

Ad esempio, **ObjectGUID in Name ID** o **UPN in Name ID**.

- e. Per l'Attribute Store, selezionare **Active Directory**.
- f. Nella colonna Attributo LDAP della tabella Mapping, digitare **objectGUID** oppure selezionare **User-Principal-Name**.
- g. Nella colonna Tipo di richiesta in uscita della tabella Mapping, selezionare **ID nome** dall'elenco a discesa.
- h. Selezionare **Fine** e quindi **OK**.

8. Verificare che i metadati siano stati importati correttamente.

- a. Fare clic con il pulsante destro del mouse sul trust della relying party per aprirne le proprietà.
- b. Verificare che i campi nelle schede **Endpoint**, **Identificatori** e **Firma** siano compilati.

Se i metadati sono mancanti, verificare che l'indirizzo dei metadati della Federazione sia corretto oppure immettere i valori manualmente.

9. Ripetere questi passaggi per configurare un trust della relying party per tutti i nodi amministrativi nel sistema StorageGRID .

10. Al termine, torna a StorageGRID e verifica tutti i trust delle relying party per confermare che siano configurati correttamente. Vedere ["Utilizzare la modalità Sandbox"](#) per istruzioni.

Creare manualmente un trust della parte affidabile

Se si sceglie di non importare i dati per i trust delle parti affidabili, è possibile immettere i valori manualmente.

Passi

1. In Windows Server Manager, seleziona **Strumenti**, quindi seleziona **Gestione AD FS**.
2. In Azioni, seleziona **Aggiungi trust della parte affidabile**.
3. Nella pagina di benvenuto, seleziona **Richiedi informazioni** e seleziona **Avvia**.
4. Selezionare **Inserisci manualmente i dati sulla parte affidabile** e selezionare **Avanti**.
5. Completare la procedura guidata Trust della parte affidabile:

- a. Inserisci un nome visualizzato per questo nodo di amministrazione.

Per coerenza, utilizzare l'identificatore della parte affidabile per il nodo di amministrazione, esattamente come appare nella pagina Single Sign-on in Grid Manager. Ad esempio, SG-DC1-ADM1 .

- b. Salta il passaggio per configurare un certificato di crittografia token facoltativo.
- c. Nella pagina Configura URL, seleziona la casella di controllo **Abilita supporto per il protocollo SAML 2.0 WebSSO**.
- d. Digitare l'URL dell'endpoint del servizio SAML per il nodo di amministrazione:

`https://Admin_Node_FQDN/api/saml-response`

Per *Admin_Node_FQDN*, immettere il nome di dominio completo per il nodo di amministrazione. (Se necessario, è possibile utilizzare l'indirizzo IP del nodo. Tuttavia, se si immette un indirizzo IP, tenere presente che sarà necessario aggiornare o ricreare questo trust della relying party se l'indirizzo IP dovesse cambiare.)

- e. Nella pagina Configura identificatori, specificare l'identificatore della parte affidabile per lo stesso nodo di amministrazione:

Admin_Node_Identifier

Per *Admin_Node_Identifier*, immettere l'identificatore della parte affidabile per il nodo di amministrazione, esattamente come appare nella pagina Single Sign-on. Ad esempio, SG-DC1-ADM1.

- f. Rivedere le impostazioni, salvare il trust della relying party e chiudere la procedura guidata.

Viene visualizzata la finestra di dialogo Modifica policy di emissione reclami.



Se la finestra di dialogo non viene visualizzata, fare clic con il pulsante destro del mouse sul trust e selezionare **Modifica policy di emissione reclami**.

- 6. Per avviare la procedura guidata Claim Rules, seleziona **Aggiungi regola**:
 - a. Nella pagina Seleziona modello di regola, seleziona **Invia attributi LDAP come claim** dall'elenco e seleziona **Avanti**.
 - b. Nella pagina Configura regola, immettere un nome visualizzato per questa regola.

Ad esempio, **ObjectGUID in Name ID** o **UPN in Name ID**.
 - c. Per l'Attribute Store, selezionare **Active Directory**.
 - d. Nella colonna Attributo LDAP della tabella Mapping, digitare **objectGUID** oppure selezionare **User-Principal-Name**.
 - e. Nella colonna Tipo di richiesta in uscita della tabella Mapping, selezionare **ID nome** dall'elenco a discesa.
 - f. Selezionare **Fine** e quindi **OK**.
- 7. Fare clic con il pulsante destro del mouse sul trust della relying party per aprirne le proprietà.
- 8. Nella scheda **Endpoint**, configurare l'endpoint per la disconnessione singola (SLO):
 - a. Selezionare **Aggiungi SAML**.
 - b. Selezionare **Tipo di endpoint > Disconnessione SAML**.
 - c. Selezionare **Associa > Reindirizza**.
 - d. Nel campo **URL attendibile**, immettere l'URL utilizzato per la disconnessione singola (SLO) da questo nodo di amministrazione:

`https://Admin_Node_FQDN/api/saml-logout`

Per `Admin_Node_FQDN`, immettere il nome di dominio completo del nodo di amministrazione. (Se necessario, è possibile utilizzare l'indirizzo IP del nodo. Tuttavia, se si immette un indirizzo IP, tenere presente che sarà necessario aggiornare o ricreare questo trust della relying party se l'indirizzo IP dovesse cambiare.)

a. Selezionare **OK**.

9. Nella scheda **Firma**, specificare il certificato di firma per questo trust della parte affidabile:

a. Aggiungi il certificato personalizzato:

- Se disponi del certificato di gestione personalizzato caricato su StorageGRID, seleziona tale certificato.
- Se non si dispone del certificato personalizzato, accedere al nodo di amministrazione, andare su `/var/local/mgmt-api` directory del nodo di amministrazione e aggiungere il `custom-server.crt` file del certificato.



Utilizzo del certificato predefinito del nodo di amministrazione(`server.crt`) non è raccomandato. Se il nodo di amministrazione non funziona, il certificato predefinito verrà rigenerato quando si ripristina il nodo e sarà necessario aggiornare il trust della parte affidabile.

b. Selezionare **Applica** e quindi **OK**.

Le proprietà del relying party vengono salvate e chiuse.

10. Ripetere questi passaggi per configurare un trust della relying party per tutti i nodi amministrativi nel sistema StorageGRID .

11. Al termine, torna a StorageGRID e verifica tutti i trust delle relying party per confermare che siano configurati correttamente. Vedere "[Utilizza la modalità sandbox](#)" per istruzioni.

Crea applicazioni aziendali in Azure AD

Puoi utilizzare Azure AD per creare un'applicazione aziendale per ogni nodo di amministrazione del tuo sistema.

Prima di iniziare

- Hai iniziato a configurare l'accesso Single Sign-On per StorageGRID e hai selezionato **Azure** come tipo di SSO.
- La **modalità sandbox** è selezionata nella pagina Single sign-on in Grid Manager. Vedere "[Utilizza la modalità sandbox](#)".
- Per ogni nodo amministrativo del sistema è disponibile il **nome dell'applicazione aziendale**. È possibile copiare questi valori dalla tabella dei dettagli del nodo di amministrazione nella pagina Single Sign-on StorageGRID .



È necessario creare un'applicazione aziendale per ciascun nodo amministrativo nel sistema StorageGRID . Disporre di un'applicazione aziendale per ciascun nodo amministrativo garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo amministrativo.

- Hai esperienza nella creazione di applicazioni aziendali in Azure Active Directory.
- Hai un account Azure con una sottoscrizione attiva.
- Nell'account Azure ricopri uno dei seguenti ruoli: amministratore globale, amministratore dell'applicazione cloud, amministratore dell'applicazione o proprietario dell'entità servizio.

Accedi ad Azure AD

Passi

1. Accedi al "[Portale di Azure](#)".
2. Vai a "[Azure Active Directory](#)".
3. Selezionare "[Applicazioni aziendali](#)".

Crea applicazioni aziendali e salva la configurazione StorageGRID SSO

Per salvare la configurazione SSO per Azure in StorageGRID, è necessario utilizzare Azure per creare un'applicazione aziendale per ciascun nodo di amministrazione. Copiare gli URL dei metadati della federazione da Azure e incollarli nei campi **URL metadati della federazione** corrispondenti nella pagina Single Sign-on di StorageGRID.

Passi

1. Ripetere i seguenti passaggi per ciascun nodo di amministrazione.
 - a. Nel riquadro Applicazioni aziendali di Azure, seleziona **Nuova applicazione**.
 - b. Seleziona **Crea la tua applicazione**.
 - c. Per il nome, immettere il **Nome dell'applicazione aziendale** copiato dalla tabella dei dettagli del nodo di amministrazione nella pagina Single Sign-on StorageGRID.
 - d. Lascia selezionato il pulsante di opzione **Integra qualsiasi altra applicazione non presente nella galleria (Non nella galleria)**.
 - e. Seleziona **Crea**.
 - f. Selezionare il link **Inizia** nel **2. Impostare la casella Single Sign-On** oppure selezionare il collegamento **Single Sign-On** sul margine sinistro.
 - g. Selezionare la casella **SAML**.
 - h. Copia l'**URL dei metadati della federazione app**, che puoi trovare in **Certificato di firma SAML del passaggio 3**.
 - i. Vai alla pagina StorageGRID Single Sign-on e incolla l'URL nel campo **URL metadati federazione** che corrisponde al **Nome applicazione aziendale** utilizzato.
2. Dopo aver incollato un URL dei metadati di federazione per ciascun nodo di amministrazione e aver apportato tutte le altre modifiche necessarie alla configurazione SSO, selezionare **Salva** nella pagina StorageGRID Single Sign-on.

Scarica i metadati SAML per ogni nodo amministrativo

Dopo aver salvato la configurazione SSO, puoi scaricare un file di metadati SAML per ogni nodo amministrativo nel tuo sistema StorageGRID.

Passi

1. Ripetere questi passaggi per ogni nodo di amministrazione.

- a. Sign in a StorageGRID dal nodo di amministrazione.
- b. Selezionare **CONFIGURAZIONE > Controllo accessi > Single sign-on**.
- c. Selezionare il pulsante per scaricare i metadati SAML per quel nodo di amministrazione.
- d. Salva il file che caricherai in Azure AD.

Carica i metadati SAML in ogni applicazione aziendale

Dopo aver scaricato un file di metadati SAML per ogni nodo di amministrazione StorageGRID , eseguire i seguenti passaggi in Azure AD:

Passi

1. Torna al portale di Azure.
2. Ripetere questi passaggi per ogni applicazione aziendale:



Potrebbe essere necessario aggiornare la pagina Applicazioni aziendali per visualizzare le applicazioni aggiunte in precedenza all'elenco.

- a. Vai alla pagina Proprietà dell'applicazione aziendale.
 - b. Impostare **Assegnazione richiesta** su **No** (a meno che non si desideri configurare separatamente le assegnazioni).
 - c. Vai alla pagina Single Sign-On.
 - d. Completare la configurazione SAML.
 - e. Selezionare il pulsante **Carica file metadati** e selezionare il file metadati SAML scaricato per il nodo di amministrazione corrispondente.
 - f. Dopo aver caricato il file, seleziona **Salva** e poi **X** per chiudere il riquadro. Verrai reindirizzato alla pagina Imposta Single Sign-On con SAML.
3. Segui i passaggi in "[Utilizza la modalità sandbox](#)" per testare ogni applicazione.

Crea connessioni al fornitore di servizi (SP) in PingFederate

Puoi utilizzare PingFederate per creare una connessione al provider di servizi (SP) per ogni nodo amministrativo del tuo sistema. Per velocizzare il processo, importerai i metadati SAML da StorageGRID.

Prima di iniziare

- Hai configurato l'accesso Single Sign-On per StorageGRID e hai selezionato **Ping Federate** come tipo di SSO.
- La **modalità sandbox** è selezionata nella pagina Single sign-on in Grid Manager. Vedere "[Utilizza la modalità sandbox](#)".
- Hai l'*ID di connessione SP * per ogni nodo amministrativo nel tuo sistema. È possibile trovare questi valori nella tabella dei dettagli dei nodi di amministrazione nella pagina StorageGRID Single Sign-on.
- Hai scaricato i **metadati SAML** per ogni nodo amministrativo nel tuo sistema.
- Hai esperienza nella creazione di connessioni SP in PingFederate Server.
- Tu hai
il https://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html ["Guida di riferimento dell'amministratore"] per PingFederate Server. La documentazione

di PingFederate fornisce istruzioni e spiegazioni dettagliate passo dopo passo.

- Tu hai il ["Autorizzazione di amministratore"](#) per PingFederate Server.

Informazioni su questo compito

Queste istruzioni riepilogano come configurare PingFederate Server versione 10.3 come provider SSO per StorageGRID. Se si utilizza un'altra versione di PingFederate, potrebbe essere necessario adattare queste istruzioni. Per istruzioni dettagliate sulla tua versione, consulta la documentazione di PingFederate Server.

Prerequisiti completi in PingFederate

Prima di poter creare le connessioni SP che utilizzerai per StorageGRID, devi completare le attività preliminari in PingFederate. Le informazioni ricavate da questi prerequisiti verranno utilizzate durante la configurazione delle connessioni SP.

Crea archivio dati

Se non lo hai già fatto, crea un archivio dati per connettere PingFederate al server LDAP di AD FS. Utilizza i valori che hai utilizzato quando ["configurazione della federazione delle identità"](#) in StorageGRID.

- **Tipo:** Directory (LDAP)
- **Tipo LDAP:** Active Directory
- **Nome attributo binario:** immettere **objectGUID** nella scheda Attributi binari LDAP esattamente come mostrato.

Crea un validatore di credenziali password

Se non l'hai già fatto, crea un validatore di credenziali password.

- **Tipo:** Nome utente LDAP Password Validatore credenziali
- **Archivio dati:** seleziona l'archivio dati che hai creato.
- **Base di ricerca:** immettere le informazioni da LDAP (ad esempio, DC=saml,DC=sgws).
- **Filtro di ricerca:** sAMAccountName=\${username}
- **Ambito:** Sottoalbero

Crea istanza dell'adattatore IdP

Se non l'hai già fatto, crea un'istanza dell'adattatore IdP.

Passi

1. Vai su **Autenticazione > Integrazione > Schede IdP**.
2. Selezionare **Crea nuova istanza**.
3. Nella scheda Tipo, seleziona **Adattatore IdP modulo HTML**.
4. Nella scheda IdP Adapter, seleziona **Aggiungi una nuova riga a 'Validatori di credenziali'**.
5. Seleziona il [validatore di credenziali password](#) che hai creato.
6. Nella scheda Attributi adattatore, selezionare l'attributo **username** per **Pseudonimo**.
7. Seleziona **Salva**.

Crea o importa il certificato di firma

Se non l'hai già fatto, crea o importa il certificato di firma.

Passi

1. Vai a **Sicurezza > Chiavi e certificati di firma e decrittazione**.
2. Creare o importare il certificato di firma.

Crea una connessione SP in PingFederate

Quando si crea una connessione SP in PingFederate, si importano i metadati SAML scaricati da StorageGRID per il nodo di amministrazione. Il file di metadati contiene molti dei valori specifici di cui hai bisogno.



È necessario creare una connessione SP per ciascun nodo di amministrazione nel sistema StorageGRID, in modo che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo. Utilizzare queste istruzioni per creare la prima connessione SP. Poi vai a [Crea connessioni SP aggiuntive](#) per creare eventuali connessioni aggiuntive di cui hai bisogno.

Scegli il tipo di connessione SP

Passi

1. Vai su **Applicazioni > Integrazione > *Connessioni SP ***.
2. Seleziona **Crea connessione**.
3. Seleziona **Non utilizzare un modello per questa connessione**.
4. Selezionare **Profili SSO del browser** e **SAML 2.0** come protocollo.

Importa metadati SP

Passi

1. Nella scheda Importa metadati, seleziona **File**.
2. Seleziona il file di metadati SAML scaricato dalla pagina Single Sign-On StorageGRID per il nodo di amministrazione.
3. Esaminare il Riepilogo dei metadati e le informazioni fornite nella scheda Informazioni generali.

L'ID entità del partner e il nome della connessione sono impostati sull'ID di connessione StorageGRID SP. (ad esempio, 10.96.105.200-DC1-ADM1-105-200). L'URL di base è l'IP del nodo di amministrazione StorageGRID.

4. Selezionare **Avanti**.

Configurare l'SSO del browser IdP

Passi

1. Dalla scheda Browser SSO, seleziona **Configura Browser SSO**.
2. Nella scheda Profili SAML, seleziona le opzioni *** SP-initiated SSO***, *** SP-initial SLO***, **IdP-initiated SSO** e **IdP-initiated SLO**.
3. Selezionare **Avanti**.
4. Nella scheda Durata asserzione, non apportare modifiche.

5. Nella scheda Creazione asserzione, selezionare **Configura creazione asserzione**.
 - a. Nella scheda Mappatura identità, selezionare **Standard**.
 - b. Nella scheda Contratto attributo, utilizzare **SAML_SUBJECT** come Contratto attributo e il formato del nome non specificato che è stato importato.
6. Per estendere il contratto, selezionare **Elimina** per rimuovere il `urn:oid`, che non viene utilizzato.

Istanza dell'adattatore della mappa

Passi

1. Nella scheda Mapping origine autenticazione, selezionare **Mappa nuova istanza adattatore**.
2. Nella scheda Istanza adattatore, selezionare **istanza dell'adattatore** che hai creato.
3. Nella scheda Metodo di mappatura, seleziona **Recupera attributi aggiuntivi da un archivio dati**.
4. Nella scheda Origine attributo e ricerca utente, seleziona **Aggiungi origine attributo**.
5. Nella scheda Archivio dati, fornire una descrizione e selezionare **archivio dati** hai aggiunto.
6. Nella scheda Ricerca directory LDAP:
 - Immettere il **DN di base**, che deve corrispondere esattamente al valore immesso in StorageGRID per il server LDAP.
 - Per l'ambito di ricerca, selezionare **Sottoalbero**.
 - Per la classe dell'oggetto radice, cercare e aggiungere uno di questi attributi: **objectGUID** o **userPrincipalName**.
7. Nella scheda Tipi di codifica degli attributi binari LDAP, selezionare **Base64** per l'attributo **objectGUID**.
8. Nella scheda Filtro LDAP, immettere **sAMAccountName=\${username}**.
9. Nella scheda Adempimento contratto attributi, seleziona **LDAP (attributo)** dal menu a discesa Origine e seleziona **objectGUID** o **userPrincipalName** dal menu a discesa Valore.
10. Rivedere e quindi salvare la fonte dell'attributo.
11. Nella scheda Failsave Attribute Source, seleziona **Abort the SSO Transaction**.
12. Rivedi il riepilogo e seleziona **Fine**.
13. Selezionare **Fatto**.

Configurare le impostazioni del protocollo

Passi

1. Nella scheda **Connessione SP * > *SSO browser > Impostazioni protocollo**, selezionare **Configura impostazioni protocollo**.
2. Nella scheda URL del servizio consumer di asserzione, accettare i valori predefiniti, che sono stati importati dai metadati SAML StorageGRID (**POST** per Binding e `/api/saml-response` per l'URL dell'endpoint).
3. Nella scheda URL del servizio SLO, accettare i valori predefiniti, che sono stati importati dai metadati SAML StorageGRID (**REDIRECT** per Binding e `/api/saml-logout` per l'URL dell'endpoint).
4. Nella scheda Binding SAML consentiti, deselezionare **ARTIFACT** e **SOAP**. Sono richiesti solo **POST** e **REDIRECT**.
5. Nella scheda Criterio di firma, lasciare selezionate le caselle di controllo **Richiedi la firma delle richieste di autorizzazione** e **Firma sempre l'asserzione**.

6. Nella scheda Criterio di crittografia, selezionare **Nessuno**.
7. Rivedi il riepilogo e seleziona **Fine** per salvare le impostazioni del protocollo.
8. Rivedi il riepilogo e seleziona **Fine** per salvare le impostazioni SSO del browser.

Configurare le credenziali

Passi

1. Dalla scheda Connessione SP , selezionare **Credenziali**.
2. Dalla scheda Credenziali, seleziona **Configura credenziali**.
3. Seleziona il [certificato di firma](#) che hai creato o importato.
4. Selezionare **Avanti** per andare a **Gestisci impostazioni di verifica della firma**.
 - a. Nella scheda Modello di fiducia, seleziona **Non ancorato**.
 - b. Nella scheda Certificato di verifica della firma, rivedere le informazioni sul certificato di firma, importate dai metadati SAML StorageGRID .
5. Rivedere le schermate di riepilogo e selezionare **Salva** per salvare la connessione SP .

Crea connessioni SP aggiuntive

Puoi copiare la prima connessione SP per creare le connessioni SP necessarie per ogni nodo amministrativo nella tua griglia. Carichi nuovi metadati per ogni copia.



Le connessioni SP per diversi nodi amministrativi utilizzano impostazioni identiche, ad eccezione dell'ID entità del partner, dell'URL di base, dell'ID connessione, del nome della connessione, della verifica della firma e dell'URL di risposta SLO.

Passi

1. Selezionare **Azione > Copia** per creare una copia della connessione SP iniziale per ogni nodo amministrativo aggiuntivo.
2. Inserisci l'ID connessione e il Nome connessione per la copia e seleziona **Salva**.
3. Selezionare il file di metadati corrispondente al nodo di amministrazione:
 - a. Selezionare **Azione > Aggiorna con metadati**.
 - b. Seleziona **Scegli file** e carica i metadati.
 - c. Selezionare **Avanti**.
 - d. Seleziona **Salva**.
4. Risolvi l'errore dovuto all'attributo non utilizzato:
 - a. Selezionare la nuova connessione.
 - b. Selezionare **Configura SSO browser > Configura creazione asserzione > Contratto attributo**.
 - c. Elimina la voce per **urn:oid**.
 - d. Seleziona **Salva**.

Disabilitare l'accesso singolo

Se non si desidera più utilizzare questa funzionalità, è possibile disattivare l'accesso Single Sign-On (SSO). È necessario disabilitare l'accesso singolo prima di poter

disabilitare la federazione delle identità.

Prima di iniziare

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

Passi

1. Selezionare **CONFIGURAZIONE** > **Controllo accessi** > **Single sign-on**.

Viene visualizzata la pagina Single Sign-on.

2. Selezionare l'opzione **Disabilitato**.
3. Seleziona **Salva**.

Viene visualizzato un messaggio di avviso che indica che ora gli utenti locali potranno effettuare l'accesso.

4. Selezionare **OK**.

Al successivo accesso a StorageGRID , verrà visualizzata la pagina Sign in a StorageGRID e sarà necessario immettere il nome utente e la password di un utente StorageGRID locale o federato.

Disattivare e riattivare temporaneamente l'accesso singolo per un nodo di amministrazione

Potresti non essere in grado di accedere a Grid Manager se il sistema Single Sign-On (SSO) non funziona. In questo caso, puoi disattivare e riattivare temporaneamente l'SSO per un nodo di amministrazione. Per disattivare e riattivare l'SSO, è necessario accedere alla shell dei comandi del nodo.

Prima di iniziare

- Hai ["autorizzazioni di accesso specifiche"](#) .
- Tu hai il `Passwords.txt` file.
- Conosci la password dell'utente root locale.

Informazioni su questo compito

Dopo aver disabilitato l'SSO per un nodo di amministrazione, puoi accedere a Grid Manager come utente root locale. Per proteggere il sistema StorageGRID , è necessario utilizzare la shell dei comandi del nodo per riabilitare l'SSO sul nodo di amministrazione non appena si esegue la disconnessione.



La disabilitazione dell'SSO per un nodo amministrativo non influisce sulle impostazioni SSO per gli altri nodi amministrativi nella griglia. La casella di controllo **Abilita SSO** nella pagina Single Sign-on in Grid Manager rimane selezionata e tutte le impostazioni SSO esistenti vengono mantenute a meno che non vengano aggiornate.

Passi

1. Accedi a un nodo di amministrazione:
 - a. Immettere il seguente comando: `ssh admin@Admin_Node_IP`
 - b. Inserisci la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla root: `su -`

d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Eseguire il seguente comando: `disable-saml`

Un messaggio indica che il comando si applica solo a questo nodo di amministrazione.

3. Conferma che vuoi disabilitare l'SSO.

Un messaggio indica che l'accesso singolo è disabilitato sul nodo.

4. Da un browser Web, accedi a Grid Manager sullo stesso nodo di amministrazione.

Ora viene visualizzata la pagina di accesso di Grid Manager perché l'SSO è stato disabilitato.

5. Sign in con il nome utente root e la password dell'utente root locale.

6. Se hai disabilitato temporaneamente l'SSO perché dovevi correggere la configurazione dell'SSO:

- a. Selezionare **CONFIGURAZIONE > Controllo accessi > Single sign-on**.
- b. Modifica le impostazioni SSO errate o obsolete.
- c. Seleziona **Salva**.

Selezionando **Salva** dalla pagina Single Sign-on, l'SSO viene automaticamente riattivato per l'intera griglia.

7. Se hai disabilitato temporaneamente l'SSO perché avevi bisogno di accedere a Grid Manager per qualche altro motivo:

- a. Esegui qualsiasi compito o compiti che devi svolgere.
- b. Selezionare **Esci** e chiudere Grid Manager.
- c. Riattivare SSO sul nodo di amministrazione. È possibile eseguire uno dei seguenti passaggi:

- Eseguire il seguente comando: `enable-saml`

Un messaggio indica che il comando si applica solo a questo nodo di amministrazione.

Conferma di voler abilitare l'SSO.

Un messaggio indica che l'accesso singolo è abilitato sul nodo.

- Riavviare il nodo della griglia: `reboot`

8. Da un browser Web, accedere a Grid Manager dallo stesso nodo di amministrazione.

9. Verificare che venga visualizzata la pagina Sign in a StorageGRID e che sia necessario immettere le credenziali SSO per accedere a Grid Manager.

Utilizzare la federazione di griglia

Che cos'è la federazione di rete?

È possibile utilizzare la federazione di griglia per clonare i tenant e replicare i loro oggetti

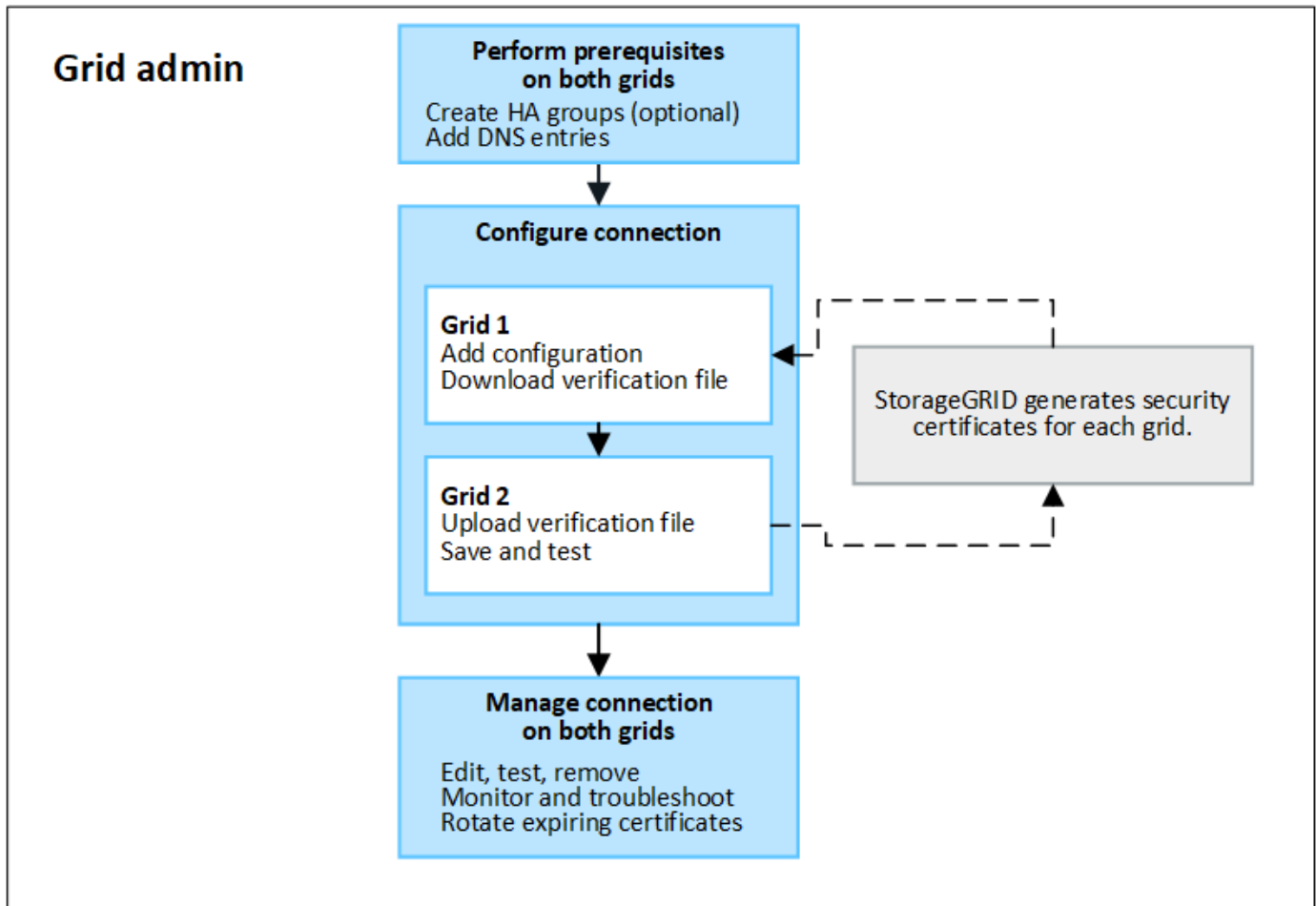
tra due sistemi StorageGRID per il ripristino di emergenza.

Che cos'è una connessione di federazione di rete?

Una connessione di federazione di griglia è una connessione bidirezionale, affidabile e sicura tra nodi di amministrazione e gateway in due sistemi StorageGRID .

Flusso di lavoro per la federazione della griglia

Il diagramma del flusso di lavoro riassume i passaggi per configurare una connessione di federazione di griglia tra due griglie.



Considerazioni e requisiti per le connessioni della federazione di rete

- Le griglie utilizzate per la federazione delle griglie devono eseguire versioni StorageGRID identiche o che non presentino più di una differenza di versione principale tra loro.

Per i dettagli sui requisiti di versione, fare riferimento a ["Note di rilascio"](#) .

- Una rete può avere una o più connessioni di federazione di rete ad altre reti. Ogni connessione della federazione di rete è indipendente da qualsiasi altra connessione. Ad esempio, se la Griglia 1 ha una connessione con la Griglia 2 e una seconda connessione con la Griglia 3, non vi è alcuna connessione implicita tra la Griglia 2 e la Griglia 3.
- Le connessioni della federazione di rete sono bidirezionali. Una volta stabilita la connessione, è possibile monitorarla e gestirla da entrambe le griglie.

- Deve esistere almeno una connessione di federazione di griglia prima di poter utilizzare ["clonazione dell'account"](#) O ["replicazione cross-grid"](#) .

Requisiti di rete e indirizzo IP

- Le connessioni di federazione della griglia possono verificarsi sulla rete della griglia, sulla rete di amministrazione o sulla rete client.
- Una connessione di federazione di rete collega una rete a un'altra rete. La configurazione per ciascuna griglia specifica un endpoint di federazione della griglia sull'altra griglia che è composta da nodi amministrativi, nodi gateway o entrambi.
- La pratica migliore è quella di connettersi ["gruppi ad alta disponibilità \(HA\)"](#) di nodi gateway e amministrativi su ciascuna griglia. L'utilizzo di gruppi HA aiuta a garantire che le connessioni della federazione di griglia rimangano online anche se i nodi non sono disponibili. Se l'interfaccia attiva in uno dei gruppi HA fallisce, la connessione può utilizzare un'interfaccia di backup.
- Non è consigliabile creare una connessione di federazione di griglia che utilizzi l'indirizzo IP di un singolo nodo di amministrazione o di un nodo gateway. Se il nodo non è più disponibile, anche la connessione alla federazione di rete non sarà più disponibile.
- ["Replicazione cross-grid"](#) degli oggetti richiede che i nodi di archiviazione su ciascuna griglia siano in grado di accedere ai nodi di amministrazione e gateway configurati sull'altra griglia. Per ogni griglia, verificare che tutti i nodi di archiviazione dispongano di un percorso ad alta larghezza di banda come i nodi di amministrazione o i nodi gateway utilizzati per la connessione.

Utilizzare i nomi di dominio completi (FQDN) per bilanciare il carico della connessione

Per un ambiente di produzione, utilizzare nomi di dominio completi (FQDN) per identificare ciascuna griglia nella connessione. Quindi, creare le voci DNS appropriate, come segue:

- FQDN per Grid 1 mappato a uno o più indirizzi IP virtuali (VIP) per gruppi HA in Grid 1 o all'indirizzo IP di uno o più nodi Admin o Gateway in Grid 1.
- FQDN per Grid 2 mappato a uno o più indirizzi VIP per Grid 2 o all'indirizzo IP di uno o più nodi Admin o Gateway in Grid 2.

Quando si utilizzano più voci DNS, le richieste di utilizzo della connessione vengono bilanciate nel modo seguente:

- Le voci DNS che mappano gli indirizzi VIP di più gruppi HA vengono bilanciate tra i nodi attivi nei gruppi HA.
- Le voci DNS che corrispondono agli indirizzi IP di più nodi amministrativi o nodi gateway vengono bilanciate tra i nodi mappati.

Requisiti portuali

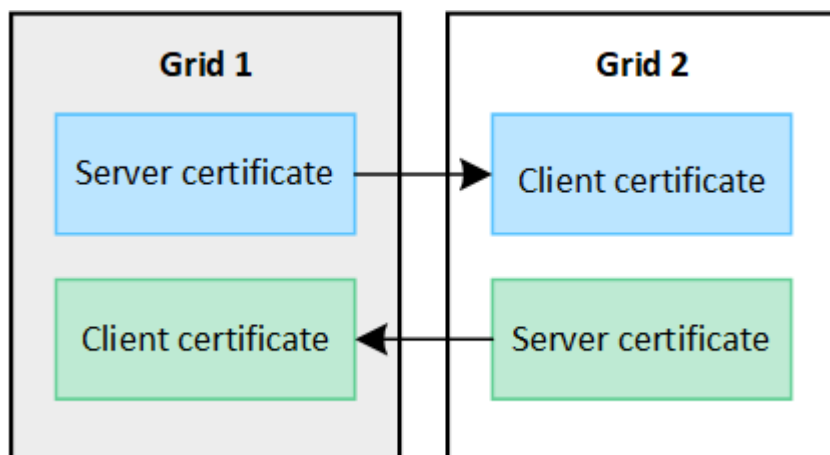
Quando si crea una connessione di federazione di griglia, è possibile specificare qualsiasi numero di porta non utilizzato compreso tra 23000 e 23999. Entrambe le griglie in questa connessione utilizzeranno la stessa porta.

È necessario assicurarsi che nessun nodo in entrambe le griglie utilizzi questa porta per altre connessioni.

Requisiti del certificato

Quando si configura una connessione di federazione di griglia, StorageGRID genera automaticamente quattro certificati SSL:

- Certificati server e client per autenticare e crittografare le informazioni inviate dalla griglia 1 alla griglia 2
- Certificati server e client per autenticare e crittografare le informazioni inviate dalla griglia 2 alla griglia 1



Per impostazione predefinita, i certificati sono validi per 730 giorni (2 anni). Quando questi certificati si avvicinano alla data di scadenza, l'avviso **Scadenza del certificato di federazione della griglia** ti ricorda di ruotare i certificati, operazione che puoi effettuare tramite Grid Manager.



Se i certificati su una delle estremità della connessione scadono, la connessione smetterà di funzionare. La replica dei dati sarà sospesa finché i certificati non saranno aggiornati.

Saperne di più

- ["Creare connessioni di federazione di griglia"](#)
- ["Gestire le connessioni della federazione di rete"](#)
- ["Risolvere gli errori di federazione della griglia"](#)

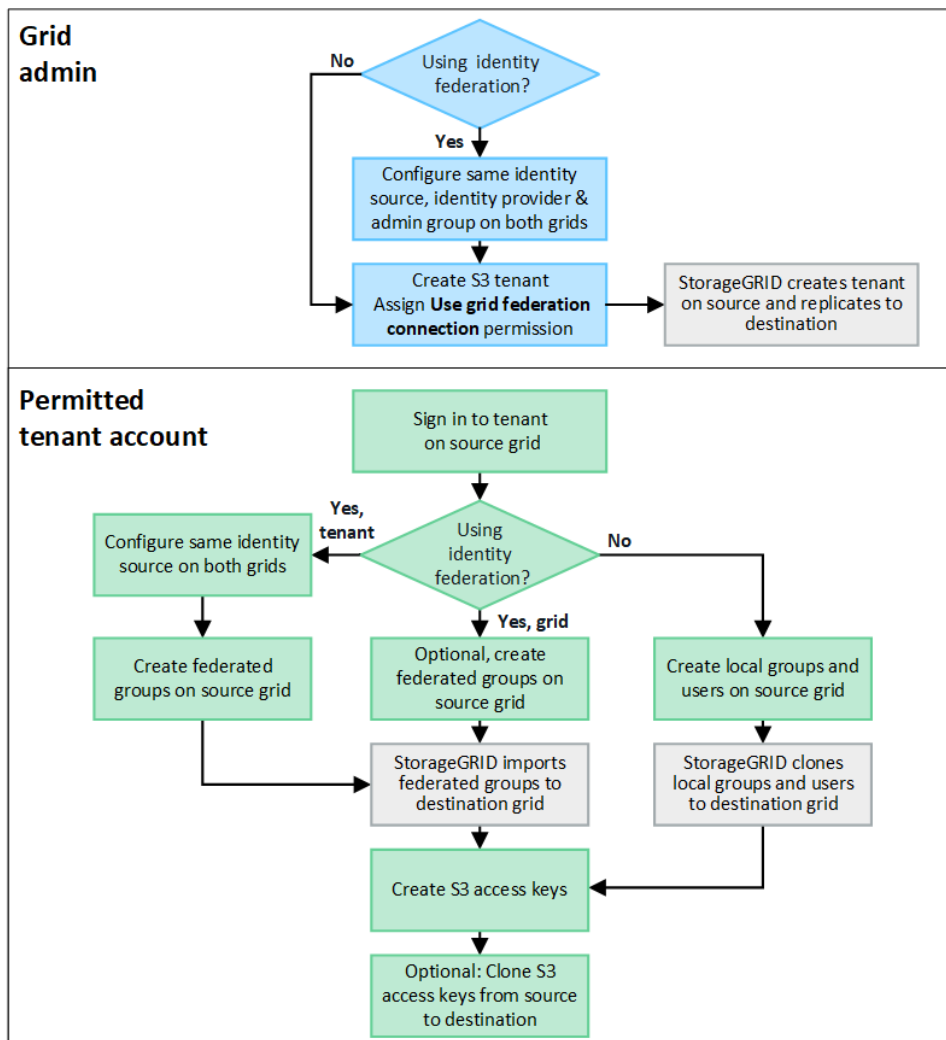
Che cos'è il clone dell'account?

Il clone dell'account è la replica automatica di un account tenant, gruppi tenant, utenti tenant e, facoltativamente, chiavi di accesso S3 tra i sistemi StorageGRID in un ["collegamento della federazione di rete"](#).

È richiesto il clone dell'account per ["replicazione cross-grid"](#). La clonazione delle informazioni dell'account da un sistema StorageGRID di origine a un sistema StorageGRID di destinazione garantisce che gli utenti e i gruppi tenant possano accedere ai bucket e agli oggetti corrispondenti su entrambe le griglie.

Flusso di lavoro per la clonazione dell'account

Il diagramma del flusso di lavoro mostra i passaggi che gli amministratori della griglia e i tenant autorizzati eseguiranno per configurare il clone dell'account. Questi passaggi vengono eseguiti dopo l'["la connessione della federazione di griglia è configurata"](#).



Flusso di lavoro dell'amministratore della griglia

I passaggi eseguiti dagli amministratori della griglia dipendono dal fatto che i sistemi StorageGRID nel "[collegamento della federazione di rete](#)" utilizzare l'accesso singolo (SSO) o la federazione delle identità.

Configura SSO per il clone dell'account (facoltativo)

Se uno dei sistemi StorageGRID nella connessione di federazione della griglia utilizza SSO, entrambe le griglie devono utilizzare SSO. Prima di creare gli account tenant per la federazione della griglia, gli amministratori della griglia di origine e di destinazione del tenant devono eseguire questi passaggi.

Passi

1. Configurare la stessa origine identità per entrambe le griglie. Vedere "[Utilizzare la federazione delle identità](#)".
2. Configurare lo stesso provider di identità SSO (IdP) per entrambe le griglie. Vedere "[Configurare l'accesso singolo](#)".
3. "[Crea lo stesso gruppo di amministratori](#)" su entrambe le griglie importando lo stesso gruppo federato.

Quando si crea il tenant, si selezionerà questo gruppo per avere l'autorizzazione di accesso Root iniziale sia per l'account tenant di origine che per quello di destinazione.



Se questo gruppo di amministratori non esiste su entrambe le griglie prima di creare il tenant, il tenant non verrà replicato nella destinazione.

Configura la federazione delle identità a livello di griglia per il clone dell'account (facoltativo)

Se uno dei sistemi StorageGRID utilizza la federazione delle identità senza SSO, entrambe le griglie devono utilizzare la federazione delle identità. Prima di creare gli account tenant per la federazione della griglia, gli amministratori della griglia di origine e di destinazione del tenant devono eseguire questi passaggi.

Passi

1. Configurare la stessa origine identità per entrambe le griglie. Vedere ["Utilizzare la federazione delle identità"](#).
2. Facoltativamente, se un gruppo federato avrà l'autorizzazione di accesso Root iniziale sia per gli account tenant di origine che di destinazione, ["creare lo stesso gruppo di amministratori"](#) su entrambe le griglie importando lo stesso gruppo federato.



Se si assegna l'autorizzazione di accesso Root a un gruppo federato che non esiste su entrambe le griglie, il tenant non viene replicato nella griglia di destinazione.

3. Se non si desidera che un gruppo federato disponga inizialmente dell'autorizzazione di accesso Root per entrambi gli account, specificare una password per l'utente root locale.

Crea un account tenant S3 consentito

Dopo aver configurato facoltativamente SSO o federazione delle identità, un amministratore della griglia esegue questi passaggi per determinare quali tenant possono replicare oggetti bucket su altri sistemi StorageGRID.

Passi

1. Determina quale griglia desideri che sia la griglia di origine del tenant per le operazioni di clonazione dell'account.

La griglia in cui il tenant viene creato originariamente è nota come *griglia sorgente* del tenant. La griglia in cui viene replicato il tenant è nota come *griglia di destinazione* del tenant.

2. Su quella griglia, crea un nuovo account tenant S3 o modifica un account esistente.
3. Assegnare l'autorizzazione **Usa connessione federazione griglia**.
4. Se l'account tenant gestirà i propri utenti federati, assegnare l'autorizzazione **Utilizza la propria origine identità**.

Se viene assegnata questa autorizzazione, sia l'account tenant di origine che quello di destinazione devono configurare la stessa origine identità prima di creare gruppi federati. I gruppi federati aggiunti al tenant di origine non possono essere clonati nel tenant di destinazione, a meno che entrambe le griglie non utilizzino la stessa origine identità.

5. Selezionare una connessione federata di rete specifica.
6. Salva il tenant nuovo o modificato.

Quando viene salvato un nuovo tenant con l'autorizzazione **Usa connessione federazione griglia**, StorageGRID crea automaticamente una replica di tale tenant sull'altra griglia, come segue:

- Entrambi gli account tenant hanno lo stesso ID account, nome, quota di archiviazione e autorizzazioni assegnate.
- Se hai selezionato un gruppo federato con autorizzazione di accesso Root per il tenant, quel gruppo viene clonato nel tenant di destinazione.
- Se hai selezionato un utente locale con autorizzazione di accesso Root per il tenant, tale utente verrà clonato nel tenant di destinazione. Tuttavia, la password di quell'utente non viene clonata.

Per maggiori dettagli, vedere ["Gestire gli inquilini autorizzati per la federazione della rete"](#).

Flusso di lavoro dell'account tenant consentito

Dopo che un tenant con l'autorizzazione **Usa connessione federazione griglia** è stato replicato nella griglia di destinazione, gli account tenant autorizzati possono eseguire questi passaggi per clonare gruppi tenant, utenti e chiavi di accesso S3.

Passi

1. Sign in all'account del tenant nella griglia di origine del tenant.
2. Se consentito, configurare la federazione delle identità sia sugli account tenant di origine che di destinazione.
3. Creare gruppi e utenti sul tenant di origine.

Quando vengono creati nuovi gruppi o utenti sul tenant di origine, StorageGRID li clona automaticamente sul tenant di destinazione, ma non avviene alcuna clonazione dalla destinazione all'origine.

4. Creare chiavi di accesso S3.
5. Facoltativamente, clonare le chiavi di accesso S3 dal tenant di origine al tenant di destinazione.

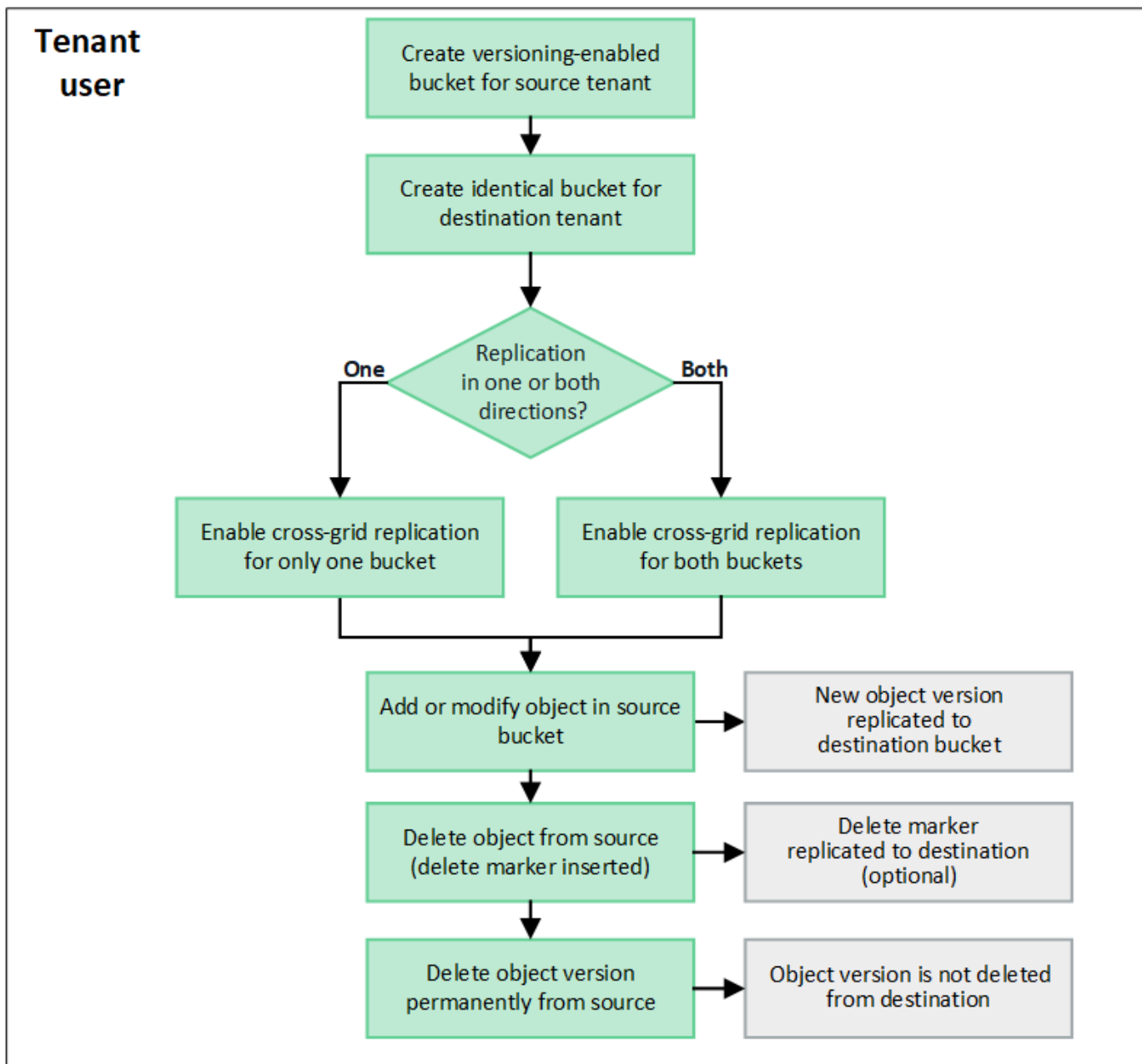
Per i dettagli sul flusso di lavoro dell'account tenant consentito e per sapere come vengono clonati gruppi, utenti e chiavi di accesso S3, vedere ["Clona gruppi tenant e utenti"](#) E ["Clona le chiavi di accesso S3 utilizzando l'API"](#).

Che cos'è la replicazione cross-grid?

La replicazione cross-grid è la replicazione automatica di oggetti tra bucket S3 selezionati in due sistemi StorageGRID connessi in un ["collegamento della federazione di rete"](#). ["Clonazione dell'account"](#) è necessario per la replicazione tra griglie.

Flusso di lavoro per la replicazione tra griglie

Il diagramma del flusso di lavoro riassume i passaggi per configurare la replica tra griglie tra bucket su due griglie.



Requisiti per la replicazione cross-grid

Se un account tenant ha l'autorizzazione **Usa connessione federazione griglia** per utilizzare una o più ["connessioni della federazione di rete"](#), un utente tenant con autorizzazione di accesso Root può creare bucket identici negli account tenant corrispondenti su ciascuna griglia. Questi secchi:

- Deve avere lo stesso nome ma può avere regioni diverse
- Deve essere abilitato il controllo delle versioni
- Deve avere il blocco oggetto S3 disabilitato
- Deve essere vuoto

Dopo aver creato entrambi i bucket, è possibile configurare la replica tra griglie per uno o entrambi i bucket.

Saperne di più

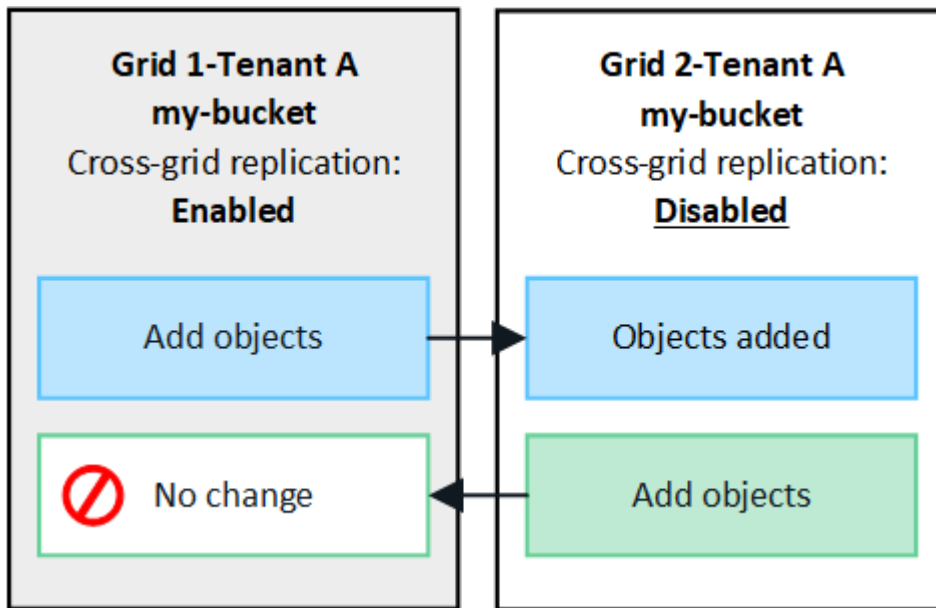
["Gestire la replicazione tra griglie"](#)

Come funziona la replicazione cross-grid

La replicazione tra griglie può essere configurata in modo che avvenga in una direzione o in entrambe le direzioni.

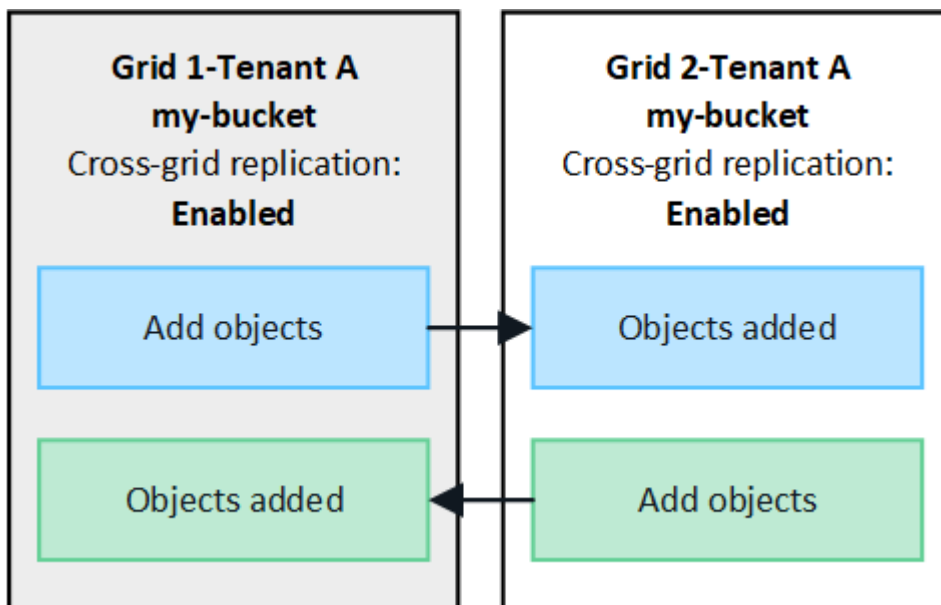
Replicazione in una direzione

Se si abilita la replica tra griglie per un bucket su una sola griglia, gli oggetti aggiunti a quel bucket (il bucket di origine) vengono replicati nel bucket corrispondente sull'altra griglia (il bucket di destinazione). Tuttavia, gli oggetti aggiunti al bucket di destinazione non vengono replicati nell'origine. Nella figura, la replicazione cross-grid è abilitata per `my-bucket` dalla Griglia 1 alla Griglia 2, ma non è abilitato nella direzione opposta.



Replicazione in entrambe le direzioni

Se si abilita la replica tra griglie per lo stesso bucket su entrambe le griglie, gli oggetti aggiunti a uno dei due bucket vengono replicati sull'altra griglia. Nella figura, la replicazione cross-grid è abilitata per `my-bucket` in entrambe le direzioni.



Cosa succede quando gli oggetti vengono ingeriti?

Quando un client S3 aggiunge un oggetto a un bucket in cui è abilitata la replica tra griglie, si verifica quanto segue:

1. StorageGRID replica automaticamente l'oggetto dal bucket di origine al bucket di destinazione. Il tempo necessario per eseguire questa operazione di replica in background dipende da diversi fattori, tra cui il numero di altre operazioni di replica in sospeso.

Il client S3 può verificare lo stato di replicazione di un oggetto inviando una richiesta `GetObject` o `HeadObject`. La risposta include uno StorageGRID specifico `x-ntap-sg-cgr-replication-status` intestazione di risposta, che avrà uno dei seguenti valori: Il client S3 può verificare lo stato di replicazione di un oggetto emettendo una richiesta `GetObject` o `HeadObject`. La risposta include uno StorageGRID specifico `x-ntap-sg-cgr-replication-status` intestazione di risposta, che avrà uno dei seguenti valori:

Griglia	Stato di replicazione
Fonte	• COMPLETO: La replica è riuscita per tutte le connessioni alla rete. • IN ATTESA: l'oggetto non è stato replicato su almeno una connessione alla griglia. • ERRORE: la replica non è in sospeso per nessuna connessione alla rete e almeno una è fallita con un errore permanente. Un utente deve risolvere l'errore.
Destinazione	REPLICA : L'oggetto è stato replicato dalla griglia di origine.



StorageGRID non supporta il `x-amz-replication-status` intestazione.

2. StorageGRID utilizza le policy ILM attive di ogni griglia per gestire gli oggetti, proprio come farebbe con qualsiasi altro oggetto. Ad esempio, l'Oggetto A sulla Griglia 1 potrebbe essere archiviato come due copie replicate e conservato per sempre, mentre la copia dell'Oggetto A replicata sulla Griglia 2 potrebbe essere archiviata utilizzando la codifica di cancellazione 2+1 ed eliminata dopo tre anni.

Cosa succede quando gli oggetti vengono eliminati?

Come descritto in "[Elimina flusso di dati](#)" StorageGRID può eliminare un oggetto per uno qualsiasi di questi motivi:

- Il client S3 invia una richiesta di eliminazione.
- Un utente Tenant Manager seleziona "[Elimina gli oggetti nel bucket](#)" opzione per rimuovere tutti gli oggetti da un bucket.
- Il bucket ha una configurazione del ciclo di vita che scade.
- L'ultimo periodo di tempo nella regola ILM per l'oggetto termina e non sono specificati ulteriori posizionamenti.

Quando StorageGRID elimina un oggetto a causa di un'operazione di eliminazione degli oggetti nel bucket, della scadenza del ciclo di vita del bucket o della scadenza del posizionamento ILM, l'oggetto replicato non viene mai eliminato dall'altra griglia in una connessione di federazione di griglia. Tuttavia, i marcatori di eliminazione aggiunti al bucket di origine dalle eliminazioni del client S3 possono essere facoltativamente

replicati nel bucket di destinazione.

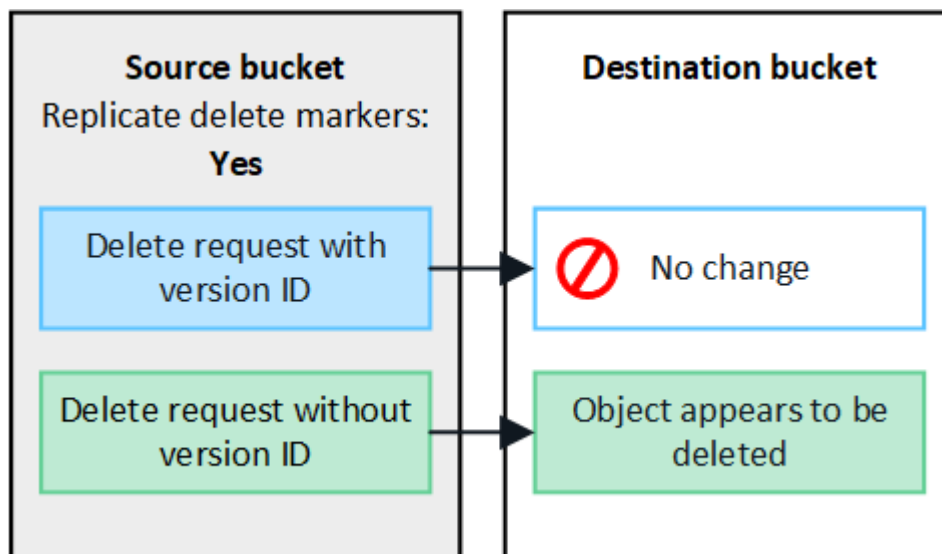
Per capire cosa succede quando un client S3 elimina oggetti da un bucket in cui è abilitata la replica tra griglie, esamina come i client S3 eliminano oggetti dai bucket in cui è abilitato il controllo delle versioni, come segue:

- Se un client S3 invia una richiesta di eliminazione che include un ID versione, quella versione dell'oggetto viene rimossa definitivamente. Nessun marcatore di eliminazione viene aggiunto al bucket.
- Se un client S3 invia una richiesta di eliminazione che non include un ID versione, StorageGRID non elimina alcuna versione dell'oggetto. Invece, aggiunge un marcatore di eliminazione al bucket. Il marcatore di eliminazione fa sì che StorageGRID agisca come se l'oggetto fosse stato eliminato:
 - Una richiesta `GetObject` senza un ID versione fallirà con `404 No Object Found`
 - Una richiesta `GetObject` con un ID versione valido avrà esito positivo e restituirà la versione dell'oggetto richiesta.

Quando un client S3 elimina un oggetto da un bucket in cui è abilitata la replica tra griglie, StorageGRID determina se replicare la richiesta di eliminazione nella destinazione, come segue:

- Se la richiesta di eliminazione include un ID versione, la versione dell'oggetto viene rimossa definitivamente dalla griglia di origine. Tuttavia, StorageGRID non replica le richieste di eliminazione che includono un ID versione, quindi la stessa versione dell'oggetto non viene eliminata dalla destinazione.
- Se la richiesta di eliminazione non include un ID versione, StorageGRID può facoltativamente replicare il marcatore di eliminazione, in base alla configurazione della replica tra griglie per il bucket:
 - Se si sceglie di replicare i marcatori di eliminazione (impostazione predefinita), un marcatore di eliminazione viene aggiunto al bucket di origine e replicato nel bucket di destinazione. In effetti, l'oggetto sembra essere stato eliminato su entrambe le griglie.
 - Se si sceglie di non replicare i marcatori di eliminazione, un marcatore di eliminazione viene aggiunto al bucket di origine ma non viene replicato nel bucket di destinazione. In effetti, gli oggetti eliminati nella griglia di origine non vengono eliminati nella griglia di destinazione.

Nella figura, **Replica elimina marcatori** è stato impostato su **Sì** quando "è stata abilitata la replicazione cross-grid". Le richieste di eliminazione per il bucket di origine che includono un ID versione non elimineranno gli oggetti dal bucket di destinazione. Le richieste di eliminazione per il bucket di origine che non includono un ID versione verranno visualizzate per eliminare gli oggetti nel bucket di destinazione.





Se si desidera mantenere sincronizzate le eliminazioni degli oggetti tra le griglie, creare le corrispondenti ["Configurazioni del ciclo di vita S3"](#) per i bucket su entrambe le griglie.

Come vengono replicati gli oggetti crittografati

Quando si utilizza la replica tra griglie per replicare oggetti tra griglie, è possibile crittografare singoli oggetti, utilizzare la crittografia predefinita dei bucket o configurare la crittografia a livello di griglia. È possibile aggiungere, modificare o rimuovere le impostazioni di crittografia predefinite per bucket o griglia prima o dopo aver abilitato la replica tra griglie per un bucket.

Per crittografare singoli oggetti, è possibile utilizzare SSE (crittografia lato server con chiavi gestite StorageGRID) quando si aggiungono gli oggetti al bucket di origine. Utilizzare il `x-amz-server-side-encryption` intestazione della richiesta e specificare `AES256`. Vedere ["Utilizzare la crittografia lato server"](#).



L'utilizzo di SSE-C (crittografia lato server con chiavi fornite dal cliente) non è supportato per la replica tra griglie. L'operazione di acquisizione non andrà a buon fine.

Per utilizzare la crittografia predefinita per un bucket, utilizzare una richiesta `PutBucketEncryption` e impostare `SSEAlgorithm` parametro a `AES256`. La crittografia a livello di bucket si applica a tutti gli oggetti ingeriti senza `x-amz-server-side-encryption` intestazione della richiesta. Vedere ["Operazioni sui bucket"](#).

Per utilizzare la crittografia a livello di griglia, impostare l'opzione **Crittografia degli oggetti memorizzati su AES-256**. La crittografia a livello di griglia si applica a tutti gli oggetti che non sono crittografati a livello di bucket o che vengono acquisiti senza `x-amz-server-side-encryption` intestazione della richiesta. Vedere ["Configurare le opzioni di rete e oggetto"](#).



SSE non supporta AES-128. Se l'opzione **Crittografia degli oggetti archiviati** è abilitata per la griglia di origine utilizzando l'opzione **AES-128**, l'uso dell'algoritmo AES-128 non verrà propagato all'oggetto replicato. Al contrario, l'oggetto replicato utilizzerà il bucket predefinito della destinazione o l'impostazione di crittografia a livello di griglia, se disponibile.

Quando si determina come crittografare gli oggetti sorgente, StorageGRID applica queste regole:

1. Utilizzare il `x-amz-server-side-encryption` intestazione di acquisizione, se presente.
2. Se non è presente un'intestazione di acquisizione, utilizzare l'impostazione di crittografia predefinita del bucket, se configurata.
3. Se non è configurata un'impostazione bucket, utilizzare l'impostazione di crittografia a livello di griglia, se configurata.
4. Se non è presente un'impostazione a livello di griglia, non crittografare l'oggetto sorgente.

Quando si determina come crittografare gli oggetti replicati, StorageGRID applica queste regole nel seguente ordine:

1. Utilizzare la stessa crittografia dell'oggetto sorgente, a meno che l'oggetto non utilizzi la crittografia AES-128.
2. Se l'oggetto di origine non è crittografato o utilizza AES-128, utilizzare l'impostazione di crittografia predefinita del bucket di destinazione, se configurata.
3. Se il bucket di destinazione non dispone di un'impostazione di crittografia, utilizzare l'impostazione di crittografia a livello di griglia della destinazione, se configurata.
4. Se non è presente un'impostazione a livello di griglia, non crittografare l'oggetto di destinazione.

PutObjectTagging e DeleteObjectTagging non sono supportati

Le richieste PutObjectTagging e DeleteObjectTagging non sono supportate per gli oggetti nei bucket in cui è abilitata la replica tra griglie.

Se un client S3 emette una richiesta PutObjectTagging o DeleteObjectTagging, 501 Not Implemented viene restituito. Il messaggio è Put (Delete) ObjectTagging is not available for buckets that have cross-grid replication configured.

Come vengono replicati gli oggetti segmentati

La dimensione massima del segmento della griglia di origine si applica agli oggetti replicati nella griglia di destinazione. Quando gli oggetti vengono replicati su un'altra griglia, l'impostazione **Dimensione massima segmento (CONFIGURAZIONE > Sistema > Opzioni di archiviazione)** della griglia di origine verrà utilizzata su entrambe le griglie. Ad esempio, supponiamo che la dimensione massima del segmento per la griglia di origine sia 1 GB, mentre la dimensione massima del segmento per la griglia di destinazione sia 50 MB. Se si acquisisce un oggetto da 2 GB nella griglia di origine, tale oggetto viene salvato come due segmenti da 1 GB. Verrà inoltre replicato nella griglia di destinazione come due segmenti da 1 GB, anche se la dimensione massima del segmento di quella griglia è di 50 MB.

Confronta la replicazione cross-grid e la replicazione CloudMirror

Quando inizi a utilizzare la federazione di griglia, rivedi le somiglianze e le differenze tra ["replicazione cross-grid"](#) e il ["Servizio di replica StorageGRID CloudMirror"](#).

	Replicazione cross-grid	Servizio di replica CloudMirror
Qual è lo scopo principale?	Un sistema StorageGRID funge da sistema di disaster recovery. Gli oggetti in un bucket possono essere replicati tra le griglie in una o entrambe le direzioni.	Consente a un tenant di replicare automaticamente gli oggetti da un bucket in StorageGRID (origine) a un bucket S3 esterno (destinazione). La replica CloudMirror crea una copia indipendente di un oggetto in un'infrastruttura S3 indipendente. Questa copia indipendente non viene utilizzata come backup, ma spesso viene ulteriormente elaborata nel cloud.
Come è impostato?	1. Configurare una connessione di federazione di rete tra due reti. 2. Aggiungere nuovi account tenant, che vengono automaticamente clonati nell'altra griglia. 3. Aggiungere nuovi gruppi di tenant e utenti, che vengono anch'essi clonati. 4. Crea bucket corrispondenti su ogni griglia e abilita la replica tra griglie in una o entrambe le direzioni.	1. Un utente tenant configura la replica di CloudMirror definendo un endpoint CloudMirror (indirizzo IP, credenziali e così via) tramite Tenant Manager o l'API S3. 2. Qualsiasi bucket di proprietà di quell'account tenant può essere configurato in modo che punti all'endpoint CloudMirror.

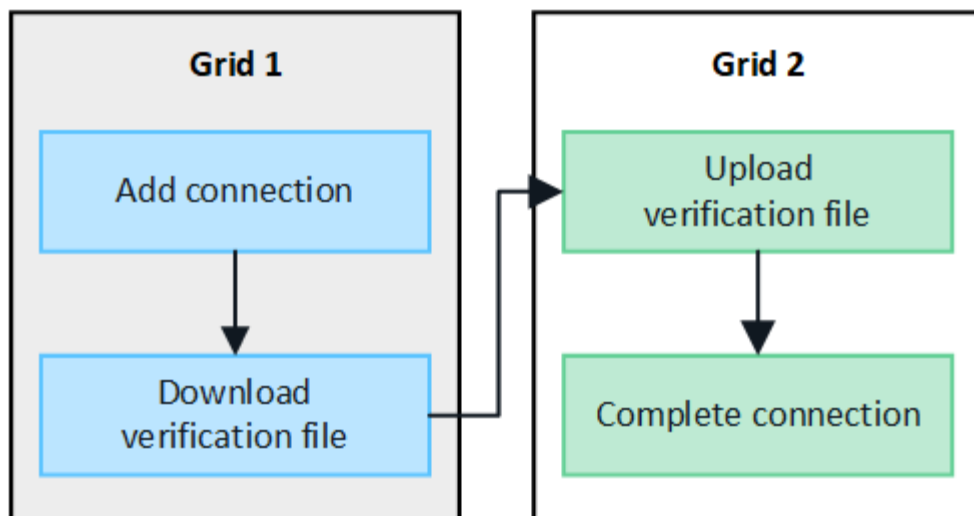
	Replicazione cross-grid	Servizio di replica CloudMirror
Chi è responsabile della sua istituzione?	• Un amministratore di rete configura la connessione e i tenant. • Gli utenti tenant configurano i gruppi, gli utenti, le chiavi e i bucket.	In genere, un utente tenant.
Qual è la destinazione?	Un bucket S3 corrispondente e identico sull'altro sistema StorageGRID nella connessione di federazione della griglia.	• Qualsiasi infrastruttura S3 compatibile (incluso Amazon S3). • Piattaforma Google Cloud (GCP)
È necessario il controllo delle versioni degli oggetti?	Sì, sia il bucket di origine che quello di destinazione devono avere il controllo delle versioni degli oggetti abilitato.	No, la replica di CloudMirror supporta qualsiasi combinazione di bucket con e senza versione, sia nell'origine che nella destinazione.
Cosa determina lo spostamento degli oggetti verso la destinazione?	Gli oggetti vengono replicati automaticamente quando vengono aggiunti a un bucket in cui è abilitata la replica tra griglie.	Gli oggetti vengono replicati automaticamente quando vengono aggiunti a un bucket configurato con un endpoint CloudMirror. Gli oggetti presenti nel bucket di origine prima che il bucket fosse configurato con l'endpoint CloudMirror non vengono replicati, a meno che non vengano modificati.
Come vengono replicati gli oggetti?	La replica tra griglie crea oggetti con versione e replica l'ID della versione dal bucket di origine al bucket di destinazione. Ciò consente di mantenere l'ordine delle versioni su entrambe le griglie.	La replica di CloudMirror non richiede bucket abilitati al controllo delle versioni, quindi CloudMirror può gestire l'ordinamento solo per una chiave all'interno di un sito. Non vi è alcuna garanzia che l'ordinamento verrà mantenuto per le richieste di un oggetto in un sito diverso.
Cosa succede se un oggetto non può essere replicato?	L'oggetto viene messo in coda per la replica, nel rispetto dei limiti di archiviazione dei metadati.	L'oggetto è in coda per la replica, soggetto ai limiti dei servizi della piattaforma (vedere "Raccomandazioni per l'utilizzo dei servizi della piattaforma").
I metadati di sistema dell'oggetto vengono replicati?	Sì, quando un oggetto viene replicato sull'altra griglia, vengono replicati anche i suoi metadati di sistema. I metadati saranno identici su entrambe le griglie.	No, quando un oggetto viene replicato nel bucket esterno, i suoi metadati di sistema vengono aggiornati. I metadati varieranno a seconda della posizione, a seconda del momento dell'acquisizione e del comportamento dell'infrastruttura S3 indipendente.

	Replicazione cross-grid	Servizio di replica CloudMirror
Come vengono recuperati gli oggetti?	Le applicazioni possono recuperare o leggere oggetti inviando una richiesta al bucket su una delle due griglie.	Le applicazioni possono recuperare o leggere oggetti inviando una richiesta a StorageGRID o alla destinazione S3. Supponiamo, ad esempio, di utilizzare la replica CloudMirror per eseguire il mirroring degli oggetti su un'organizzazione partner. Il partner può utilizzare le proprie applicazioni per leggere o aggiornare gli oggetti direttamente dalla destinazione S3. Non è obbligatorio utilizzare StorageGRID .
Cosa succede se un oggetto viene eliminato?	• Le richieste di eliminazione che includono un ID versione non vengono mai replicate nella griglia di destinazione. • Le richieste di eliminazione che non includono un ID versione aggiungono un marcatore di eliminazione al bucket di origine, che può essere facoltativamente replicato nella griglia di destinazione. • Se la replica tra griglie è configurata per una sola direzione, gli oggetti nel bucket di destinazione possono essere eliminati senza influire sulla sorgente.	I risultati varieranno in base allo stato di versioning dei bucket di origine e di destinazione (che non devono essere necessariamente gli stessi): • Se entrambi i bucket sono sottoposti a versioning, una richiesta di eliminazione aggiungerà un marcatore di eliminazione in entrambe le posizioni. • Se solo il bucket di origine è sottoposto a versioning, una richiesta di eliminazione aggiungerà un marcatore di eliminazione all'origine ma non alla destinazione. • Se nessuno dei due bucket è sottoposto a versioning, una richiesta di eliminazione eliminerà l'oggetto dall'origine ma non dalla destinazione. Allo stesso modo, gli oggetti nel bucket di destinazione possono essere eliminati senza influire sulla sorgente.

Creare connessioni di federazione di griglia

È possibile creare una connessione di federazione di griglia tra due sistemi StorageGRID se si desidera clonare i dettagli dei tenant e replicare i dati degli oggetti.

Come mostrato nella figura, la creazione di una connessione di federazione di griglia include passaggi su entrambe le griglie. Si aggiunge la connessione su una griglia e la si completa sull'altra griglia. È possibile iniziare da entrambe le griglie.



Prima di iniziare

- Hai esaminato il "[considerazioni e requisiti](#)" per configurare le connessioni della federazione di griglia.
- Se si prevede di utilizzare nomi di dominio completi (FQDN) per ogni griglia anziché indirizzi IP o VIP, si sa quali nomi utilizzare e si è verificato che il server DNS per ogni griglia disponga delle voci appropriate.
- Stai utilizzando un "[browser web supportato](#)".
- Hai l'autorizzazione di accesso Root e la passphrase di provisioning per entrambe le griglie.

Aggiungi connessione

Eseguire questi passaggi su uno dei due sistemi StorageGRID .

Passi

1. Sign in a Grid Manager dal nodo di amministrazione principale su una delle due griglie.
2. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.
3. Seleziona **Aggiungi connessione**.
4. Inserisci i dettagli per la connessione.

Campo	Descrizione
Nome della connessione	Un nome univoco che ti aiuti a riconoscere questa connessione, ad esempio "Griglia 1-Griglia 2".
FQDN o IP per questa griglia	Uno dei seguenti: • Il nome di dominio completo della griglia a cui hai effettuato l'accesso • Un indirizzo VIP di un gruppo HA su questa griglia • Un indirizzo IP di un nodo di amministrazione o di un nodo gateway su questa griglia. L'IP può trovarsi su qualsiasi rete raggiungibile dalla griglia di destinazione.

Campo	Descrizione
Porta	La porta che vuoi utilizzare per questa connessione. È possibile immettere qualsiasi numero di porta non utilizzato compreso tra 23000 e 23999. Entrambe le griglie in questa connessione utilizzeranno la stessa porta. È necessario assicurarsi che nessun nodo in entrambe le griglie utilizzi questa porta per altre connessioni.
Giorni di validità del certificato per questa griglia	Numero di giorni per cui si desidera che i certificati di sicurezza per questa griglia nella connessione siano validi. Il valore predefinito è 730 giorni (2 anni), ma è possibile immettere qualsiasi valore compreso tra 1 e 762 giorni. StorageGRID genera automaticamente certificati client e server per ogni griglia quando si salva la connessione.
Passphrase di provisioning per questa griglia	La passphrase di provisioning per la griglia a cui hai effettuato l'accesso.
FQDN o IP per l'altra griglia	Uno dei seguenti: • Il nome di dominio completo della rete a cui vuoi connetterti • Un indirizzo VIP di un gruppo HA sull'altra griglia • Un indirizzo IP di un nodo di amministrazione o di un nodo gateway sull'altra griglia. L'IP può trovarsi su qualsiasi rete raggiungibile dalla griglia sorgente.

5. Seleziona **Salva e continua**.

6. Per il passaggio Scarica file di verifica, seleziona **Scarica file di verifica**.

Una volta completata la connessione sull'altra griglia, non sarà più possibile scaricare il file di verifica da nessuna delle due griglie.

7. Individua il file scaricato(*connection-name.grid-federation*) e salvarlo in un luogo sicuro.



Questo file contiene segreti (mascherati come **★**) e altri dati sensibili e devono essere conservati e trasmessi in modo sicuro.

8. Selezionare **Chiudi** per tornare alla pagina Federazione Grid.

9. Verificare che la nuova connessione sia visualizzata e che il suo **Stato di connessione** sia **In attesa di connessione**.

10. Fornire il *connection-name.grid-federation* file all'amministratore della griglia per l'altra griglia.

Connessione completa

Eseguire questi passaggi sul sistema StorageGRID a cui ci si sta connettendo (l'altra griglia).

Passi

1. Sign in a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.
3. Seleziona **Carica file di verifica** per accedere alla pagina di caricamento.
4. Seleziona **Carica file di verifica**. Quindi, vai e seleziona il file che è stato scaricato dalla prima griglia(`connection-name.grid-federation`).

Vengono mostrati i dettagli della connessione.

5. Facoltativamente, immettere un numero diverso di giorni validi per i certificati di sicurezza per questa griglia. Per impostazione predefinita, la voce **Giorni di validità del certificato** è impostata sul valore immesso nella prima griglia, ma ogni griglia può utilizzare date di scadenza diverse.

In generale, utilizzare lo stesso numero di giorni per i certificati su entrambi i lati della connessione.



Se i certificati su una delle estremità della connessione scadono, la connessione smetterà di funzionare e le repliche saranno in sospenso finché i certificati non verranno aggiornati.

6. Inserisci la passphrase di provisioning per la griglia a cui hai effettuato l'accesso.
7. Seleziona **Salva e prova**.

I certificati vengono generati e la connessione viene testata. Se la connessione è valida, viene visualizzato un messaggio di conferma e la nuova connessione viene elencata nella pagina Federazione Grid. Lo **Stato della connessione** sarà **Connesso**.

Se viene visualizzato un messaggio di errore, risolvere eventuali problemi. Vedere "[Risolvere gli errori di federazione della griglia](#)".

8. Vai alla pagina della federazione Grid sulla prima griglia e aggiorna il browser. Verificare che lo **Stato della connessione** sia ora **Connesso**.
9. Dopo aver stabilito la connessione, eliminare in modo sicuro tutte le copie del file di verifica.

Se modifichi questa connessione, verrà creato un nuovo file di verifica. Il file originale non può essere riutilizzato.

Dopo aver finito

- Rivedere le considerazioni per "[gestione degli inquilini autorizzati](#)".
- "[Crea uno o più nuovi account tenant](#)", assegnare l'autorizzazione **Usa connessione federazione griglia** e selezionare la nuova connessione.
- "[Gestisci la connessione](#)" come richiesto. È possibile modificare i valori di connessione, testare una connessione, ruotare i certificati di connessione o rimuovere una connessione.
- "[Monitorare la connessione](#)" come parte delle normali attività di monitoraggio StorageGRID.
- "[Risolvere i problemi di connessione](#)", inclusa la risoluzione di eventuali avvisi ed errori relativi alla clonazione dell'account e alla replica tra griglie.

Gestire le connessioni della federazione di rete

La gestione delle connessioni di federazione della griglia tra i sistemi StorageGRID include la modifica dei dettagli della connessione, la rotazione dei certificati, la rimozione delle autorizzazioni dei tenant e la rimozione delle connessioni non utilizzate.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager su entrambe le griglie utilizzando un ["browser web supportato"](#).
- Tu hai il ["Permesso di accesso root"](#) per la griglia a cui hai effettuato l'accesso.

Modifica una connessione di federazione di griglia

È possibile modificare una connessione di federazione di griglia accedendo al nodo di amministrazione principale su una delle griglie nella connessione. Dopo aver apportato modifiche alla prima griglia, è necessario scaricare un nuovo file di verifica e caricarlo sull'altra griglia.



Durante la modifica della connessione, le richieste di clonazione dell'account o di replica tra griglie continueranno a utilizzare le impostazioni di connessione esistenti. Tutte le modifiche apportate alla prima griglia vengono salvate localmente, ma non vengono utilizzate finché non vengono caricate sulla seconda griglia, salvate e testate.

Inizia a modificare la connessione

Passi

1. Sign in a Grid Manager dal nodo di amministrazione principale su una delle due griglie.
2. Seleziona **NODI** e verifica che tutti gli altri nodi amministrativi nel tuo sistema siano online.



Quando si modifica una connessione di federazione della griglia, StorageGRID tenta di salvare un file di "configurazione candidata" su tutti i nodi amministrativi della prima griglia. Se questo file non può essere salvato su tutti i nodi di amministrazione, verrà visualizzato un messaggio di avviso quando si seleziona **Salva e verifica**.

3. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.
4. Modifica i dettagli della connessione utilizzando il menu **Azioni** nella pagina Federazione Grid o nella pagina dei dettagli per una connessione specifica. Vedere ["Creare connessioni di federazione di griglia"](#) per cosa inserire.

Menu Azioni

- a. Selezionare il pulsante di opzione per la connessione.
- b. Selezionare **Azioni > Modifica**.
- c. Inserisci le nuove informazioni.

Pagina dei dettagli

- a. Selezionare il nome di una connessione per visualizzarne i dettagli.
- b. Selezionare **Modifica**.
- c. Inserisci le nuove informazioni.

5. Inserisci la passphrase di provisioning per la griglia a cui hai effettuato l'accesso.
6. Seleziona **Salva e continua**.

I nuovi valori vengono salvati, ma non verranno applicati alla connessione finché non avrai caricato il nuovo file di verifica sull'altra griglia.

7. Seleziona **Scarica file di verifica**.

Per scaricare questo file in un secondo momento, vai alla pagina dei dettagli della connessione.

8. Individua il file scaricato(*connection-name.grid-federation*) e salvarlo in un luogo sicuro.



Il file di verifica contiene segreti e deve essere conservato e trasmesso in modo sicuro.

9. Selezionare **Chiudi** per tornare alla pagina Federazione Grid.

10. Verificare che lo **Stato della connessione** sia **In attesa di modifica**.



Se lo stato della connessione era diverso da **Connesso** quando hai iniziato a modificare la connessione, non cambierà in **In attesa di modifica**.

11. Fornire il *connection-name.grid-federation* file all'amministratore della griglia per l'altra griglia.

Completa la modifica della connessione

Completa la modifica della connessione caricando il file di verifica sull'altra griglia.

Passi

1. Sign in a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.
3. Seleziona **Carica file di verifica** per accedere alla pagina di caricamento.
4. Seleziona **Carica file di verifica**. Quindi, cerca e seleziona il file scaricato dalla prima griglia.
5. Inserisci la passphrase di provisioning per la griglia a cui hai effettuato l'accesso.
6. Seleziona **Salva e prova**.

Se la connessione può essere stabilita utilizzando i valori modificati, viene visualizzato un messaggio di successo. In caso contrario, verrà visualizzato un messaggio di errore. Rivedi il messaggio e risolvi eventuali problemi.

7. Chiudere la procedura guidata per tornare alla pagina Federazione Grid.
8. Verificare che lo **Stato della connessione** sia **Connesso**.
9. Vai alla pagina della federazione Grid sulla prima griglia e aggiorna il browser. Verificare che lo **Stato della connessione** sia ora **Connesso**.
10. Dopo aver stabilito la connessione, eliminare in modo sicuro tutte le copie del file di verifica.

Testa una connessione di federazione di griglia

Passi

1. Sign in a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.
3. Verificare la connessione utilizzando il menu **Azioni** nella pagina Federazione Grid o nella pagina dei dettagli per una connessione specifica.

Menu Azioni

- a. Selezionare il pulsante di opzione per la connessione.
- b. Selezionare **Azioni > Test**.

Pagina dei dettagli

- a. Selezionare il nome di una connessione per visualizzarne i dettagli.
- b. Selezionare **Test connessione**.

4. Controlla lo stato della connessione:

Stato della connessione	Descrizione
Collegato	Entrambe le reti sono collegate e comunicano normalmente.
Errore	La connessione è in stato di errore. Ad esempio, un certificato è scaduto o un valore di configurazione non è più valido.
Modifica in sospeso	Hai modificato la connessione su questa griglia, ma la connessione utilizza ancora la configurazione esistente. Per completare la modifica, carica il nuovo file di verifica nell'altra griglia.
In attesa di connessione	Hai configurato la connessione su questa griglia, ma la connessione non è stata completata sull'altra griglia. Scarica il file di verifica da questa griglia e caricalo sull'altra griglia.
Sconosciuto	La connessione è in uno stato sconosciuto, probabilmente a causa di un problema di rete o di un nodo offline.

5. Se lo stato della connessione è **Errore**, risolvere eventuali problemi. Quindi, seleziona nuovamente **Test connessione** per confermare che il problema è stato risolto.

Ruota i certificati di connessione

Ogni connessione di federazione di griglia utilizza quattro certificati SSL generati automaticamente per proteggere la connessione. Quando i due certificati per ciascuna griglia si avvicinano alla data di scadenza, l'avviso **Scadenza del certificato di federazione della griglia** ricorda di ruotare i certificati.



Se i certificati su una delle estremità della connessione scadono, la connessione smetterà di funzionare e le repliche saranno in sospeso finché i certificati non verranno aggiornati.

Passi

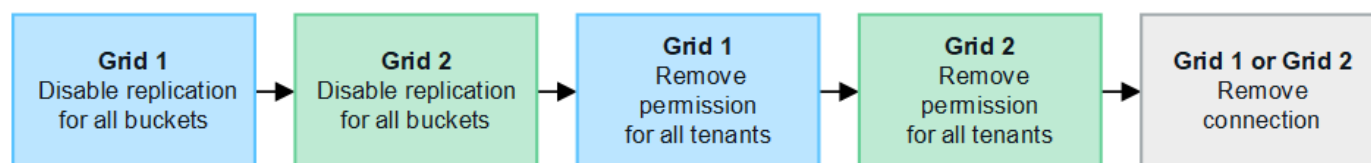
1. Sign in a Grid Manager dal nodo di amministrazione principale su una delle due griglie.
2. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.
3. Da una delle due schede della pagina Federazione Grid, seleziona il nome della connessione per visualizzarne i dettagli.
4. Selezionare la scheda **Certificati**.

5. Seleziona **Ruota certificati**.
6. Specificare per quanti giorni i nuovi certificati devono essere validi.
7. Inserisci la passphrase di provisioning per la griglia a cui hai effettuato l'accesso.
8. Seleziona **Ruota certificati**.
9. Se necessario, ripetere questi passaggi sull'altra griglia nella connessione.

In generale, utilizzare lo stesso numero di giorni per i certificati su entrambi i lati della connessione.

Rimuovere una connessione di federazione di griglia

È possibile rimuovere una connessione di federazione di griglia da entrambe le griglie nella connessione. Come mostrato nella figura, è necessario eseguire i passaggi preliminari su entrambe le griglie per confermare che la connessione non sia utilizzata da alcun tenant su nessuna delle due griglie.



Prima di rimuovere una connessione, tenere presente quanto segue:

- La rimozione di una connessione non elimina gli elementi già copiati tra le griglie. Ad esempio, gli utenti, i gruppi e gli oggetti tenant presenti su entrambe le griglie non vengono eliminati da nessuna delle due griglie quando viene rimossa l'autorizzazione del tenant. Se si desidera eliminare questi elementi, è necessario eliminarli manualmente da entrambe le griglie.
- Quando si rimuove una connessione, la replica di tutti gli oggetti in attesa di replicazione (ingeriti ma non ancora replicati nell'altra griglia) non riuscirà più.

Disabilita la replica per tutti i bucket tenant

Passi

1. Partendo da una delle due griglie, accedi a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.
3. Selezionare il nome della connessione per visualizzarne i dettagli.
4. Nella scheda **Tenant consentiti**, determinare se la connessione è utilizzata da qualche tenant.
5. Se sono elencati degli inquilini, istruire tutti gli inquilini a ["disabilitare la replicazione tra griglie"](#) per tutti i loro bucket su entrambe le griglie nella connessione.



Non è possibile rimuovere l'autorizzazione **Usa connessione federazione griglia** se in uno qualsiasi dei bucket tenant è abilitata la replica tra griglie. Ogni account tenant deve disabilitare la replica tra griglie per i propri bucket su entrambe le griglie.

Rimuovi l'autorizzazione per ogni tenant

Dopo aver disabilitato la replica tra griglie per tutti i bucket tenant, rimuovere l'autorizzazione **Usa federazione griglie** da tutti i tenant su entrambe le griglie.

Passi

1. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.
2. Selezionare il nome della connessione per visualizzarne i dettagli.
3. Per ogni tenant nella scheda **Tenant consentiti**, rimuovere l'autorizzazione **Usa connessione federazione griglia** da ciascun tenant. Vedere ["Gestire gli inquilini autorizzati"](#) .
4. Ripetere questi passaggi per gli inquilini autorizzati sull'altra griglia.

Rimuovi connessione

Passi

1. Se nessun tenant su nessuna delle due griglie utilizza la connessione, selezionare **Rimuovi**.
2. Rivedi il messaggio di conferma e seleziona **Rimuovi**.
 - Se la connessione può essere rimossa, viene visualizzato un messaggio di conferma. La connessione della federazione di rete è ora rimossa da entrambe le reti.
 - Se la connessione non può essere rimossa (ad esempio perché è ancora in uso o si è verificato un errore di connessione), viene visualizzato un messaggio di errore. Puoi procedere in uno dei seguenti modi:
 - Risolvi l'errore (consigliato). Vedere ["Risolvere gli errori di federazione della griglia"](#) .
 - Rimuovere la connessione con la forza. Vedere la sezione successiva.

Rimuovere forzatamente una connessione di federazione di griglia

Se necessario, è possibile forzare la rimozione di una connessione che non ha lo stato **Connesso**.

La rimozione forzata elimina solo la connessione dalla rete locale. Per rimuovere completamente la connessione, eseguire gli stessi passaggi su entrambe le griglie.

Passi

1. Nella finestra di dialogo di conferma, seleziona **Forza rimozione**.

Viene visualizzato un messaggio di successo. Questa connessione di federazione di rete non può più essere utilizzata. Tuttavia, nei bucket tenant potrebbe essere ancora abilitata la replica tra griglie e alcune copie degli oggetti potrebbero essere già state replicate tra le griglie nella connessione.
2. Dall'altra griglia nella connessione, accedi a Grid Manager dal nodo di amministrazione principale.
3. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.
4. Selezionare il nome della connessione per visualizzarne i dettagli.
5. Selezionare **Rimuovi** e **Sì**.
6. Selezionare **Forza rimozione** per rimuovere la connessione da questa griglia.

Gestire gli inquilini autorizzati per la federazione della rete

È possibile consentire agli account tenant S3 di utilizzare una connessione federata di griglia tra due sistemi StorageGRID . Quando agli inquilini è consentito utilizzare una connessione, sono necessari passaggi speciali per modificare i dettagli dell'inquilino o per rimuovere definitivamente l'autorizzazione di un inquilino a utilizzare la connessione.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager su entrambe le griglie utilizzando un ["browser web supportato"](#).
- Tu hai il ["Permesso di accesso root"](#) per la griglia a cui hai effettuato l'accesso.
- Hai ["ha creato una connessione di federazione di rete"](#) tra due griglie.
- Hai esaminato i flussi di lavoro per ["clonazione dell'account"](#) E ["replicazione cross-grid"](#).
- Come richiesto, hai già configurato l'accesso singolo (SSO) o identificato la federazione per entrambe le griglie nella connessione. Vedere ["Che cosa è il clone dell'account"](#).

Creare un inquilino autorizzato

Se si desidera consentire a un account tenant nuovo o esistente di utilizzare una connessione di federazione di griglia per la clonazione dell'account e la replica tra griglie, seguire le istruzioni generali per ["creare un nuovo tenant S3"](#) O ["modificare un account inquilino"](#) e notare quanto segue:

- È possibile creare il tenant da entrambe le griglie nella connessione. La griglia in cui viene creato un tenant è la *griglia di origine del tenant*.
- Lo stato della connessione deve essere **Connesso**.
- Quando il tenant viene creato o modificato per abilitare l'autorizzazione **Usa connessione federazione griglia** e quindi salvato sulla prima griglia, un tenant identico viene automaticamente replicato sull'altra griglia. La griglia in cui viene replicato il tenant è la *griglia di destinazione del tenant*.
- Gli inquilini su entrambe le griglie avranno lo stesso ID account di 20 cifre, nome, descrizione, quota e autorizzazioni. Facoltativamente, puoi utilizzare il campo **Descrizione** per identificare quale sia il tenant di origine e quale quello di destinazione. Ad esempio, questa descrizione per un tenant creato sulla Griglia 1 apparirà anche per il tenant replicato sulla Griglia 2: "Questo tenant è stato creato sulla Griglia 1".
- Per motivi di sicurezza, la password di un utente root locale non viene copiata nella griglia di destinazione.



Prima che un utente root locale possa accedere al tenant replicato sulla griglia di destinazione, un amministratore di griglia per quella griglia deve ["cambiare la password per l'utente root locale"](#).

- Dopo che il tenant nuovo o modificato è disponibile su entrambe le griglie, gli utenti del tenant possono eseguire queste operazioni:
 - Dalla griglia di origine del tenant, crea gruppi e utenti locali, che vengono automaticamente clonati nella griglia di destinazione del tenant. Vedere ["Clona gruppi tenant e utenti"](#).
 - Crea nuove chiavi di accesso S3, che possono essere facoltativamente clonate nella griglia di destinazione del tenant. Vedere ["Clona le chiavi di accesso S3 utilizzando l'API"](#).
 - Crea bucket identici su entrambe le griglie nella connessione e abilita la replica tra griglie in una direzione o in entrambe le direzioni. Vedere ["Gestire la replicazione tra griglie"](#).

Visualizza un inquilino autorizzato

È possibile visualizzare i dettagli di un tenant autorizzato a utilizzare una connessione di federazione di rete.

Passi

1. Selezionare **INQUILINI**.
2. Dalla pagina Inquilini, seleziona il nome dell'inquilino per visualizzare la pagina dei dettagli dell'inquilino.

Se questa è la griglia di origine del tenant (ovvero se il tenant è stato creato su questa griglia), viene visualizzato un banner per ricordare che il tenant è stato clonato in un'altra griglia. Se modifichi o elimini

questo tenant, le modifiche non verranno sincronizzate con l'altra griglia.

Tenants > tenant A for grid federation

tenant A for grid federation

Tenant ID: 0899 6970 1700 0930 0009

Protocol: S3

Object count: 0

Quota utilization: —

Logical space used: 0 bytes

Quota: —

Description: this tenant was created on Grid 1

Sign in

Edit

Actions ▾

This tenant has been cloned to another grid. If you edit or delete this tenant, your changes will not be synced to the other grid.

Space breakdown

Allowed features

Grid federation

Remove permission

Clear error

Search...

Displaying one result

Connection name	Connection status	Remote grid hostname	Last error
Grid 1 to Grid 2	Connected	10.96.106.230	Check for errors

3. Facoltativamente, seleziona la scheda **Federazione griglia** per"monitorare la connessione della federazione di rete" .

Modifica un inquilino autorizzato

Se è necessario modificare un tenant che dispone dell'autorizzazione **Usa connessione federazione griglia**, seguire le istruzioni generali per"modifica di un account inquilino" e notare quanto segue:

- Se un tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, è possibile modificare i dettagli del tenant da entrambe le griglie nella connessione. Tuttavia, le modifiche apportate non verranno copiate nell'altra griglia. Se si desidera mantenere sincronizzati i dettagli del tenant tra le griglie, è necessario apportare le stesse modifiche su entrambe le griglie.
- Non è possibile cancellare l'autorizzazione **Usa connessione federazione griglia** quando si modifica un tenant.
- Non è possibile selezionare una connessione di federazione di griglia diversa quando si modifica un tenant.

Elimina un inquilino autorizzato

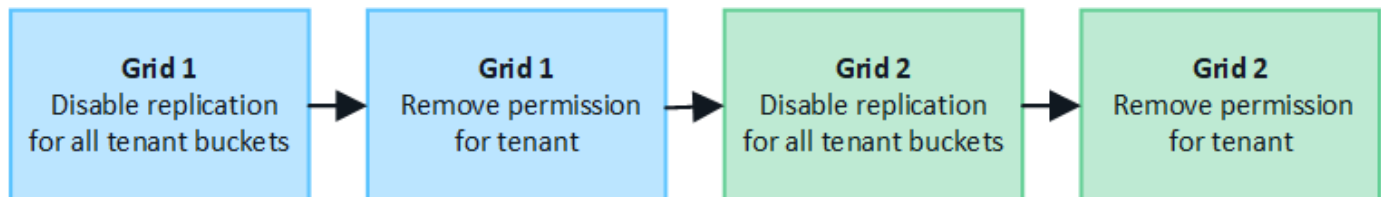
Se è necessario rimuovere un tenant che dispone dell'autorizzazione **Usa connessione federazione griglia**, seguire le istruzioni generali per ["eliminazione di un account tenant"](#) e notare quanto segue:

- Prima di poter rimuovere il tenant originale dalla griglia di origine, è necessario rimuovere tutti i bucket per l'account dalla griglia di origine.
- Prima di poter rimuovere il tenant clonato dalla griglia di destinazione, è necessario rimuovere tutti i bucket per l'account dalla griglia di destinazione.
- Se si rimuove il tenant originale o quello clonato, l'account non potrà più essere utilizzato per la replica tra griglie.
- Se si rimuove il tenant originale dalla griglia di origine, eventuali gruppi di tenant, utenti o chiavi clonati nella griglia di destinazione non saranno interessati. È possibile eliminare il tenant clonato oppure consentirgli di gestire i propri gruppi, utenti, chiavi di accesso e bucket.
- Se si rimuove il tenant clonato dalla griglia di destinazione, si verificheranno errori di clonazione se nuovi gruppi o utenti vengono aggiunti al tenant originale.

Per evitare questi errori, rimuovere l'autorizzazione del tenant a utilizzare la connessione federata della griglia prima di eliminare il tenant da questa griglia.

Rimuovi Usa autorizzazione di connessione alla federazione della griglia

Per impedire a un tenant di utilizzare una connessione federata alla griglia, è necessario rimuovere l'autorizzazione **Usa connessione federata alla griglia**.



Prima di revocare l'autorizzazione di un tenant a utilizzare una connessione di federazione di rete, tenere presente quanto segue:

- Non è possibile rimuovere l'autorizzazione **Usa connessione federazione griglia** se uno qualsiasi dei bucket del tenant ha abilitata la replica tra griglie. L'account tenant deve prima disabilitare la replica tra griglie per tutti i propri bucket.
- La rimozione dell'autorizzazione **Usa connessione federazione griglia** non elimina gli elementi che sono già stati replicati tra le griglie. Ad esempio, tutti gli utenti, i gruppi e gli oggetti tenant presenti su entrambe le griglie non vengono eliminati da nessuna delle due griglie quando viene rimossa l'autorizzazione del tenant. Se si desidera eliminare questi elementi, è necessario eliminarli manualmente da entrambe le griglie.
- Se si desidera riattivare questa autorizzazione con la stessa connessione di federazione della griglia, eliminare prima questo tenant sulla griglia di destinazione; in caso contrario, la riattivazione di questa autorizzazione genererà un errore.



Riattivando l'autorizzazione **Usa connessione federazione griglia**, la griglia locale diventa la griglia di origine e viene attivata la clonazione sulla griglia remota specificata dalla connessione federazione griglia selezionata. Se l'account tenant esiste già sulla griglia remota, la clonazione genererà un errore di conflitto.

Prima di iniziare

- Stai utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Permesso di accesso root"](#) per entrambe le griglie.

Disabilita la replica per i bucket tenant

Come primo passaggio, disabilitare la replica tra griglie per tutti i bucket tenant.

Passi

1. Partendo da una delle due griglie, accedi a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.
3. Selezionare il nome della connessione per visualizzarne i dettagli.
4. Nella scheda **Tenant consentiti**, determinare se il tenant sta utilizzando la connessione.
5. Se l'inquilino è elencato, istruirlo a ["disabilitare la replicazione tra griglie"](#) per tutti i loro bucket su entrambe le griglie nella connessione.



Non è possibile rimuovere l'autorizzazione **Usa connessione federazione griglia** se in uno qualsiasi dei bucket tenant è abilitata la replica tra griglie. Il tenant deve disabilitare la replica tra griglie per i propri bucket su entrambe le griglie.

Rimuovi l'autorizzazione per l'inquilino

Dopo aver disabilitato la replica tra griglie per i bucket tenant, è possibile rimuovere l'autorizzazione del tenant a utilizzare la connessione federata della griglia.

Passi

1. Sign in a Grid Manager dal nodo di amministrazione principale.
2. Rimuovere l'autorizzazione dalla pagina Federazione della griglia o dalla pagina Tenant.

Pagina della federazione della griglia

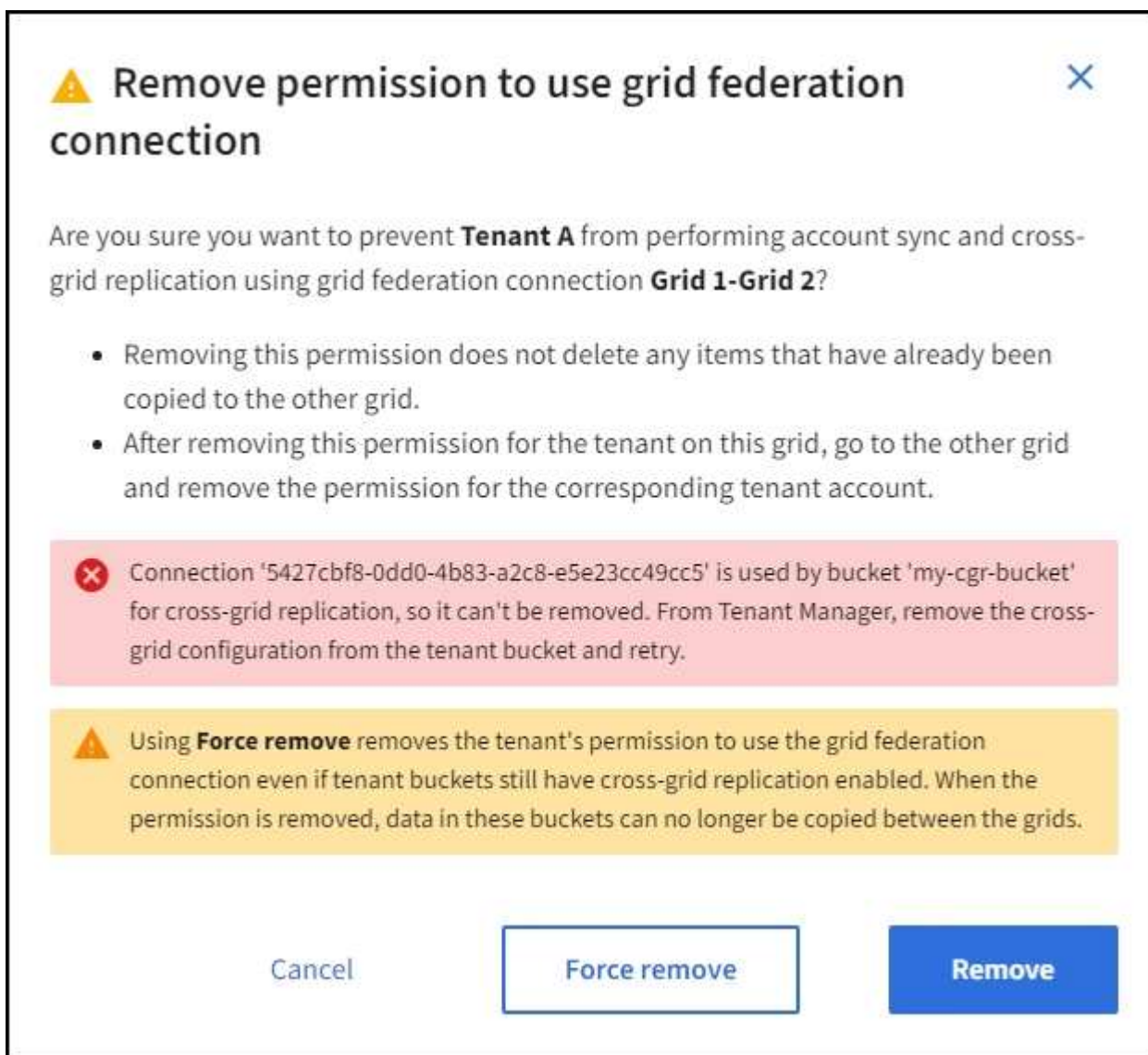
- a. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.
- b. Selezionare il nome della connessione per visualizzarne la pagina dei dettagli.
- c. Nella scheda **Locatari consentiti**, selezionare il pulsante di opzione per il locatario.
- d. Seleziona **Rimuovi autorizzazione**.

Pagina degli inquilini

- a. Selezionare **INQUILINI**.
- b. Selezionare il nome dell'inquilino per visualizzare la pagina dei dettagli.
- c. Nella scheda **Federazione di griglia**, selezionare il pulsante di opzione per la connessione.
- d. Seleziona **Rimuovi autorizzazione**.

3. Esaminare gli avvisi nella finestra di dialogo di conferma e selezionare **Rimuovi**.
 - Se l'autorizzazione può essere rimossa, verrai reindirizzato alla pagina dei dettagli e verrà visualizzato un messaggio di conferma dell'operazione. Questo tenant non può più utilizzare la connessione alla federazione di rete.

- Se uno o più bucket tenant hanno ancora la replica tra griglie abilitata, viene visualizzato un errore.



Puoi procedere in uno dei seguenti modi:

- (Raccomandato.) Sign in a Tenant Manager e disabilita la replica per ciascun bucket del tenant. Vedere "[Gestire la replicazione tra griglie](#)". Quindi, ripetere i passaggi per rimuovere l'autorizzazione **Usa connessione alla rete**.
 - Rimuovere l'autorizzazione con la forza. Vedere la sezione successiva.
4. Passare all'altra griglia e ripetere questi passaggi per rimuovere l'autorizzazione per lo stesso tenant sull'altra griglia.

Rimuovi il permesso con la forza

Se necessario, è possibile forzare la rimozione dell'autorizzazione di un tenant a utilizzare una connessione di federazione di griglia anche se nei bucket del tenant è abilitata la replica tra griglie.

Prima di revocare con la forza il permesso di un inquilino, tenere presente le considerazioni generali per [rimozione del permesso](#) oltre a queste considerazioni aggiuntive:

- Se si rimuove forzatamente l'autorizzazione **Usa connessione federazione griglia**, tutti gli oggetti in

attesa di replica sull'altra griglia (ingeriti ma non ancora replicati) continueranno a essere replicati. Per impedire che questi oggetti in corso raggiungano il bucket di destinazione, è necessario rimuovere l'autorizzazione del tenant anche sull'altra griglia.

- Tutti gli oggetti inseriti nel bucket di origine dopo aver rimosso l'autorizzazione **Usa connessione federazione griglia** non verranno mai replicati nel bucket di destinazione.

Passi

1. Sign in a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **CONFIGURAZIONE > Sistema > Federazione di griglia**.
3. Selezionare il nome della connessione per visualizzarne la pagina dei dettagli.
4. Nella scheda **Locatari consentiti**, selezionare il pulsante di opzione per il locatario.
5. Seleziona **Rimuovi autorizzazione**.
6. Rivedi gli avvisi nella finestra di dialogo di conferma e seleziona **Forza rimozione**.

Viene visualizzato un messaggio di successo. Questo tenant non può più utilizzare la connessione alla federazione di rete.

7. Se necessario, vai all'altra griglia e ripeti questi passaggi per forzare la rimozione dell'autorizzazione per lo stesso account tenant sull'altra griglia. Ad esempio, dovresti ripetere questi passaggi sull'altra griglia per impedire che gli oggetti in corso di elaborazione raggiungano il bucket di destinazione.

Risolvere gli errori di federazione della griglia

Potrebbe essere necessario risolvere avvisi ed errori relativi alle connessioni della federazione della griglia, alla clonazione degli account e alla replica tra griglie.

Avvisi ed errori di connessione della federazione di rete

Potresti ricevere avvisi o riscontrare errori con le connessioni della federazione di rete.

Dopo aver apportato modifiche per risolvere un problema di connessione, testare la connessione per assicurarsi che lo stato della connessione torni a **Connesso**. Per le istruzioni, vedere ["Gestire le connessioni della federazione di rete"](#).

Avviso di errore di connessione alla federazione di rete

Problema

È stato attivato l'avviso **Errore di connessione alla federazione di rete**.

Dettagli

Questo avviso indica che la connessione di federazione di rete tra le reti non funziona.

Azioni consigliate

1. Rivedere le impostazioni nella pagina Federazione della griglia per entrambe le griglie. Verificare che tutti i valori siano corretti. Vedere ["Gestire le connessioni della federazione di rete"](#).
2. Esaminare i certificati utilizzati per la connessione. Assicurarsi che non vi siano avvisi relativi a certificati di federazione della griglia scaduti e che i dettagli di ciascun certificato siano validi. Vedere le istruzioni per la rotazione dei certificati di connessione in ["Gestire le connessioni della federazione di rete"](#).
3. Verificare che tutti i nodi Admin e Gateway in entrambe le griglie siano online e disponibili. Risolvi eventuali avvisi che potrebbero interessare questi nodi e riprova.

4. Se hai fornito un nome di dominio completo (FQDN) per la griglia locale o remota, verifica che il server DNS sia online e disponibile. Vedere ["Che cos'è la federazione di rete?"](#) per requisiti di rete, indirizzo IP e DNS.

Avviso di scadenza del certificato di federazione della griglia

Problema

È stato attivato l'avviso **Scadenza del certificato di federazione della griglia**.

Dettagli

Questo avviso indica che uno o più certificati di federazione della griglia stanno per scadere.

Azioni consigliate

Vedere le istruzioni per la rotazione dei certificati di connessione in ["Gestire le connessioni della federazione di rete"](#).

Errore durante la modifica di una connessione di federazione di griglia

Problema

Quando si modifica una connessione di federazione di griglia, viene visualizzato il seguente messaggio di avviso quando si seleziona **Salva e verifica**: "Impossibile creare un file di configurazione candidato su uno o più nodi".

Dettagli

Quando si modifica una connessione di federazione della griglia, StorageGRID tenta di salvare un file di "configurazione candidata" su tutti i nodi amministrativi della prima griglia. Viene visualizzato un messaggio di avviso se il file non può essere salvato su tutti i nodi amministrativi, ad esempio perché un nodo amministrativo è offline.

Azioni consigliate

1. Dalla griglia che stai utilizzando per modificare la connessione, seleziona **NODI**.
2. Verificare che tutti i nodi amministrativi per quella griglia siano online.
3. Se alcuni nodi sono offline, riportali online e prova a modificare nuovamente la connessione.

Errori di clonazione dell'account

Impossibile accedere a un account tenant clonato

Problema

Non è possibile accedere a un account tenant clonato. Il messaggio di errore nella pagina di accesso di Tenant Manager è "Le credenziali per questo account non sono valide. Per favore riprova."

Dettagli

Per motivi di sicurezza, quando un account tenant viene clonato dalla griglia di origine del tenant alla griglia di destinazione del tenant, la password impostata per l'utente root locale del tenant non viene clonata. Allo stesso modo, quando un tenant crea utenti locali sulla sua griglia di origine, le password degli utenti locali non vengono clonate nella griglia di destinazione.

Azioni consigliate

Prima che l'utente root possa accedere alla griglia di destinazione del tenant, un amministratore della griglia deve prima ["cambiare la password per l'utente root locale"](#) sulla griglia di destinazione.

Prima che un utente locale clonato possa accedere alla griglia di destinazione del tenant, l'utente root del tenant clonato deve aggiungere una password per l'utente sulla griglia di destinazione. Per le istruzioni, vedere ["Gestisci gli utenti locali"](#) nelle istruzioni per l'utilizzo di Tenant Manager.

Tenant creato senza un clone

Problema

Dopo aver creato un nuovo tenant con l'autorizzazione **Usa connessione federazione griglia**, viene visualizzato il messaggio "Tenant creato senza un clone".

Dettagli

Questo problema può verificarsi se gli aggiornamenti allo stato della connessione vengono ritardati, il che potrebbe causare l'elenco di una connessione non funzionante come **Connesso**.

Azioni consigliate

1. Esaminare il motivo elencato nel messaggio di errore e risolvere eventuali problemi di rete o di altro tipo che potrebbero impedire il funzionamento della connessione. Vedere [Avvisi ed errori di connessione alla federazione di rete](#).
2. Seguire le istruzioni per testare una connessione di federazione di griglia in ["Gestire le connessioni della federazione di rete"](#) per confermare che il problema è stato risolto.
3. Dalla griglia di origine dell'inquilino, seleziona **INQUILINI**.
4. Individuare l'account tenant che non è stato possibile clonare.
5. Selezionare il nome del tenant per visualizzare la pagina dei dettagli.
6. Seleziona **Riprova clonazione account**.

Tenants > test

test

Tenant ID: 0040 2213 8117 4859 6503

Protocol: S3

Object count: 0

Quota utilization: —

Logical space used: 0 bytes

Quota: —

Sign in

Edit

Actions

✖

Tenant account could not be cloned to the other grid.
Reason: Internal server error. The server encountered an error and could not complete your request. Try again. If the problem persists, contact support. Internal Server Error

Retry account clone

Se l'errore è stato risolto, l'account tenant verrà ora clonato nell'altra griglia.

Avvisi ed errori di replicazione tra griglie

Ultimo errore visualizzato per la connessione o il tenant

Problema

Quando "visualizzazione di una connessione di federazione di rete" (o quando "gestione degli inquilini autorizzati" per una connessione), si nota un errore nella colonna **Ultimo errore** nella pagina dei dettagli della connessione. Per esempio:

Grid 1 - Grid 2

Local hostname (this grid):10.96.130.64

Port:23000

Remote hostname (other grid):10.96.130.76

Connection status:

Connected

Edit

Download file

Test connection

Remove

Permitted tenants

Certificates

Remove permission

Clear error

Search...

Displaying one result

Tenant name	Last error
Tenant A	2022-12-22 16:19:20 MST Cross-grid replication has encountered an error. Failed to send cross-grid replication request from source bucket 'my-bucket' to destination bucket 'my-bucket'. Error code: DestinationRequestError. Detail: InvalidBucketState. Confirm that the source and destination buckets have object versioning enabled and S3 Object Lock disabled. (logID 13916508109026943924) Check for errors

Dettagli

Per ogni connessione di federazione di griglia, la colonna **Ultimo errore** mostra l'errore più recente verificatosi, se presente, durante la replica dei dati di un tenant sull'altra griglia. Questa colonna mostra solo l'ultimo errore di replicazione tra griglie verificatosi; gli errori precedenti che potrebbero essersi verificati non verranno mostrati. Un errore in questa colonna potrebbe verificarsi per uno dei seguenti motivi:

- La versione dell'oggetto sorgente non è stata trovata.
- Il bucket di origine non è stato trovato.
- Il bucket di destinazione è stato eliminato.
- Il bucket di destinazione è stato ricreato da un account diverso.
- Il controllo delle versioni del bucket di destinazione è sospeso.
- Il bucket di destinazione è stato ricreato dallo stesso account, ma ora non è più sottoposto a controllo di versione.

Azioni consigliate

Se nella colonna **Ultimo errore** viene visualizzato un messaggio di errore, procedere come segue:

1. Rivedi il testo del messaggio.
2. Eseguire tutte le azioni consigliate. Ad esempio, se il controllo delle versioni è stato sospeso sul bucket di destinazione per la replica tra griglie, riattivare il controllo delle versioni per quel bucket.

3. Selezionare la connessione o l'account tenant dalla tabella.
4. Seleziona **Cancella errore**.
5. Selezionare **Sì** per cancellare il messaggio e aggiornare lo stato del sistema.
6. Aspetta 5-6 minuti e poi ingerisci un nuovo oggetto nel secchio. Verificare che il messaggio di errore non venga più visualizzato.



Per garantire che il messaggio di errore venga cancellato, attendere almeno 5 minuti dopo il timestamp nel messaggio prima di acquisire un nuovo oggetto.



Dopo aver eliminato l'errore, potrebbe apparire un nuovo **Ultimo errore** se gli oggetti vengono inseriti in un bucket diverso che presenta anch'esso un errore.

7. Per determinare se la replica di alcuni oggetti non è riuscita a causa dell'errore del bucket, vedere "[Identificare e riprovare le operazioni di replicazione non riuscite](#)".

Avviso di errore permanente della replicazione tra griglie

Problema

È stato attivato l'avviso **Errore permanente nella replicazione tra griglie**.

Dettagli

Questo avviso indica che gli oggetti tenant non possono essere replicati tra i bucket su due griglie per un motivo che richiede l'intervento dell'utente per essere risolto. Questo avviso è in genere causato da una modifica al bucket di origine o di destinazione.

Azioni consigliate

1. Sign in alla griglia in cui è stato attivato l'avviso.
2. Vai su **CONFIGURAZIONE > Sistema > Federazione di griglia** e individua il nome della connessione elencato nell'avviso.
3. Nella scheda Tenant autorizzati, controlla la colonna **Ultimo errore** per determinare quali account tenant presentano errori.
4. Per saperne di più sul guasto, vedere le istruzioni in "[Monitorare le connessioni della federazione di rete](#)" per rivedere le metriche di replicazione tra griglie.
5. Per ogni account inquilino interessato:
 - a. Vedere le istruzioni in "[Monitorare l'attività degli inquilini](#)" per confermare che il tenant non ha superato la sua quota sulla griglia di destinazione per la replica tra griglie.
 - b. Se necessario, aumentare la quota del tenant sulla griglia di destinazione per consentire il salvataggio di nuovi oggetti.
6. Per ogni tenant interessato, accedi a Tenant Manager su entrambe le griglie, in modo da poter confrontare l'elenco dei bucket.
7. Per ogni bucket in cui è abilitata la replica tra griglie, confermare quanto segue:
 - Esiste un bucket corrispondente per lo stesso tenant sull'altra griglia (è necessario utilizzare il nome esatto).
 - In entrambi i bucket è abilitato il controllo delle versioni degli oggetti (il controllo delle versioni non può essere sospeso su nessuna delle due griglie).
 - In entrambi i bucket il blocco oggetti S3 è disabilitato.

◦ Nessuno dei bucket è nello stato **Eliminazione oggetti: sola lettura**.

8. Per confermare che il problema è stato risolto, consultare le istruzioni in "[Monitorare le connessioni della federazione di rete](#)" per rivedere le metriche di replicazione tra griglie oppure eseguire questi passaggi:
 - a. Torna alla pagina Federazione Grid.
 - b. Selezionare il tenant interessato e selezionare **Cancella errore** nella colonna **Ultimo errore**.
 - c. Selezionare **Sì** per cancellare il messaggio e aggiornare lo stato del sistema.
 - d. Aspetta 5-6 minuti e poi ingerisci un nuovo oggetto nel secchio. Verificare che il messaggio di errore non venga più visualizzato.



Per garantire che il messaggio di errore venga cancellato, attendere almeno 5 minuti dopo il timestamp nel messaggio prima di acquisire un nuovo oggetto.



Potrebbe volerci fino a un giorno prima che l'avviso venga cancellato una volta risolto.

- a. Vai a "[Identificare e riprovare le operazioni di replicazione non riuscite](#)" per identificare eventuali oggetti o eliminare i marcatori che non sono riusciti a replicare nell'altra griglia e per riprovare la replicazione se necessario.

Avviso di risorsa di replicazione tra griglie non disponibile

Problema

È stato attivato l'avviso **Risorsa di replicazione tra griglie non disponibile**.

Dettagli

Questo avviso indica che le richieste di replica tra griglie sono in sospeso perché una risorsa non è disponibile. Ad esempio, potrebbe esserci un errore di rete.

Azioni consigliate

1. Monitorare l'avviso per verificare se il problema si risolve da solo.
2. Se il problema persiste, verificare se una delle due griglie presenta un avviso **Errore di connessione alla federazione della griglia** per la stessa connessione o un avviso **Impossibile comunicare con il nodo** per un nodo. Questo avviso potrebbe essere risolto quando risolvi gli avvisi precedenti.
3. Per saperne di più sul guasto, vedere le istruzioni in "[Monitorare le connessioni della federazione di rete](#)" per rivedere le metriche di replicazione tra griglie.
4. Se non riesci a risolvere il problema, contatta l'assistenza tecnica.

Una volta risolto il problema, la replica tra griglie proseguirà normalmente.

Identificare e riprovare le operazioni di replicazione non riuscite

Dopo aver risolto l'avviso **Errore permanente nella replica tra griglie**, dovresti determinare se qualche oggetto o marcatore di eliminazione non è riuscito a essere replicato sull'altra griglia. È quindi possibile reingestire questi oggetti o utilizzare l'API Grid Management per riprovare la replica.

L'avviso **Errore permanente nella replica tra griglie** indica che gli oggetti tenant non possono essere replicati tra i bucket su due griglie per un motivo che richiede l'intervento dell'utente per essere risolto. Questo avviso è in genere causato da una modifica al bucket di origine o di destinazione. Per maggiori dettagli, vedere

"Risolvere gli errori di federazione della griglia" .

Determina se qualche oggetto non è stato replicato

Per determinare se oggetti o marcatori di eliminazione non sono stati replicati nell'altra griglia, è possibile cercare nel registro di controllo "[CGRR \(richiesta di replica tra griglie\)](#)" messaggi. Questo messaggio viene aggiunto al registro quando StorageGRID non riesce a replicare un oggetto, un oggetto multiparte o a eliminare un marcatore nel bucket di destinazione.

Puoi usare il "[strumento di verifica e spiegazione](#)" per tradurre i risultati in un formato più facile da leggere.

Prima di iniziare

- Hai i permessi di accesso Root.
- Tu hai il `Passwords.txt` file.
- Conosci l'indirizzo IP del nodo di amministrazione primario.

Passi

1. Accedi al nodo di amministrazione principale:

- a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- b. Inserisci la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla root: `su -`
- d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#` .

2. Cercare i messaggi CGRR nel file `audit.log` e utilizzare lo strumento `audit-explain` per formattare i risultati.

Ad esempio, questo comando cerca tutti i messaggi CGRR degli ultimi 30 minuti e utilizza lo strumento `audit-explain`.

```
# awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date {
print }' audit.log | grep CGRR | audit-explain
```

I risultati del comando saranno simili a questo esempio, che contiene voci per sei messaggi CGRR. Nell'esempio, tutte le richieste di replica tra griglie hanno restituito un errore generale perché l'oggetto non poteva essere replicato. I primi tre errori riguardano le operazioni di "replica oggetto", mentre gli ultimi tre errori riguardano le operazioni di "replica eliminazione marcatore".

```

CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-0"
version:QjRBNDIzODAtNjQ3My0xMUVELTg2QjEtODJBMjAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-3"
version:QjRDOTRCOUMtNjQ3My0xMUVELTkzM0YtOTg1MTAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-1"
version:NUQ0OEYxMDAtNjQ3NC0xMUVELTg2NjMtOTY5NzAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-5"
version:NUQ1ODUwQkUtNjQ3NC0xMUVELTg1NTItRDkwNzAwQkI3NEM4 error:general
error

```

Ogni voce contiene le seguenti informazioni:

Campo	Descrizione
Richiesta di replicazione tra griglie CGRR	Il nome della richiesta
inquilino	ID account dell'inquilino
connessione	L'ID della connessione della federazione di rete
operazione	Tipo di operazione di replicazione che si stava tentando: • replicare l'oggetto • replica elimina marcatore • replicare un oggetto multiparte
secchio	Il nome del bucket
oggetto	Il nome dell'oggetto
versione	L'ID della versione per l'oggetto

Campo	Descrizione
errore	Il tipo di errore. Se la replica tra griglie non riesce, l'errore è "Errore generale".

Riprova le repliche non riuscite

Dopo aver generato un elenco di oggetti ed eliminato i marcatori che non sono stati replicati nel bucket di destinazione e aver risolto i problemi sottostanti, è possibile riprovare la replica in uno dei due modi seguenti:

- Reinserisci ogni oggetto nel bucket di origine.
- Utilizzare l'API privata di Grid Management, come descritto.

Passi

1. Nella parte superiore di Grid Manager, seleziona l'icona della guida e seleziona **Documentazione API**.
2. Seleziona **Vai alla documentazione API privata**.



Gli endpoint dell'API StorageGRID contrassegnati come "Privati" sono soggetti a modifiche senza preavviso. Anche gli endpoint privati StorageGRID ignorano la versione API della richiesta.

3. Nella sezione **cross-grid-replication-advanced**, seleziona il seguente endpoint:

```
POST /private/cross-grid-replication-retry-failed
```

4. Seleziona **Provalo**.
5. Nella casella di testo **corpo**, sostituire la voce di esempio per **versionID** con un ID versione dal file audit.log corrispondente a una richiesta di replica tra griglie non riuscita.

Assicuratevi di mantenere le virgolette doppie attorno alla stringa.
6. Selezionare **Esegui**.
7. Verificare che il codice di risposta del server sia **204**, a indicare che l'oggetto o il marcatore di eliminazione è stato contrassegnato come in sospeso per la replica tra griglie sull'altra griglia.



In sospeso significa che la richiesta di replicazione tra griglie è stata aggiunta alla coda interna per l'elaborazione.

Monitorare i tentativi di replicazione

È necessario monitorare le operazioni di ripetizione della replica per assicurarsi che vengano completate.



Potrebbero volerci diverse ore o più prima che un oggetto o un marcatore di eliminazione venga replicato nell'altra griglia.

È possibile monitorare le operazioni di ripetizione in uno dei due modi seguenti:

- Utilizzare un S3 **"HeadObject"** O **"OttieniOggetto"** richiesta. La risposta include StorageGRID-specifico `x-ntap-sg-cgr-replication-status` intestazione di risposta, che avrà uno dei seguenti valori:

Griglia	Stato di replicazione
Fonte	• COMPLETO: La replica è riuscita. • IN ATTESA: L'oggetto non è stato ancora replicato. • ERRORE: La replica non è riuscita con un errore permanente. Un utente deve risolvere l'errore.
Destinazione	REPLICA : L'oggetto è stato replicato dalla griglia di origine.

- Utilizzare l'API privata di Grid Management, come descritto.

Passi

1. Nella sezione **cross-grid-replication-advanced** della documentazione API privata, seleziona il seguente endpoint:

```
GET /private/cross-grid-replication-object-status/{id}
```

2. Seleziona **Provalo**.
3. Nella sezione Parametro, inserisci l'ID della versione utilizzata in `cross-grid-replication-retry-failed` richiesta.
4. Selezionare **Esegui**.
5. Verificare che il codice di risposta del server sia **200**.
6. Esaminare lo stato della replicazione, che sarà uno dei seguenti:
 - **IN ATTESA**: L'oggetto non è stato ancora replicato.
 - **COMPLETO**: La replica è riuscita.
 - **FAILED**: La replica non è riuscita con un errore permanente. Un utente deve risolvere l'errore.

Gestire la sicurezza

Gestire la sicurezza

È possibile configurare diverse impostazioni di sicurezza da Grid Manager per proteggere il sistema StorageGRID .

Gestisci la crittografia

StorageGRID offre diverse opzioni per la crittografia dei dati. Dovresti [rivedere i metodi di crittografia disponibili](#) per determinare quali soddisfano i tuoi requisiti di protezione dei dati.

Gestisci i certificati

Puoi [configurare e gestire i certificati del server](#) utilizzato per le connessioni HTTP o i certificati client utilizzati per autenticare l'identità di un client o di un utente sul server.

Configurare i server di gestione delle chiavi

Utilizzando un [server di gestione delle chiavi](#) consente di proteggere i dati StorageGRID anche se un dispositivo viene rimosso dal data center. Dopo aver crittografato i volumi dell'appliance, non sarà possibile

accedere ai dati sull'appliance a meno che il nodo non sia in grado di comunicare con il KMS.



Per utilizzare la gestione delle chiavi di crittografia, è necessario abilitare l'impostazione **Crittografia nodo** per ogni appliance durante l'installazione, prima che l'appliance venga aggiunta alla griglia.

Gestisci le impostazioni proxy

Se si utilizzano servizi della piattaforma S3 o pool di archiviazione cloud, è possibile configurare un **"server proxy di archiviazione"** tra i nodi di archiviazione e gli endpoint S3 esterni. Se si inviano pacchetti AutoSupport tramite HTTPS o HTTP, è possibile configurare un **"server proxy di amministrazione"** tra i nodi amministrativi e il supporto tecnico.

Controllare i firewall

Per migliorare la sicurezza del sistema, è possibile controllare l'accesso ai nodi di amministrazione StorageGRID aprendo o chiudendo porte specifiche a livello **"firewall esterno"**. È inoltre possibile controllare l'accesso alla rete per ciascun nodo configurandone **"firewall interno"**. È possibile impedire l'accesso a tutte le porte, ad eccezione di quelle necessarie per la distribuzione.

Esaminare i metodi di crittografia StorageGRID

StorageGRID offre diverse opzioni per la crittografia dei dati. Dovresti esaminare i metodi disponibili per determinare quali metodi soddisfano i tuoi requisiti di protezione dei dati.

La tabella fornisce un riepilogo di alto livello dei metodi di crittografia disponibili in StorageGRID.

Opzione di crittografia	Come funziona	Si applica a
Server di gestione delle chiavi (KMS) in Grid Manager	Voi "configurare un server di gestione delle chiavi" per il sito StorageGRID e "abilitare la crittografia dei nodi per l'appliance" . Quindi, un nodo appliance si connette al KMS per richiedere una chiave di crittografia (KEK). Questa chiave crittografa e decrittografa la chiave di crittografia dei dati (DEK) su ciascun volume.	Nodi dell'appliance in cui è abilitata la Crittografia nodo durante l'installazione. Tutti i dati presenti sull'appliance sono protetti contro la perdita fisica o la rimozione dal data center. Nota: la gestione delle chiavi di crittografia con un KMS è supportata solo per i nodi di archiviazione e le appliance di servizi.

Opzione di crittografia	Come funziona	Si applica a
Pagina Crittografia unità nel programma di installazione dell'appliance StorageGRID	Se l'appliance contiene unità che supportano la crittografia hardware, è possibile impostare una passphrase dell'unità durante l'installazione. Quando si imposta una passphrase per l'unità, è impossibile per chiunque recuperare dati validi dalle unità rimosse dal sistema, a meno che non si conosca la passphrase. Prima di iniziare l'installazione, vai su Configura hardware > Crittografia unità per impostare una passphrase dell'unità che si applichi a tutte le unità auto-crittografanti gestite da StorageGRID in un nodo.	Dispositivi che contengono unità auto-crittografanti. Tutti i dati presenti sulle unità protette sono protetti contro la perdita fisica o la rimozione dal data center. La crittografia dell'unità non si applica alle unità gestite SANtricity. Se si dispone di un dispositivo di archiviazione con unità auto-crittografanti e controller SANtricity, è possibile abilitare la sicurezza delle unità in SANtricity.
Sicurezza dell'unità in SANtricity System Manager	Se la funzionalità Drive Security è abilitata per l'appliance StorageGRID, è possibile utilizzare "Gestore del sistema SANtricity" per creare e gestire la chiave di sicurezza. La chiave è necessaria per accedere ai dati presenti sulle unità protette.	Dispositivi di archiviazione dotati di unità FDE (Full Disk Encryption) o unità auto-crittografanti. Tutti i dati presenti sulle unità protette sono protetti contro la perdita fisica o la rimozione dal data center. Non può essere utilizzato con alcuni elettrodomestici o con apparecchi di servizio.
Crittografia degli oggetti memorizzati	Si abilita il "Crittografia degli oggetti memorizzati" opzione nel Grid Manager. Se abilitata, tutti i nuovi oggetti che non sono crittografati a livello di bucket o a livello di oggetto vengono crittografati durante l'acquisizione.	Dati di oggetti S3 appena acquisiti. Gli oggetti archiviati esistenti non sono crittografati. I metadati degli oggetti e altri dati sensibili non sono crittografati.
Crittografia del bucket S3	Si invia una richiesta PutBucketEncryption per abilitare la crittografia per il bucket. Tutti i nuovi oggetti che non sono crittografati a livello di oggetto vengono crittografati durante l'acquisizione.	Solo dati di oggetti S3 appena acquisiti. È necessario specificare la crittografia per il bucket. Gli oggetti bucket esistenti non sono crittografati. I metadati degli oggetti e altri dati sensibili non sono crittografati. "Operazioni sui bucket"

Opzione di crittografia	Come funziona	Si applica a
Crittografia lato server (SSE) degli oggetti S3	Si invia una richiesta S3 per memorizzare un oggetto e includere <code>x-amz-server-side-encryption</code> intestazione della richiesta.	Solo dati di oggetti S3 appena acquisiti. È necessario specificare la crittografia per l'oggetto. I metadati degli oggetti e altri dati sensibili non sono crittografati. StorageGRID gestisce le chiavi. "Utilizzare la crittografia lato server"
Crittografia lato server degli oggetti S3 con chiavi fornite dal cliente (SSE-C)	Si invia una richiesta S3 per memorizzare un oggetto e si includono tre intestazioni di richiesta. • <code>x-amz-server-side-encryption-customer-algorithm</code> • <code>x-amz-server-side-encryption-customer-key</code> • <code>x-amz-server-side-encryption-customer-key-MD5</code>	Solo dati di oggetti S3 appena acquisiti. È necessario specificare la crittografia per l'oggetto. I metadati degli oggetti e altri dati sensibili non sono crittografati. Le chiavi vengono gestite all'esterno di StorageGRID. "Utilizzare la crittografia lato server"
Crittografia del volume esterno o dell'archivio dati	Per crittografare un intero volume o un intero datastore, è possibile utilizzare un metodo di crittografia esterno a StorageGRID, se supportato dalla piattaforma di distribuzione.	Tutti i dati degli oggetti, i metadati e i dati di configurazione del sistema, presupponendo che ogni volume o archivio dati sia crittografato. Un metodo di crittografia esterno garantisce un controllo più rigoroso sugli algoritmi e sulle chiavi di crittografia. Può essere combinato con gli altri metodi elencati.

Opzione di crittografia	Come funziona	Si applica a
Crittografia degli oggetti al di fuori di StorageGRID	Si utilizza un metodo di crittografia esterno a StorageGRID per crittografare i dati e i metadati degli oggetti prima che vengano acquisiti in StorageGRID.	Solo dati e metadati degli oggetti (i dati di configurazione del sistema non sono crittografati). Un metodo di crittografia esterno garantisce un controllo più rigoroso sugli algoritmi e sulle chiavi di crittografia. Può essere combinato con gli altri metodi elencati. "Amazon Simple Storage Service - Guida per l'utente: protezione dei dati mediante crittografia lato client"

Utilizzare più metodi di crittografia

A seconda delle esigenze, è possibile utilizzare più di un metodo di crittografia contemporaneamente. Per esempio:

- È possibile utilizzare un KMS per proteggere i nodi degli apparecchi e anche utilizzare la funzionalità di sicurezza dell'unità in SANtricity System Manager per "crittografare due volte" i dati sulle unità auto-crittografanti negli stessi apparecchi.
- È possibile utilizzare un KMS per proteggere i dati sui nodi dell'appliance e utilizzare anche l'opzione di crittografia degli oggetti archiviati per crittografare tutti gli oggetti quando vengono acquisiti.

Se solo una piccola parte dei tuoi oggetti richiede la crittografia, valuta la possibilità di controllare la crittografia a livello di bucket o di singolo oggetto. L'abilitazione di più livelli di crittografia comporta un costo aggiuntivo in termini di prestazioni.

Gestisci i certificati

Gestire i certificati di sicurezza

I certificati di sicurezza sono piccoli file di dati utilizzati per creare connessioni sicure e affidabili tra i componenti StorageGRID e tra i componenti StorageGRID e i sistemi esterni.

StorageGRID utilizza due tipi di certificati di sicurezza:

- **I certificati del server** sono obbligatori quando si utilizzano connessioni HTTPS. I certificati server vengono utilizzati per stabilire connessioni sicure tra client e server, autenticando l'identità di un server rispetto ai suoi client e fornendo un percorso di comunicazione sicuro per i dati. Sia il server che il client dispongono ciascuno di una copia del certificato.
- **I certificati client** autenticano l'identità di un client o di un utente sul server, garantendo un'autenticazione più sicura rispetto alle sole password. I certificati client non crittografano i dati.

Quando un client si connette al server tramite HTTPS, il server risponde con il certificato del server, che contiene una chiave pubblica. Il client verifica questo certificato confrontando la firma del server con la firma presente sulla propria copia del certificato. Se le firme corrispondono, il client avvia una sessione con il server utilizzando la stessa chiave pubblica.

StorageGRID funge da server per alcune connessioni (ad esempio l'endpoint del bilanciatore del carico) o da client per altre connessioni (ad esempio il servizio di replica CloudMirror).

Certificato CA predefinito della griglia

StorageGRID include un'autorità di certificazione (CA) integrata che genera un certificato CA Grid interno durante l'installazione del sistema. Per impostazione predefinita, il certificato Grid CA viene utilizzato per proteggere il traffico StorageGRID interno. Un'autorità di certificazione (CA) esterna può rilasciare certificati personalizzati pienamente conformi alle policy di sicurezza delle informazioni della tua organizzazione. Sebbene sia possibile utilizzare il certificato Grid CA per un ambiente non di produzione, la procedura consigliata per un ambiente di produzione è quella di utilizzare certificati personalizzati firmati da un'autorità di certificazione esterna. Sono supportate anche le connessioni non protette senza certificato, ma non sono consigliate.

- I certificati CA personalizzati non rimuovono i certificati interni; tuttavia, i certificati personalizzati dovrebbero essere quelli specificati per la verifica delle connessioni al server.
- Tutti i certificati personalizzati devono soddisfare i ["linee guida per il rafforzamento del sistema per i certificati del server"](#).
- StorageGRID supporta il raggruppamento dei certificati di una CA in un singolo file (noto come pacchetto di certificati CA).



StorageGRID include anche certificati CA del sistema operativo che sono gli stessi su tutte le griglie. Negli ambienti di produzione, assicurarsi di specificare un certificato personalizzato firmato da un'autorità di certificazione esterna al posto del certificato CA del sistema operativo.

Le varianti dei tipi di certificato server e client vengono implementate in diversi modi. Prima di configurare il sistema, è necessario disporre di tutti i certificati necessari per la configurazione specifica StorageGRID.

Certificati di sicurezza di accesso

È possibile accedere alle informazioni su tutti i certificati StorageGRID in un'unica posizione, insieme ai collegamenti al flusso di lavoro di configurazione per ciascun certificato.

Passi

1. Da Grid Manager, seleziona **CONFIGURAZIONE > Sicurezza > Certificati**.

Certificates

View and manage the certificates that secure HTTPS connections between StorageGRID and external clients, such as S3 or Swift, and external servers, such as a key management server (KMS).

Global

Grid CA

Client

Load balancer endpoints

Tenants

Other

The StorageGRID certificate authority ("grid CA") generates and signs two global certificates during installation. The management interface certificate on Admin Nodes secures the management interface. The S3 and Swift API certificate on Storage and Gateway Nodes secures client access. You should replace each default certificate with your own custom certificate signed by an external certificate authority.

Name	Description	Type ⓘ	Expiration date ⓘ ⌵
Management interface certificate	Secures the connection between client web browsers and the Grid Manager, Tenant Manager, Grid Management API, and Tenant Management API.	Custom	Jun 4th, 2022
S3 and Swift API certificate	Secures the connections between S3 and Swift clients and Storage Nodes or between clients and the deprecated CLB service on Gateway Nodes. You can optionally use this certificate for a load balancer endpoint as well.	Custom	Jun 4th, 2022

2. Selezionare una scheda nella pagina Certificati per informazioni su ciascuna categoria di certificato e per accedere alle impostazioni del certificato. Puoi accedere a una scheda se hai ["autorizzazione appropriata"](#) .

- **Globale:** Protegge l'accesso a StorageGRID da browser Web e client API esterni.
- **Grid CA:** protegge il traffico StorageGRID interno.
- **Client:** protegge le connessioni tra client esterni e il database StorageGRID Prometheus.
- **Endpoint del bilanciatore del carico:** protegge le connessioni tra i client S3 e il bilanciatore del carico StorageGRID .
- **Tenant:** protegge le connessioni ai server di federazione delle identità o dagli endpoint dei servizi di piattaforma alle risorse di archiviazione S3.
- **Altro:** protegge le connessioni StorageGRID che richiedono certificati specifici.

Di seguito viene descritta ogni scheda con link ad ulteriori dettagli sul certificato.

Globale

I certificati globali proteggono l'accesso a StorageGRID dai browser Web e dai client API S3 esterni. Durante l'installazione, inizialmente l'autorità di certificazione StorageGRID genera due certificati globali. La procedura migliore per un ambiente di produzione è quella di utilizzare certificati personalizzati firmati da un'autorità di certificazione esterna.

- [Certificato di interfaccia di gestione](#): Protegge le connessioni del browser Web del client alle interfacce di gestione StorageGRID .
- [Certificato API S3](#): Protegge le connessioni API client ai nodi di archiviazione, ai nodi di amministrazione e ai nodi gateway, che le applicazioni client S3 utilizzano per caricare e scaricare i dati degli oggetti.

Le informazioni sui certificati globali installati includono:

- **Nome**: Nome del certificato con collegamento alla gestione del certificato.
- **Descrizione**
- **Tipo**: personalizzato o predefinito. + Per una maggiore sicurezza della rete, dovresti sempre utilizzare un certificato personalizzato.
- **Data di scadenza**: se si utilizza il certificato predefinito, non viene visualizzata alcuna data di scadenza.

Puoi:

- Sostituisci i certificati predefiniti con certificati personalizzati firmati da un'autorità di certificazione esterna per migliorare la sicurezza della griglia:
 - ["Sostituisci il certificato dell'interfaccia di gestione predefinita generata da StorageGRID"](#) utilizzato per le connessioni Grid Manager e Tenant Manager.
 - ["Sostituisci il certificato API S3"](#) utilizzato per le connessioni del nodo di archiviazione e dell'endpoint del bilanciatore del carico (facoltativo).
- ["Ripristina il certificato dell'interfaccia di gestione predefinita"](#) .
- ["Ripristina il certificato API S3 predefinito"](#) .
- ["Utilizzare uno script per generare un nuovo certificato di interfaccia di gestione autofirmato"](#) .
- Copia o scarica il ["certificato di interfaccia di gestione"](#) O ["Certificato API S3"](#) .

Griglia CA

IL [Certificato CA di Grid](#) , generato dall'autorità di certificazione StorageGRID durante l'installazione StorageGRID , protegge tutto il traffico interno StorageGRID .

Le informazioni sul certificato includono la data di scadenza e il contenuto del certificato.

Puoi ["copia o scarica il certificato Grid CA"](#) , ma non puoi cambiarlo.

Cliente

[Certificati client](#), generati da un'autorità di certificazione esterna, proteggono le connessioni tra gli strumenti di monitoraggio esterni e il database StorageGRID Prometheus.

La tabella dei certificati contiene una riga per ogni certificato client configurato e indica se il certificato può essere utilizzato per l'accesso al database Prometheus, insieme alla data di scadenza del certificato.

Puoi:

- ["Carica o genera un nuovo certificato client."](#)
- Seleziona un nome di certificato per visualizzarne i dettagli, dove puoi:
 - ["Cambia il nome del certificato client."](#)
 - ["Imposta l'autorizzazione di accesso a Prometheus."](#)
 - ["Carica e sostituisci il certificato client."](#)
 - ["Copia o scarica il certificato client."](#)
 - ["Rimuovere il certificato client."](#)
- Seleziona **Azioni** per eseguire rapidamente ["modificare"](#), ["allegare"](#), o ["rimuovere"](#) un certificato client. È possibile selezionare fino a 10 certificati client e rimuoverli contemporaneamente utilizzando **Azioni > Rimuovi**.

Endpoint del bilanciatore del carico

[Certificati degli endpoint del bilanciatore del carico](#) proteggere le connessioni tra i client S3 e il servizio StorageGRID Load Balancer sui nodi gateway e sui nodi amministrativi.

La tabella degli endpoint del bilanciatore del carico contiene una riga per ogni endpoint del bilanciatore del carico configurato e indica se per l'endpoint viene utilizzato il certificato API S3 globale o un certificato endpoint del bilanciatore del carico personalizzato. Per ogni certificato viene visualizzata anche la data di scadenza.



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

Puoi:

- ["Visualizza un endpoint del bilanciatore del carico"](#), compresi i dettagli del suo certificato.
- ["Specificare un certificato dell'endpoint del bilanciatore del carico per FabricPool."](#)
- ["Utilizzare il certificato API S3 globale"](#) invece di generare un nuovo certificato dell'endpoint del bilanciatore del carico.

inquilini

Gli inquilini possono utilizzare [certificati del server di federazione delle identità](#) o [certificati endpoint del servizio di piattaforma](#) per proteggere le loro connessioni con StorageGRID.

La tabella dei tenant contiene una riga per ogni tenant e indica se ogni tenant ha l'autorizzazione a utilizzare la propria fonte di identità o i servizi della piattaforma.

Puoi:

- ["Seleziona un nome di tenant per accedere a Tenant Manager"](#)
- ["Seleziona un nome tenant per visualizzare i dettagli della federazione dell'identità del tenant"](#)
- ["Seleziona un nome tenant per visualizzare i dettagli dei servizi della piattaforma tenant"](#)
- ["Specificare un certificato dell'endpoint del servizio di piattaforma durante la creazione dell'endpoint"](#)

Altro

StorageGRID utilizza altri certificati di sicurezza per scopi specifici. Questi certificati sono elencati in base al loro nome funzionale. Altri certificati di sicurezza includono:

- [Certificati del pool di archiviazione cloud](#)
- [Certificati di notifica di avviso via e-mail](#)
- [Certificati del server syslog esterno](#)
- [Certificati di connessione alla federazione di rete](#)
- [Certificati di federazione delle identità](#)
- [Certificati del server di gestione delle chiavi \(KMS\)](#)
- [Certificati Single Sign-On](#)

Le informazioni indicano il tipo di certificato utilizzato da una funzione e le date di scadenza dei certificati server e client, se applicabile. Selezionando il nome di una funzione si apre una scheda del browser in cui è possibile visualizzare e modificare i dettagli del certificato.



È possibile visualizzare e accedere alle informazioni per altri certificati solo se si dispone dell'"[autorizzazione appropriata](#)".

Puoi:

- ["Specificare un certificato Cloud Storage Pool per S3, C2S S3 o Azure"](#)
- ["Specificare un certificato per le notifiche e-mail di avviso"](#)
- ["Utilizzare un certificato per un server syslog esterno"](#)
- ["Ruotare i certificati di connessione della federazione di rete"](#)
- ["Visualizzare e modificare un certificato di federazione delle identità"](#)
- ["Carica i certificati del server e del client del server di gestione delle chiavi \(KMS\)"](#)
- ["Specificare manualmente un certificato SSO per un trust della parte affidabile"](#)

Dettagli del certificato di sicurezza

Di seguito viene descritto ciascun tipo di certificato di sicurezza, con link alle istruzioni di implementazione.

Certificato di interfaccia di gestione

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione tra i browser Web client e l'interfaccia di gestione StorageGRID , consentendo agli utenti di accedere a Grid Manager e Tenant Manager senza avvisi di sicurezza. Questo certificato autentica anche le connessioni Grid Management API e Tenant Management API. È possibile utilizzare il certificato predefinito creato durante l'installazione oppure caricare un certificato personalizzato.	CONFIGURAZIONE > Sicurezza > Certificati , seleziona la scheda Globale , quindi seleziona Certificato dell'interfaccia di gestione	"Configurare i certificati dell'interfaccia di gestione"

Certificato API S3

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica le connessioni client S3 sicure a un nodo di archiviazione e agli endpoint del bilanciatore del carico (facoltativo).	CONFIGURAZIONE > Sicurezza > Certificati , seleziona la scheda Globale , quindi seleziona Certificato API S3	"Configurare i certificati API S3"

Certificato CA di Grid

Vedi il [Descrizione del certificato CA Grid predefinito](#) .

Certificato client amministratore

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Cliente	Installato su ciascun client, consente a StorageGRID di autenticare l'accesso dei client esterni. • Consente ai client esterni autorizzati di accedere al database StorageGRID Prometheus. • Consente il monitoraggio sicuro di StorageGRID tramite strumenti esterni.	CONFIGURAZIONE > Sicurezza > Certificati e quindi selezionare la scheda Client	"Configurare i certificati client"

Certificato dell'endpoint del bilanciatore del carico

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione tra i client S3 e il servizio StorageGRID Load Balancer sui nodi gateway e sui nodi amministrativi. È possibile caricare o generare un certificato del bilanciatore del carico quando si configura un endpoint del bilanciatore del carico. Le applicazioni client utilizzano il certificato del bilanciatore del carico quando si connettono a StorageGRID per salvare e recuperare i dati degli oggetti. Puoi anche utilizzare una versione personalizzata del globale Certificato API S3 certificato per autenticare le connessioni al servizio Load Balancer. Se il certificato globale viene utilizzato per autenticare le connessioni del bilanciatore del carico, non è necessario caricare o generare un certificato separato per ogni endpoint del bilanciatore del carico. Nota: il certificato utilizzato per l'autenticazione del bilanciatore del carico è il certificato più utilizzato durante il normale funzionamento StorageGRID .	CONFIGURAZIONE > Rete > Endpoint del bilanciatore del carico	• "Configurare gli endpoint del bilanciatore del carico" • "Creare un endpoint del bilanciatore del carico per FabricPool"

Certificato endpoint del pool di archiviazione cloud

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione da un pool di archiviazione cloud StorageGRID a una posizione di archiviazione esterna, ad esempio S3 Glacier o Microsoft Azure Blob Storage. Per ogni tipo di provider cloud è richiesto un certificato diverso.	ILM > Pool di archiviazione	"Creare un pool di archiviazione cloud"

Certificato di notifica di avviso via e-mail

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server e client	Autentica la connessione tra un server di posta elettronica SMTP e StorageGRID utilizzata per le notifiche di avviso. • Se le comunicazioni con il server SMTP richiedono Transport Layer Security (TLS), è necessario specificare il certificato CA del server di posta elettronica. • Specificare un certificato client solo se il server di posta elettronica SMTP richiede certificati client per l'autenticazione.	AVVISI > Configurazione e-mail	"Imposta notifiche e-mail per gli avvisi"

Certificato del server syslog esterno

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione TLS o RELP/TLS tra un server syslog esterno che registra gli eventi in StorageGRID. Nota: non è richiesto un certificato del server syslog esterno per le connessioni TCP, RELP/TCP e UDP a un server syslog esterno.	CONFIGURAZIONE > Monitoraggio > Server di audit e syslog	"Utilizzare un server syslog esterno"

Certificato di connessione alla federazione di rete

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server e client	Autenticare e crittografare le informazioni inviate tra l'attuale sistema StorageGRID e un'altra griglia in una connessione di federazione di griglia.	CONFIGURAZIONE > Sistema > Federazione di griglia	• "Creare connessioni di federazione di griglia" • "Ruota i certificati di connessione"

Certificato di federazione dell'identità

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione tra StorageGRID e un provider di identità esterno, come Active Directory, OpenLDAP o Oracle Directory Server. Utilizzato per la federazione delle identità, che consente la gestione di gruppi di amministratori e utenti da parte di un sistema esterno.	CONFIGURAZIONE > Controllo accessi > Federazione identità	"Utilizzare la federazione delle identità"

Certificato del server di gestione delle chiavi (KMS)

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server e client	Autentica la connessione tra StorageGRID e un server di gestione delle chiavi esterno (KMS), che fornisce chiavi di crittografia ai nodi dell'appliance StorageGRID .	CONFIGURAZIONE > Sicurezza > Server di gestione delle chiavi	" Aggiungi server di gestione delle chiavi (KMS) "

Certificato endpoint dei servizi di piattaforma

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione dal servizio della piattaforma StorageGRID a una risorsa di archiviazione S3.	Gestore inquilino > ARCHIVIAZIONE (S3) > Endpoint dei servizi della piattaforma	" Crea endpoint dei servizi della piattaforma " " Modifica endpoint dei servizi della piattaforma "

Certificato Single Sign-On (SSO)

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione tra i servizi di federazione delle identità, come Active Directory Federation Services (AD FS) e StorageGRID , utilizzati per le richieste Single Sign-On (SSO).	CONFIGURAZIONE > Controllo accessi > Single sign-on	" Configurare l'accesso singolo "

Esempi di certificati

Esempio 1: servizio Load Balancer

In questo esempio, StorageGRID funge da server.

1. È possibile configurare un endpoint del bilanciatore del carico e caricare o generare un certificato del server in StorageGRID.
2. Si configura una connessione client S3 all'endpoint del bilanciatore del carico e si carica lo stesso certificato sul client.
3. Quando il client desidera salvare o recuperare dati, si connette all'endpoint del bilanciatore del carico tramite HTTPS.
4. StorageGRID risponde con il certificato del server, che contiene una chiave pubblica, e con una firma

basata sulla chiave privata.

5. Il client verifica questo certificato confrontando la firma del server con la firma presente sulla propria copia del certificato. Se le firme corrispondono, il client avvia una sessione utilizzando la stessa chiave pubblica.
6. Il client invia i dati dell'oggetto a StorageGRID.

Esempio 2: Server di gestione delle chiavi esterno (KMS)

In questo esempio, StorageGRID funge da client.

1. Utilizzando il software Key Management Server esterno, è possibile configurare StorageGRID come client KMS e ottenere un certificato server firmato da una CA, un certificato client pubblico e la chiave privata per il certificato client.
2. Utilizzando Grid Manager, puoi configurare un server KMS e caricare i certificati del server e del client, nonché la chiave privata del client.
3. Quando un nodo StorageGRID necessita di una chiave di crittografia, invia una richiesta al server KMS che include i dati del certificato e una firma basata sulla chiave privata.
4. Il server KMS convalida la firma del certificato e decide che StorageGRID può essere considerato attendibile.
5. Il server KMS risponde utilizzando la connessione convalidata.

Tipi di certificati server supportati

Il sistema StorageGRID supporta certificati personalizzati crittografati con RSA o ECDSA (Elliptic Curve Digital Signature Algorithm).



Il tipo di cifratura per la policy di sicurezza deve corrispondere al tipo di certificato del server. Ad esempio, i cifrari RSA richiedono certificati RSA, mentre i cifrari ECDSA richiedono certificati ECDSA. Vedere ["Gestire i certificati di sicurezza"](#). Se si configura un criterio di sicurezza personalizzato che non è compatibile con il certificato del server, è possibile ["ripristinare temporaneamente la politica di sicurezza predefinita"](#).

Per ulteriori informazioni su come StorageGRID protegge le connessioni client, vedere ["Sicurezza per i client S3"](#).

Configurare i certificati dell'interfaccia di gestione

È possibile sostituire il certificato dell'interfaccia di gestione predefinita con un singolo certificato personalizzato che consente agli utenti di accedere a Grid Manager e Tenant Manager senza visualizzare avvisi di sicurezza. È anche possibile ripristinare il certificato dell'interfaccia di gestione predefinito o generarne uno nuovo.

Informazioni su questo compito

Per impostazione predefinita, a ogni nodo amministrativo viene rilasciato un certificato firmato dalla CA della griglia. Questi certificati firmati da CA possono essere sostituiti da un singolo certificato di interfaccia di gestione personalizzata comune e dalla corrispondente chiave privata.

Poiché per tutti i nodi amministrativi viene utilizzato un singolo certificato di interfaccia di gestione personalizzata, è necessario specificare il certificato come certificato jolly o multidominio se i client devono verificare il nome host durante la connessione a Grid Manager e Tenant Manager. Definisci il certificato personalizzato in modo che corrisponda a tutti i nodi amministrativi nella griglia.

È necessario completare la configurazione sul server e, a seconda dell'autorità di certificazione radice (CA) utilizzata, gli utenti potrebbero dover installare anche il certificato Grid CA nel browser Web che utilizzeranno per accedere a Grid Manager e Tenant Manager.



Per garantire che le operazioni non vengano interrotte da un certificato server non riuscito, l'avviso **Scadenza del certificato server per l'interfaccia di gestione** viene attivato quando il certificato server sta per scadere. Se necessario, è possibile visualizzare la data di scadenza del certificato corrente selezionando **CONFIGURAZIONE > Sicurezza > Certificati** e controllando la data di scadenza del certificato dell'interfaccia di gestione nella scheda Globale.



Se si accede a Grid Manager o Tenant Manager utilizzando un nome di dominio anziché un indirizzo IP, il browser visualizza un errore di certificato senza un'opzione per ignorarlo se si verifica una delle seguenti situazioni:

- Il certificato dell'interfaccia di gestione personalizzata scade.
- [Voi ripristinare un certificato di interfaccia di gestione personalizzato al certificato del server predefinito](#) .

Aggiungi un certificato di interfaccia di gestione personalizzato

Per aggiungere un certificato di interfaccia di gestione personalizzato, puoi fornire il tuo certificato o generarne uno utilizzando Grid Manager.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Certificati**.
2. Nella scheda **Globale**, seleziona **Certificato dell'interfaccia di gestione**.
3. Seleziona **Usa certificato personalizzato**.
4. Carica o genera il certificato.

Carica il certificato

Caricare i file del certificato del server richiesti.

a. Seleziona **Carica certificato**.

b. Carica i file del certificato del server richiesti:

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



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

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

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

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

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

Ad esempio: `storagegrid_certificate.pem`

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

d. Seleziona **Salva**. + Il certificato dell'interfaccia di gestione personalizzata viene utilizzato per tutte le nuove connessioni successive a Grid Manager, Tenant Manager, Grid Manager API o Tenant Manager API.

Genera certificato

Generare i file del certificato del server.



La procedura consigliata per un ambiente di produzione è quella di utilizzare un certificato di interfaccia di gestione personalizzato firmato da un'autorità di certificazione esterna.

a. Seleziona **Genera certificato**.

b. Specificare le informazioni del certificato:

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

Campo	Descrizione
Proprietà intellettuale	Uno o più indirizzi IP da includere nel certificato.
Oggetto (facoltativo)	Soggetto X.509 o nome distinto (DN) del proprietario del certificato. Se non viene immesso alcun valore in questo campo, il certificato generato utilizza il primo nome di dominio o indirizzo IP come nome comune (CN) del soggetto.
Giorni validi	Numero di giorni dopo la creazione in cui scade il certificato.
Aggiungi estensioni di utilizzo delle chiavi	Se selezionata (impostazione predefinita e consigliata), le estensioni per l'utilizzo delle chiavi e per l'utilizzo esteso delle chiavi vengono aggiunte al certificato generato. Queste estensioni definiscono lo scopo della chiave contenuta nel certificato. Nota: lasciare selezionata questa casella di controllo a meno che non si riscontrino problemi di connessione con client più vecchi quando i certificati includono queste estensioni.

c. Seleziona **Genera**.

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

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

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

Ad esempio: `storagegrid_certificate.pem`

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

e. Seleziona **Salva**. + Il certificato dell'interfaccia di gestione personalizzata viene utilizzato per tutte le nuove connessioni successive a Grid Manager, Tenant Manager, Grid Manager API o Tenant Manager API.

5. Aggiorna la pagina per assicurarti che il browser web sia aggiornato.



Dopo aver caricato o generato un nuovo certificato, attendere fino a un giorno affinché tutti gli avvisi di scadenza del certificato correlati vengano cancellati.

6. Dopo aver aggiunto un certificato di interfaccia di gestione personalizzato, la pagina Certificato di interfaccia di gestione visualizza informazioni dettagliate sui certificati in uso. + È possibile scaricare o copiare il certificato PEM a seconda delle necessità.

Ripristina il certificato dell'interfaccia di gestione predefinita

È possibile tornare a utilizzare il certificato dell'interfaccia di gestione predefinito per le connessioni Grid

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Certificati**.
2. Nella scheda **Globale**, seleziona **Certificato dell'interfaccia di gestione**.
3. Selezionare **Usa certificato predefinito**.

Quando si ripristina il certificato dell'interfaccia di gestione predefinita, i file del certificato del server personalizzato configurati vengono eliminati e non possono essere recuperati dal sistema. Per tutte le successive nuove connessioni client verrà utilizzato il certificato dell'interfaccia di gestione predefinita.

4. Aggiorna la pagina per assicurarti che il browser web sia aggiornato.

Utilizzare uno script per generare un nuovo certificato di interfaccia di gestione autofirmato

Se è richiesta una convalida rigorosa del nome host, è possibile utilizzare uno script per generare il certificato dell'interfaccia di gestione.

Prima di iniziare

- Hai ["autorizzazioni di accesso specifiche"](#) .
- Tu hai il `Passwords.txt` file.

Informazioni su questo compito

La procedura migliore per un ambiente di produzione è quella di utilizzare un certificato firmato da un'autorità di certificazione esterna.

Passi

1. Ottieni il nome di dominio completo (FQDN) di ciascun nodo di amministrazione.
2. Accedi al nodo di amministrazione principale:
 - a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Inserisci la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla root: `su -`
 - d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#` .

3. Configurare StorageGRID con un nuovo certificato autofirmato.

```
$ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
```

- Per `--domains` , utilizzare i caratteri jolly per rappresentare i nomi di dominio completi di tutti i nodi di amministrazione. Per esempio, `*.ui.storagegrid.example.com` usa il carattere jolly `*` per rappresentare `admin1.ui.storagegrid.example.com` e `admin2.ui.storagegrid.example.com` .
- Impostato `--type A management` per configurare il certificato dell'interfaccia di gestione, utilizzato da Grid Manager e Tenant Manager.
- Per impostazione predefinita, i certificati generati sono validi per un anno (365 giorni) e devono essere ricreati prima della scadenza. Puoi usare il `--days` argomento per sovrascrivere il periodo di validità

predefinito.



Il periodo di validità di un certificato inizia quando `make-certificate` è in esecuzione. È necessario assicurarsi che il client di gestione sia sincronizzato con la stessa origine oraria di StorageGRID; in caso contrario, il client potrebbe rifiutare il certificato.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type  
management --days 720
```

L'output risultante contiene il certificato pubblico richiesto dal client API di gestione.

4. Seleziona e copia il certificato.

Includi i tag BEGIN e END nella tua selezione.

5. Disconnettersi dalla shell dei comandi. `$ exit`

6. Conferma che il certificato è stato configurato:

- a. Accedi al Grid Manager.
- b. Selezionare **CONFIGURAZIONE > Sicurezza > Certificati**
- c. Nella scheda **Globale**, seleziona **Certificato dell'interfaccia di gestione**.

7. Configura il tuo client di gestione per utilizzare il certificato pubblico che hai copiato. Includi i tag BEGIN e END.

Scarica o copia il certificato dell'interfaccia di gestione

È possibile salvare o copiare il contenuto del certificato dell'interfaccia di gestione per utilizzarlo altrove.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Certificati**.
2. Nella scheda **Globale**, seleziona **Certificato dell'interfaccia di gestione**.
3. Selezionare la scheda **Server** o **bundle CA**, quindi scaricare o copiare il certificato.

Scarica il file del certificato o il pacchetto CA

Scarica il certificato o il pacchetto CA .pem file. Se si utilizza un bundle CA facoltativo, ogni certificato nel bundle viene visualizzato nella propria sotto-scheda.

a. Selezionare **Scarica certificato** o **Scarica pacchetto CA**.

Se si scarica un bundle CA, tutti i certificati nelle schede secondarie del bundle CA vengono scaricati come un singolo file.

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

Ad esempio: `storagegrid_certificate.pem`

Copia certificato o pacchetto CA PEM

Copia il testo del certificato per incollarlo altrove. Se si utilizza un bundle CA facoltativo, ogni certificato nel bundle viene visualizzato nella propria sotto-scheda.

a. Selezionare **Copia certificato PEM** o **Copia pacchetto CA PEM**.

Se si copia un bundle CA, tutti i certificati nelle schede secondarie del bundle CA vengono copiati insieme.

b. Incolla il certificato copiato in un editor di testo.

c. Salva il file di testo con l'estensione .pem .

Ad esempio: `storagegrid_certificate.pem`

Configurare i certificati API S3

È possibile sostituire o ripristinare il certificato del server utilizzato per le connessioni client S3 ai nodi di archiviazione o agli endpoint del bilanciatore del carico. Il certificato server personalizzato sostitutivo è specifico per la tua organizzazione.



I dettagli su Swift sono stati rimossi da questa versione del sito di documentazione. Vedere ["StorageGRID 11.8: configurare i certificati API S3 e Swift"](#) .

Informazioni su questo compito

Per impostazione predefinita, a ogni nodo di archiviazione viene rilasciato un certificato server X.509 firmato dalla CA della griglia. Questi certificati firmati da CA possono essere sostituiti da un singolo certificato server personalizzato comune e dalla corrispondente chiave privata.

Per tutti i nodi di archiviazione viene utilizzato un singolo certificato server personalizzato, pertanto è necessario specificare il certificato come carattere jolly o certificato multidominio se i client devono verificare il nome host durante la connessione all'endpoint di archiviazione. Definire il certificato personalizzato in modo che corrisponda a tutti i nodi di archiviazione nella griglia.

Dopo aver completato la configurazione sul server, potrebbe essere necessario installare anche il certificato Grid CA nel client API S3 che utilizzerai per accedere al sistema, a seconda dell'autorità di certificazione

radice (CA) che stai utilizzando.



Per garantire che le operazioni non vengano interrotte da un certificato server non riuscito, l'avviso **Scadenza del certificato server globale per l'API S3** viene attivato quando il certificato del server radice sta per scadere. Se necessario, è possibile visualizzare la data di scadenza del certificato corrente selezionando **CONFIGURAZIONE > Sicurezza > Certificati** e controllando la data di scadenza del certificato API S3 nella scheda Globale.

È possibile caricare o generare un certificato API S3 personalizzato.

Aggiungi un certificato API S3 personalizzato

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Certificati**.
2. Nella scheda **Globale**, seleziona **Certificato API S3**.
3. Seleziona **Usa certificato personalizzato**.
4. Carica o genera il certificato.

Carica il certificato

Caricare i file del certificato del server richiesti.

a. Seleziona **Carica certificato**.

b. Carica i file del certificato del server richiesti:

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



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

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

c. Selezionare i dettagli del certificato per visualizzare i metadati e il PEM per ciascun certificato API S3 personalizzato caricato. Se hai caricato un bundle CA facoltativo, ogni certificato verrà visualizzato in una scheda separata.

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

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

Ad esempio: `storagegrid_certificate.pem`

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

d. Seleziona **Salva**.

Il certificato server personalizzato viene utilizzato per le successive nuove connessioni client S3.

Genera certificato

Generare i file del certificato del server.

a. Seleziona **Genera certificato**.

b. Specificare le informazioni del certificato:

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

Campo	Descrizione
Oggetto (facoltativo)	Soggetto X.509 o nome distinto (DN) del proprietario del certificato. Se non viene immesso alcun valore in questo campo, il certificato generato utilizza il primo nome di dominio o indirizzo IP come nome comune (CN) del soggetto.
Giorni validi	Numero di giorni dopo la creazione in cui scade il certificato.
Aggiungi estensioni di utilizzo delle chiavi	Se selezionata (impostazione predefinita e consigliata), le estensioni per l'utilizzo delle chiavi e per l'utilizzo esteso delle chiavi vengono aggiunte al certificato generato. Queste estensioni definiscono lo scopo della chiave contenuta nel certificato. Nota: lasciare selezionata questa casella di controllo a meno che non si riscontrino problemi di connessione con client più vecchi quando i certificati includono queste estensioni.

c. Seleziona **Genera**.

d. Selezionare **Dettagli certificato** per visualizzare i metadati e il PEM per il certificato API S3 personalizzato generato.

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

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

Ad esempio: `storagegrid_certificate.pem`

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

e. Seleziona **Salva**.

Il certificato server personalizzato viene utilizzato per le successive nuove connessioni client S3.

5. Selezionare una scheda per visualizzare i metadati per il certificato del server StorageGRID predefinito, un certificato firmato da una CA caricato o un certificato personalizzato generato.



Dopo aver caricato o generato un nuovo certificato, attendere fino a un giorno affinché tutti gli avvisi di scadenza del certificato correlati vengano cancellati.

6. Aggiorna la pagina per assicurarti che il browser web sia aggiornato.

7. Dopo aver aggiunto un certificato API S3 personalizzato, la pagina del certificato API S3 visualizza informazioni dettagliate sul certificato API S3 personalizzato in uso. + È possibile scaricare o copiare il certificato PEM a seconda delle necessità.

Ripristina il certificato API S3 predefinito

È possibile tornare a utilizzare il certificato API S3 predefinito per le connessioni client S3 ai nodi di archiviazione. Tuttavia, non è possibile utilizzare il certificato API S3 predefinito per un endpoint del bilanciatore del carico.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Certificati**.
2. Nella scheda **Globale**, seleziona **Certificato API S3**.
3. Selezionare **Usa certificato predefinito**.

Quando si ripristina la versione predefinita del certificato API S3 globale, i file del certificato del server personalizzato configurati vengono eliminati e non possono essere recuperati dal sistema. Per le successive nuove connessioni client S3 ai nodi di archiviazione verrà utilizzato il certificato API S3 predefinito.

4. Selezionare **OK** per confermare l'avviso e ripristinare il certificato API S3 predefinito.

Se si dispone dell'autorizzazione di accesso Root e per le connessioni degli endpoint del bilanciatore del carico è stato utilizzato il certificato API S3 personalizzato, verrà visualizzato un elenco degli endpoint del bilanciatore del carico che non saranno più accessibili utilizzando il certificato API S3 predefinito. Vai a ["Configurare gli endpoint del bilanciatore del carico"](#) per modificare o rimuovere gli endpoint interessati.

5. Aggiorna la pagina per assicurarti che il browser web sia aggiornato.

Scarica o copia il certificato API S3

È possibile salvare o copiare il contenuto del certificato API S3 per utilizzarlo altrove.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Certificati**.
2. Nella scheda **Globale**, seleziona **Certificato API S3**.
3. Selezionare la scheda **Server** o **bundle CA**, quindi scaricare o copiare il certificato.

Scarica il file del certificato o il pacchetto CA

Scarica il certificato o il pacchetto CA .pem file. Se si utilizza un bundle CA facoltativo, ogni certificato nel bundle viene visualizzato nella propria sotto-scheda.

a. Selezionare **Scarica certificato** o **Scarica pacchetto CA**.

Se si scarica un bundle CA, tutti i certificati nelle schede secondarie del bundle CA vengono scaricati come un singolo file.

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

Ad esempio: `storagegrid_certificate.pem`

Copia certificato o pacchetto CA PEM

Copia il testo del certificato per incollarlo altrove. Se si utilizza un bundle CA facoltativo, ogni certificato nel bundle viene visualizzato nella propria sotto-scheda.

a. Selezionare **Copia certificato PEM** o **Copia pacchetto CA PEM**.

Se si copia un bundle CA, tutti i certificati nelle schede secondarie del bundle CA vengono copiati insieme.

b. Incolla il certificato copiato in un editor di testo.

c. Salva il file di testo con l'estensione .pem .

Ad esempio: `storagegrid_certificate.pem`

Informazioni correlate

- ["Utilizzare l'API REST S3"](#)
- ["Configurare i nomi di dominio degli endpoint S3"](#)

Copia il certificato Grid CA

StorageGRID utilizza un'autorità di certificazione (CA) interna per proteggere il traffico interno. Questo certificato non cambia se carichi i tuoi certificati.

Prima di iniziare

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

Informazioni su questo compito

Se è stato configurato un certificato server personalizzato, le applicazioni client devono verificare il server utilizzando il certificato server personalizzato. Non devono copiare il certificato CA dal sistema StorageGRID .

Passi

1. Selezionare **CONFIGURAZIONE** > **Sicurezza** > **Certificati** e quindi selezionare la scheda **CA griglia**.

2. Nella sezione **Certificato PEM**, scaricare o copiare il certificato.

Scarica il file del certificato

Scarica il certificato .pem file.

- Seleziona **Scarica certificato**.
- Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione .pem .

Ad esempio: `storagegrid_certificate.pem`

Copia certificato PEM

Copia il testo del certificato per incollarlo altrove.

- Selezionare **Copia certificato PEM**.
- Incolla il certificato copiato in un editor di testo.
- Salva il file di testo con l'estensione .pem .

Ad esempio: `storagegrid_certificate.pem`

Configurare i certificati StorageGRID per FabricPool

Per i client S3 che eseguono la convalida rigorosa del nome host e non supportano la disabilitazione della convalida rigorosa del nome host, come i client ONTAP che utilizzano FabricPool, è possibile generare o caricare un certificato server quando si configura l'endpoint del bilanciatore del carico.

Prima di iniziare

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

Informazioni su questo compito

Quando si crea un endpoint del bilanciatore del carico, è possibile generare un certificato server autofirmato o caricare un certificato firmato da un'autorità di certificazione (CA) nota. Negli ambienti di produzione, è consigliabile utilizzare un certificato firmato da una CA nota. I certificati firmati da una CA possono essere ruotati senza interruzioni. Sono anche più sicuri perché offrono una migliore protezione contro gli attacchi man-in-the-middle.

I passaggi seguenti forniscono linee guida generali per i client S3 che utilizzano FabricPool. Per informazioni e procedure più dettagliate, vedere ["Configurare StorageGRID per FabricPool"](#) .

Passi

- Facoltativamente, configurare un gruppo ad alta disponibilità (HA) da utilizzare per FabricPool .
- Creare un endpoint del bilanciatore del carico S3 da utilizzare per FabricPool .

Quando si crea un endpoint del bilanciatore del carico HTTPS, viene richiesto di caricare il certificato del server, la chiave privata del certificato e il bundle CA facoltativo.

3. Collegare StorageGRID come livello cloud in ONTAP.

Specificare la porta dell'endpoint del bilanciatore del carico e il nome di dominio completo utilizzato nel certificato CA caricato. Quindi, fornire il certificato CA.



Se il certificato StorageGRID è stato emesso da una CA intermedia, è necessario fornire il certificato della CA intermedia. Se il certificato StorageGRID è stato emesso direttamente dalla CA radice, è necessario fornire il certificato della CA radice.

Configurare i certificati client

I certificati client consentono ai client esterni autorizzati di accedere al database StorageGRID Prometheus, offrendo agli strumenti esterni un modo sicuro per monitorare StorageGRID.

Se è necessario accedere a StorageGRID tramite uno strumento di monitoraggio esterno, è necessario caricare o generare un certificato client tramite Grid Manager e copiare le informazioni del certificato nello strumento esterno.

Vedere ["Gestire i certificati di sicurezza"](#) E ["Configurare certificati server personalizzati"](#) .



Per garantire che le operazioni non vengano interrotte da un certificato server non riuscito, l'avviso **Scadenza dei certificati client configurati nella pagina Certificati** viene attivato quando il certificato server sta per scadere. Se necessario, è possibile visualizzare la data di scadenza del certificato corrente selezionando **CONFIGURAZIONE > Sicurezza > Certificati** e controllando la data di scadenza del certificato client nella scheda Client.



Se si utilizza un server di gestione delle chiavi (KMS) per proteggere i dati sui nodi appliance configurati in modo speciale, consultare le informazioni specifiche su ["caricamento di un certificato client KMS"](#) .

Prima di iniziare

- Hai i permessi di accesso Root.
- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Per configurare un certificato client:
 - Hai l'indirizzo IP o il nome di dominio del nodo di amministrazione.
 - Se hai configurato il certificato dell'interfaccia di gestione StorageGRID , disponi della CA, del certificato client e della chiave privata utilizzati per configurare il certificato dell'interfaccia di gestione.
 - Per caricare il tuo certificato, la chiave privata del certificato è disponibile sul tuo computer locale.
 - La chiave privata deve essere stata salvata o registrata al momento della sua creazione. Se non si dispone della chiave privata originale, è necessario crearne una nuova.
- Per modificare un certificato client:
 - Hai l'indirizzo IP o il nome di dominio del nodo di amministrazione.
 - Per caricare il tuo certificato o un nuovo certificato, la chiave privata, il certificato client e la CA (se utilizzata) sono disponibili sul tuo computer locale.

Aggiungi certificati client

Per aggiungere il certificato client, utilizzare una di queste procedure:

- [Certificato dell'interfaccia di gestione già configurato](#)
- [Certificato client rilasciato da CA](#)
- [Certificato generato da Grid Manager](#)

Certificato dell'interfaccia di gestione già configurato

Utilizzare questa procedura per aggiungere un certificato client se un certificato dell'interfaccia di gestione è già configurato utilizzando una CA fornita dal cliente, un certificato client e una chiave privata.

Passi

1. In Grid Manager, seleziona **CONFIGURAZIONE > Sicurezza > Certificati** e quindi seleziona la scheda **Client**.
2. Selezionare **Aggiungi**.
3. Inserisci un nome per il certificato.
4. Per accedere alle metriche di Prometheus tramite il tuo strumento di monitoraggio esterno, seleziona **Consenti Prometheus**.
5. Selezionare **Continua**.
6. Per il passaggio **Allega certificati**, caricare il certificato dell'interfaccia di gestione.
 - a. Seleziona **Carica certificato**.
 - b. Selezionare **Sfoglia** e selezionare il file del certificato dell'interfaccia di gestione(.pem).
 - Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.
 - Selezionare **Copia certificato PEM** per copiare il contenuto del certificato e incollarlo altrove.
 - c. Selezionare **Crea** per salvare il certificato in Grid Manager.

Il nuovo certificato viene visualizzato nella scheda Client.
7. [Configurare uno strumento di monitoraggio esterno](#), come Grafana.

Certificato client rilasciato da CA

Utilizzare questa procedura per aggiungere un certificato client amministratore se non è stato configurato un certificato dell'interfaccia di gestione e si prevede di aggiungere un certificato client per Prometheus che utilizza un certificato client rilasciato da una CA e una chiave privata.

Passi

1. Eseguire i passaggi per ["configurare un certificato di interfaccia di gestione"](#) .
2. In Grid Manager, seleziona **CONFIGURAZIONE > Sicurezza > Certificati** e quindi seleziona la scheda **Client**.
3. Selezionare **Aggiungi**.
4. Inserisci un nome per il certificato.
5. Per accedere alle metriche di Prometheus tramite il tuo strumento di monitoraggio esterno, seleziona **Consenti Prometheus**.

6. Selezionare **Continua**.
7. Per la fase **Allega certificati**, carica i file del certificato client, della chiave privata e del bundle CA:
 - a. Seleziona **Carica certificato**.
 - b. Selezionare **Sfoglia** e selezionare il certificato client, la chiave privata e i file bundle CA(`.pem`).
 - Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.
 - Selezionare **Copia certificato PEM** per copiare il contenuto del certificato e incollarlo altrove.
 - c. Selezionare **Crea** per salvare il certificato in Grid Manager.

I nuovi certificati vengono visualizzati nella scheda Client.
8. [Configurare uno strumento di monitoraggio esterno](#), come Grafana.

Certificato generato da Grid Manager

Utilizzare questa procedura per aggiungere un certificato client amministratore se non è stato configurato un certificato dell'interfaccia di gestione e si prevede di aggiungere un certificato client per Prometheus che utilizza la funzione di generazione del certificato in Grid Manager.

Passi

1. In Grid Manager, seleziona **CONFIGURAZIONE > Sicurezza > Certificati** e quindi seleziona la scheda **Client**.
2. Selezionare **Aggiungi**.
3. Inserisci un nome per il certificato.
4. Per accedere alle metriche di Prometheus tramite il tuo strumento di monitoraggio esterno, seleziona **Consenti Prometheus**.
5. Selezionare **Continua**.
6. Per il passaggio **Allega certificati**, seleziona **Genera certificato**.
7. Specificare le informazioni del certificato:
 - **Oggetto** (facoltativo): soggetto X.509 o nome distinto (DN) del proprietario del certificato.
 - **Giorni di validità**: numero di giorni di validità del certificato generato, a partire dal momento in cui viene generato.
 - **Aggiungi estensioni per l'utilizzo delle chiavi**: se selezionato (impostazione predefinita e consigliata), le estensioni per l'utilizzo delle chiavi e l'utilizzo esteso delle chiavi vengono aggiunte al certificato generato.

Queste estensioni definiscono lo scopo della chiave contenuta nel certificato.



Lasciare selezionata questa casella di controllo a meno che non si riscontrino problemi di connessione con client più vecchi quando i certificati includono queste estensioni.

8. Seleziona **Genera**.
9. Selezionare **Dettagli del certificato client** per visualizzare i metadati del certificato e il PEM del certificato.



Dopo aver chiuso la finestra di dialogo, non sarà possibile visualizzare la chiave privata del certificato. Copia o scarica la chiave in un luogo sicuro.

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

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

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copia chiave privata** per copiare la chiave privata del certificato e incollarla altrove.
- Selezionare **Scarica chiave privata** per salvare la chiave privata come file.

Specificare il nome del file della chiave privata e il percorso di download.

10. Selezionare **Crea** per salvare il certificato in Grid Manager.

Il nuovo certificato viene visualizzato nella scheda Client.

11. In Grid Manager, seleziona **CONFIGURAZIONE > Sicurezza > Certificati** e quindi seleziona la scheda **Globale**.

12. Selezionare **Certificato interfaccia di gestione**.

13. Seleziona **Usa certificato personalizzato**.

14. Carica i file `certificate.pem` e `private_key.pem` da [dettagli del certificato client](#) fare un passo. Non è necessario caricare il bundle CA.
 - a. Selezionare **Carica certificato** e poi **Continua**.
 - b. Carica ogni file di certificato(`.pem`).
 - c. Selezionare **Salva** per salvare il certificato in Grid Manager.

Il nuovo certificato viene visualizzato nella pagina dei certificati dell'interfaccia di gestione.

15. [Configurare uno strumento di monitoraggio esterno](#), come Grafana.

Configura uno strumento di monitoraggio esterno

Passi

1. Configura le seguenti impostazioni sul tuo strumento di monitoraggio esterno, come Grafana.

- a. **Nome**: inserisci un nome per la connessione.

StorageGRID non richiede queste informazioni, ma è necessario fornire un nome per testare la connessione.

- b. **URL**: immettere il nome di dominio o l'indirizzo IP per il nodo di amministrazione. Specificare HTTPS e la porta 9091.

Ad esempio: `https://admin-node.example.com:9091`

- c. Abilita **TLS Client Auth** e **Con certificato CA**.
- d. In Dettagli autorizzazione TLS/SSL, copia e incolla: +

- Il certificato CA dell'interfaccia di gestione per **CA Cert**
- Il certificato client per **Client Cert**
- La chiave privata per **Chiave client**

e. **ServerName**: immettere il nome di dominio del nodo di amministrazione.

ServerName deve corrispondere al nome di dominio così come appare nel certificato dell'interfaccia di gestione.

2. Salvare e testare il certificato e la chiave privata copiati da StorageGRID o da un file locale.

Ora puoi accedere alle metriche Prometheus da StorageGRID con il tuo strumento di monitoraggio esterno.

Per informazioni sulle metriche, vedere ["istruzioni per il monitoraggio StorageGRID"](#) .

Modifica i certificati client

È possibile modificare un certificato client amministratore per cambiarne il nome, abilitare o disabilitare l'accesso a Prometheus o caricare un nuovo certificato quando quello attuale è scaduto.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Certificati** e quindi selezionare la scheda **Client**.

Nella tabella sono elencate le date di scadenza dei certificati e le autorizzazioni di accesso a Prometheus. Se un certificato sta per scadere o è già scaduto, nella tabella viene visualizzato un messaggio e viene attivato un avviso.

2. Seleziona il certificato che vuoi modificare.

3. Seleziona **Modifica** e poi seleziona **Modifica nome e autorizzazione**

4. Inserisci un nome per il certificato.

5. Per accedere alle metriche di Prometheus tramite il tuo strumento di monitoraggio esterno, seleziona **Consenti Prometheus**.

6. Selezionare **Continua** per salvare il certificato in Grid Manager.

Il certificato aggiornato viene visualizzato nella scheda Client.

Allega nuovo certificato client

È possibile caricare un nuovo certificato quando quello attuale è scaduto.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Certificati** e quindi selezionare la scheda **Client**.

Nella tabella sono elencate le date di scadenza dei certificati e le autorizzazioni di accesso a Prometheus. Se un certificato sta per scadere o è già scaduto, nella tabella viene visualizzato un messaggio e viene attivato un avviso.

2. Seleziona il certificato che vuoi modificare.

3. Selezionare **Modifica** e quindi selezionare un'opzione di modifica.

Carica il certificato

Copia il testo del certificato per incollarlo altrove.

- a. Selezionare **Carica certificato** e poi **Continua**.
- b. Carica il nome del certificato client(.pem).

Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.

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

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

Ad esempio: storagegrid_certificate.pem

- Selezionare **Copia certificato PEM** per copiare il contenuto del certificato e incollarlo altrove.
- c. Selezionare **Crea** per salvare il certificato in Grid Manager.

Il certificato aggiornato viene visualizzato nella scheda Client.

Genera certificato

Genera il testo del certificato da incollare altrove.

- a. Seleziona **Genera certificato**.
- b. Specificare le informazioni del certificato:

- **Oggetto** (facoltativo): soggetto X.509 o nome distinto (DN) del proprietario del certificato.
- **Giorni di validità**: numero di giorni di validità del certificato generato, a partire dal momento in cui viene generato.
- **Aggiungi estensioni per l'utilizzo delle chiavi**: se selezionato (impostazione predefinita e consigliata), le estensioni per l'utilizzo delle chiavi e l'utilizzo esteso delle chiavi vengono aggiunte al certificato generato.

Queste estensioni definiscono lo scopo della chiave contenuta nel certificato.



Lasciare selezionata questa casella di controllo a meno che non si riscontrino problemi di connessione con client più vecchi quando i certificati includono queste estensioni.

- c. Seleziona **Genera**.
- d. Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.



Dopo aver chiuso la finestra di dialogo, non sarà possibile visualizzare la chiave privata del certificato. Copia o scarica la chiave in un luogo sicuro.

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

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

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

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copia chiave privata** per copiare la chiave privata del certificato e incollarla altrove.
- Selezionare **Scarica chiave privata** per salvare la chiave privata come file.

Specificare il nome del file della chiave privata e il percorso di download.

e. Selezionare **Crea** per salvare il certificato in Grid Manager.

Il nuovo certificato viene visualizzato nella scheda Client.

Scarica o copia i certificati client

È possibile scaricare o copiare un certificato client per utilizzarlo altrove.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Certificati** e quindi selezionare la scheda **Client**.
2. Seleziona il certificato che vuoi copiare o scaricare.
3. Scarica o copia il certificato.

Scarica il file del certificato

Scarica il certificato `.pem` file.

- a. Seleziona **Scarica certificato**.
- b. Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

Copia il certificato

Copia il testo del certificato per incollarlo altrove.

- a. Selezionare **Copia certificato PEM**.
- b. Incolla il certificato copiato in un editor di testo.
- c. Salva il file di testo con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

Rimuovere i certificati client

Se non hai più bisogno di un certificato client amministratore, puoi rimuoverlo.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Certificati** e quindi selezionare la scheda **Client**.
2. Seleziona il certificato che desideri rimuovere.
3. Selezionare **Elimina** e quindi confermare.



Per rimuovere fino a 10 certificati, seleziona ciascun certificato da rimuovere nella scheda Client, quindi seleziona **Azioni > Elimina**.

Dopo la rimozione di un certificato, i client che lo utilizzavano devono specificare un nuovo certificato client per accedere al database StorageGRID Prometheus.

Configurare le impostazioni di sicurezza

Gestire la politica TLS e SSH

La policy TLS e SSH determina quali protocolli e cifrari vengono utilizzati per stabilire connessioni TLS sicure con le applicazioni client e connessioni SSH sicure con i servizi StorageGRID interni.

La policy di sicurezza controlla il modo in cui TLS e SSH crittografano i dati in movimento. In generale, utilizzare il criterio di compatibilità moderna (predefinito), a meno che il sistema non debba essere conforme ai Common Criteria o non sia necessario utilizzare altri cifrari.



Alcuni servizi StorageGRID non sono stati aggiornati per utilizzare le cifrature in queste policy.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Permesso di accesso root"](#) .

Seleziona una politica di sicurezza

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Impostazioni di sicurezza**.

La scheda **Criteri TLS e SSH** mostra i criteri disponibili. La policy attualmente attiva è contrassegnata da un segno di spunta verde nel riquadro della policy.



2. Esamina i riquadri per scoprire le policy disponibili.

Politica	Descrizione
Compatibilità moderna (predefinita)	Utilizzare il criterio predefinito se è necessaria una crittografia avanzata e a meno che non si abbiano requisiti particolari. Questa policy è compatibile con la maggior parte dei client TLS e SSH.
Compatibilità legacy	Utilizza questa policy se hai bisogno di opzioni di compatibilità aggiuntive per i client più vecchi. Le opzioni aggiuntive presenti in questa policy potrebbero renderla meno sicura rispetto alla policy di compatibilità moderna.
Criteri comuni	Utilizzare questa politica se è necessaria la certificazione Common Criteria.
FIPS rigoroso	Utilizzare questa policy se è richiesta la certificazione Common Criteria e si deve utilizzare NetApp Cryptographic Security Module 3.0.8 per le connessioni client esterne agli endpoint del bilanciatore del carico, Tenant Manager e Grid Manager. L'utilizzo di questa policy potrebbe ridurre le prestazioni. Nota: Dopo aver selezionato questa policy, tutti i nodi devono essere "riavviato in modo progressivo" per attivare il modulo di sicurezza crittografica NetApp . Utilizzare Manutenzione > Riavvio progressivo per avviare e monitorare i riavvii.
Costume	Crea una policy personalizzata se devi applicare i tuoi cifrari.

3. Per visualizzare i dettagli sui cifrari, i protocolli e gli algoritmi di ogni policy, seleziona **Visualizza dettagli**.

4. Per modificare la policy corrente, seleziona **Usa policy**.

Accanto a **Criterio attuale** nel riquadro del criterio appare un segno di spunta verde.

Crea una policy di sicurezza personalizzata

È possibile creare una policy personalizzata se è necessario applicare cifrari personalizzati.

Passi

1. Dal riquadro della policy più simile alla policy personalizzata che desideri creare, seleziona **Visualizza dettagli**.
2. Selezionare **Copia negli appunti**, quindi selezionare **Annulla**.



3. Dal riquadro **Criterio personalizzato**, seleziona **Configura e usa**.
4. Incolla il JSON che hai copiato e apporta le modifiche necessarie.
5. Seleziona **Utilizza policy**.

Accanto a **Criterio attuale** nel riquadro Criterio personalizzato appare un segno di spunta verde.

6. Facoltativamente, seleziona **Modifica configurazione** per apportare ulteriori modifiche alla nuova policy personalizzata.

Ripristina temporaneamente la politica di sicurezza predefinita

Se hai configurato un criterio di sicurezza personalizzato, potresti non essere in grado di accedere a Grid Manager se il criterio TLS configurato non è compatibile con ["certificato del server configurato"](#).

È possibile ripristinare temporaneamente i criteri di sicurezza predefiniti.

Passi

1. Accedi a un nodo di amministrazione:
 - a. Immettere il seguente comando: `ssh admin@Admin_Node_IP`
 - b. Inserisci la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla root: `su -`
 - d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$` a `#`.

2. Esegui il seguente comando:

```
restore-default-cipher-configurations
```

3. Da un browser Web, accedi a Grid Manager sullo stesso nodo di amministrazione.
4. Segui i passaggi in [Seleziona una politica di sicurezza](#) per configurare nuovamente la policy.

È possibile configurare la sicurezza di rete e degli oggetti per crittografare gli oggetti archiviati, per impedire determinate richieste S3 o per consentire alle connessioni client ai nodi di archiviazione di utilizzare HTTP anziché HTTPS.

Crittografia degli oggetti memorizzati

La crittografia degli oggetti archiviati consente la crittografia di tutti i dati degli oggetti quando vengono acquisiti tramite S3. Per impostazione predefinita, gli oggetti archiviati non sono crittografati, ma è possibile scegliere di crittografarli utilizzando l'algoritmo di crittografia AES-128 o AES-256. Quando si abilita l'impostazione, tutti gli oggetti appena acquisiti vengono crittografati, ma non viene apportata alcuna modifica agli oggetti archiviati esistenti. Se si disabilita la crittografia, gli oggetti attualmente crittografati rimangono crittografati, ma gli oggetti appena acquisiti non vengono crittografati.

L'impostazione di crittografia degli oggetti archiviati si applica solo agli oggetti S3 che non sono stati crittografati tramite crittografia a livello di bucket o di oggetto.

Per maggiori dettagli sui metodi di crittografia StorageGRID , vedere ["Esaminare i metodi di crittografia StorageGRID"](#) .

Impedisci la modifica del client

Impedisci modifiche al client è un'impostazione a livello di sistema. Quando è selezionata l'opzione **Impedisci modifiche client**, le seguenti richieste vengono rifiutate.

API REST S3

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

Abilita HTTP per le connessioni del nodo di archiviazione

Per impostazione predefinita, le applicazioni client utilizzano il protocollo di rete HTTPS per tutte le connessioni dirette ai nodi di archiviazione. Facoltativamente, è possibile abilitare HTTP per queste connessioni, ad esempio quando si testa una griglia non di produzione.

Utilizzare HTTP per le connessioni ai nodi di archiviazione solo se i client S3 devono effettuare connessioni HTTP direttamente ai nodi di archiviazione. Non è necessario utilizzare questa opzione per i client che utilizzano solo connessioni HTTPS o per i client che si connettono al servizio Load Balancer (perché è possibile ["configurare ogni endpoint del bilanciatore del carico"](#) per utilizzare HTTP o HTTPS).

Vedere ["Riepilogo: indirizzi IP e porte per le connessioni client"](#) per scoprire quali porte utilizzano i client S3 quando si connettono ai nodi di archiviazione tramite HTTP o HTTPS.

Seleziona le opzioni

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Hai i permessi di accesso Root.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Impostazioni di sicurezza**.
2. Selezionare la scheda **Rete e oggetti**.
3. Per la crittografia degli oggetti archiviati, utilizzare l'impostazione **Nessuno** (predefinita) se non si desidera che gli oggetti archiviati vengano crittografati oppure selezionare **AES-128** o **AES-256** per crittografare gli oggetti archiviati.
4. Facoltativamente, seleziona **Impedisci modifica client** se vuoi impedire ai client S3 di effettuare richieste specifiche.



Se si modifica questa impostazione, ci vorrà circa un minuto prima che la nuova impostazione venga applicata. Il valore configurato viene memorizzato nella cache per migliorare le prestazioni e il ridimensionamento.

5. Facoltativamente, selezionare **Abilita HTTP per le connessioni ai nodi di archiviazione** se i client si connettono direttamente ai nodi di archiviazione e si desidera utilizzare le connessioni HTTP.



Prestare attenzione quando si abilita HTTP per una griglia di produzione perché le richieste verranno inviate non crittografate.

6. Seleziona **Salva**.

Modificare le impostazioni di sicurezza dell'interfaccia

Le impostazioni di sicurezza dell'interfaccia consentono di controllare se gli utenti vengono disconnessi se rimangono inattivi per un periodo di tempo superiore a quello specificato e se una traccia dello stack viene inclusa nelle risposte di errore dell'API.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai ["Permesso di accesso root"](#).

Informazioni su questo compito

La pagina **Impostazioni di sicurezza** include le impostazioni **Timeout di inattività del browser** e **Stack trace dell'API di gestione**.

Timeout di inattività del browser

Indica per quanto tempo il browser di un utente può rimanere inattivo prima che l'utente venga disconnesso. Il valore predefinito è 15 minuti.

Il timeout di inattività del browser è controllato anche da quanto segue:

- Un timer StorageGRID separato e non configurabile, incluso per la sicurezza del sistema. Il token di autenticazione di ciascun utente scade 16 ore dopo l'accesso dell'utente. Quando scade l'autenticazione di un utente, l'utente viene automaticamente disconnesso, anche se il timeout di inattività del browser è disabilitato o il valore per il timeout del browser non è stato raggiunto. Per rinnovare il token, l'utente deve effettuare nuovamente l'accesso.
- Impostazioni di timeout per il provider di identità, presupponendo che l'accesso Single Sign-On (SSO) sia abilitato per StorageGRID.

Se l'SSO è abilitato e il browser di un utente scade, l'utente deve reinserire le proprie credenziali SSO per accedere nuovamente a StorageGRID. Vedere ["Configurare l'accesso singolo"](#).

Stack trace dell'API di gestione

Controlla se viene restituita una traccia dello stack nelle risposte di errore dell'API Grid Manager e Tenant Manager.

Questa opzione è disabilitata per impostazione predefinita, ma potrebbe essere opportuno abilitare questa funzionalità per un ambiente di prova. In generale, negli ambienti di produzione è consigliabile lasciare la traccia dello stack disabilitata per evitare di rivelare dettagli software interni quando si verificano errori API.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Impostazioni di sicurezza**.
2. Selezionare la scheda **Interfaccia**.
3. Per modificare l'impostazione del timeout di inattività del browser:
 - a. Espandi la fisarmonica.
 - b. Per modificare il periodo di timeout, specificare un valore compreso tra 60 secondi e 7 giorni. Il timeout predefinito è 15 minuti.
 - c. Per disattivare questa funzione, deselezionare la casella di controllo.
 - d. Seleziona **Salva**.

La nuova impostazione non ha effetto sugli utenti che hanno effettuato l'accesso. Gli utenti devono effettuare nuovamente l'accesso o aggiornare il browser affinché la nuova impostazione di timeout abbia effetto.

4. Per modificare l'impostazione per la traccia dello stack dell'API di gestione:
 - a. Espandi la fisarmonica.
 - b. Selezionare la casella di controllo per restituire una traccia dello stack nelle risposte di errore dell'API Grid Manager e Tenant Manager.



Lasciare la traccia dello stack disabilitata negli ambienti di produzione per evitare di rivelare dettagli software interni quando si verificano errori API.

- c. Seleziona **Salva**.

Configurare i server di gestione delle chiavi

Che cos'è un server di gestione delle chiavi (KMS)?

Un server di gestione delle chiavi (KMS) è un sistema esterno di terze parti che fornisce chiavi di crittografia ai nodi dell'appliance StorageGRID nel sito StorageGRID associato utilizzando il protocollo KMIP (Key Management Interoperability Protocol).

StorageGRID supporta solo determinati server di gestione delle chiavi. Per un elenco dei prodotti e delle versioni supportati, utilizzare ["Strumento matrice di interoperabilità NetApp \(IMT\)"](#).

È possibile utilizzare uno o più server di gestione delle chiavi per gestire le chiavi di crittografia dei nodi per tutti i nodi dell'appliance StorageGRID in cui è abilitata l'impostazione **Crittografia nodi** durante l'installazione. Utilizzando server di gestione delle chiavi con questi nodi appliance è possibile proteggere i dati anche se un'appliance viene rimossa dal data center. Dopo aver crittografato i volumi dell'appliance, non sarà possibile accedere ai dati sull'appliance a meno che il nodo non sia in grado di comunicare con il KMS.



StorageGRID non crea né gestisce le chiavi esterne utilizzate per crittografare e decrittografare i nodi dell'appliance. Se si prevede di utilizzare un server di gestione delle chiavi esterno per proteggere i dati StorageGRID, è necessario comprendere come configurare tale server e come gestire le chiavi di crittografia. L'esecuzione di attività di gestione chiave esula dallo scopo di queste istruzioni. Se hai bisogno di aiuto, consulta la documentazione del tuo server di gestione delle chiavi o contatta l'assistenza tecnica.

Configurazione KMS e appliance

Prima di poter utilizzare un server di gestione delle chiavi (KMS) per proteggere i dati StorageGRID sui nodi dell'appliance, è necessario completare due attività di configurazione: impostare uno o più server KMS e abilitare la crittografia dei nodi per i nodi dell'appliance. Una volta completate queste due attività di configurazione, il processo di gestione delle chiavi avviene automaticamente.

Il diagramma di flusso mostra i passaggi principali per utilizzare un KMS per proteggere i dati StorageGRID sui nodi dell'appliance.

Il diagramma di flusso mostra la configurazione di KMS e la configurazione dell'appliance che avvengono in parallelo; tuttavia, è possibile configurare i server di gestione delle chiavi prima o dopo aver abilitato la crittografia dei nodi per i nuovi nodi dell'appliance, in base alle proprie esigenze.

Configurare il server di gestione delle chiavi (KMS)

La configurazione di un server di gestione delle chiavi comprende i seguenti passaggi generali.

Fare un passo	Fare riferimento a
Accedi al software KMS e aggiungi un client per StorageGRID a ciascun KMS o cluster KMS.	"Configurare StorageGRID come client nel KMS"
Ottenere le informazioni richieste per il client StorageGRID sul KMS.	"Configurare StorageGRID come client nel KMS"
Aggiungere il KMS a Grid Manager, assegnarlo a un singolo sito o a un gruppo predefinito di siti, caricare i certificati richiesti e salvare la configurazione del KMS.	"Aggiungere un server di gestione delle chiavi (KMS)"

Impostare l'apparecchio

La configurazione di un nodo appliance per l'utilizzo KMS include i seguenti passaggi generali.

1. Durante la fase di configurazione hardware dell'installazione dell'appliance, utilizzare StorageGRID Appliance Installer per abilitare l'impostazione **Crittografia nodo** per l'appliance.



Non è possibile abilitare l'impostazione **Crittografia nodo** dopo aver aggiunto un'appliance alla griglia e non è possibile utilizzare la gestione delle chiavi esterne per le appliance che non hanno la crittografia nodo abilitata.

2. Eseguire il programma di installazione dell'appliance StorageGRID . Durante l'installazione, a ciascun volume dell'appliance viene assegnata una chiave di crittografia dati casuale (DEK), come segue:
 - Le DEK vengono utilizzate per crittografare i dati su ciascun volume. Queste chiavi vengono generate utilizzando la crittografia del disco Linux Unified Key Setup (LUKS) nel sistema operativo dell'appliance e non possono essere modificate.
 - Ogni singolo DEK è crittografato da una chiave di crittografia a chiave master (KEK). La KEK iniziale è una chiave temporanea che crittografa le DEK finché l'appliance non riesce a connettersi al KMS.
3. Aggiungere il nodo dell'appliance a StorageGRID.

Vedere ["Abilita la crittografia del nodo"](#) per i dettagli.

Processo di crittografia della gestione delle chiavi (avviene automaticamente)

La crittografia della gestione delle chiavi include i seguenti passaggi di alto livello che vengono eseguiti automaticamente.

1. Quando si installa un'appliance con crittografia dei nodi abilitata nella griglia, StorageGRID determina se esiste una configurazione KMS per il sito che contiene il nuovo nodo.
 - Se per il sito è già stato configurato un KMS, l'appliance riceve la configurazione KMS.
 - Se non è ancora stato configurato un KMS per il sito, i dati sull'appliance continuano a essere crittografati dalla KEK temporanea finché non si configura un KMS per il sito e l'appliance non riceve la configurazione KMS.
2. L'appliance utilizza la configurazione KMS per connettersi al KMS e richiedere una chiave di crittografia.
3. Il KMS invia una chiave di crittografia all'appliance. La nuova chiave del KMS sostituisce la KEK temporanea e ora viene utilizzata per crittografare e decrittografare le DEK per i volumi dell'appliance.



Tutti i dati esistenti prima che il nodo dell'appliance crittografata si connetta al KMS configurato vengono crittografati con una chiave temporanea. Tuttavia, i volumi dell'appliance non devono essere considerati protetti dalla rimozione dal data center finché la chiave temporanea non viene sostituita dalla chiave di crittografia KMS.

4. Se l'appliance viene accesa o riavviata, si riconnette al KMS per richiedere la chiave. La chiave, che viene salvata nella memoria volatile, non può sopravvivere a un'interruzione di corrente o a un riavvio.

Considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi

Prima di configurare un server di gestione delle chiavi esterno (KMS), è necessario comprendere le considerazioni e i requisiti.

Quale versione di KMIP è supportata?

StorageGRID supporta KMIP versione 1.4.

["Specifiche del protocollo di interoperabilità per la gestione delle chiavi versione 1.4"](#)

Quali sono le considerazioni da fare in merito alla rete?

Le impostazioni del firewall di rete devono consentire a ciascun nodo dell'appliance di comunicare tramite la porta utilizzata per le comunicazioni KMIP (Key Management Interoperability Protocol). La porta KMIP predefinita è 5696.

È necessario assicurarsi che ogni nodo dell'appliance che utilizza la crittografia dei nodi abbia accesso alla rete del KMS o del cluster KMS configurato per il sito.

Quali versioni di TLS sono supportate?

Le comunicazioni tra i nodi dell'appliance e il KMS configurato utilizzano connessioni TLS sicure. StorageGRID può supportare il protocollo TLS 1.2 o TLS 1.3 quando effettua connessioni KMIP a un KMS o a un cluster KMS, in base a ciò che il KMS supporta e a quale ["Politica TLS e SSH"](#) che stai utilizzando.

StorageGRID negozia il protocollo e la crittografia (TLS 1.2) o la suite di crittografia (TLS 1.3) con il KMS quando effettua la connessione. Per vedere quali versioni del protocollo e cifrari/suite di cifrari sono disponibili, rivedere `tlsOutbound` sezione della policy TLS e SSH attiva della griglia (**CONFIGURAZIONE > Sicurezza Impostazioni di sicurezza**).

Quali elettrodomestici sono supportati?

È possibile utilizzare un server di gestione delle chiavi (KMS) per gestire le chiavi di crittografia per qualsiasi appliance StorageGRID nella griglia in cui sia abilitata l'impostazione **Crittografia nodo**. Questa impostazione può essere abilitata solo durante la fase di configurazione hardware dell'installazione dell'appliance tramite StorageGRID Appliance Installer.



Non è possibile abilitare la crittografia dei nodi dopo aver aggiunto un'appliance alla griglia e non è possibile utilizzare la gestione delle chiavi esterne per le appliance che non hanno la crittografia dei nodi abilitata.

È possibile utilizzare il KMS configurato per appliance StorageGRID e nodi appliance.

Non è possibile utilizzare il KMS configurato per i nodi basati su software (non appliance), inclusi i seguenti:

- Nodi distribuiti come macchine virtuali (VM)
- Nodi distribuiti all'interno di motori di container su host Linux

I nodi distribuiti su queste altre piattaforme possono utilizzare la crittografia al di fuori di StorageGRID a livello di datastore o disco.

Quando dovrei configurare i server di gestione delle chiavi?

Per una nuova installazione, in genere è necessario configurare uno o più server di gestione delle chiavi in Grid Manager prima di creare i tenant. Questo ordine garantisce che i nodi siano protetti prima che i dati degli oggetti vengano memorizzati su di essi.

È possibile configurare i server di gestione delle chiavi in Grid Manager prima o dopo aver installato i nodi dell'appliance.

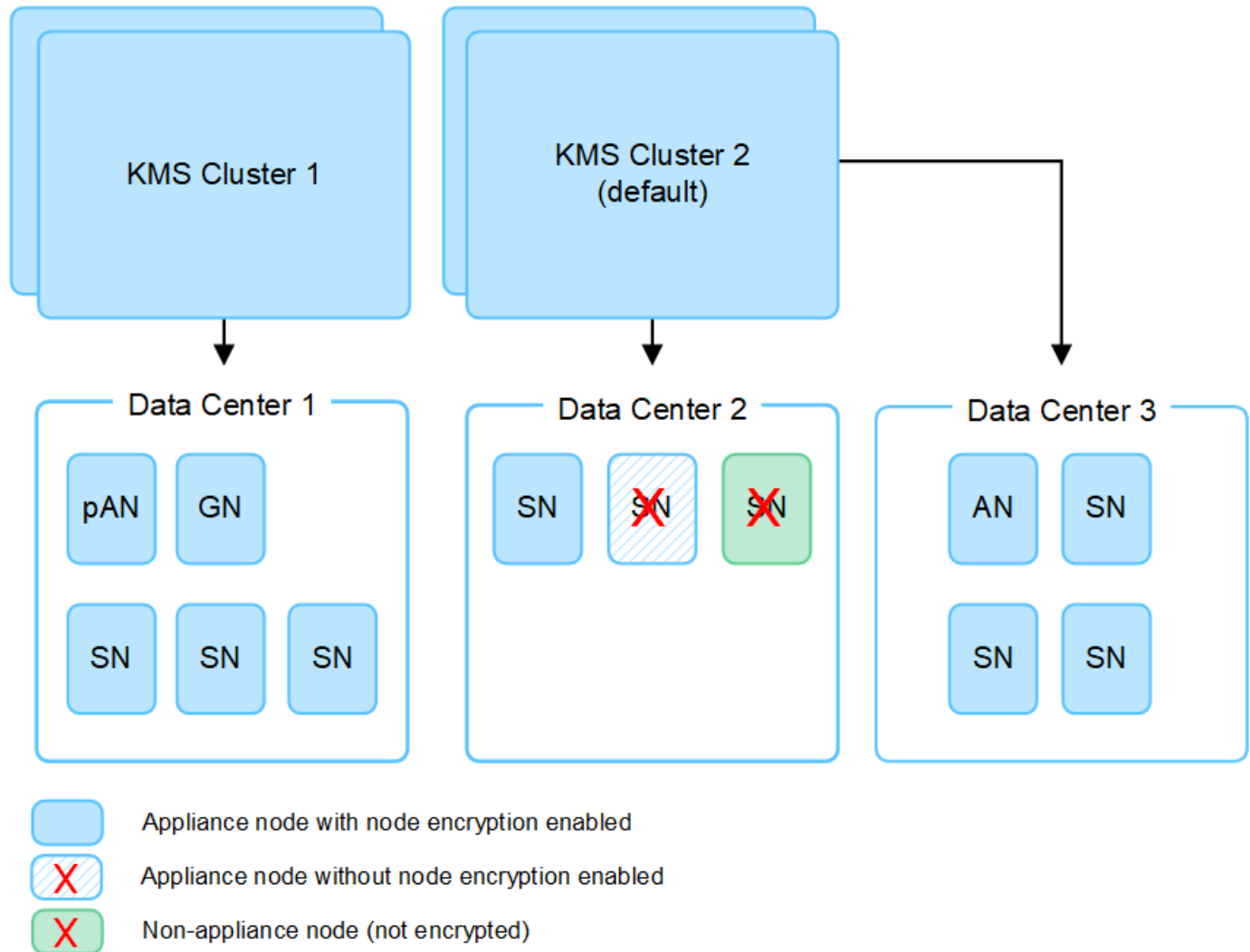
Di quanti server di gestione delle chiavi ho bisogno?

È possibile configurare uno o più server di gestione delle chiavi esterni per fornire chiavi di crittografia ai nodi dell'appliance nel sistema StorageGRID. Ogni KMS fornisce una singola chiave di crittografia ai nodi dell'appliance StorageGRID in un singolo sito o in un gruppo di siti.

StorageGRID supporta l'uso di cluster KMS. Ogni cluster KMS contiene più server di gestione delle chiavi replicati che condividono impostazioni di configurazione e chiavi di crittografia. Si consiglia di utilizzare cluster KMS per la gestione delle chiavi perché migliorano le capacità di failover di una configurazione ad alta disponibilità.

Ad esempio, supponiamo che il tuo sistema StorageGRID abbia tre siti di data center. È possibile configurare un cluster KMS per fornire una chiave a tutti i nodi dell'appliance nel Data Center 1 e un secondo cluster KMS per fornire una chiave a tutti i nodi dell'appliance in tutti gli altri siti. Quando si aggiunge il secondo cluster KMS, è possibile configurare un KMS predefinito per Data Center 2 e Data Center 3.

Tieni presente che non puoi utilizzare un KMS per nodi non appliance o per nodi appliance per i quali non è stata abilitata l'impostazione **Crittografia nodo** durante l'installazione.



Cosa succede quando si ruota una chiave?

Come buona pratica di sicurezza, dovresti periodicamente ["ruotare la chiave di crittografia"](#) utilizzato da ciascun KMS configurato.

Quando sarà disponibile la nuova versione della chiave:

- Viene distribuito automaticamente ai nodi dell'appliance crittografata nel sito o nei siti associati al KMS. La distribuzione dovrebbe avvenire entro un'ora dalla rotazione della chiave.
- Se il nodo dell'appliance crittografata è offline quando viene distribuita la nuova versione della chiave, il nodo riceverà la nuova chiave non appena si riavvia.
- Se per qualsiasi motivo non è possibile utilizzare la nuova versione della chiave per crittografare i volumi dell'appliance, viene attivato l'avviso **Rotazione chiave di crittografia KMS non riuscita** per il nodo

dell'appliance. Potrebbe essere necessario contattare l'assistenza tecnica per ricevere aiuto nella risoluzione di questo avviso.

Posso riutilizzare un nodo appliance dopo averlo crittografato?

Se è necessario installare un'appliance crittografata in un altro sistema StorageGRID, è necessario prima disattivare il nodo della griglia per spostare i dati dell'oggetto su un altro nodo. Quindi, è possibile utilizzare StorageGRID Appliance Installer per ["cancellare la configurazione KMS"](#). La cancellazione della configurazione KMS disabilita l'impostazione **Crittografia nodo** e rimuove l'associazione tra il nodo dell'appliance e la configurazione KMS per il sito StorageGRID.



Senza accesso alla chiave di crittografia KMS, tutti i dati rimasti sul dispositivo non saranno più accessibili e saranno bloccati in modo permanente.

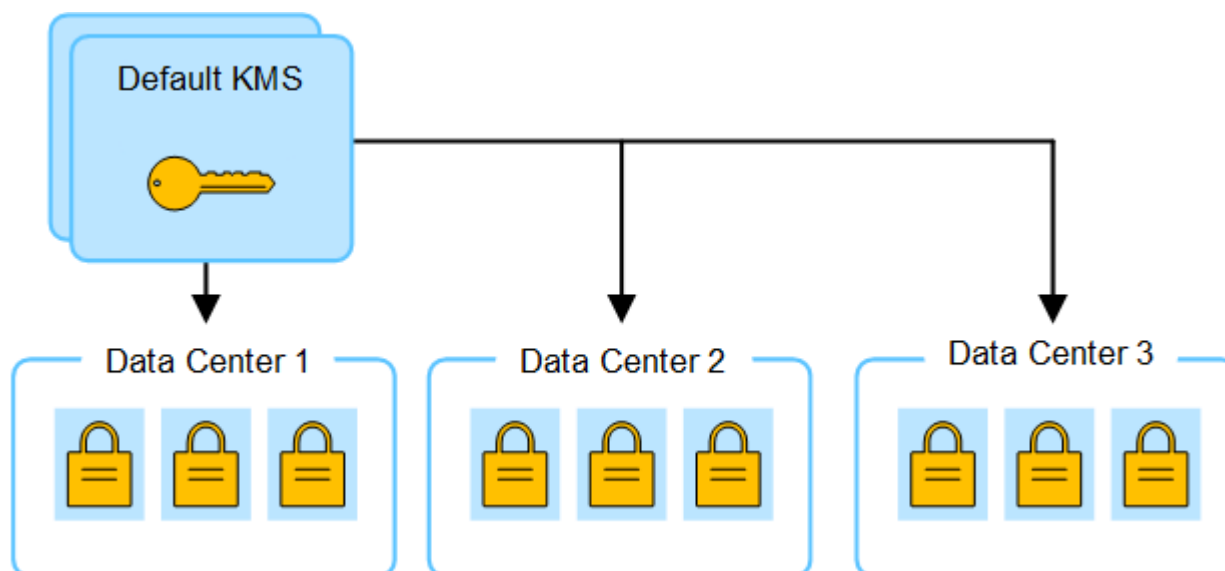
Considerazioni sulla modifica del KMS per un sito

Ogni server di gestione delle chiavi (KMS) o cluster KMS fornisce una chiave di crittografia a tutti i nodi dell'appliance in un singolo sito o in un gruppo di siti. Se è necessario modificare il KMS utilizzato per un sito, potrebbe essere necessario copiare la chiave di crittografia da un KMS a un altro.

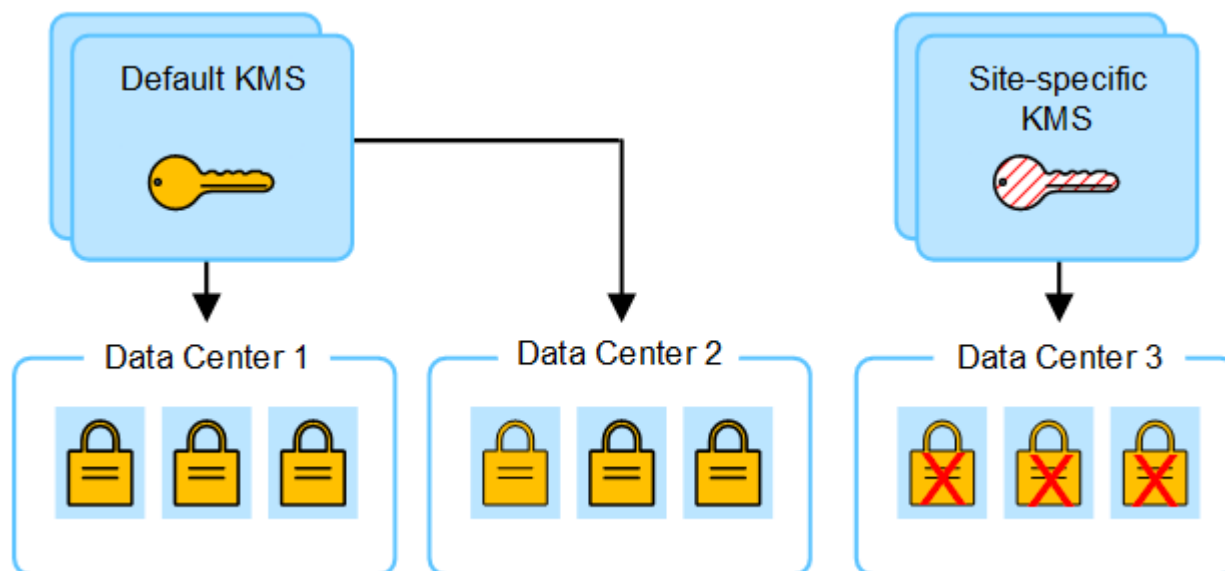
Se si modifica il KMS utilizzato per un sito, è necessario assicurarsi che i nodi dell'appliance precedentemente crittografati in quel sito possano essere decrittografati utilizzando la chiave memorizzata sul nuovo KMS. In alcuni casi, potrebbe essere necessario copiare la versione corrente della chiave di crittografia dal KMS originale al nuovo KMS. È necessario assicurarsi che il KMS disponga della chiave corretta per decrittografare i nodi dell'appliance crittografati nel sito.

Per esempio:

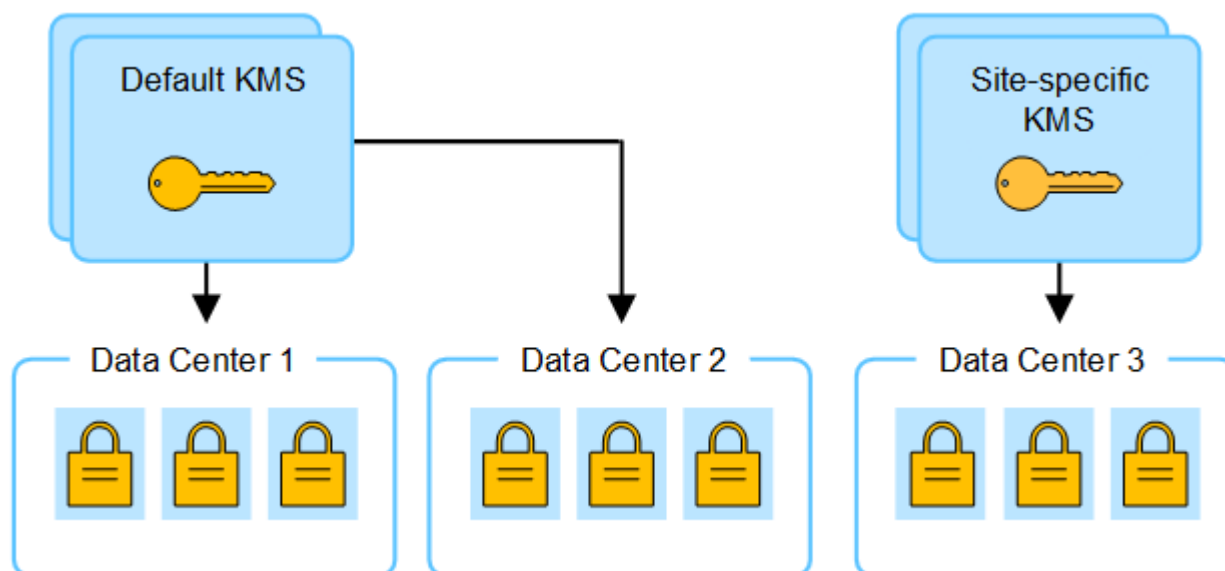
1. Inizialmente si configura un KMS predefinito che si applica a tutti i siti che non dispongono di un KMS dedicato.
2. Una volta salvato il KMS, tutti i nodi dell'appliance in cui è abilitata l'impostazione **Crittografia nodo** si connettono al KMS e richiedono la chiave di crittografia. Questa chiave viene utilizzata per crittografare i nodi dell'appliance in tutti i siti. La stessa chiave deve essere utilizzata anche per decifrare tali apparecchi.



3. Si decide di aggiungere un KMS specifico per un sito (Data Center 3 nella figura). Tuttavia, poiché i nodi dell'appliance sono già crittografati, si verifica un errore di convalida quando si tenta di salvare la configurazione per il KMS specifico del sito. L'errore si verifica perché il KMS specifico del sito non dispone della chiave corretta per decrittografare i nodi in quel sito.



4. Per risolvere il problema, copiare la versione corrente della chiave di crittografia dal KMS predefinito al nuovo KMS. (Tecnicamente, si copia la chiave originale in una nuova chiave con lo stesso alias. (La chiave originale diventa una versione precedente della nuova chiave.) Il KMS specifico del sito ora dispone della chiave corretta per decrittografare i nodi dell'appliance nel Data Center 3, in modo che possa essere salvata in StorageGRID.



Casi d'uso per modificare il KMS utilizzato per un sito

La tabella riassume i passaggi richiesti nei casi più comuni di modifica del KMS per un sito.

Caso d'uso per la modifica del KMS di un sito	Passaggi richiesti
Hai una o più voci KMS specifiche del sito e vuoi usarne una come KMS predefinito.	Modifica il KMS specifico del sito. Nel campo Gestisci chiavi per , seleziona Siti non gestiti da un altro KMS (KMS predefinito) . Il KMS specifico del sito verrà ora utilizzato come KMS predefinito. Si applicherà a tutti i siti che non dispongono di un KMS dedicato. "Modifica un server di gestione delle chiavi (KMS)"
Hai un KMS predefinito e aggiungi un nuovo sito in un'espansione. Non vuoi utilizzare il KMS predefinito per il nuovo sito.	1. Se i nodi dell'appliance nel nuovo sito sono già stati crittografati dal KMS predefinito, utilizzare il software KMS per copiare la versione corrente della chiave di crittografia dal KMS predefinito a un nuovo KMS. 2. Utilizzando Grid Manager, aggiungi il nuovo KMS e seleziona il sito. "Aggiungere un server di gestione delle chiavi (KMS)"
Si desidera che il KMS di un sito utilizzi un server diverso.	1. Se i nodi dell'appliance nel sito sono già stati crittografati dal KMS esistente, utilizzare il software KMS per copiare la versione corrente della chiave di crittografia dal KMS esistente al nuovo KMS. 2. Utilizzando Grid Manager, modifica la configurazione KMS esistente e inserisci il nuovo nome host o indirizzo IP. "Aggiungere un server di gestione delle chiavi (KMS)"

Configurare StorageGRID come client nel KMS

È necessario configurare StorageGRID come client per ciascun server di gestione delle chiavi esterno o cluster KMS prima di poter aggiungere il KMS a StorageGRID.



Queste istruzioni si applicano a Thales CipherTrust Manager e Hashicorp Vault. Per un elenco dei prodotti e delle versioni supportati, utilizzare ["Strumento matrice di interoperabilità NetApp \(IMT\)"](#).

Passi

1. Dal software KMS, crea un client StorageGRID per ogni KMS o cluster KMS che intendi utilizzare.

Ogni KMS gestisce una singola chiave di crittografia per i nodi degli appliance StorageGRID in un singolo sito o in un gruppo di siti.

2. Crea una chiave utilizzando uno dei due metodi seguenti:
 - Utilizzare la pagina di gestione delle chiavi del prodotto KMS. Creare una chiave di crittografia AES per ogni KMS o cluster KMS.

La chiave di crittografia deve essere pari o superiore a 2.048 bit e deve essere esportabile.

- Chiedi a StorageGRID di creare la chiave. Ti verrà chiesto quando esegui il test e salvi dopo ["caricamento dei certificati client"](#).
3. Registrare le seguenti informazioni per ciascun KMS o cluster KMS.

Quando aggiungi il KMS a StorageGRID, hai bisogno di queste informazioni:

- Nome host o indirizzo IP per ciascun server.
 - Porta KMIP utilizzata dal KMS.
 - Alias della chiave per la chiave di crittografia nel KMS.
4. Per ogni KMS o cluster KMS, ottenere un certificato server firmato da un'autorità di certificazione (CA) o un bundle di certificati che contenga ciascuno dei file di certificato CA codificati in PEM, concatenati nell'ordine della catena di certificati.

Il certificato del server consente al KMS esterno di autenticarsi su StorageGRID.

- Il certificato deve utilizzare il formato X.509 codificato Base-64 Privacy Enhanced Mail (PEM).
- Il campo Subject Alternative Name (SAN) in ciascun certificato del server deve includere il nome di dominio completo (FQDN) o l'indirizzo IP a cui StorageGRID si conatterà.



Quando si configura il KMS in StorageGRID, è necessario immettere gli stessi FQDN o indirizzi IP nel campo **Nome host**.

- Il certificato del server deve corrispondere al certificato utilizzato dall'interfaccia KMIP del KMS, che in genere utilizza la porta 5696.
5. Ottenere il certificato client pubblico rilasciato a StorageGRID dal KMS esterno e la chiave privata per il certificato client.

Il certificato client consente a StorageGRID di autenticarsi al KMS.

Aggiungere un server di gestione delle chiavi (KMS)

Per aggiungere ciascun KMS o cluster KMS, utilizzare la procedura guidata StorageGRID Key Management Server.

Prima di iniziare

- Hai esaminato il "[considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi](#)".
- Hai "[StorageGRID configurato come client nel KMS](#)" e disponi delle informazioni richieste per ciascun KMS o cluster KMS.
- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Tu hai il "[Permesso di accesso root](#)".

Informazioni su questo compito

Se possibile, configurare eventuali server di gestione delle chiavi specifici del sito prima di configurare un KMS predefinito che si applichi a tutti i siti non gestiti da un altro KMS. Se si crea prima il KMS predefinito, tutti gli apparecchi crittografati tramite nodo nella griglia verranno crittografati dal KMS predefinito. Se in un secondo momento si desidera creare un KMS specifico per il sito, è necessario prima copiare la versione corrente della chiave di crittografia dal KMS predefinito al nuovo KMS. Vedere "[Considerazioni sulla modifica del KMS per un sito](#)" per i dettagli.

Passaggio 1: dettagli KMS

Nel passaggio 1 (dettagli KMS) della procedura guidata Aggiungi un server di gestione delle chiavi, è necessario fornire dettagli sul KMS o sul cluster KMS.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Server di gestione delle chiavi**.

Viene visualizzata la pagina del server di gestione delle chiavi con la scheda Dettagli configurazione selezionata.

2. Seleziona **Crea**.

Viene visualizzato il passaggio 1 (dettagli KMS) della procedura guidata Aggiungi un server di gestione delle chiavi.

3. Immettere le seguenti informazioni per il KMS e il client StorageGRID configurato in tale KMS.

Campo	Descrizione
Nome KMS	Un nome descrittivo che ti aiuti a identificare questo KMS. Deve contenere tra 1 e 64 caratteri.
Nome chiave	L'alias chiave esatto per il client StorageGRID nel KMS. Deve contenere tra 1 e 255 caratteri. Nota: se non hai creato una chiave utilizzando il tuo prodotto KMS, ti verrà chiesto di farla creare a StorageGRID .
Gestisce le chiavi per	Il sito StorageGRID che sarà associato a questo KMS. Se possibile, è opportuno configurare eventuali server di gestione delle chiavi specifici del sito prima di configurare un KMS predefinito che si applichi a tutti i siti non gestiti da un altro KMS. • Selezionare un sito se questo KMS gestirà le chiavi di crittografia per i nodi dell'appliance in un sito specifico. • Seleziona Siti non gestiti da un altro KMS (KMS predefinito) per configurare un KMS predefinito che verrà applicato a tutti i siti che non dispongono di un KMS dedicato e a tutti i siti aggiunti nelle espansioni successive. Nota: si verificherà un errore di convalida quando si salva la configurazione KMS se si seleziona un sito precedentemente crittografato dal KMS predefinito ma non è stata fornita la versione corrente della chiave di crittografia originale al nuovo KMS.
Porta	La porta utilizzata dal server KMS per le comunicazioni KMIP (Key Management Interoperability Protocol). Il valore predefinito è 5696, che è la porta standard KMIP.

Campo	Descrizione
Nome host	Il nome di dominio completo o l'indirizzo IP per il KMS. Nota: il campo Subject Alternative Name (SAN) del certificato del server deve includere l'FQDN o l'indirizzo IP immesso qui. In caso contrario, StorageGRID non sarà in grado di connettersi al KMS o a tutti i server in un cluster KMS.

- Se si sta configurando un cluster KMS, selezionare **Aggiungi un altro nome host** per aggiungere un nome host per ciascun server nel cluster.
- Selezionare **Continua**.

Passaggio 2: carica il certificato del server

Nel passaggio 2 (Carica certificato server) della procedura guidata Aggiungi un server di gestione delle chiavi, caricare il certificato server (o il pacchetto di certificati) per il KMS. Il certificato del server consente al KMS esterno di autenticarsi su StorageGRID.

Passi

- Dal **Passaggio 2 (Carica certificato server)**, vai alla posizione del certificato server salvato o del pacchetto di certificati.
- Carica il file del certificato.

Vengono visualizzati i metadati del certificato del server.



Se hai caricato un pacchetto di certificati, i metadati di ciascun certificato vengono visualizzati in una scheda separata.

- Selezionare **Continua**.

Passaggio 3: Carica i certificati client

Nel passaggio 3 (Caricamento dei certificati client) della procedura guidata Aggiungi un server di gestione delle chiavi, caricare il certificato client e la chiave privata del certificato client. Il certificato client consente a StorageGRID di autenticarsi presso il KMS.

Passi

- Dal **Passaggio 3 (Caricamento certificati client)**, accedere alla posizione del certificato client.
- Carica il file del certificato client.

Vengono visualizzati i metadati del certificato client.

- Passare alla posizione della chiave privata per il certificato client.
- Carica il file della chiave privata.
- Seleziona **Test e salva**.

Se non esiste una chiave, verrà richiesto a StorageGRID di crearne una.

Vengono testate le connessioni tra il server di gestione delle chiavi e i nodi dell'appliance. Se tutte le connessioni sono valide e la chiave corretta viene trovata sul KMS, il nuovo server di gestione delle chiavi

viene aggiunto alla tabella nella pagina Server di gestione delle chiavi.



Subito dopo aver aggiunto un KMS, lo stato del certificato nella pagina Key Management Server appare come Sconosciuto. StorageGRID potrebbe impiegare fino a 30 minuti per ottenere lo stato effettivo di ciascun certificato. Per visualizzare lo stato attuale, è necessario aggiornare il browser web.

6. Se viene visualizzato un messaggio di errore quando si seleziona **Test e salva**, rivedere i dettagli del messaggio e quindi selezionare **OK**.

Ad esempio, potresti ricevere un errore 422: Entità non elaborabile se un test di connessione non riesce.

7. Se è necessario salvare la configurazione corrente senza testare la connessione esterna, selezionare **Forza salvataggio**.



Selezionando **Forza salvataggio** la configurazione KMS viene salvata, ma non viene testata la connessione esterna da ciascun dispositivo a quel KMS. Se si verifica un problema con la configurazione, potrebbe non essere possibile riavviare i nodi dell'appliance in cui è abilitata la crittografia dei nodi nel sito interessato. Potresti perdere l'accesso ai tuoi dati finché i problemi non saranno risolti.

8. Rivedi l'avviso di conferma e seleziona **OK** se sei sicuro di voler forzare il salvataggio della configurazione.

La configurazione KMS viene salvata ma la connessione al KMS non viene testata.

Gestire un KMS

La gestione di un server di gestione delle chiavi (KMS) implica la visualizzazione o la modifica dei dettagli, la gestione dei certificati, la visualizzazione dei nodi crittografati e la rimozione di un KMS quando non è più necessario.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Tu hai il "[autorizzazione di accesso richiesta](#)".

Visualizza i dettagli KMS

È possibile visualizzare informazioni su ciascun server di gestione delle chiavi (KMS) nel sistema StorageGRID, inclusi i dettagli delle chiavi e lo stato corrente dei certificati del server e del client.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Server di gestione delle chiavi**.

Viene visualizzata la pagina del server di gestione delle chiavi, che mostra le seguenti informazioni:

- Nella scheda Dettagli configurazione sono elencati tutti i server di gestione delle chiavi configurati.
- Nella scheda Nodi crittografati sono elencati tutti i nodi in cui è abilitata la crittografia dei nodi.

2. Per visualizzare i dettagli di un KMS specifico ed eseguire operazioni su tale KMS, selezionare il nome del KMS. Nella pagina dei dettagli del KMS sono elencate le seguenti informazioni:

Campo	Descrizione
Gestisce le chiavi per	Il sito StorageGRID associato al KMS. Questo campo visualizza il nome di un sito StorageGRID specifico o Siti non gestiti da un altro KMS (KMS predefinito).
Nome host	Il nome di dominio completo o l'indirizzo IP del KMS. Se è presente un cluster di due server di gestione delle chiavi, vengono elencati il nome di dominio completo o l'indirizzo IP di entrambi i server. Se in un cluster sono presenti più di due server di gestione delle chiavi, viene elencato il nome di dominio completo o l'indirizzo IP del primo KMS, insieme al numero di server di gestione delle chiavi aggiuntivi nel cluster. Per esempio: 10.10.10.10 and 10.10.10.11 O 10.10.10.10 and 2 others . Per visualizzare tutti i nomi host in un cluster, selezionare un KMS e selezionare Modifica o Azioni > Modifica.

3. Selezionare una scheda nella pagina dei dettagli KMS per visualizzare le seguenti informazioni:

Scheda	Campo	Descrizione
Dettagli chiave	Nome chiave	L'alias chiave per il client StorageGRID nel KMS.
UID chiave	L'identificatore univoco dell'ultima versione della chiave.	Ultima modifica
Data e ora dell'ultima versione della chiave.	Certificato del server	Metadati
I metadati del certificato, come il numero di serie, la data e l'ora di scadenza e il PEM del certificato.	Certificato PEM	Il contenuto del file PEM (privacy enhanced mail) per il certificato.
Certificato cliente	Metadati	I metadati del certificato, come il numero di serie, la data e l'ora di scadenza e il PEM del certificato.

4. Seleziona **Ruota chiave** o utilizza il software KMS ogni volta che le pratiche di sicurezza della tua organizzazione lo richiedono, per creare una nuova versione della chiave.

Quando la rotazione della chiave ha esito positivo, i campi UID chiave e Ultima modifica vengono aggiornati.

Se si ruota la chiave di crittografia utilizzando il software KMS, ruotarla dall'ultima versione utilizzata della chiave a una nuova versione della stessa chiave. Non ruotare su una tonalità completamente diversa.



Non tentare mai di ruotare una chiave modificando il nome della chiave (alias) per il KMS. StorageGRID richiede che tutte le versioni delle chiavi utilizzate in precedenza (così come quelle future) siano accessibili dal KMS con lo stesso alias della chiave. Se modifichi l'alias della chiave per un KMS configurato, StorageGRID potrebbe non essere in grado di decrittografare i dati.

Gestisci i certificati

Risolvere tempestivamente eventuali problemi relativi ai certificati del server o del client. Se possibile, sostituire i certificati prima che scadano.



Per mantenere l'accesso ai dati, è necessario risolvere il prima possibile eventuali problemi relativi ai certificati.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Server di gestione delle chiavi**.
2. Nella tabella, osserva il valore della Scadenza del certificato per ciascun KMS.
3. Se la scadenza del certificato per un KMS è sconosciuta, attendere fino a 30 minuti e quindi aggiornare il browser Web.
4. Se la colonna Scadenza certificato indica che un certificato è scaduto o sta per scadere, selezionare il KMS per andare alla pagina dei dettagli del KMS.
 - a. Selezionare **Certificato server** e verificare il valore per il campo "Scade il".
 - b. Per sostituire il certificato, seleziona **Modifica certificato** per caricare un nuovo certificato.
 - c. Ripetere questi sotto-passaggi e selezionare **Certificato client** anziché Certificato server.
5. Quando vengono attivati gli avvisi **Scadenza certificato CA KMS**, **Scadenza certificato client KMS** e **Scadenza certificato server KMS**, annotare la descrizione di ciascun avviso ed eseguire le azioni consigliate.

Potrebbero volerci fino a 30 minuti prima che StorageGRID riceva gli aggiornamenti sulla scadenza del certificato. Aggiorna il browser web per visualizzare i valori correnti.



Se viene visualizzato lo stato **Lo stato del certificato del server è sconosciuto**, accertarsi che il KMS consenta di ottenere un certificato del server senza richiedere un certificato del client.

Visualizza i nodi crittografati

È possibile visualizzare informazioni sui nodi dell'appliance nel sistema StorageGRID in cui è abilitata l'impostazione **Crittografia nodi**.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Server di gestione delle chiavi**.

Viene visualizzata la pagina Key Management Server. La scheda Dettagli configurazione mostra tutti i server di gestione delle chiavi che sono stati configurati.

2. Nella parte superiore della pagina, seleziona la scheda **Nodi crittografati**.

Nella scheda Nodi crittografati sono elencati i nodi dell'appliance nel sistema StorageGRID in cui è abilitata l'impostazione **Crittografia nodi**.

3. Esaminare le informazioni nella tabella per ciascun nodo dell'appliance.

Colonna	Descrizione
Nome del nodo	Il nome del nodo dell'appliance.
Tipo di nodo	Tipo di nodo: Storage, Admin o Gateway.
Sito	Nome del sito StorageGRID in cui è installato il nodo.
Nome KMS	Nome descrittivo del KMS utilizzato per il nodo. Se non è elencato alcun KMS, selezionare la scheda Dettagli configurazione per aggiungerne uno. "Aggiungere un server di gestione delle chiavi (KMS)"
UID chiave	ID univoco della chiave di crittografia utilizzata per crittografare e decrittografare i dati sul nodo dell'appliance. Per visualizzare l'intero UID della chiave, selezionare il testo. Un trattino (--) indica che l'UID della chiave è sconosciuto, probabilmente a causa di un problema di connessione tra il nodo dell'appliance e il KMS.
Stato	Lo stato della connessione tra il KMS e il nodo dell'appliance. Se il nodo è connesso, il timestamp viene aggiornato ogni 30 minuti. Dopo le modifiche alla configurazione KMS, potrebbero essere necessari diversi minuti prima che lo stato della connessione venga aggiornato. Nota: aggiorna il browser web per visualizzare i nuovi valori.

4. Se la colonna Stato indica un problema KMS, risolverlo immediatamente.

Durante le normali operazioni KMS, lo stato sarà **Connesso a KMS**. Se un nodo è disconnesso dalla rete, viene visualizzato lo stato di connessione del nodo (Amministrativamente inattivo o Sconosciuto).

Altri messaggi di stato corrispondono agli avvisi StorageGRID con gli stessi nomi:

- Impossibile caricare la configurazione KMS
- Errore di connettività KMS
- Nome della chiave di crittografia KMS non trovato
- Rotazione della chiave di crittografia KMS non riuscita
- La chiave KMS non è riuscita a decrittografare un volume dell'appliance
- KMS non è configurato

Eseguire le azioni consigliate per questi avvisi.



È necessario risolvere immediatamente qualsiasi problema per garantire la completa protezione dei dati.

Modifica un KMS

Potrebbe essere necessario modificare la configurazione di un server di gestione delle chiavi, ad esempio se un certificato sta per scadere.

Prima di iniziare

- Se si prevede di aggiornare il sito selezionato per un KMS, è necessario aver esaminato il ["considerazioni sulla modifica del KMS per un sito"](#).
- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["Permesso di accesso root"](#).

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Server di gestione delle chiavi**.

Viene visualizzata la pagina Server di gestione delle chiavi, che mostra tutti i server di gestione delle chiavi configurati.

2. Seleziona il KMS che vuoi modificare e seleziona **Azioni > Modifica**.

È anche possibile modificare un KMS selezionando il nome del KMS nella tabella e selezionando **Modifica** nella pagina dei dettagli del KMS.

3. Facoltativamente, aggiornare i dettagli nel **Passaggio 1 (Dettagli KMS)** della procedura guidata Modifica un server di gestione delle chiavi.

Campo	Descrizione
Nome KMS	Un nome descrittivo che ti aiuti a identificare questo KMS. Deve contenere tra 1 e 64 caratteri.
Nome chiave	L'alias chiave esatto per il client StorageGRID nel KMS. Deve contenere tra 1 e 255 caratteri. Solo in rari casi è necessario modificare il nome della chiave. Ad esempio, è necessario modificare il nome della chiave se l'alias è stato rinominato nel KMS o se tutte le versioni della chiave precedente sono state copiate nella cronologia delle versioni del nuovo alias.

Campo	Descrizione
Gestisce le chiavi per	Se stai modificando un KMS specifico del sito e non hai ancora un KMS predefinito, seleziona facoltativamente Siti non gestiti da un altro KMS (KMS predefinito). Questa selezione converte un KMS specifico del sito nel KMS predefinito, che verrà applicato a tutti i siti che non dispongono di un KMS dedicato e a tutti i siti aggiunti in un'espansione. Nota: se stai modificando un KMS specifico di un sito, non puoi selezionare un altro sito. Se stai modificando il KMS predefinito, non puoi selezionare un sito specifico.
Porta	La porta utilizzata dal server KMS per le comunicazioni KMIP (Key Management Interoperability Protocol). Il valore predefinito è 5696, che è la porta standard KMIP.
Nome host	Il nome di dominio completo o l'indirizzo IP per il KMS. Nota: il campo Subject Alternative Name (SAN) del certificato del server deve includere l'FQDN o l'indirizzo IP immesso qui. In caso contrario, StorageGRID non sarà in grado di connettersi al KMS o a tutti i server in un cluster KMS.

4. Se si sta configurando un cluster KMS, selezionare **Aggiungi un altro nome host** per aggiungere un nome host per ciascun server nel cluster.

5. Selezionare **Continua**.

Viene visualizzato il passaggio 2 (Carica certificato server) della procedura guidata Modifica un server di gestione delle chiavi.

6. Se è necessario sostituire il certificato del server, selezionare **Sfoggia** e caricare il nuovo file.

7. Selezionare **Continua**.

Viene visualizzato il passaggio 3 (Caricamento dei certificati client) della procedura guidata Modifica un server di gestione delle chiavi.

8. Se è necessario sostituire il certificato client e la chiave privata del certificato client, selezionare **Sfoggia** e caricare i nuovi file.

9. Seleziona **Test e salva**.

Vengono testate le connessioni tra il server di gestione delle chiavi e tutti i nodi dell'appliance crittografati tramite nodo nei siti interessati. Se tutte le connessioni dei nodi sono valide e la chiave corretta viene trovata sul KMS, il server di gestione delle chiavi viene aggiunto alla tabella nella pagina Server di gestione delle chiavi.

10. Se viene visualizzato un messaggio di errore, rivedere i dettagli del messaggio e selezionare **OK**.

Ad esempio, potresti ricevere un errore 422: Entità non elaborabile se il sito selezionato per questo KMS è già gestito da un altro KMS o se un test di connessione non è riuscito.

11. Se è necessario salvare la configurazione corrente prima di risolvere gli errori di connessione, selezionare **Forza salvataggio**.



Selezionando **Forza salvataggio** la configurazione KMS viene salvata, ma non viene testata la connessione esterna da ciascun dispositivo a quel KMS. Se si verifica un problema con la configurazione, potrebbe non essere possibile riavviare i nodi dell'appliance in cui è abilitata la crittografia dei nodi nel sito interessato. Potresti perdere l'accesso ai tuoi dati finché i problemi non saranno risolti.

La configurazione KMS è stata salvata.

12. Rivedi l'avviso di conferma e seleziona **OK** se sei sicuro di voler forzare il salvataggio della configurazione.

La configurazione KMS viene salvata, ma la connessione al KMS non viene testata.

Rimuovere un server di gestione delle chiavi (KMS)

In alcuni casi potrebbe essere necessario rimuovere un server di gestione delle chiavi. Ad esempio, potresti voler rimuovere un KMS specifico di un sito se hai dismesso il sito.

Prima di iniziare

- Hai esaminato il ["considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi"](#) .
- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Permesso di accesso root"](#) .

Informazioni su questo compito

È possibile rimuovere un KMS nei seguenti casi:

- È possibile rimuovere un KMS specifico del sito se il sito è stato dismesso o se non include nodi appliance con crittografia dei nodi abilitata.
- È possibile rimuovere il KMS predefinito se per ogni sito che dispone di nodi appliance con crittografia dei nodi abilitata esiste già un KMS specifico.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Server di gestione delle chiavi**.

Viene visualizzata la pagina Server di gestione delle chiavi, che mostra tutti i server di gestione delle chiavi configurati.

2. Seleziona il KMS che vuoi rimuovere e seleziona **Azioni > Rimuovi**.

È anche possibile rimuovere un KMS selezionando il nome del KMS nella tabella e selezionando **Rimuovi** dalla pagina dei dettagli del KMS.

3. Conferma che quanto segue è vero:

- Si sta rimuovendo un KMS specifico del sito per un sito che non dispone di alcun nodo appliance con crittografia del nodo abilitata.
- Stai rimuovendo il KMS predefinito, ma per ogni sito esiste già un KMS specifico con crittografia dei nodi.

4. Selezionare **Sì**.

La configurazione KMS è stata rimossa.

Gestisci le impostazioni proxy

Configurare il proxy di archiviazione

Se si utilizzano servizi di piattaforma o pool di archiviazione cloud, è possibile configurare un proxy non trasparente tra i nodi di archiviazione e gli endpoint S3 esterni. Ad esempio, potrebbe essere necessario un proxy non trasparente per consentire l'invio di messaggi dei servizi della piattaforma a endpoint esterni, come un endpoint su Internet.



Le impostazioni del proxy di archiviazione configurate non si applicano agli endpoint dei servizi della piattaforma Kafka.

Prima di iniziare

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

Informazioni su questo compito

È possibile configurare le impostazioni per un singolo proxy di archiviazione.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Impostazioni proxy**.
2. Nella scheda **Archiviazione**, seleziona la casella di controllo **Abilita proxy di archiviazione**.
3. Selezionare il protocollo per il proxy di archiviazione.
4. Inserisci il nome host o l'indirizzo IP del server proxy.
5. Facoltativamente, immettere la porta utilizzata per connettersi al server proxy.

Lasciare vuoto questo campo per utilizzare la porta predefinita per il protocollo: 80 per HTTP o 1080 per SOCKS5.

6. Seleziona **Salva**.

Dopo aver salvato il proxy di archiviazione, è possibile configurare e testare nuovi endpoint per i servizi della piattaforma o i pool di archiviazione cloud.



Le modifiche apportate al proxy potrebbero richiedere fino a 10 minuti per diventare effettive.

7. Controllare le impostazioni del server proxy per assicurarsi che i messaggi relativi al servizio della piattaforma provenienti da StorageGRID non vengano bloccati.
8. Se è necessario disattivare un proxy di archiviazione, deselezionare la casella di controllo e selezionare **Salva**.

Configurare le impostazioni del proxy amministratore

Se si inviano pacchetti AutoSupport tramite HTTP o HTTPS, è possibile configurare un server proxy non trasparente tra i nodi di amministrazione e il supporto tecnico (AutoSupport).

Per ulteriori informazioni su AutoSupport, vedere ["Configura AutoSupport"](#).

Prima di iniziare

- Hai "autorizzazioni di accesso specifiche" .
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato" .

Informazioni su questo compito

È possibile configurare le impostazioni per un singolo proxy amministratore.

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Impostazioni proxy**.

Viene visualizzata la pagina Impostazioni proxy. Per impostazione predefinita, nel menu delle schede è selezionata l'opzione Archiviazione.

2. Selezionare la scheda **Amministrazione**.
3. Selezionare la casella di controllo **Abilita proxy amministratore**.
4. Inserisci il nome host o l'indirizzo IP del server proxy.
5. Inserisci la porta utilizzata per connettersi al server proxy.
6. Facoltativamente, inserisci un nome utente e una password per il server proxy.

Lasciare vuoti questi campi se il server proxy non richiede un nome utente o una password.

7. Seleziona una delle seguenti opzioni:
 - Se si desidera proteggere la connessione al proxy di amministrazione, selezionare **Verifica certificato proxy**. Carica un bundle CA per verificare l'autenticità dei certificati SSL presentati dal server proxy di amministrazione.



AutoSupport on Demand, E-Series AutoSupport tramite StorageGRID e la determinazione del percorso di aggiornamento nella pagina di aggiornamento StorageGRID non funzioneranno se è verificato un certificato proxy.

Dopo aver caricato il bundle CA, vengono visualizzati i relativi metadati.

- Se non si desidera convalidare i certificati durante la comunicazione con il server proxy di amministrazione, selezionare **Non verificare il certificato proxy**.

8. Seleziona **Salva**.

Dopo aver salvato il proxy di amministrazione, viene configurato il server proxy tra i nodi di amministrazione e il supporto tecnico.



Le modifiche apportate al proxy potrebbero richiedere fino a 10 minuti per diventare effettive.

9. Se è necessario disattivare il proxy amministratore, deselezionare la casella di controllo **Abilita proxy amministratore**, quindi selezionare **Salva**.

Controllare i firewall

Controllare l'accesso al firewall esterno

È possibile aprire o chiudere porte specifiche sul firewall esterno.

È possibile controllare l'accesso alle interfacce utente e alle API sui nodi di amministrazione StorageGRID aprendo o chiudendo porte specifiche sul firewall esterno. Ad esempio, potresti voler impedire ai tenant di connettersi a Grid Manager tramite il firewall, oltre a utilizzare altri metodi per controllare l'accesso al sistema.

Se si desidera configurare il firewall interno StorageGRID, vedere ["Configurare il firewall interno"](#).

Porta	Descrizione	Se la porta è aperta...
443	Porta HTTPS predefinita per i nodi di amministrazione	I browser Web e i client API di gestione possono accedere a Grid Manager, Grid Management API, Tenant Manager e Tenant Management API. Nota: la porta 443 viene utilizzata anche per parte del traffico interno.
8443	Porta Grid Manager limitata sui nodi amministrativi	• I browser Web e i client API di gestione possono accedere a Grid Manager e alla Grid Management API tramite HTTPS. • I browser Web e i client API di gestione non possono accedere a Tenant Manager o all'API Tenant Management. • Le richieste di contenuti interni verranno respinte.
9443	Porta Tenant Manager limitata sui nodi amministrativi	• I browser Web e i client API di gestione possono accedere a Tenant Manager e all'API Tenant Management tramite HTTPS. • I browser Web e i client API di gestione non possono accedere a Grid Manager o all'API Grid Management. • Le richieste di contenuti interni verranno respinte.



L'accesso Single Sign-On (SSO) non è disponibile sulle porte riservate di Grid Manager o Tenant Manager. Se si desidera che gli utenti eseguano l'autenticazione tramite Single Sign-On, è necessario utilizzare la porta HTTPS predefinita (443).

Informazioni correlate

- ["Sign in a Grid Manager"](#)
- ["Crea un account inquilino"](#)
- ["Comunicazioni esterne"](#)

Gestire i controlli del firewall interno

StorageGRID include un firewall interno su ciascun nodo che migliora la sicurezza della griglia consentendo di controllare l'accesso di rete al nodo. Utilizzare il firewall per impedire l'accesso alla rete su tutte le porte, ad eccezione di quelle necessarie per la

distribuzione specifica della griglia. Le modifiche alla configurazione apportate nella pagina di controllo del firewall vengono distribuite a ciascun nodo.

Utilizza le tre schede nella pagina di controllo del firewall per personalizzare l'accesso necessario per la tua griglia.

- **Elenco indirizzi privilegiati:** utilizzare questa scheda per consentire l'accesso selezionato alle porte chiuse. È possibile aggiungere indirizzi IP o subnet in notazione CIDR che possono accedere alle porte chiuse utilizzando la scheda Gestisci accesso esterno.
- **Gestisci accesso esterno:** usa questa scheda per chiudere le porte aperte per impostazione predefinita o per riaprire quelle chiuse in precedenza.
- **Rete client non attendibile:** utilizzare questa scheda per specificare se un nodo considera attendibile il traffico in entrata dalla rete client.

Le impostazioni in questa scheda sostituiscono quelle nella scheda Gestisci accesso esterno.

- Un nodo con una rete client non attendibile accetterà solo connessioni sulle porte degli endpoint del bilanciatore del carico configurate su quel nodo (endpoint globali, interfaccia nodo e tipo nodo).
- Le porte degli endpoint del bilanciatore del carico *sono le uniche porte aperte* sulle reti client non attendibili, indipendentemente dalle impostazioni nella scheda Gestisci reti esterne.
- Se attendibili, tutte le porte aperte nella scheda Gestisci accesso esterno sono accessibili, così come tutti gli endpoint del bilanciatore del carico aperti sulla rete client.



Le impostazioni effettuate in una scheda possono influire sulle modifiche di accesso effettuate in un'altra scheda. Assicurati di controllare le impostazioni in tutte le schede per verificare che la tua rete si comporti come previsto.

Per configurare i controlli del firewall interno, vedere ["Configurare i controlli del firewall"](#).

Per ulteriori informazioni sui firewall esterni e sulla sicurezza di rete, vedere ["Controllare l'accesso al firewall esterno"](#).

Elenco indirizzi privilegiati e schede Gestisci accesso esterno

La scheda Elenco indirizzi privilegiati consente di registrare uno o più indirizzi IP a cui è concesso l'accesso alle porte della griglia chiuse. La scheda Gestisci accesso esterno consente di chiudere l'accesso esterno alle porte esterne selezionate o a tutte le porte esterne aperte (le porte esterne sono porte accessibili per impostazione predefinita dai nodi non di griglia). Spesso è possibile utilizzare insieme queste due schede per personalizzare l'esatto accesso alla rete che si desidera consentire alla propria griglia.



Per impostazione predefinita, gli indirizzi IP privilegiati non hanno accesso alla porta della griglia interna.

Esempio 1: utilizzare un jump host per le attività di manutenzione

Supponiamo di voler utilizzare un jump host (un host con sicurezza rafforzata) per l'amministrazione della rete. Potresti seguire questi passaggi generali:

1. Utilizzare la scheda Elenco indirizzi privilegiati per aggiungere l'indirizzo IP dell'host jump.
2. Utilizzare la scheda Gestisci accesso esterno per bloccare tutte le porte.



Aggiungere l'indirizzo IP privilegiato prima di bloccare le porte 443 e 8443. Tutti gli utenti attualmente connessi a una porta bloccata, incluso te, perderanno l'accesso a Grid Manager a meno che il loro indirizzo IP non sia stato aggiunto all'elenco degli indirizzi privilegiati.

Dopo aver salvato la configurazione, tutte le porte esterne sul nodo di amministrazione nella griglia verranno bloccate per tutti gli host, ad eccezione dell'host jump. È quindi possibile utilizzare l'host jump per eseguire attività di manutenzione sulla griglia in modo più sicuro.

Esempio 2: Bloccare le porte sensibili

Supponiamo di voler bloccare porte sensibili e il servizio su quella porta (ad esempio, SSH sulla porta 22). È possibile seguire i seguenti passaggi generali:

1. Utilizzare la scheda Elenco indirizzi privilegiati per concedere l'accesso solo agli host che necessitano di accedere al servizio.
2. Utilizzare la scheda Gestisci accesso esterno per bloccare tutte le porte.



Aggiungere l'indirizzo IP privilegiato prima di bloccare l'accesso a qualsiasi porta assegnata per accedere a Grid Manager e Tenant Manager (le porte preimpostate sono 443 e 8443). Tutti gli utenti attualmente connessi a una porta bloccata, incluso te, perderanno l'accesso a Grid Manager a meno che il loro indirizzo IP non sia stato aggiunto all'elenco degli indirizzi privilegiati.

Dopo aver salvato la configurazione, la porta 22 e il servizio SSH saranno disponibili per gli host nell'elenco degli indirizzi privilegiati. A tutti gli altri host verrà negato l'accesso al servizio, indipendentemente dall'interfaccia da cui proviene la richiesta.

Esempio 3: Disabilitare l'accesso ai servizi non utilizzati

A livello di rete, potresti disattivare alcuni servizi che non intendi utilizzare. Ad esempio, per bloccare il traffico client HTTP S3, è necessario utilizzare l'interruttore nella scheda Gestisci accesso esterno per bloccare la porta 18084.

Scheda Reti client non attendibili

Se si utilizza una rete client, è possibile proteggere StorageGRID da attacchi ostili accettando il traffico client in entrata solo su endpoint configurati in modo esplicito.

Per impostazione predefinita, la rete client su ciascun nodo della griglia è *attendibile*. Ciò significa che, per impostazione predefinita, StorageGRID considera attendibili le connessioni in ingresso a ciascun nodo della griglia su tutti ["porte esterne disponibili"](#).

È possibile ridurre la minaccia di attacchi ostili al sistema StorageGRID specificando che la rete client su ciascun nodo sia *non attendibile*. Se la rete client di un nodo non è attendibile, il nodo accetta solo connessioni in entrata su porte configurate esplicitamente come endpoint del bilanciatore del carico. Vedere ["Configurare gli endpoint del bilanciatore del carico"](#) e ["Configurare i controlli del firewall"](#).

Esempio 1: il nodo gateway accetta solo richieste HTTPS S3

Supponiamo di voler far sì che un nodo gateway rifiuti tutto il traffico in entrata sulla rete client, ad eccezione delle richieste HTTPS S3. Dovresti eseguire questi passaggi generali:

1. Dal ["Endpoint del bilanciatore del carico"](#) pagina, configura un endpoint del bilanciatore del carico per S3 su

HTTPS sulla porta 443.

2. Nella pagina Controllo firewall, selezionare Non attendibile per specificare che la rete client sul nodo gateway non è attendibile.

Dopo aver salvato la configurazione, tutto il traffico in entrata sulla rete client del nodo gateway viene interrotto, ad eccezione delle richieste HTTPS S3 sulla porta 443 e delle richieste ICMP echo (ping).

Esempio 2: il nodo di archiviazione invia richieste di servizi della piattaforma S3

Supponiamo di voler abilitare il traffico dei servizi della piattaforma S3 in uscita da un nodo di archiviazione, ma di voler impedire qualsiasi connessione in ingresso a tale nodo di archiviazione sulla rete client. Dovresti eseguire questo passaggio generale:

- Dalla scheda Reti client non attendibili della pagina di controllo del firewall, indicare che la rete client sul nodo di archiviazione non è attendibile.

Dopo aver salvato la configurazione, il nodo di archiviazione non accetta più traffico in entrata sulla rete client, ma continua a consentire richieste in uscita verso le destinazioni dei servizi della piattaforma configurati.

Esempio 3: limitazione dell'accesso a Grid Manager a una subnet

Supponiamo di voler consentire l'accesso a Grid Manager solo su una subnet specifica. Dovresti eseguire i seguenti passaggi:

1. Collega la rete client dei tuoi nodi amministrativi alla subnet.
2. Utilizzare la scheda Rete client non attendibile per configurare la rete client come non attendibile.
3. Quando si crea un endpoint del bilanciatore del carico dell'interfaccia di gestione, immettere la porta e selezionare l'interfaccia di gestione a cui la porta accederà.
4. Selezionare **Sì** per Rete client non attendibile.
5. Utilizzare la scheda Gestisci accesso esterno per bloccare tutte le porte esterne (con o senza indirizzi IP privilegiati impostati per gli host esterni a quella subnet).

Dopo aver salvato la configurazione, solo gli host nella subnet specificata potranno accedere a Grid Manager. Tutti gli altri host sono bloccati.

Configurare il firewall interno

È possibile configurare il firewall StorageGRID per controllare l'accesso alla rete a porte specifiche sui nodi StorageGRID .

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Hai ["autorizzazioni di accesso specifiche"](#) .
- Hai esaminato le informazioni in ["Gestire i controlli del firewall"](#) E ["Linee guida per il networking"](#) .
- Se si desidera che un nodo di amministrazione o un nodo gateway accetti il traffico in entrata solo su endpoint configurati in modo esplicito, è necessario definire gli endpoint del bilanciatore del carico.



Quando si modifica la configurazione della rete client, le connessioni client esistenti potrebbero non funzionare se gli endpoint del bilanciatore del carico non sono stati configurati.

Informazioni su questo compito

StorageGRID include un firewall interno su ciascun nodo che consente di aprire o chiudere alcune porte sui nodi della griglia. È possibile utilizzare le schede di controllo Firewall per aprire o chiudere le porte aperte per impostazione predefinita sulla rete Grid, sulla rete di amministrazione e sulla rete client. È anche possibile creare un elenco di indirizzi IP privilegiati che possono accedere alle porte della griglia chiuse. Se si utilizza una rete client, è possibile specificare se un nodo si fida del traffico in entrata dalla rete client e configurare l'accesso di porte specifiche sulla rete client.

Limitare il numero di porte aperte agli indirizzi IP esterni alla rete solo a quelle assolutamente necessarie aumenta la sicurezza della rete stessa. Utilizzare le impostazioni in ciascuna delle tre schede di controllo del firewall per garantire che siano aperte solo le porte necessarie.

Per ulteriori informazioni sull'utilizzo dei controlli del firewall, inclusi esempi, vedere ["Gestire i controlli del firewall"](#).

Per ulteriori informazioni sui firewall esterni e sulla sicurezza di rete, vedere ["Controllare l'accesso al firewall esterno"](#).

Controlli del firewall di accesso

Passi

1. Selezionare **CONFIGURAZIONE > Sicurezza > Controllo firewall**.

Le tre schede in questa pagina sono descritte in ["Gestire i controlli del firewall"](#).

2. Selezionare una scheda qualsiasi per configurare i controlli del firewall.

È possibile utilizzare queste schede in qualsiasi ordine. Le configurazioni impostate in una scheda non limitano le operazioni eseguibili nelle altre schede; tuttavia, le modifiche apportate alla configurazione in una scheda potrebbero modificare il comportamento delle porte configurate nelle altre schede.

Elenco indirizzi privilegiati

Utilizzare la scheda Elenco indirizzi privilegiati per concedere agli host l'accesso alle porte chiuse per impostazione predefinita o chiuse dalle impostazioni nella scheda Gestisci accesso esterno.

Per impostazione predefinita, gli indirizzi IP e le subnet privilegiati non dispongono di accesso alla griglia interna. Inoltre, gli endpoint del bilanciatore del carico e le porte aggiuntive aperte nella scheda Elenco indirizzi privilegiati sono accessibili anche se bloccati nella scheda Gestisci accesso esterno.



Le impostazioni nella scheda Elenco indirizzi privilegiati non possono sovrascrivere le impostazioni nella scheda Rete client non attendibile.

Passi

1. Nella scheda Elenco indirizzi privilegiati, immettere l'indirizzo o la subnet IP a cui si desidera concedere l'accesso alle porte chiuse.
2. Facoltativamente, seleziona **Aggiungi un altro indirizzo IP o subnet in notazione CIDR** per aggiungere altri client privilegiati.



Aggiungere il minor numero possibile di indirizzi all'elenco privilegiato.

3. Facoltativamente, seleziona ***Consenti agli indirizzi IP privilegiati di accedere alle porte interne**

StorageGRID *. Vedere ["Porte interne StorageGRID"](#) .



Questa opzione rimuove alcune protezioni per i servizi interni. Se possibile, lascialo disattivato.

4. Seleziona **Salva**.

Gestisci l'accesso esterno

Quando una porta viene chiusa nella scheda Gestisci accesso esterno, non è possibile accedervi da nessun indirizzo IP non in rete, a meno che non si aggiunga l'indirizzo IP all'elenco degli indirizzi privilegiati. Puoi chiudere solo le porte che sono aperte per impostazione predefinita e puoi aprire solo le porte che hai chiuso.



Le impostazioni nella scheda Gestisci accesso esterno non possono sostituire le impostazioni nella scheda Rete client non attendibile. Ad esempio, se un nodo non è attendibile, la porta SSH/22 viene bloccata sulla rete client anche se è aperta nella scheda Gestisci accesso esterno. Le impostazioni nella scheda Rete client non attendibile sovrascrivono le porte chiuse (ad esempio 443, 8443, 9443) sulla rete client.

Passi

1. Seleziona **Gestisci accesso esterno**. La scheda visualizza una tabella con tutte le porte esterne (porte accessibili per impostazione predefinita dai nodi non in griglia) per i nodi nella griglia.
2. Configura le porte che vuoi aprire e chiudere utilizzando le seguenti opzioni:
 - Utilizzare il pulsante accanto a ciascuna porta per aprire o chiudere la porta selezionata.
 - Selezionare **Apri tutte le porte visualizzate** per aprire tutte le porte elencate nella tabella.
 - Selezionare **Chiudi tutte le porte visualizzate** per chiudere tutte le porte elencate nella tabella.



Se chiudi le porte 443 o 8443 di Grid Manager, tutti gli utenti attualmente connessi su una porta bloccata, incluso te, perderanno l'accesso a Grid Manager, a meno che il loro indirizzo IP non sia stato aggiunto all'elenco degli indirizzi privilegiati.



Utilizzare la barra di scorrimento sul lato destro della tabella per assicurarsi di aver visualizzato tutte le porte disponibili. Utilizzare il campo di ricerca per trovare le impostazioni per qualsiasi porta esterna inserendo un numero di porta. È possibile immettere un numero di porta parziale. Ad esempio, se si immette **2**, vengono visualizzate tutte le porte che contengono la stringa "2" nel loro nome.

3. Seleziona **Salva**

Rete client non attendibile

Se la rete client di un nodo non è attendibile, il nodo accetta solo il traffico in entrata sulle porte configurate come endpoint del bilanciatore del carico e, facoltativamente, sulle porte aggiuntive selezionate in questa scheda. È possibile utilizzare questa scheda anche per specificare l'impostazione predefinita per i nuovi nodi aggiunti in un'espansione.



Le connessioni client esistenti potrebbero non riuscire se gli endpoint del bilanciatore del carico non sono stati configurati.

Le modifiche alla configurazione apportate nella scheda **Rete client non attendibile** sovrascrivono le impostazioni nella scheda **Gestisci accesso esterno**.

Passi

1. Selezionare **Rete client non attendibile**.
2. Nella sezione Imposta nuovo nodo predefinito, specificare quale deve essere l'impostazione predefinita quando vengono aggiunti nuovi nodi alla griglia in una procedura di espansione.
 - **Affidabile** (predefinito): quando un nodo viene aggiunto in un'espansione, la sua rete client è attendibile.
 - **Non attendibile**: quando un nodo viene aggiunto a un'espansione, la sua rete client non è attendibile.

Se necessario, è possibile tornare a questa scheda per modificare l'impostazione per un nuovo nodo specifico.



Questa impostazione non influisce sui nodi esistenti nel sistema StorageGRID .

3. Utilizzare le seguenti opzioni per selezionare i nodi che devono consentire connessioni client solo su endpoint del bilanciatore del carico configurati in modo esplicito o porte aggiuntive selezionate:
 - Selezionare **Non considerare attendibili i nodi visualizzati** per aggiungere tutti i nodi visualizzati nella tabella all'elenco Reti client non attendibili.
 - Selezionare **Considera attendibili i nodi visualizzati** per rimuovere tutti i nodi visualizzati nella tabella dall'elenco Reti client non attendibili.
 - Utilizzare il pulsante di attivazione/disattivazione accanto a ciascun nodo per impostare la rete client come attendibile o non attendibile per il nodo selezionato.

Ad esempio, è possibile selezionare **Non considerare attendibili i nodi visualizzati** per aggiungere tutti i nodi all'elenco Reti client non attendibili e quindi utilizzare il pulsante di attivazione/disattivazione accanto a un singolo nodo per aggiungere quel singolo nodo all'elenco Reti client attendibili.



Utilizzare la barra di scorrimento sul lato destro della tabella per assicurarsi di aver visualizzato tutti i nodi disponibili. Utilizzare il campo di ricerca per trovare le impostazioni di qualsiasi nodo immettendone il nome. È possibile immettere un nome parziale. Ad esempio, se si immette **GW**, verranno visualizzati tutti i nodi che hanno la stringa "GW" come parte del loro nome.

4. Seleziona **Salva**.

Le nuove impostazioni del firewall vengono applicate e rese effettive immediatamente. Le connessioni client esistenti potrebbero non riuscire se gli endpoint del bilanciatore del carico non sono stati configurati.

Gestire gli inquilini

Cosa sono i conti degli inquilini?

Un account tenant consente di utilizzare l'API REST Simple Storage Service (S3) per archiviare e recuperare oggetti in un sistema StorageGRID .



I dettagli su Swift sono stati rimossi da questa versione del sito di documentazione. Vedere ["StorageGRID 11.8: Gestisci i tenant"](#).

In qualità di amministratore della griglia, crei e gestisci gli account tenant che i client S3 utilizzano per archiviare e recuperare gli oggetti.

Ogni account tenant ha gruppi, utenti, bucket S3 e oggetti federati o locali.

Gli account tenant possono essere utilizzati per separare gli oggetti archiviati da entità diverse. Ad esempio, è possibile utilizzare più account tenant per uno qualsiasi di questi casi d'uso:

- **Caso d'uso aziendale:** se si amministra un sistema StorageGRID in un'applicazione aziendale, potrebbe essere opportuno separare l'archiviazione degli oggetti della griglia in base ai diversi reparti dell'organizzazione. In questo caso, potresti creare account tenant per il reparto Marketing, il reparto Assistenza Clienti, il reparto Risorse Umane e così via.



Se si utilizza il protocollo client S3, è possibile utilizzare bucket S3 e policy di bucket per separare gli oggetti tra i reparti di un'azienda. Non è necessario utilizzare account tenant. Vedi le istruzioni per l'implementazione ["Bucket S3 e policy dei bucket"](#) per maggiori informazioni.

- **Caso d'uso del fornitore di servizi:** se si amministra un sistema StorageGRID come fornitore di servizi, è possibile separare l'archiviazione degli oggetti della griglia in base alle diverse entità che prenderanno in leasing l'archiviazione sulla griglia. In questo caso, dovresti creare account tenant per la Società A, la Società B, la Società C e così via.

Per ulteriori informazioni, consultare ["Utilizzare un account tenant"](#).

Come posso creare un account tenant?

Utilizzare Grid Manager per creare un account tenant. Quando si crea un account tenant, si specificano le seguenti informazioni:

- Informazioni di base, tra cui il nome del tenant, il tipo di client (S3) e la quota di archiviazione facoltativa.
- Autorizzazioni per l'account tenant, ad esempio se l'account tenant può utilizzare i servizi della piattaforma S3, configurare la propria origine identità, utilizzare S3 Select o utilizzare una connessione di federazione di griglia.
- L'accesso root iniziale per il tenant, a seconda che il sistema StorageGRID utilizzi gruppi e utenti locali, federazione delle identità o Single Sign-On (SSO).

Inoltre, è possibile abilitare l'impostazione S3 Object Lock per il sistema StorageGRID se gli account tenant S3 devono essere conformi ai requisiti normativi. Quando S3 Object Lock è abilitato, tutti gli account tenant S3 possono creare e gestire bucket conformi.

A cosa serve Tenant Manager?

Dopo aver creato l'account tenant, gli utenti tenant possono accedere a Tenant Manager per eseguire attività come le seguenti:

- Impostare la federazione delle identità (a meno che l'origine dell'identità non sia condivisa con la griglia)
- Gestisci gruppi e utenti
- Utilizzare la federazione di griglia per la clonazione degli account e la replica tra griglie

- Gestisci le chiavi di accesso S3
- Crea e gestisci bucket S3
- Utilizzare i servizi della piattaforma S3
- Utilizzare S3 Select
- Monitorare l'utilizzo dello spazio di archiviazione



Mentre gli utenti tenant S3 possono creare e gestire bucket e chiavi di accesso S3 con Tenant Manager, devono utilizzare un'applicazione client S3 per acquisire e gestire gli oggetti. Vedere ["Utilizzare l'API REST S3"](#) per i dettagli.

Crea un account inquilino

È necessario creare almeno un account tenant per controllare l'accesso allo storage nel sistema StorageGRID .

I passaggi per la creazione di un account tenant variano a seconda che ["federazione di identità"](#) E ["accesso unico"](#) sono configurati e se l'account Grid Manager utilizzato per creare l'account tenant appartiene a un gruppo di amministratori con autorizzazione di accesso Root.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Accesso root o autorizzazione account tenant"](#) .
- Se l'account tenant utilizzerà l'origine identità configurata per Grid Manager e si desidera concedere l'autorizzazione di accesso Root per l'account tenant a un gruppo federato, è stato importato tale gruppo federato in Grid Manager. Non è necessario assegnare alcuna autorizzazione Grid Manager a questo gruppo di amministratori. Vedere ["Gestisci gruppi di amministratori"](#) .
- Se si desidera consentire a un tenant S3 di clonare i dati dell'account e replicare gli oggetti bucket su un'altra griglia utilizzando una connessione di federazione della griglia:
 - Hai ["configurato la connessione della federazione di griglia"](#) .
 - Lo stato della connessione è **Connesso**.
 - Hai i permessi di accesso Root.
 - Hai esaminato le considerazioni per ["gestione degli inquilini autorizzati per la federazione della rete"](#) .
 - Se l'account tenant utilizzerà l'origine identità configurata per Grid Manager, significa che hai importato lo stesso gruppo federato in Grid Manager su entrambe le griglie.

Quando si crea il tenant, si selezionerà questo gruppo per avere l'autorizzazione di accesso Root iniziale sia per l'account tenant di origine che per quello di destinazione.



Se questo gruppo di amministratori non esiste su entrambe le griglie prima di creare il tenant, il tenant non verrà replicato nella destinazione.

Accedi alla procedura guidata

Passi

1. Selezionare **INQUILINI**.

2. Seleziona **Crea**.

Inserisci i dettagli

Passi

1. Inserisci i dettagli dell'inquilino.

Campo	Descrizione
Nome	Un nome per l'account dell'inquilino. I nomi degli inquilini non devono essere univoci. Quando viene creato l'account tenant, questo riceve un ID account univoco di 20 cifre.
Descrizione (facoltativa)	Una descrizione che aiuti a identificare l'inquilino. Se si sta creando un tenant che utilizzerà una connessione di federazione di griglia, è possibile utilizzare questo campo per identificare il tenant di origine e quello di destinazione. Ad esempio, questa descrizione per un tenant creato sulla Griglia 1 apparirà anche per il tenant replicato sulla Griglia 2: "Questo tenant è stato creato sulla Griglia 1".
Tipo di cliente	Il tipo di protocollo client che questo tenant utilizzerà, S3 o Swift . Nota: il supporto per le applicazioni client Swift è stato deprecato e verrà rimosso in una versione futura.
Quota di archiviazione (facoltativa)	Se si desidera che questo tenant disponga di una quota di archiviazione, specificare un valore numerico per la quota e le unità.

2. Selezionare **Continua**.

Seleziona autorizzazioni

Passi

1. Facoltativamente, seleziona le autorizzazioni di base che desideri assegnare a questo tenant.



Alcune di queste autorizzazioni prevedono requisiti aggiuntivi. Per maggiori dettagli, seleziona l'icona della guida per ogni autorizzazione.

Permesso	Se selezionato...
Consenti i servizi della piattaforma	Il tenant può utilizzare i servizi della piattaforma S3 come CloudMirror. Vedere "Gestire i servizi della piattaforma per gli account tenant S3" .
Utilizzare la propria fonte di identità	Il tenant può configurare e gestire la propria fonte di identità per gruppi e utenti federati. Questa opzione è disabilitata se hai "SSO configurato" per il tuo sistema StorageGRID.

Permesso	Se selezionato...
Consenti selezione S3	Il tenant può inviare richieste API S3 SelectObjectContent per filtrare e recuperare i dati degli oggetti. Vedere "Gestisci S3 Select per gli account tenant" . Importante: le richieste SelectObjectContent possono ridurre le prestazioni del bilanciamento del carico per tutti i client S3 e tutti i tenant. Abilitare questa funzionalità solo quando necessario e solo per i tenant attendibili.

2. Facoltativamente, seleziona le autorizzazioni avanzate che desideri assegnare a questo tenant.

Permesso	Se selezionato...
Collegamento della federazione di rete	L'inquilino può utilizzare una connessione di federazione di rete, che: • Fa sì che questo tenant e tutti i gruppi e gli utenti tenant aggiunti all'account vengano clonati da questa griglia (la <i>griglia di origine</i>) all'altra griglia nella connessione selezionata (la <i>griglia di destinazione</i>). • Consente a questo tenant di configurare la replica tra griglie tra i bucket corrispondenti su ciascuna griglia. Vedere "Gestire gli inquilini autorizzati per la federazione della rete" .
Blocco oggetto S3	Consentire al tenant di utilizzare funzionalità specifiche di S3 Object Lock: • Imposta periodo massimo di conservazione definisce per quanto tempo i nuovi oggetti aggiunti a questo bucket devono essere conservati, a partire dal momento in cui vengono acquisiti. • Consenti modalità di conformità impedisce agli utenti di sovrascrivere o eliminare versioni di oggetti protetti durante il periodo di conservazione.

3. Selezionare **Continua**.

Definisci l'accesso root e crea il tenant

Passi

1. Definisci l'accesso root per l'account tenant, a seconda che il tuo sistema StorageGRID utilizzi la federazione delle identità, il Single Sign-On (SSO) o entrambi.

Opzione	Fai questo
Se la federazione delle identità non è abilitata	Specificare la password da utilizzare quando si accede al tenant come utente root locale.
Se la federazione delle identità è abilitata	a. Selezionare un gruppo federato esistente per ottenere l'autorizzazione di accesso Root per il tenant. b. Facoltativamente, specificare la password da utilizzare quando si accede al tenant come utente root locale.

Opzione	Fai questo
Se sono abilitati sia la federazione delle identità che il Single Sign-On (SSO)	Selezionare un gruppo federato esistente per ottenere l'autorizzazione di accesso Root per il tenant. Nessun utente locale può effettuare l'accesso.

2. Selezionare **Crea tenant**.

Viene visualizzato un messaggio di conferma e il nuovo inquilino viene elencato nella pagina Inquilini. Per informazioni su come visualizzare i dettagli degli inquilini e monitorarne l'attività, vedere ["Monitorare l'attività degli inquilini"](#).



L'applicazione delle impostazioni del tenant sulla griglia potrebbe richiedere 15 minuti o più, a seconda della connettività di rete, dello stato del nodo e delle operazioni di Cassandra.

3. Se hai selezionato l'autorizzazione **Usa connessione federata alla griglia** per il tenant:

- Verificare che un tenant identico sia stato replicato sull'altra griglia nella connessione. Gli inquilini su entrambe le griglie avranno lo stesso ID account di 20 cifre, nome, descrizione, quota e autorizzazioni.



Se viene visualizzato il messaggio di errore "Tenant creato senza un clone", fare riferimento alle istruzioni in ["Risolvere gli errori di federazione della griglia"](#).

- Se hai fornito una password utente root locale quando hai definito l'accesso root, ["cambiare la password per l'utente root locale"](#) per l'inquilino replicato.



Un utente root locale non può accedere a Tenant Manager sulla griglia di destinazione finché non viene modificata la password.

Sign in al tenant (facoltativo)

Se necessario, puoi accedere subito al nuovo tenant per completare la configurazione oppure puoi accedere al tenant in un secondo momento. I passaggi per l'accesso variano a seconda che tu abbia effettuato l'accesso a Grid Manager tramite la porta predefinita (443) o una porta con restrizioni. Vedere ["Controllare l'accesso al firewall esterno"](#).

Sign in ora

Se stai utilizzando...	Fai questo...
Porta 443 e si imposta una password per l'utente root locale	- Seleziona * Sign in come root*. Quando effettui l'accesso, vengono visualizzati i link per configurare bucket, federazione delle identità, gruppi e utenti. - Selezionare i link per configurare l'account tenant. Ogni collegamento apre la pagina corrispondente in Tenant Manager. Per completare la pagina, vedere il "istruzioni per l'utilizzo degli account degli inquilini".

Se stai utilizzando...	Fai questo...
Porta 443 e non hai impostato una password per l'utente root locale	Selezionare * Sign in* e immettere le credenziali di un utente nel gruppo federato con accesso root.
Un porto limitato	1. Seleziona Fine 2. Selezionare Limitato nella tabella Tenant per saperne di più sull'accesso a questo account tenant. L'URL per Tenant Manager ha questo formato: <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/</pre> ◦ `FQDN_or_Admin_Node_IP` è un nome di dominio completamente qualificato o l'indirizzo IP di un nodo di amministrazione ◦ `port` è la porta riservata al tenant ◦ `20-digit-account-id` è l'ID account univoco del tenant

Sign in più tardi

Se stai utilizzando...	Fai una di queste cose...
Porta 443	• Da Grid Manager, seleziona TENANT e seleziona * Sign in* a destra del nome del tenant. • Inserisci l'URL del tenant in un browser web: <pre>https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/</pre> ◦ `FQDN_or_Admin_Node_IP` è un nome di dominio completamente qualificato o l'indirizzo IP di un nodo di amministrazione ◦ `20-digit-account-id` è l'ID account univoco del tenant
Un porto limitato	• Da Grid Manager, seleziona TENANTS e seleziona Restricted. • Inserisci l'URL del tenant in un browser web: <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id</pre> ◦ `FQDN_or_Admin_Node_IP` è un nome di dominio completamente qualificato o l'indirizzo IP di un nodo di amministrazione ◦ `port` è la porta riservata solo al tenant ◦ `20-digit-account-id` è l'ID account univoco del tenant

Configurare il tenant

Seguire le istruzioni in ["Utilizzare un account tenant"](#) per gestire gruppi di tenant e utenti, chiavi di accesso S3, bucket, servizi di piattaforma, clonazione di account e replica tra griglie.

Modifica account inquilino

È possibile modificare un account tenant per cambiare il nome visualizzato, la quota di archiviazione o le autorizzazioni del tenant.



Se un tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, è possibile modificare i dettagli del tenant da entrambe le griglie nella connessione. Tuttavia, tutte le modifiche apportate a una griglia nella connessione non verranno copiate nell'altra griglia. Se si desidera che i dettagli degli inquilini siano perfettamente sincronizzati tra le griglie, apportare le stesse modifiche su entrambe le griglie. Vedere ["Gestire gli inquilini autorizzati per la connessione alla federazione di rete"](#).

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["Accesso root o autorizzazione account tenant"](#).



L'applicazione delle impostazioni del tenant sulla griglia potrebbe richiedere 15 minuti o più, a seconda della connettività di rete, dello stato del nodo e delle operazioni di Cassandra.

Passi

1. Selezionare **INQUILINI**.

Tenants							
View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.							
Create	Export to CSV	Actions ▾	Search tenants by name or ID		Displaying 5 results		
☐	Name ?	Logical space used ?	Quota utilization ?	Quota ?	Object count ?	Sign in/Copy URL ?	
☐	Tenant 01	2.00 GB	10%	20.00 GB	100	→	📄
☐	Tenant 02	85.00 GB	85%	100.00 GB	500	→	📄
☐	Tenant 03	500.00 TB	50%	1.00 PB	10,000	→	📄
☐	Tenant 04	475.00 TB	95%	500.00 TB	50,000	→	📄
☐	Tenant 05	5.00 GB	—	—	500	→	📄

2. Individua l'account tenant che desideri modificare.

Utilizzare la casella di ricerca per cercare un inquilino per nome o ID inquilino.

3. Selezionare l'inquilino. Puoi procedere in uno dei seguenti modi:

- Selezionare la casella di controllo per il tenant e selezionare **Azioni > Modifica**.
 - Selezionare il nome del tenant per visualizzare la pagina dei dettagli e selezionare **Modifica**.
4. Facoltativamente, modifica i valori per questi campi:
- **Nome**
 - **Descrizione**
 - **Quota di archiviazione**
5. Selezionare **Continua**.
6. Selezionare o deselezionare le autorizzazioni per l'account tenant.
- Se disabiliti i **Servizi di piattaforma** per un tenant che li sta già utilizzando, i servizi che ha configurato per i suoi bucket S3 smetteranno di funzionare. Non viene inviato alcun messaggio di errore al tenant. Ad esempio, se il tenant ha configurato la replica CloudMirror per un bucket S3, può comunque archiviare oggetti nel bucket, ma le copie di tali oggetti non verranno più create nel bucket S3 esterno che ha configurato come endpoint. Vedere ["Gestire i servizi della piattaforma per gli account tenant S3"](#).
 - Modificare l'impostazione **Usa la propria origine identità** per determinare se l'account tenant utilizzerà la propria origine identità o l'origine identità configurata per Grid Manager.

Se **Utilizza la propria fonte di identità** è:

- Disabilitato e selezionato, il tenant ha già abilitato la propria fonte di identità. Un tenant deve disabilitare la propria origine identità prima di poter utilizzare l'origine identità configurata per Grid Manager.
 - Disabilitato e non selezionato, SSO è abilitato per il sistema StorageGRID. Il tenant deve utilizzare l'origine identità configurata per Grid Manager.
- Selezionare o deselezionare l'autorizzazione **Consenti selezione S3** in base alle esigenze. Vedere ["Gestisci S3 Select per gli account tenant"](#).
 - Per rimuovere l'autorizzazione **Usa connessione federazione griglia**:
 - i. Selezionare la scheda **Federazione di griglia**.
 - ii. Seleziona **Rimuovi autorizzazione**.
 - Per aggiungere l'autorizzazione **Usa connessione federata griglia**:
 - i. Selezionare la scheda **Federazione di griglia**.
 - ii. Selezionare la casella di controllo **Usa connessione federata alla griglia**.
 - iii. Facoltativamente, seleziona **Clona utenti e gruppi locali esistenti** per clonarli nella griglia remota. Se lo desideri, puoi interrompere la clonazione in corso o riprovare se alcuni utenti o gruppi locali non sono riusciti a essere clonati dopo il completamento dell'ultima operazione di clonazione.
 - Per impostare un periodo di conservazione massimo o consentire la modalità di conformità:



Prima di poter utilizzare queste impostazioni, è necessario abilitare il blocco oggetti S3 sulla griglia.

- i. Selezionare la scheda **Blocco oggetto S3**.
- ii. Per **Imposta periodo massimo di conservazione**, immettere un valore e selezionare il periodo di tempo dal menu a discesa.
- iii. Per **Consenti modalità conformità**, seleziona la casella di controllo.

Cambia la password per l'utente root locale del tenant

Potrebbe essere necessario modificare la password per l'utente root locale di un tenant se l'utente root è bloccato fuori dall'account.

Prima di iniziare

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

Informazioni su questo compito

Se per il sistema StorageGRID è abilitato l'accesso Single Sign-On (SSO), l'utente root locale non può accedere all'account tenant. Per eseguire attività come utente root, gli utenti devono appartenere a un gruppo federato che dispone dell'autorizzazione di accesso root per il tenant.

Passi

1. Selezionare **INQUILINI**.

Tenants							
View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.							
Create	Export to CSV	Actions ▾	Search tenants by name or ID		Displaying 5 results		
☐	Name ? ↕	Logical space used ? ↕	Quota utilization ? ↕	Quota ? ↕	Object count ? ↕	Sign in/Copy URL ?	
☐	Tenant 01	2.00 GB	10%	20.00 GB	100	→ 📄	
☐	Tenant 02	85.00 GB	85%	100.00 GB	500	→ 📄	
☐	Tenant 03	500.00 TB	50%	1.00 PB	10,000	→ 📄	
☐	Tenant 04	475.00 TB	95%	500.00 TB	50,000	→ 📄	
☐	Tenant 05	5.00 GB	—	—	500	→ 📄	

2. Selezionare l'account dell'inquilino. Puoi procedere in uno dei seguenti modi:
 - Selezionare la casella di controllo per il tenant e selezionare **Azioni > Cambia password di root**.
 - Selezionare il nome del tenant per visualizzare la pagina dei dettagli e selezionare **Azioni > Modifica password root**.
3. Inserisci la nuova password per l'account tenant.
4. Seleziona **Salva**.

Elimina account inquilino

È possibile eliminare un account tenant se si desidera rimuovere definitivamente l'accesso del tenant al sistema.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Hai ["autorizzazioni di accesso specifiche"](#) .
- Sono stati rimossi tutti i bucket e gli oggetti S3 associati all'account tenant.
- Se all'inquilino è consentito utilizzare una connessione di federazione di rete, hai esaminato le considerazioni per ["eliminazione di un tenant con l'autorizzazione Usa connessione federazione griglia"](#) .

Passi

1. Selezionare **INQUILINI**.
2. Individua l'account o gli account tenant che desideri eliminare.

Utilizzare la casella di ricerca per cercare un inquilino per nome o ID inquilino.
3. Per eliminare più tenant, seleziona le caselle di controllo e seleziona **Azioni > Elimina**.
4. Per eliminare un singolo tenant, procedere in uno dei seguenti modi:
 - Selezionare la casella di controllo e selezionare **Azioni > Elimina**.
 - Selezionare il nome del tenant per visualizzare la pagina dei dettagli, quindi selezionare **Azioni > Elimina**.
5. Selezionare **Sì**.

Gestire i servizi della piattaforma

Cosa sono i servizi di piattaforma?

I servizi della piattaforma includono la replica CloudMirror, le notifiche degli eventi e il servizio di integrazione della ricerca.

Se si abilitano i servizi della piattaforma per gli account tenant S3, è necessario configurare la griglia in modo che i tenant possano accedere alle risorse esterne necessarie per utilizzare questi servizi.

Replica CloudMirror

Il servizio di replica StorageGRID CloudMirror viene utilizzato per eseguire il mirroring di oggetti specifici da un bucket StorageGRID a una destinazione esterna specificata.

Ad esempio, potresti utilizzare la replica di CloudMirror per eseguire il mirroring di record specifici dei clienti in Amazon S3 e quindi sfruttare i servizi AWS per eseguire analisi sui tuoi dati.



La replica di CloudMirror presenta alcune importanti somiglianze e differenze con la funzionalità di replica tra griglie. Per saperne di più, vedere ["Confronta la replicazione cross-grid e la replicazione CloudMirror"](#) .



La replica CloudMirror non è supportata se nel bucket di origine è abilitato S3 Object Lock.

Notifiche

Le notifiche degli eventi per bucket vengono utilizzate per inviare notifiche su azioni specifiche eseguite sugli oggetti a un cluster Kafka esterno specificato o ad Amazon Simple Notification Service.

Ad esempio, è possibile configurare l'invio di avvisi agli amministratori per ogni oggetto aggiunto a un bucket,

dove gli oggetti rappresentano file di registro associati a un evento di sistema critico.



Sebbene la notifica degli eventi possa essere configurata su un bucket con S3 Object Lock abilitato, i metadati di S3 Object Lock (inclusi gli stati Conserva fino alla data e Conservazione legale) degli oggetti non saranno inclusi nei messaggi di notifica.

Servizio di integrazione della ricerca

Il servizio di integrazione della ricerca viene utilizzato per inviare metadati di oggetti S3 a un indice Elasticsearch specificato, dove è possibile ricercare o analizzare i metadati utilizzando il servizio esterno.

Ad esempio, puoi configurare i tuoi bucket per inviare metadati di oggetti S3 a un servizio Elasticsearch remoto. Potresti quindi utilizzare Elasticsearch per effettuare ricerche tra i bucket e realizzare analisi sofisticate dei modelli presenti nei metadati degli oggetti.



Sebbene l'integrazione di Elasticsearch possa essere configurata su un bucket con S3 Object Lock abilitato, i metadati di S3 Object Lock (inclusi gli stati Retain Until Date e Legal Hold) degli oggetti non saranno inclusi nei messaggi di notifica.

I servizi della piattaforma offrono agli inquilini la possibilità di utilizzare risorse di archiviazione esterne, servizi di notifica e servizi di ricerca o analisi con i propri dati. Poiché la posizione di destinazione per i servizi della piattaforma è in genere esterna alla distribuzione StorageGRID, è necessario decidere se si desidera consentire ai tenant di utilizzare questi servizi. In tal caso, è necessario abilitare l'utilizzo dei servizi della piattaforma quando si creano o si modificano gli account tenant. È inoltre necessario configurare la rete in modo che i messaggi dei servizi della piattaforma generati dai tenant possano raggiungere le loro destinazioni.

Raccomandazioni per l'utilizzo dei servizi della piattaforma

Prima di utilizzare i servizi della piattaforma, tieni presente i seguenti consigli:

- Se in un bucket S3 del sistema StorageGRID sono abilitati sia il controllo delle versioni sia la replica CloudMirror, è necessario abilitare anche il controllo delle versioni del bucket S3 per l'endpoint di destinazione. Ciò consente alla replica CloudMirror di generare versioni di oggetti simili sull'endpoint.
- Non dovresti utilizzare più di 100 tenant attivi con richieste S3 che richiedono la replica, le notifiche e l'integrazione della ricerca di CloudMirror. Avere più di 100 tenant attivi può comportare prestazioni più lente del client S3.
- Le richieste a un endpoint che non possono essere completate verranno messe in coda fino a un massimo di 500.000 richieste. Questo limite è equamente ripartito tra gli inquilini attivi. Ai nuovi inquilini è consentito superare temporaneamente questo limite di 500.000 unità, in modo che i nuovi inquilini non vengano ingiustamente penalizzati.

Informazioni correlate

- ["Gestire i servizi della piattaforma"](#)
- ["Configurare le impostazioni del proxy di archiviazione"](#)
- ["Monitorare StorageGRID"](#)

Rete e porte per i servizi della piattaforma

Se si consente a un tenant S3 di utilizzare i servizi della piattaforma, è necessario configurare la rete per la griglia per garantire che i messaggi dei servizi della piattaforma possano essere recapitati alle rispettive destinazioni.

È possibile abilitare i servizi della piattaforma per un account tenant S3 quando si crea o si aggiorna l'account tenant. Se i servizi della piattaforma sono abilitati, il tenant può creare endpoint che fungono da destinazione per la replica di CloudMirror, le notifiche degli eventi o i messaggi di integrazione della ricerca dai suoi bucket S3. Questi messaggi dei servizi di piattaforma vengono inviati dai nodi di archiviazione che eseguono il servizio ADC agli endpoint di destinazione.

Ad esempio, i tenant potrebbero configurare i seguenti tipi di endpoint di destinazione:

- Un cluster Elasticsearch ospitato localmente
- Un'applicazione locale che supporta la ricezione di messaggi Amazon Simple Notification Service
- Un cluster Kafka ospitato localmente
- Un bucket S3 ospitato localmente sulla stessa o su un'altra istanza di StorageGRID
- Un endpoint esterno, ad esempio un endpoint su Amazon Web Services.

Per garantire che i messaggi dei servizi della piattaforma possano essere recapitati, è necessario configurare la rete o le reti contenenti i nodi di archiviazione ADC. È necessario assicurarsi che le seguenti porte possano essere utilizzate per inviare messaggi di servizi di piattaforma agli endpoint di destinazione.

Per impostazione predefinita, i messaggi dei servizi della piattaforma vengono inviati sulle seguenti porte:

- **80**: Per gli URI degli endpoint che iniziano con http (la maggior parte degli endpoint)
- **443**: Per gli URI degli endpoint che iniziano con https (la maggior parte degli endpoint)
- **9092**: Per gli URI degli endpoint che iniziano con http o https (solo endpoint Kafka)

Gli inquilini possono specificare una porta diversa quando creano o modificano un endpoint.



Se si utilizza una distribuzione StorageGRID come destinazione per la replica di CloudMirror, i messaggi di replica potrebbero essere ricevuti su una porta diversa da 80 o 443. Assicurarsi che la porta utilizzata per S3 dalla distribuzione StorageGRID di destinazione sia specificata nell'endpoint.

Se si utilizza un server proxy non trasparente, è necessario anche ["configurare le impostazioni del proxy di archiviazione"](#) per consentire l'invio di messaggi a endpoint esterni, ad esempio un endpoint su Internet.

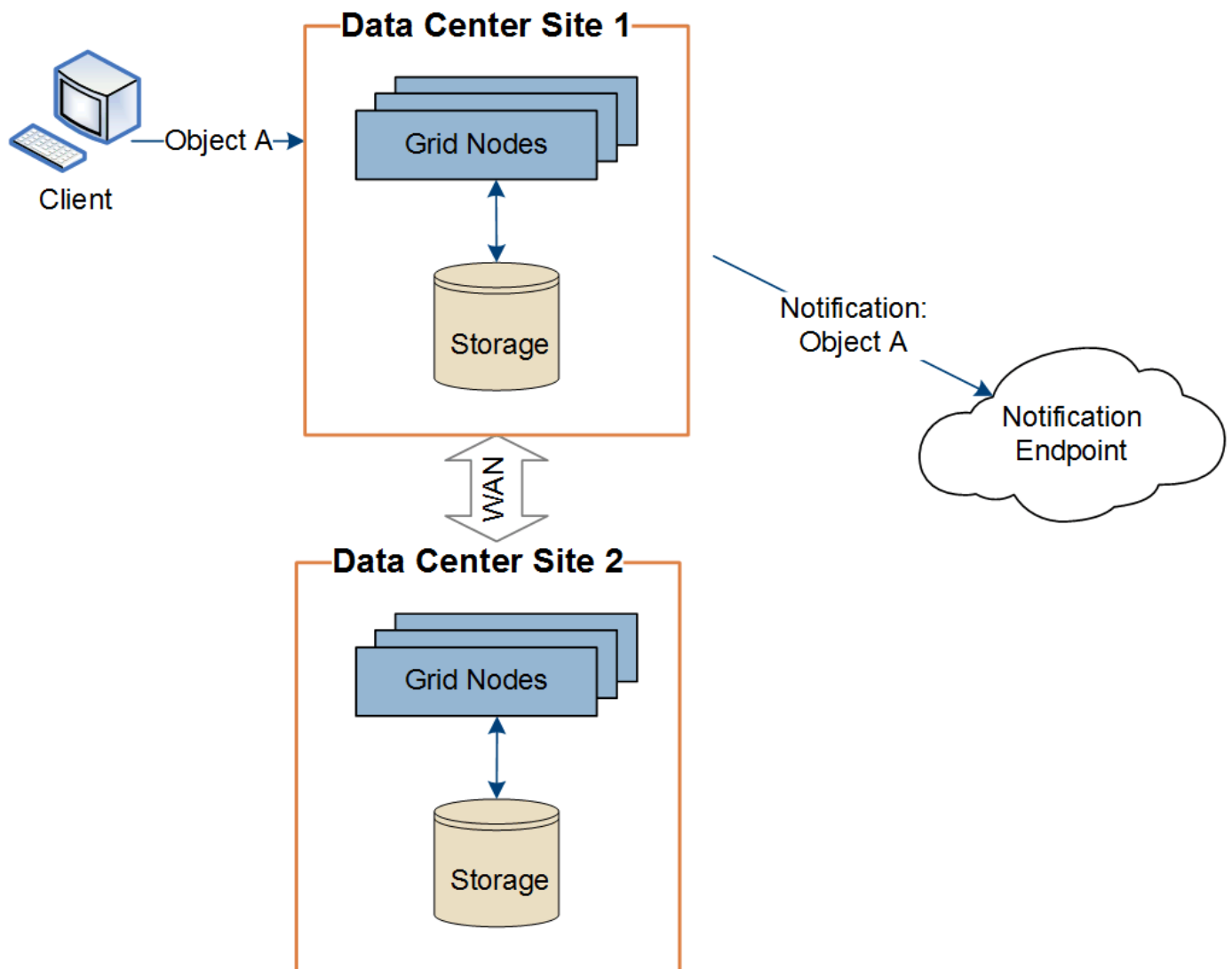
Informazioni correlate

["Utilizzare un account tenant"](#)

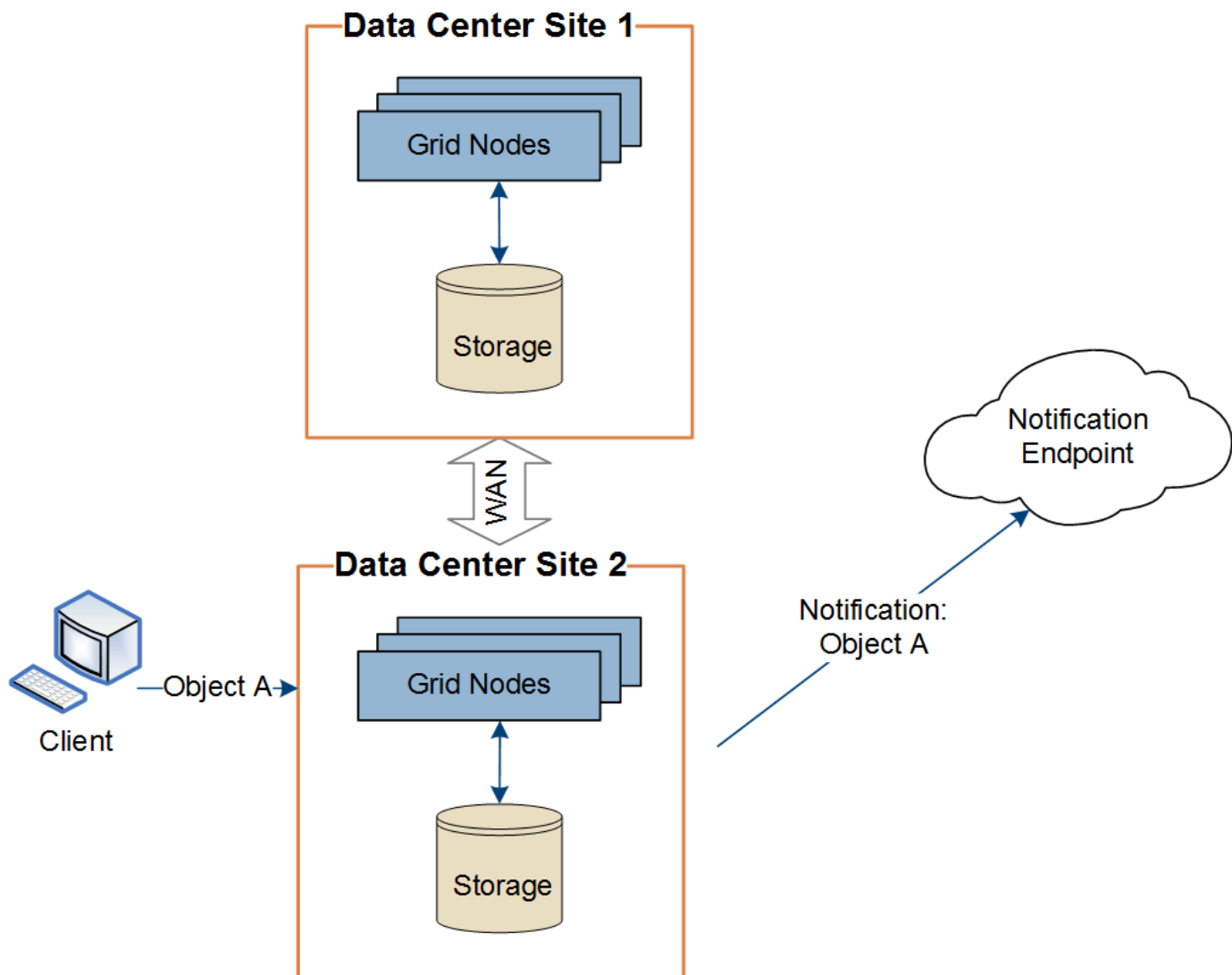
Consegna per sito di messaggi di servizi di piattaforma

Tutte le operazioni dei servizi della piattaforma vengono eseguite per ogni sito.

Ciò significa che se un tenant utilizza un client per eseguire un'operazione di creazione API S3 su un oggetto connettendosi a un nodo gateway nel sito del data center 1, la notifica relativa a tale azione viene attivata e inviata dal sito del data center 1.



Se successivamente il client esegue un'operazione di eliminazione dell'API S3 sullo stesso oggetto dal sito del Data Center 2, la notifica relativa all'azione di eliminazione viene attivata e inviata dal sito del Data Center 2.



Assicurarsi che la rete in ogni sito sia configurata in modo tale che i messaggi dei servizi della piattaforma possano essere recapitati alle rispettive destinazioni.

Risolvere i problemi dei servizi della piattaforma

Gli endpoint utilizzati nei servizi della piattaforma vengono creati e gestiti dagli utenti tenant in Tenant Manager; tuttavia, se un tenant riscontra problemi nella configurazione o nell'utilizzo dei servizi della piattaforma, è possibile utilizzare Grid Manager per risolvere il problema.

Problemi con i nuovi endpoint

Prima che un tenant possa utilizzare i servizi della piattaforma, deve creare uno o più endpoint utilizzando Tenant Manager. Ogni endpoint rappresenta una destinazione esterna per un servizio di piattaforma, ad esempio un bucket StorageGRID S3, un bucket Amazon Web Services, un argomento Amazon Simple Notification Service, un argomento Kafka o un cluster Elasticsearch ospitato localmente o su AWS. Ogni endpoint include sia la posizione della risorsa esterna sia le credenziali necessarie per accedere a tale risorsa.

Quando un tenant crea un endpoint, il sistema StorageGRID verifica che l'endpoint esista e che possa essere raggiunto utilizzando le credenziali specificate. La connessione all'endpoint viene convalidata da un nodo in ogni sito.

Se la convalida dell'endpoint fallisce, un messaggio di errore ne spiega il motivo. L'utente tenant dovrebbe risolvere il problema, quindi provare a creare nuovamente l'endpoint.



La creazione dell'endpoint non riuscirà se i servizi della piattaforma non sono abilitati per l'account tenant.

Problemi con gli endpoint esistenti

Se si verifica un errore quando StorageGRID tenta di raggiungere un endpoint esistente, viene visualizzato un messaggio nella dashboard di Tenant Manager.



One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

Gli utenti tenant possono andare alla pagina Endpoint per esaminare il messaggio di errore più recente per ciascun endpoint e per determinare quanto tempo fa si è verificato l'errore. La colonna **Ultimo errore** visualizza il messaggio di errore più recente per ciascun endpoint e indica da quanto tempo si è verificato l'errore. Errori che includono il  l'icona si è verificata negli ultimi 7 giorni.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.



One or more endpoints have experienced an error. Select the endpoint for more details about the error. Meanwhile, the platform service request will be retried automatically.

5 endpoints

Create endpoint

Delete endpoint

☐	Display name  	Last error  	Type  	URI  	URN  
☐	my-endpoint-2	 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es::mydomain/sveloso/_doc
☐	my-endpoint-3	 3 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
☐	my-endpoint-5	12 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example3
☐	my-endpoint-4		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example2
☐	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1



Alcuni messaggi di errore nella colonna **Ultimo errore** potrebbero includere un logID tra parentesi. Un amministratore di rete o il supporto tecnico possono utilizzare questo ID per individuare informazioni più dettagliate sull'errore nel file bycast.log.

Problemi relativi ai server proxy

Se hai configurato un "[proxy di archiviazione](#)" tra i nodi di archiviazione e gli endpoint del servizio di piattaforma, potrebbero verificarsi errori se il servizio proxy non consente messaggi da StorageGRID. Per risolvere questi problemi, controlla le impostazioni del tuo server proxy per assicurarti che i messaggi relativi ai servizi della piattaforma non siano bloccati.

Determina se si è verificato un errore

Se si sono verificati errori dell'endpoint negli ultimi 7 giorni, la dashboard in Tenant Manager visualizza un messaggio di avviso. Puoi andare alla pagina Endpoint per vedere maggiori dettagli sull'errore.

Le operazioni del client falliscono

Alcuni problemi relativi ai servizi della piattaforma potrebbero causare il fallimento delle operazioni client sul bucket S3. Ad esempio, le operazioni del client S3 non riusciranno se il servizio RSM (Replicated State Machine) interno si arresta o se sono presenti troppi messaggi dei servizi della piattaforma in coda per la consegna.

Per verificare lo stato dei servizi:

1. Selezionare **SUPPORTO > Strumenti > Topologia griglia**.
2. Selezionare **sito > Nodo di archiviazione > SSM > Servizi**.

Errori di endpoint recuperabili e irrecuperabili

Dopo la creazione degli endpoint, possono verificarsi errori nella richiesta del servizio di piattaforma per vari motivi. Alcuni errori sono recuperabili con l'intervento dell'utente. Ad esempio, gli errori recuperabili potrebbero verificarsi per i seguenti motivi:

- Le credenziali dell'utente sono state eliminate o sono scadute.
- Il bucket di destinazione non esiste.
- La notifica non può essere recapitata.

Se StorageGRID riscontra un errore recuperabile, la richiesta del servizio di piattaforma verrà ripetuta finché non avrà esito positivo.

Altri errori non sono recuperabili. Ad esempio, se l'endpoint viene eliminato, si verifica un errore irrecuperabile.

Se StorageGRID riscontra un errore di endpoint irreversibile:

- In Grid Manager, vai su **Supporto > Strumenti > Metriche > Grafana > Panoramica dei servizi della piattaforma** per visualizzare i dettagli dell'errore.
- In Tenant Manager, vai su **STORAGE (S3) > Platform Services Endpoints** per visualizzare i dettagli dell'errore.
- Controlla il `/var/local/log/bycast-err.log` per errori correlati. I nodi di archiviazione dotati del servizio ADC contengono questo file di registro.

I messaggi dei servizi della piattaforma non possono essere recapitati

Se la destinazione riscontra un problema che le impedisce di accettare i messaggi dei servizi della piattaforma, l'operazione client sul bucket riesce, ma il messaggio dei servizi della piattaforma non viene recapitato. Ad esempio, questo errore potrebbe verificarsi se le credenziali vengono aggiornate sulla destinazione in modo

tale che StorageGRID non possa più autenticarsi al servizio di destinazione.

Controlla gli avvisi correlati.

Prestazioni più lente per le richieste di servizi della piattaforma

Il software StorageGRID potrebbe limitare le richieste S3 in arrivo per un bucket se la velocità con cui vengono inviate le richieste supera la velocità con cui l'endpoint di destinazione può riceverle. La limitazione si verifica solo quando è presente un arretrato di richieste in attesa di essere inviate all'endpoint di destinazione.

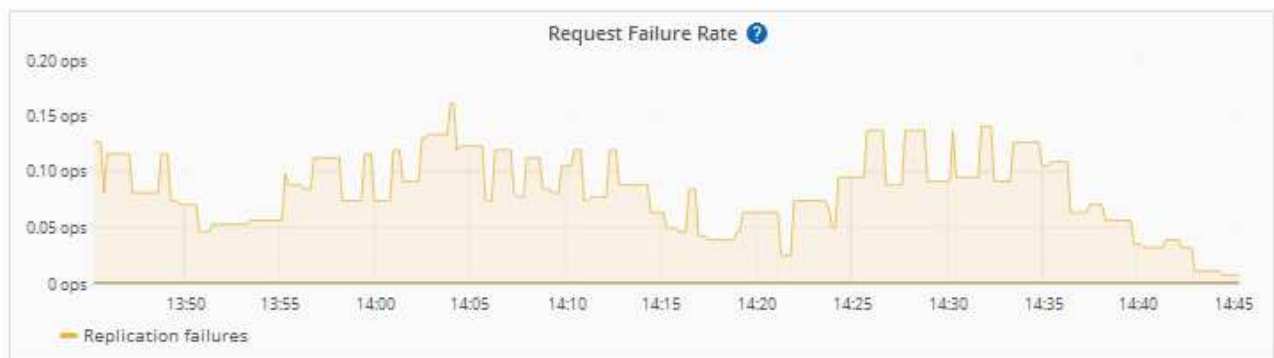
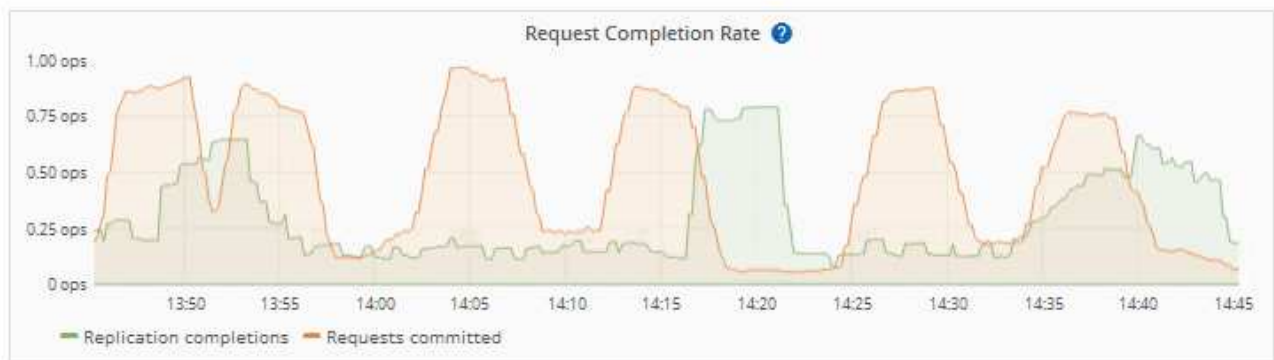
L'unico effetto visibile è che le richieste S3 in arrivo impiegheranno più tempo per essere eseguite. Se si inizia a rilevare un rallentamento significativo delle prestazioni, è opportuno ridurre la velocità di acquisizione o utilizzare un endpoint con capacità maggiore. Se l'arretrato di richieste continua ad aumentare, le operazioni S3 del client (come le richieste PUT) alla fine falliranno.

Le richieste CloudMirror hanno maggiori probabilità di essere influenzate dalle prestazioni dell'endpoint di destinazione, perché in genere comportano un trasferimento di dati maggiore rispetto alle richieste di integrazione della ricerca o di notifica degli eventi.

Le richieste di servizio della piattaforma falliscono

Per visualizzare il tasso di errore delle richieste per i servizi della piattaforma:

1. Selezionare **NODES**.
2. Seleziona **site > Servizi piattaforma**.
3. Visualizza il grafico del tasso di errore delle richieste.



Avviso di servizi di piattaforma non disponibili

L'avviso **Servizi di piattaforma non disponibili** indica che non è possibile eseguire alcuna operazione di servizio di piattaforma in un sito perché sono in esecuzione o disponibili troppi pochi nodi di archiviazione con il servizio RSM.

Il servizio RSM garantisce che le richieste di servizio della piattaforma vengano inviate ai rispettivi endpoint.

Per risolvere questo avviso, determinare quali nodi di archiviazione nel sito includono il servizio RSM. (Il servizio RSM è presente sui nodi di archiviazione che includono anche il servizio ADC.) Quindi, assicurarsi che la maggioranza semplice di tali nodi di archiviazione sia in esecuzione e disponibile.



Se più di un nodo di archiviazione contenente il servizio RSM si guasta in un sito, si perdono tutte le richieste di servizio della piattaforma in sospeso per quel sito.

Ulteriori indicazioni per la risoluzione dei problemi per gli endpoint dei servizi della piattaforma

Per ulteriori informazioni vedere [Utilizzare un account tenant](#) › [Risoluzione dei problemi degli endpoint dei servizi della piattaforma](#).

Informazioni correlate

["Risoluzione dei problemi del sistema StorageGRID"](#)

Gestisci S3 Select per gli account tenant

È possibile consentire a determinati tenant S3 di utilizzare S3 Select per inviare richieste `SelectObjectContent` su singoli oggetti.

S3 Select offre un modo efficiente per effettuare ricerche in grandi quantità di dati senza dover implementare un database e le risorse associate per abilitare le ricerche. Riduce inoltre i costi e la latenza del recupero dei dati.

Che cos'è S3 Select?

S3 Select consente ai client S3 di utilizzare le richieste `SelectObjectContent` per filtrare e recuperare solo i dati necessari da un oggetto. L'implementazione StorageGRID di S3 Select include un sottoinsieme di comandi e funzionalità di S3 Select.

Considerazioni e requisiti per l'utilizzo di S3 Select

Requisiti di amministrazione della rete

L'amministratore della rete deve concedere ai tenant la capacità S3 Select. Seleziona **Consenti selezione S3** quando ["creazione di un inquilino"](#) o ["modifica di un inquilino"](#).

Requisiti del formato dell'oggetto

L'oggetto che si desidera interrogare deve essere in uno dei seguenti formati:

- **CSV.** Può essere utilizzato così com'è o compresso in archivi GZIP o BZIP2.
- **Parquet.** Requisiti aggiuntivi per gli oggetti Parquet:
 - S3 Select supporta solo la compressione colonnare tramite GZIP o Snappy. S3 Select non supporta la compressione dell'intero oggetto per gli oggetti Parquet.
 - S3 Select non supporta l'output Parquet. È necessario specificare il formato di output come CSV o JSON.
 - La dimensione massima del gruppo di righe non compresso è 512 MB.
 - È necessario utilizzare i tipi di dati specificati nello schema dell'oggetto.
 - Non è possibile utilizzare i tipi logici INTERVAL, JSON, LIST, TIME o UUID.

Requisiti dell'endpoint

La richiesta `SelectObjectContent` deve essere inviata a un ["Endpoint del bilanciamento del carico StorageGRID"](#).

I nodi Admin e Gateway utilizzati dall'endpoint devono essere uno dei seguenti:

- Un nodo di appliance di servizi
- Un nodo software basato su VMware
- Un nodo bare metal che esegue un kernel con cgroup v2 abilitato

Considerazioni generali

Le query non possono essere inviate direttamente ai nodi di archiviazione.



Le richieste SelectObjectContent possono ridurre le prestazioni del bilanciatore del carico per tutti i client S3 e tutti i tenant. Abilitare questa funzionalità solo quando necessario e solo per i tenant attendibili.

Vedi il ["istruzioni per l'uso di S3 Select"](#).

Per visualizzare ["Grafici Grafana"](#) per le operazioni di selezione S3 nel tempo, selezionare **SUPPORTO > Strumenti > Metriche** in Grid Manager.

Configurare le connessioni client

Configurare le connessioni client S3

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



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

Attività di configurazione

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

Compiti richiesti

È necessario ottenere:

- indirizzi IP
- Nomi di dominio
- Certificato SSL

Attività facoltative

Facoltativamente, configurare:

- Federazione delle identità
- SSO

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

Utilizzare la procedura guidata di configurazione S3

Seguire i passaggi della procedura guidata di configurazione S3.

Configurare manualmente

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

1. Utilizzare l'applicazione S3 per completare la connessione a StorageGRID. Crea voci DNS per associare gli indirizzi IP a tutti i nomi di dominio che intendi utilizzare.

Se necessario, eseguire ulteriori configurazioni dell'applicazione.

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

Informazioni necessarie per collegare StorageGRID a un'applicazione client

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

Di quali valori ho bisogno?

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

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

Valore	Dove è configurato il valore	Dove viene utilizzato il valore
Nome del bucket/contenitore	StorageGRID > Tenant e bucket	Applicazione client

Come posso ottenere questi valori?

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

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



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

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



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

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

Sicurezza per i client S3

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

Riepilogo

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

Sicurezza della connessione

TLS

Autenticazione del server

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

Autenticazione del client

ID chiave di accesso all'account S3 e chiave di accesso segreta

Autorizzazione del cliente

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

Come StorageGRID fornisce sicurezza per le applicazioni client

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

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

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

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

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

HTTPS è il protocollo predefinito ed è consigliato.

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

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

Certificati di sicurezza e applicazioni client

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

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

Vedere ["Considerazioni sul bilanciamento del carico"](#) .

- Quando le applicazioni client si connettono direttamente a un nodo di archiviazione, utilizzano i certificati server generati dal sistema per i nodi di archiviazione al momento dell'installazione del sistema StorageGRID (firmati dall'autorità di certificazione del sistema) oppure un singolo certificato server personalizzato fornito per la griglia da un amministratore della griglia. Vedere ["aggiungi un certificato API S3 personalizzato"](#) .

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

Algoritmi di hashing e crittografia supportati per le librerie TLS

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

Versioni supportate di TLS

StorageGRID supporta TLS 1.2 e TLS 1.3.



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

Utilizzare la procedura guidata di configurazione S3

Utilizzare la procedura guidata di configurazione S3: considerazioni e requisiti

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

Quando utilizzare la procedura guidata di configurazione S3

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

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

Prima di utilizzare la procedura guidata

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

Ottenere indirizzi IP e configurare le interfacce VLAN

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

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

Configurare la federazione delle identità e SSO

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

Ottieni e configura i nomi di dominio

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

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

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

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

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

Configurare tutte le connessioni della federazione di griglia

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

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

Accedi e completa la procedura guidata di configurazione S3

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

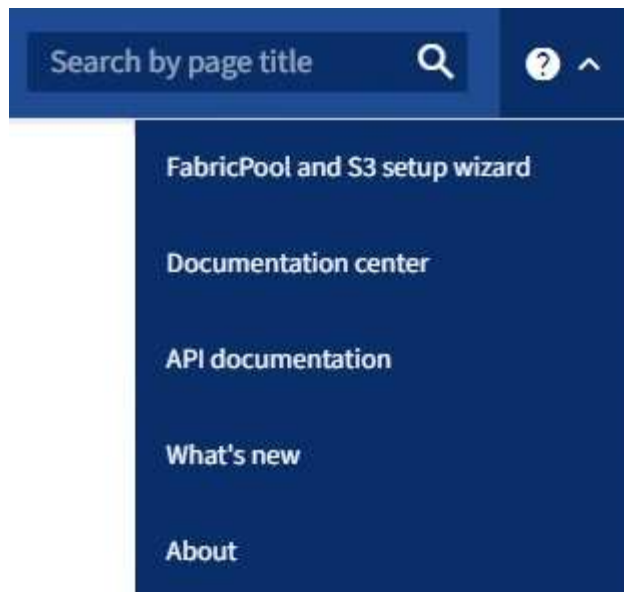
Prima di iniziare

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

Accedi alla procedura guidata

Passi

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



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

Passaggio 1 di 6: configurare il gruppo HA

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

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

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

Passi

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

Crea gruppo HA

- a. Per creare un nuovo gruppo HA, seleziona **Crea gruppo HA**.
- b. Per la fase **Inserisci dettagli**, compila i seguenti campi.

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

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

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

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

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

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

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

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

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

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

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

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

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

Utilizzare il gruppo HA esistente

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

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

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

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

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

Per i dettagli su questa attività, vedere "[Considerazioni sul bilanciamento del carico](#)".

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

Crea endpoint

Passi

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

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint.
Porta	La porta StorageGRID che si desidera utilizzare per il bilanciamento del carico. Per impostazione predefinita, questo campo è impostato su 10433 per il primo endpoint creato, ma è possibile immettere qualsiasi porta esterna non utilizzata. Se si immette 80 o 443, l'endpoint viene configurato solo sui nodi gateway, perché queste porte sono riservate sui nodi amministrativi. Nota: non sono consentite le porte utilizzate da altri servizi di rete. Vedi il "Riferimento porta di rete".
Tipo di cliente	Deve essere S3 .
Protocollo di rete	Selezionare HTTPS. Nota: la comunicazione con StorageGRID senza crittografia TLS è supportata ma non consigliata.

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

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

Modalità	Descrizione
Tipo di nodo	In base al tipo di nodo selezionato, i client devono utilizzare l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di amministrazione oppure l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo gateway per accedere a questo endpoint.

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

Campo	Descrizione
Consenti tutti i tenant (predefinito)	Tutti gli account tenant possono utilizzare questo endpoint per accedere ai propri bucket.
Consenti inquilini selezionati	Solo gli account tenant selezionati possono utilizzare questo endpoint per accedere ai propri bucket.
Blocca gli inquilini selezionati	Gli account tenant selezionati non possono utilizzare questo endpoint per accedere ai propri bucket. Tutti gli altri tenant possono utilizzare questo endpoint.

5. Per il passaggio **Allega certificato**, seleziona una delle seguenti opzioni:

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

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

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



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

Utilizzare l'endpoint del bilanciatore del carico esistente

Passi

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

Utilizzare un bilanciatore di carico esterno

Passi

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

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

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

Passaggio 3 di 6: creare tenant e bucket

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

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

Per i dettagli su questa attività, vedere ["Crea un account inquilino"](#) e ["Crea bucket S3"](#).

Passi

1. Inserisci un nome per l'account tenant.

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

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

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

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

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

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

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



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

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

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

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

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

- Seleziona **Crea e continua**.

Passaggio 4 di 6: Scarica i dati

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

Passi

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



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

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

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

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

Passi

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

Fase 6 di 6: Riepilogo della revisione

Passi

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

Gestire i gruppi HA

Cosa sono i gruppi ad alta disponibilità (HA)?

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

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

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

- I gruppi HA che includono nodi gateway, nodi amministrativi o entrambi forniscono connessioni dati ad alta disponibilità per i client S3.
- I gruppi HA che includono solo nodi amministrativi forniscono connessioni ad alta disponibilità al Grid Manager e al Tenant Manager.
- Un gruppo HA che include solo appliance di servizi e nodi software basati su VMware può fornire connessioni ad alta disponibilità per ["Tenant S3 che utilizzano S3 Select"](#) . I gruppi HA sono consigliati quando si utilizza S3 Select, ma non sono obbligatori.

Come si crea un gruppo HA?

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



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

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

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

Qual è l'interfaccia attiva?

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

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

Visualizza lo stato attuale del gruppo HA di un nodo

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

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

- **Attivo:** il gruppo HA è attualmente ospitato su questo nodo.
- **Backup:** il gruppo HA non sta attualmente utilizzando questo nodo; questa è un'interfaccia di backup.
- **Arrestato:** il gruppo HA non può essere ospitato su questo nodo perché il servizio High Availability (keepalived) è stato arrestato manualmente.
- **Errore:** il gruppo HA non può essere ospitato su questo nodo a causa di uno o più dei seguenti motivi:
 - Il servizio Load Balancer (nginx-gw) non è in esecuzione sul nodo.
 - L'interfaccia eth0 o VIP del nodo è inattiva.
 - Il nodo è inattivo.

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

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 fallisce?

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

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

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



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

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

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

Come vengono utilizzati i gruppi HA?

È possibile utilizzare gruppi ad alta disponibilità (HA) per fornire connessioni ad alta disponibilità a StorageGRID per i dati degli oggetti e per uso amministrativo.

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

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

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

Scopo del gruppo HA	Aggiungi nodi di questo tipo al gruppo HA
Accesso a Grid Manager	• Nodo amministratore primario (Primario) • Nodi amministrativi non primari Nota: il nodo di amministrazione primario deve essere l'interfaccia primaria. Alcune procedure di manutenzione possono essere eseguite solo dal nodo di amministrazione primario.
Accesso solo al Tenant Manager	• Nodi amministrativi primari o non primari
Accesso client S3 - Servizio Load Balancer	• Nodi amministrativi • Nodi gateway
Accesso client S3 per "S3 Seleziona"	• Servizi elettrodomestici • Nodi software basati su VMware Nota: i gruppi HA sono consigliati quando si utilizza S3 Select, ma non sono obbligatori.

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

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

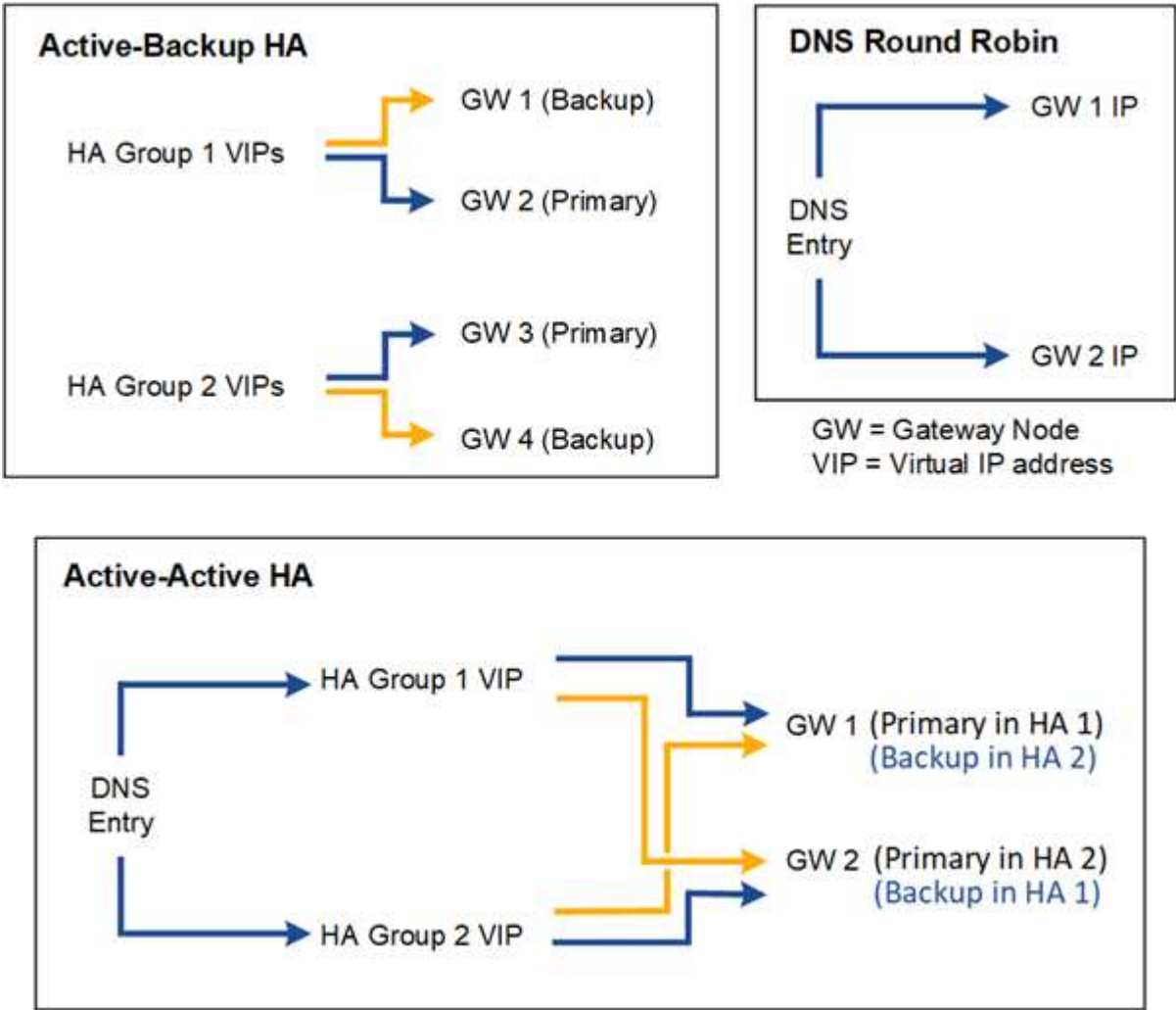
Se hai effettuato l'accesso a Grid Manager o Tenant Manager quando si verifica il failover, verrai disconnesso e dovrai effettuare nuovamente l'accesso per riprendere l'attività.

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

Opzioni di configurazione per i gruppi HA

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

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



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

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

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

Configurare gruppi ad alta disponibilità

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

Prima di iniziare

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

Creare un gruppo ad alta disponibilità

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

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

Accedi alla procedura guidata

Passi

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

2. Seleziona **Crea**.

Inserisci i dettagli per il gruppo HA

Passi

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

Aggiungere interfacce al gruppo HA

Passi

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

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

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
☐	DC1-ADM1-104-96	eth0	DC1	10.96.104.0/22	Primary Admin Node
☐	DC1-ADM1-104-96	eth2	DC1	—	Primary Admin Node
☐	DC2-ADM1-104-103	eth0	DC2	10.96.104.0/22	Admin Node
☐	DC2-ADM1-104-103	eth2	DC2	—	Admin Node

0 interfaces selected



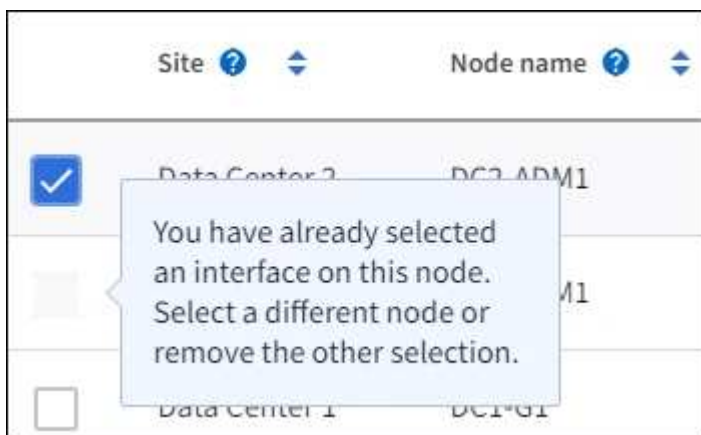
Dopo aver creato un'interfaccia VLAN, attendere fino a 5 minuti affinché la nuova interfaccia venga visualizzata nella tabella.

Linee guida per la selezione delle interfacce

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

che se si verifica un failover, i servizi forniti dal nodo precedentemente attivo potrebbero non essere disponibili sul nodo nuovamente attivo. Ad esempio, un nodo gateway di backup non può fornire protezione HA dei servizi del nodo amministrativo. Allo stesso modo, un Admin Node di backup non può eseguire tutte le procedure di manutenzione che può fornire il Admin Node primario.

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



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

2. Selezionare **Continua**.

Determinare l'ordine di priorità

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

Passi

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

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

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.

2. Selezionare **Continua**.

Inserisci gli indirizzi IP

Passi

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

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



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

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

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

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

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

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

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

Prossimi passi

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

Modifica un gruppo ad alta disponibilità

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

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

Passi

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

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

2. Selezionare la casella di controllo per il gruppo HA che si desidera modificare.

3. A seconda di cosa vuoi aggiornare, procedi in uno dei seguenti modi:

- Selezionare **Azioni > Modifica indirizzo IP virtuale** per aggiungere o rimuovere indirizzi VIP.
- Selezionare **Azioni > Modifica gruppo HA** per aggiornare il nome o la descrizione del gruppo, aggiungere o rimuovere interfacce, modificare l'ordine di priorità o aggiungere o rimuovere indirizzi VIP.

4. Se hai selezionato **Modifica indirizzo IP virtuale**:

- a. Aggiornare gli indirizzi IP virtuali per il gruppo HA.
- b. Seleziona **Salva**.
- c. Selezionare **Fine**.

5. Se hai selezionato **Modifica gruppo HA**:

- a. Facoltativamente, aggiorna il nome o la descrizione del gruppo.
- b. Facoltativamente, seleziona o deseleziona le caselle di controllo per aggiungere o rimuovere le interfacce.



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

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

Rimuovere un gruppo ad alta disponibilità

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



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

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

Passi

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

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

Gestire il bilanciamento del carico

Considerazioni sul bilanciamento del carico

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

Che cos'è il bilanciamento del carico?

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

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

Il servizio Load Balancer su ciascun nodo funziona in modo indipendente quando inoltra il traffico client ai nodi di archiviazione. Attraverso un processo di ponderazione, il servizio Load Balancer indirizza più richieste ai

nodi di archiviazione con maggiore disponibilità della CPU.



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

Di quanti nodi di bilanciamento del carico ho bisogno?

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

Che cos'è un endpoint di bilanciamento del carico?

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

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

- ["Configurare gli endpoint del bilanciatore del carico"](#)
- ["Utilizzare la procedura guidata di configurazione S3"](#)
- ["Utilizzare la procedura guidata di configurazione FabricPool"](#)

Considerazioni per il porto

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

Non sono consentite le porte utilizzate da altri servizi di rete. Vedi il ["Riferimento porta di rete"](#).

Considerazioni sul protocollo di rete

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

Considerazioni sui certificati degli endpoint del bilanciatore del carico

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

- **Carica un certificato firmato (consigliato).** Questo certificato può essere firmato da un'autorità di certificazione (CA) pubblica o privata. La procedura consigliata per proteggere la connessione è quella di utilizzare un certificato del server CA pubblicamente attendibile. A differenza dei certificati generati, i certificati firmati da una CA possono essere ruotati senza interruzioni, il che può aiutare a evitare problemi di scadenza.

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

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

Di quali valori ho bisogno?

Per creare il certificato, è necessario conoscere tutti i nomi di dominio e gli indirizzi IP che le applicazioni client S3 utilizzeranno per accedere all'endpoint.

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

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

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

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

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



Se si utilizzano caratteri jolly per i nomi di dominio, rivedere il "[Linee guida per il rafforzamento dei certificati del server](#)".

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

Come posso gestire i certificati in scadenza?



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

Per evitare problemi di scadenza dei certificati, seguire queste best practice:

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

Considerazioni sulla modalità di rilegatura

La modalità di associazione consente di controllare quali indirizzi IP possono essere utilizzati per accedere a un endpoint del bilanciatore del carico. Se un endpoint utilizza una modalità di associazione, le applicazioni client possono accedere all'endpoint solo se utilizzano un indirizzo IP consentito o il corrispondente nome di dominio completo (FQDN). Le applicazioni client che utilizzano un altro indirizzo IP o FQDN non possono accedere all'endpoint.

È possibile specificare una qualsiasi delle seguenti modalità di associazione:

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

Considerazioni sull'accesso degli inquilini

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

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



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

Esempio di accesso dell'inquilino

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

1. Hai creato due endpoint del bilanciatore del carico, come segue:
 - Endpoint **pubblico**: utilizza la porta 10443 e consente l'accesso a tutti i tenant.
 - Endpoint **Top secret**: utilizza la porta 10444 e consente l'accesso solo al tenant **Top secret**. A tutti gli altri tenant è impedito l'accesso a questo endpoint.
2. IL `top-secret.pdf` si trova in un bucket di proprietà del tenant **Top secret**.

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

disponibilità della CPU

Il servizio Load Balancer su ciascun nodo amministrativo e nodo gateway funziona in modo indipendente quando inoltra il traffico S3 ai nodi di archiviazione. Attraverso un processo di ponderazione, il servizio Load Balancer indirizza più richieste ai nodi di archiviazione con maggiore disponibilità della CPU. Le informazioni sul carico della CPU del nodo vengono aggiornate ogni pochi minuti, ma la ponderazione potrebbe essere aggiornata più frequentemente. A tutti i nodi di archiviazione viene assegnato un valore di peso di base minimo, anche se un nodo segnala un utilizzo del 100% o non segnala il proprio utilizzo.

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

Configurare gli endpoint del bilanciatore del carico

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



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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["Permesso di accesso root"](#).
- Hai esaminato il ["considerazioni per il bilanciamento del carico"](#).
- Se in precedenza hai rimappato una porta che intendi utilizzare per l'endpoint del bilanciatore del carico, hai ["rimosso il rimappaggio della porta"](#).
- Hai creato tutti i gruppi ad alta disponibilità (HA) che intendi utilizzare. I gruppi HA sono consigliati, ma non obbligatori. Vedere ["Gestire gruppi ad alta disponibilità"](#).
- Se l'endpoint del bilanciatore del carico verrà utilizzato da ["Tenant S3 per S3 Select"](#), non deve utilizzare gli indirizzi IP o i nomi di dominio completi di alcun nodo bare-metal. Per gli endpoint del bilanciatore del carico utilizzati per S3 Select sono consentiti solo appliance di servizi e nodi software basati su VMware.

- Hai configurato tutte le interfacce VLAN che intendi utilizzare. Vedere ["Configurare le interfacce VLAN"](#) .
- Se si sta creando un endpoint HTTPS (consigliato), si dispone delle informazioni per il certificato del server.



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

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

Creare un endpoint del bilanciatore del carico

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

Accedi alla procedura guidata

Passi

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

Inserisci i dettagli dell'endpoint

Passi

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

Client S3 o Swift

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

Interfaccia di gestione

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint, che apparirà nella tabella nella pagina Endpoint del bilanciatore del carico.
Porta	La porta StorageGRID che si desidera utilizzare per accedere a Grid Manager, Tenant Manager o entrambi. • Responsabile della griglia: 8443 • Responsabile dell'affitto: 9443 • Sia il gestore della griglia che il gestore dell'inquilino: 443 Nota: è possibile utilizzare queste porte preimpostate o altre porte disponibili.
Tipo di interfaccia	Selezionare il pulsante di opzione per l'interfaccia StorageGRID a cui si accederà tramite questo endpoint.

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

1. Selezionare **Continua**.

Seleziona una modalità di rilegatura

Passi

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

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

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

Se più endpoint utilizzano la stessa porta, StorageGRID utilizza questo ordine di priorità per decidere quale endpoint utilizzare: **IP virtuali dei gruppi HA** > **Interfacce nodo** > **Tipo di nodo** > **Globale**.

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

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

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

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

Controlla l'accesso degli inquilini



Un endpoint dell'interfaccia di gestione può controllare l'accesso del tenant solo quando l'endpoint ha [tipo di interfaccia di Tenant Manager](#).

Passi

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

Campo	Descrizione
Consenti tutti i tenant (predefinito)	Tutti gli account tenant possono utilizzare questo endpoint per accedere ai propri bucket. È necessario selezionare questa opzione se non è ancora stato creato alcun account tenant. Dopo aver aggiunto gli account tenant, puoi modificare l'endpoint del bilanciatore del carico per consentire o bloccare account specifici.
Consenti inquilini selezionati	Solo gli account tenant selezionati possono utilizzare questo endpoint per accedere ai propri bucket.
Blocca gli inquilini selezionati	Gli account tenant selezionati non possono utilizzare questo endpoint per accedere ai propri bucket. Tutti gli altri tenant possono utilizzare questo endpoint.

2. Se si crea un endpoint **HTTP**, non è necessario allegare un certificato. Selezionare **Crea** per aggiungere il nuovo endpoint del bilanciatore del carico. Poi vai a [Dopo aver finito](#). Altrimenti, seleziona **Continua** per allegare il certificato.

Allega il certificato

Passi

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

Il certificato protegge le connessioni tra i client S3 e il servizio Load Balancer sui nodi di amministrazione o sui nodi gateway.

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

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

- **Utilizzare il certificato dell'interfaccia di gestione.** Selezionare questa opzione se si desidera utilizzare il certificato dell'interfaccia di gestione globale, che può essere utilizzato anche per le connessioni dirette ai nodi di amministrazione.

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

Carica il certificato

- a. Seleziona **Carica certificato**.
- b. Carica i file del certificato del server richiesti:
 - **Certificato del server**: file del certificato del server personalizzato in codifica PEM.
 - **Chiave privata del certificato**: file della chiave privata del certificato del server personalizzato(`.key`).



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

- **Bundle CA**: un singolo file facoltativo contenente i certificati di ciascuna autorità di certificazione (CA) emittente intermedia. Il file dovrebbe contenere ciascuno dei file di certificato CA codificati in PEM, concatenati nell'ordine della catena di certificati.
- c. Espandi **Dettagli certificato** per visualizzare i metadati di ciascun certificato caricato. Se hai caricato un bundle CA facoltativo, ogni certificato verrà visualizzato in una scheda separata.
 - Selezionare **Scarica certificato** per salvare il file del certificato oppure selezionare **Scarica bundle CA** per salvare il bundle del certificato.

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

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copia certificato PEM** o **Copia pacchetto CA PEM** per copiare il contenuto del certificato e incollarlo altrove.
- d. Seleziona **Crea**. + L'endpoint del bilanciatore del carico è stato creato. Il certificato personalizzato viene utilizzato per tutte le nuove connessioni successive tra i client S3 o l'interfaccia di gestione e l'endpoint.

Genera certificato

- a. Seleziona **Genera certificato**.
- b. Specificare le informazioni del certificato:

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

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

c. Seleziona **Genera**.

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

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

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

Ad esempio: `storagegrid_certificate.pem`

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

e. Seleziona **Crea**.

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

Dopo aver finito

Passi

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

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

- Se hai configurato un gruppo HA, i client si connetteranno agli indirizzi IP virtuali di quel gruppo HA.
- Se non si utilizza un gruppo HA, i client si connetteranno al servizio StorageGRID Load Balancer utilizzando l'indirizzo IP di un nodo gateway o di un nodo amministrativo.

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

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

- Numero di porta

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

Visualizza e modifica gli endpoint del bilanciatore del carico

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

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

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 Endpoint del bilanciatore del carico.



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



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

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

Rimuovere gli endpoint del bilanciatore del carico

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



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



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

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

Configurare i nomi di dominio degli endpoint S3

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



L'utilizzo di un indirizzo IP per un nome di dominio endpoint non è supportato. Le versioni future impediranno questa configurazione.

Prima di iniziare

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



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

Informazioni su questo compito

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

- Utilizzare Grid Manager per aggiungere i nomi di dominio degli endpoint S3 al sistema StorageGRID.
- Assicurarsi che il "[certificato utilizzato dal client per le connessioni HTTPS a StorageGRID](#)" è firmato per

tutti i nomi di dominio richiesti dal cliente.

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

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



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

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

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



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

Aggiungi un nome di dominio dell'endpoint S3

Passi

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

Risultato

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

Rinominare un nome di dominio dell'endpoint S3

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

Passi

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

Elimina un nome di dominio dell'endpoint S3

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

Passi

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

Informazioni correlate

- ["Utilizzare l'API REST S3"](#)
- ["Visualizza gli indirizzi IP"](#)
- ["Configurare gruppi ad alta disponibilità"](#)

Riepilogo: indirizzi IP e porte per le connessioni client

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

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

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

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

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

URL di esempio

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

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

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

`https://192.0.2.5:10443`

Dove trovare gli indirizzi IP

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

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

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



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

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



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

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

Gestire reti e connessioni

Configurare le impostazioni di rete

È possibile configurare varie impostazioni di rete da Grid Manager per ottimizzare il funzionamento del sistema StorageGRID .

Configurare le interfacce VLAN

Puoi ["creare interfacce LAN virtuali \(VLAN\)"](#) per isolare e partizionare il traffico per garantire sicurezza, flessibilità e prestazioni. Ogni interfaccia VLAN è associata a una o più interfacce padre sui nodi amministrativi e sui nodi gateway. È possibile utilizzare le interfacce VLAN nei gruppi HA e negli endpoint del bilanciatore del carico per separare il traffico client o amministrativo in base all'applicazione o al tenant.

Politiche di classificazione del traffico

Puoi usare ["politiche di classificazione del traffico"](#) per identificare e gestire diversi tipi di traffico di rete, incluso il traffico correlato a bucket, tenant, subnet client o endpoint del bilanciatore del carico specifici. Queste politiche possono aiutare a limitare e monitorare il traffico.

Linee guida per le reti StorageGRID

È possibile utilizzare Grid Manager per configurare e gestire le reti e le connessioni StorageGRID .

Vedere ["Configurare le connessioni client S3"](#) per imparare a connettere i client S3.

Reti StorageGRID predefinite

Per impostazione predefinita, StorageGRID supporta tre interfacce di rete per nodo della griglia, consentendo di configurare la rete per ogni singolo nodo della griglia in base ai requisiti di sicurezza e accesso.

Per ulteriori informazioni sulla topologia di rete, vedere ["Linee guida per il networking"](#) .

Rete a griglia

Necessario. La rete Grid viene utilizzata per tutto il traffico StorageGRID interno. Fornisce connettività tra tutti i nodi della griglia, in tutti i siti e le sottoreti.

Rete di amministrazione

Opzionale. La rete di amministrazione viene solitamente utilizzata per l'amministrazione e la manutenzione del sistema. Può essere utilizzato anche per l'accesso al protocollo client. La rete di amministrazione è in genere una rete privata e non deve essere instradabile tra i siti.

Rete clienti

Opzionale. La rete client è una rete aperta solitamente utilizzata per fornire accesso alle applicazioni client S3, in modo che la rete Grid possa essere isolata e protetta. La rete client può comunicare con qualsiasi subnet raggiungibile tramite il gateway locale.

Linee guida

- Ogni nodo StorageGRID richiede un'interfaccia di rete dedicata, un indirizzo IP, una subnet mask e un gateway per ogni rete a cui è assegnato.
- Un nodo della griglia non può avere più di un'interfaccia su una rete.
- È supportato un singolo gateway per rete, per nodo della griglia, che deve trovarsi sulla stessa subnet del nodo. Se necessario, è possibile implementare un routing più complesso nel gateway.
- Su ogni nodo, ogni rete è mappata su un'interfaccia di rete specifica.

Rete	Nome dell'interfaccia
Griglia	eth0
Amministratore (facoltativo)	eth1
Cliente (facoltativo)	eth2

- Se il nodo è connesso a un dispositivo StorageGRID , per ogni rete vengono utilizzate porte specifiche. Per maggiori dettagli, consultare le istruzioni di installazione dell'elettrodomestico.
- Il percorso predefinito viene generato automaticamente, per nodo. Se eth2 è abilitato, 0.0.0.0/0 utilizza la rete client su eth2. Se eth2 non è abilitato, 0.0.0.0/0 utilizza la rete Grid su eth0.
- La rete client non diventa operativa finché il nodo della griglia non si è unito alla griglia
- La rete di amministrazione può essere configurata durante la distribuzione del nodo della griglia per consentire l'accesso all'interfaccia utente di installazione prima che la griglia sia completamente installata.

Interfacce opzionali

Facoltativamente, è possibile aggiungere interfacce extra a un nodo. Ad esempio, potresti voler aggiungere un'interfaccia trunk a un nodo di amministrazione o gateway, in modo da poter utilizzare ["Interfacce VLAN"](#) per separare il traffico appartenente a diverse applicazioni o tenant. Oppure, potresti voler aggiungere un'interfaccia di accesso da utilizzare in un ["gruppo ad alta disponibilità \(HA\)"](#) .

Per aggiungere interfacce trunk o di accesso, vedere quanto segue:

- **VMware (dopo l'installazione del nodo):** ["VMware: aggiungi trunk o interfacce di accesso a un nodo"](#)
 - **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"](#)
 - **RHEL, Ubuntu o Debian (dopo aver installato il nodo):** ["Linux: aggiungere interfacce trunk o di accesso a un nodo"](#)

Visualizza gli indirizzi IP

È possibile visualizzare l'indirizzo IP di ciascun nodo della griglia nel sistema StorageGRID . È quindi possibile utilizzare questo indirizzo IP per accedere al nodo della griglia tramite la riga di comando ed eseguire varie procedure di manutenzione.

Prima di iniziare

Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .

Informazioni su questo compito

Per informazioni sulla modifica degli indirizzi IP, vedere ["Configurare gli indirizzi IP"](#) .

Passi

1. Selezionare **NODI > *nodo griglia* > Panoramica**.
2. Selezionare **Mostra altro** a destra del titolo Indirizzi IP.

Gli indirizzi IP per quel nodo della griglia sono elencati in una tabella.

[Overview](#) [Hardware](#) [Network](#) [Storage](#) [Objects](#) [ILM](#) [Tasks](#)Node information [?](#)

Name: DC2-SGA-010-096-106-021

Type: Storage Node

ID: f0890e03-4c72-401f-ae92-245511a38e51

Connection state:  Connected

Storage used:

Object data		7%	?
Object metadata		5%	?

Software version: 11.6.0 (build 20210915.1941.afce2d9)

IP addresses: 10.96.106.21 - eth0 (Grid Network)

[Hide additional IP addresses](#) [^](#)

Interface ^	IP address ^
eth0 (Grid Network)	10.96.106.21
eth0 (Grid Network)	fe80::2a0:98ff:fe64:6582
hic2	10.96.106.21
hic4	10.96.106.21
mtc2	169.254.0.1

Alerts

Alert name ^	Severity ? ^	Time triggered ^	Current values
ILM placement unachievable 🔗	 Major	2 hours ago ?	
A placement instruction in an ILM rule cannot be achieved for certain objects.			

Configurare le interfacce VLAN

È possibile creare interfacce LAN virtuali (VLAN) sui nodi di amministrazione e sui nodi gateway e utilizzarle nei gruppi HA e negli endpoint del bilanciatore del carico per isolare e partizionare il traffico per garantire sicurezza, flessibilità e prestazioni. I nodi selezionati nel gruppo HA possono utilizzare le interfacce VLAN per condividere fino a 10 indirizzi IP virtuali, in modo che se un nodo si guasta, un altro nodo subentri nel traffico da e verso gli indirizzi IP virtuali.

Considerazioni sulle interfacce VLAN

- Per creare un'interfaccia VLAN, immettere un ID VLAN e scegliere un'interfaccia padre su uno o più nodi.
- Un'interfaccia padre deve essere configurata come interfaccia trunk sullo switch.

- Un'interfaccia padre può essere la rete Grid (eth0), la rete client (eth2) o un'interfaccia trunk aggiuntiva per la VM o l'host bare-metal (ad esempio, ens256).
- Per ogni interfaccia VLAN, è possibile selezionare solo un'interfaccia padre per un dato nodo. Ad esempio, non è possibile utilizzare sia l'interfaccia Grid Network che l'interfaccia Client Network sullo stesso Gateway Node come interfaccia padre per la stessa VLAN.
- Se l'interfaccia VLAN è destinata al traffico del nodo amministrativo, che include il traffico relativo al Grid Manager e al Tenant Manager, selezionare le interfacce solo sui nodi amministrativi.
- Se l'interfaccia VLAN è destinata al traffico client S3, selezionare le interfacce sui nodi amministrativi o sui nodi gateway.
- Se è necessario aggiungere interfacce trunk, vedere quanto segue per i dettagli:
 - **VMware (dopo l'installazione del nodo):** ["VMware: aggiungi trunk o interfacce di accesso a un nodo"](#)
 - **RHEL (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, Ubuntu o Debian (dopo aver installato il nodo):** ["Linux: aggiungere interfacce trunk o di accesso a un nodo"](#)

Creare un'interfaccia VLAN

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["Permesso di accesso root"](#).
- Un'interfaccia trunk è stata configurata nella rete e collegata alla VM o al nodo Linux. Conosci il nome dell'interfaccia trunk.
- Conosci l'ID della VLAN che stai configurando.

Informazioni su questo compito

L'amministratore di rete potrebbe aver configurato una o più interfacce trunk e una o più VLAN per separare il traffico client o amministrativo appartenente a diverse applicazioni o tenant. Ogni VLAN è identificata da un ID numerico o 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, si specifica l'ID VLAN e si selezionano le interfacce padre (trunk) su uno o più nodi.

Accedi alla procedura guidata

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Interfacce VLAN**.
2. Seleziona **Crea**.

Inserisci i dettagli per le interfacce VLAN

Passi

1. Specificare l'ID della VLAN nella rete. È possibile immettere qualsiasi 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.

2. Facoltativamente, immettere una breve descrizione per l'interfaccia VLAN.
3. Selezionare **Continua**.

Scegli le interfacce padre

Nella tabella sono elencate le interfacce disponibili per tutti i nodi amministrativi e i nodi gateway in ciascun sito della griglia. Le interfacce Admin Network (eth1) non possono essere utilizzate come interfacce padre e non vengono visualizzate.

Passi

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

Ad esempio, potresti voler collegare una VLAN all'interfaccia Client Network (eth2) per un Gateway Node e un Admin Node.

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.

	Site ?	Node name ?	Interface ?	Description ?	Node type ?	Attached VLANs ?
☐	Data Center 2	DC2-ADM1	eth0	Grid Network	Non-primary Admin	—
☒	Data Center 2	DC2-ADM1	eth2	Client Network	Non-primary Admin	—
☐	Data Center 1	DC1-G1	eth0	Grid Network	Gateway	—
☒	Data Center 1	DC1-G1	eth2	Client Network	Gateway	—
☐	Data Center 1	DC1-ADM1	eth0	Grid Network	Primary Admin	—

2 interfaces are selected.

[Previous](#)[Continue](#)

2. Selezionare **Continua**.

Conferma le impostazioni

Passi

1. Rivedere la configurazione e apportare eventuali modifiche.
 - Se devi modificare l'ID o la descrizione della VLAN, seleziona **Inserisci dettagli VLAN** nella parte superiore della pagina.
 - Se devi modificare un'interfaccia padre, seleziona **Scegli interfacce padre** nella parte superiore della pagina oppure seleziona **Precedente**.

- Se devi rimuovere un'interfaccia padre, seleziona il cestino  .

2. Seleziona **Salva**.

3. Attendere fino a 5 minuti affinché la nuova interfaccia venga visualizzata come selezione nella pagina Gruppi ad alta disponibilità e venga elencata nella tabella **Interfacce di rete** per il nodo (**NODI > nodo interfaccia padre > Rete**).

Modifica 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, potresti voler rimuovere un'interfaccia padre da un'interfaccia VLAN se intendi dismettere il nodo associato.

Notare 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, supponiamo 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 non utilizzata per il nodo B, ma non è possibile rimuovere l'interfaccia padre utilizzata per il nodo A.

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Interfacce VLAN**.
2. Selezionare la casella di controllo relativa all'interfaccia VLAN che si desidera modificare. Quindi, seleziona **Azioni > Modifica**.
3. Facoltativamente, aggiorna l'ID VLAN o la descrizione. Quindi, seleziona **Continua**.

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

4. Facoltativamente, seleziona o deseleziona le caselle di controllo per aggiungere interfacce padre o per rimuovere interfacce non utilizzate. Quindi, seleziona **Continua**.
5. Rivedere la configurazione e apportare eventuali modifiche.
6. Seleziona **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. Prima di poter rimuovere l'interfaccia VLAN dal gruppo HA, è necessario rimuoverla.

Per evitare interruzioni nel traffico dei clienti, si consiglia di effettuare 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 l'interfaccia 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 primaria, quindi rimuovere la vecchia interfaccia dal gruppo HA. Infine, eliminare l'interfaccia VLAN su quel nodo.

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Interfacce VLAN**.
2. Selezionare la casella di controllo per ogni interfaccia VLAN che si desidera rimuovere. Quindi, seleziona **Azioni > Elimina**.
3. Selezionare **Sì** per confermare la selezione.

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

Gestire le policy di classificazione del traffico

Quali sono le politiche di classificazione del traffico?

Le policy di classificazione del traffico consentono di identificare e monitorare diversi tipi di traffico di rete. Queste policy possono aiutare a limitare e monitorare il traffico per migliorare le offerte di qualità del servizio (QoS).

I criteri di classificazione del traffico vengono applicati agli endpoint del servizio StorageGRID Load Balancer per i nodi gateway e i nodi amministrativi. Per creare policy di classificazione del traffico, è necessario aver già creato gli endpoint del bilanciatore del carico.

Regole di corrispondenza

Ogni criterio di classificazione del traffico contiene una o più regole di corrispondenza per identificare il traffico di rete correlato a una o più delle seguenti entità:

- Secchi
- Sottorete
- Inquilino
- Endpoint del bilanciatore del carico

StorageGRID monitora il traffico che corrisponde a qualsiasi regola all'interno della policy in base agli obiettivi della regola. Tutto il traffico che corrisponde a una regola di una policy viene gestito da quella policy. Al contrario, è possibile impostare regole in modo che corrispondano a tutto il traffico, ad eccezione di un'entità specificata.

Limitazione del traffico

Facoltativamente, è possibile aggiungere i seguenti tipi di limite a una policy:

- Larghezza di banda aggregata
- Larghezza di banda per richiesta
- Richieste simultanee
- Richiedi tariffa

I valori limite vengono applicati in base al bilanciatore del carico. Se il traffico viene distribuito simultaneamente su più bilanciatori del carico, le tariffe massime totali sono un multiplo dei limiti di tariffa specificati.



È possibile creare policy per limitare la larghezza di banda aggregata o per limitare la larghezza di banda per richiesta. Tuttavia, StorageGRID non può limitare entrambi i tipi di larghezza di banda contemporaneamente. I limiti aggregati di larghezza di banda potrebbero avere un impatto minore aggiuntivo sulle prestazioni del traffico non limitato.

Per i limiti di larghezza di banda aggregati o per richiesta, le richieste vengono trasmesse in entrata o in uscita alla velocità impostata. StorageGRID può imporre una sola velocità, quindi viene applicata la corrispondenza più specifica della policy, in base al tipo di matcher. La larghezza di banda consumata dalla richiesta non viene conteggiata in relazione ad altre policy di corrispondenza meno specifiche contenenti policy di limite di larghezza di banda aggregate. Per tutti gli altri tipi di limite, le richieste dei client vengono ritardate di 250 millisecondi e ricevono una risposta 503 Slow Down per le richieste che superano qualsiasi limite di policy corrispondente.

In Grid Manager puoi visualizzare i grafici del traffico e verificare che le policy applichino i limiti di traffico previsti.

Utilizzare criteri di classificazione del traffico con SLA

È possibile utilizzare criteri di classificazione del traffico insieme ai limiti di capacità e alla protezione dei dati per applicare accordi sul livello di servizio (SLA) che forniscono specifiche per capacità, protezione dei dati e prestazioni.

L'esempio seguente mostra tre livelli di un SLA. È possibile creare criteri di classificazione del traffico per raggiungere gli obiettivi prestazionali di ciascun livello SLA.

Livello di servizio	Capacità	Protezione dei dati	Massima prestazione consentita	Costo
Oro	1 PB di spazio di archiviazione consentito	Regola ILM a 3 copie	25 K richieste/sec Larghezza di banda 5 GB/sec (40 Gbps)	\$\$\$ al mese
Argento	250 TB di spazio di archiviazione consentito	Regola ILM a 2 copie	10 K richieste/sec Larghezza di banda 1,25 GB/sec (10 Gbps)	\$\$ al mese
Bronzo	100 TB di spazio di archiviazione consentito	Regola ILM a 2 copie	5 K richieste/sec Larghezza di banda di 1 GB/sec (8 Gbps)	\$ al mese

Creare criteri di classificazione del traffico

È possibile creare criteri di classificazione del traffico se si desidera monitorare e,

facoltativamente, limitare il traffico di rete in base a bucket, espressione regolare del bucket, CIDR, endpoint del bilanciamento del carico o tenant. Facoltativamente, è possibile impostare limiti per una policy in base alla larghezza di banda, al numero di richieste simultanee o alla frequenza delle richieste.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["Permesso di accesso root"](#).
- Hai creato tutti gli endpoint del bilanciamento del carico che desideri abbinare.
- Hai creato tutti gli inquilini che desideri abbinare.

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Classificazione del traffico**.
2. Seleziona **Crea**.
3. Inserisci un nome e una descrizione (facoltativa) per la policy e seleziona **Continua**.

Ad esempio, descrivi a cosa si applica questa politica di classificazione del traffico e cosa limiterà.

4. Selezionare **Aggiungi regola** e specificare i seguenti dettagli per creare una o più regole corrispondenti per il criterio. Ogni policy creata dovrebbe avere almeno una regola corrispondente. Selezionare **Continua**.

Campo	Descrizione
Tipo	Seleziona i tipi di traffico a cui si applica la regola di corrispondenza. I tipi di traffico sono bucket, bucket regex, CIDR, endpoint del bilanciamento del carico e tenant.
Valore della corrispondenza	Immettere il valore corrispondente al tipo selezionato. • Bucket: inserisci uno o più nomi di bucket. • Espressione regolare bucket: inserisci una o più espressioni regolari utilizzate per trovare una corrispondenza con un set di nomi di bucket. L'espressione regolare non è ancorata. Utilizzare l'ancoraggio ^ per la corrispondenza all'inizio del nome del bucket e l'ancoraggio \$ per la corrispondenza alla fine del nome. La corrispondenza delle espressioni regolari supporta un sottoinsieme della sintassi PCRE (espressione regolare compatibile con Perl). • CIDR: immettere una o più subnet IPv4, in notazione CIDR, che corrispondano alla subnet desiderata. • Endpoint del bilanciamento del carico: seleziona un nome per l'endpoint. Questi sono gli endpoint del bilanciamento del carico definiti su "Configurare gli endpoint del bilanciamento del carico". • Tenant: la corrispondenza del tenant utilizza l'ID della chiave di accesso. Se la richiesta non contiene un ID chiave di accesso (ad esempio, accesso anonimo), la proprietà del bucket a cui si accede viene utilizzata per determinare il tenant.

Campo	Descrizione
Corrispondenza inversa	Se si desidera far corrispondere tutto il traffico di rete <i>eccetto</i> il traffico coerente con il Tipo e il Valore di corrispondenza appena definiti, selezionare la casella di controllo Corrispondenza inversa. In caso contrario, lasciare la casella di controllo deselezionata. Ad esempio, se si desidera che questo criterio venga applicato a tutti gli endpoint del bilanciatore del carico tranne uno, specificare l'endpoint del bilanciatore del carico da escludere e selezionare Corrispondenza inversa. Per una policy contenente più matcher, di cui almeno uno è un matcher inverso, fare attenzione a non creare una policy che corrisponda a tutte le richieste.

5. Facoltativamente, seleziona **Aggiungi un limite** e seleziona i seguenti dettagli per aggiungere uno o più limiti per controllare il traffico di rete corrispondente a una regola.



StorageGRID raccoglie le metriche anche se non si aggiungono limiti, in modo da poter comprendere le tendenze del traffico.

Campo	Descrizione
Tipo	Il tipo di limite che si desidera applicare al traffico di rete a cui corrisponde la regola. Ad esempio, è possibile limitare la larghezza di banda o la velocità delle richieste. Nota: è possibile creare policy per limitare la larghezza di banda aggregata o per limitare la larghezza di banda per richiesta. Tuttavia, StorageGRID non può limitare entrambi i tipi di larghezza di banda contemporaneamente. Quando è in uso la larghezza di banda aggregata, la larghezza di banda per richiesta non è disponibile. Al contrario, quando è in uso la larghezza di banda per richiesta, la larghezza di banda aggregata non è disponibile. I limiti aggregati di larghezza di banda potrebbero avere un impatto minore aggiuntivo sulle prestazioni del traffico non limitato. Per i limiti di larghezza di banda, StorageGRID applica la policy che meglio corrisponde al tipo di limite impostato. Ad esempio, se si dispone di una policy che limita il traffico in una sola direzione, il traffico nella direzione opposta sarà illimitato, anche se è presente traffico che corrisponde a policy aggiuntive che hanno limiti di larghezza di banda. StorageGRID implementa le corrispondenze "migliori" per i limiti di larghezza di banda nel seguente ordine: • Indirizzo IP esatto (maschera /32) • Nome esatto del bucket • Espressione regolare del bucket • Inquilino • Punto finale • Corrispondenze CIDR non esatte (non /32) • Corrispondenze inverse

Campo	Descrizione
Si applica a	Se questo limite si applica alle richieste di lettura del client (GET o HEAD) o alle richieste di scrittura (PUT, POST o DELETE).
Valore	Valore a cui verrà limitato il traffico di rete, in base all'unità selezionata. Ad esempio, immettere 10 e selezionare MiB/s per impedire che il traffico di rete a cui corrisponde questa regola superi i 10 MiB/s. Nota: a seconda delle impostazioni delle unità, le unità disponibili saranno binarie (ad esempio, GiB) o decimali (ad esempio, GB). Per modificare l'impostazione delle unità, seleziona il menu a discesa dell'utente in alto a destra di Grid Manager, quindi seleziona Preferenze utente.
Unità	L'unità che descrive il valore immesso.

Ad esempio, se si desidera creare un limite di larghezza di banda di 40 GB/s per un livello SLA, creare due limiti di larghezza di banda aggregati: GET/HEAD a 40 GB/s e PUT/POST/DELETE a 40 GB/s.

6. Selezionare **Continua**.

7. Leggere e rivedere la politica di classificazione del traffico. Utilizzare il pulsante **Precedente** per tornare indietro e apportare le modifiche desiderate. Quando sei soddisfatto della policy, seleziona **Salva e continua**.

Il traffico del client S3 viene ora gestito in base alla politica di classificazione del traffico.

Dopo aver finito

["Visualizza le metriche del traffico di rete"](#) per verificare che le norme rispettino i limiti di traffico previsti.

Modifica la politica di classificazione del traffico

È possibile modificare una policy di classificazione del traffico per cambiarne il nome o la descrizione oppure per creare, modificare o eliminare regole o limiti per la policy.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["Permesso di accesso root"](#).

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Classificazione del traffico**.

Viene visualizzata la pagina Criteri di classificazione del traffico e i criteri esistenti sono elencati in una tabella.

2. Modifica la policy utilizzando il menu Azioni o la pagina dei dettagli. Vedere ["creare politiche di classificazione del traffico"](#) per cosa inserire.

Menu Azioni

- a. Selezionare la casella di controllo per la policy.
- b. Selezionare **Azioni > Modifica**.

Pagina dei dettagli

- a. Selezionare il nome della policy.
- b. Selezionare il pulsante **Modifica** accanto al nome della policy.

3. Per il passaggio Inserisci nome criterio, modifica facoltativamente il nome o la descrizione del criterio e seleziona **Continua**.
4. Per il passaggio Aggiungi regole di corrispondenza, aggiungere facoltativamente una regola o modificare il **Tipo** e il **Valore di corrispondenza** della regola esistente, quindi selezionare **Continua**.
5. Per il passaggio Imposta limiti, puoi aggiungere, modificare o eliminare un limite e selezionare **Continua**.
6. Rivedi la policy aggiornata e seleziona **Salva e continua**.

Le modifiche apportate alla policy vengono salvate e il traffico di rete viene ora gestito in base alle policy di classificazione del traffico. Puoi visualizzare i grafici del traffico e verificare che le norme rispettino i limiti di traffico previsti.

Eliminare una policy di classificazione del traffico

È possibile eliminare una policy di classificazione del traffico se non ne hai più bisogno. Assicurati di eliminare la policy corretta perché una policy eliminata non può essere recuperata.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Tu hai il "[Permesso di accesso root](#)".

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Classificazione del traffico**.

Viene visualizzata la pagina Criteri di classificazione del traffico con i criteri esistenti elencati in una tabella.

2. Eliminare la policy utilizzando il menu Azioni o la pagina dei dettagli.

Menu Azioni

- a. Selezionare la casella di controllo per la policy.
- b. Selezionare **Azioni > Rimuovi**.

Pagina dei dettagli della politica

- a. Selezionare il nome della policy.
- b. Selezionare il pulsante **Rimuovi** accanto al nome della policy.

3. Selezionare **Sì** per confermare che si desidera eliminare il criterio.

La politica è stata eliminata.

Visualizza le metriche del traffico di rete

È possibile monitorare il traffico di rete visualizzando i grafici disponibili nella pagina Criteri di classificazione del traffico.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["Accesso root o autorizzazione account tenant"](#).

Informazioni su questo compito

Per qualsiasi policy di classificazione del traffico esistente, è possibile visualizzare le metriche per il servizio di bilanciamento del carico per determinare se la policy sta limitando correttamente il traffico sulla rete. I dati nei grafici possono aiutarti a stabilire se è necessario modificare la polizza.

Anche se non vengono stabiliti limiti per una politica di classificazione del traffico, vengono raccolte metriche e i grafici forniscono informazioni utili per comprendere le tendenze del traffico.

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Classificazione del traffico**.

Viene visualizzata la pagina Criteri di classificazione del traffico e i criteri esistenti sono elencati nella tabella.

2. Selezionare il nome del criterio di classificazione del traffico per il quale si desidera visualizzare le metriche.
3. Selezionare la scheda **Metriche**.

Vengono visualizzati i grafici della politica di classificazione del traffico. I grafici mostrano le metriche solo per il traffico che corrisponde alla policy selezionata.

Nella pagina sono inclusi i seguenti grafici.

- Frequenza delle richieste: questo grafico fornisce la quantità di larghezza di banda corrispondente a questa policy gestita da tutti i bilanciatori del carico. I dati ricevuti includono le intestazioni delle richieste per tutte le richieste e le dimensioni dei dati del corpo per le risposte che contengono dati del corpo. Inviato include le intestazioni di risposta per tutte le richieste e le dimensioni dei dati del corpo della risposta per le richieste che includono dati del corpo nella risposta.



Una volta completate le richieste, questo grafico mostra solo l'utilizzo della larghezza di banda. Per richieste di oggetti lenti o di grandi dimensioni, la larghezza di banda istantanea effettiva potrebbe differire dai valori riportati in questo grafico.

- Tasso di risposta agli errori: questo grafico fornisce una frequenza approssimativa con cui le richieste che corrispondono a questa policy restituiscono errori (codice di stato HTTP ≥ 400) ai client.
- Durata media della richiesta (senza errori): questo grafico fornisce la durata media delle richieste riuscite che corrispondono a questa policy.
- Utilizzo della larghezza di banda della policy: questo grafico mostra la quantità di larghezza di banda corrispondente a questa policy gestita da tutti i bilanciatori del carico. I dati ricevuti includono le intestazioni delle richieste per tutte le richieste e le dimensioni dei dati del corpo per le risposte che

contengono dati del corpo. Inviato include le intestazioni di risposta per tutte le richieste e le dimensioni dei dati del corpo della risposta per le richieste che includono dati del corpo nella risposta.

4. Posiziona il cursore su un grafico a linee per visualizzare una finestra pop-up con i valori relativi a una parte specifica del grafico.
5. Selezionare **Dashboard Grafana** subito sotto il titolo Metriche per visualizzare tutti i grafici relativi a una policy. Oltre ai quattro grafici della scheda **Metriche**, puoi visualizzare altri due grafici:
 - Frequenza delle richieste di scrittura in base alle dimensioni dell'oggetto: frequenza delle richieste PUT/POST/DELETE che corrispondono a questa policy. Il posizionamento su una singola cella mostra le velocità al secondo. Le tariffe mostrate nella vista hover vengono troncate a conteggi interi e potrebbero riportare 0 quando nel bucket sono presenti richieste diverse da zero.
 - Frequenza delle richieste di lettura in base alle dimensioni dell'oggetto: frequenza delle richieste GET/HEAD che corrispondono a questa policy. Il posizionamento su una singola cella mostra le velocità al secondo. Le tariffe mostrate nella vista hover vengono troncate a conteggi interi e potrebbero riportare 0 quando nel bucket sono presenti richieste diverse da zero.
6. In alternativa, è possibile accedere ai grafici dal menu **SUPPORTO**.
 - a. Selezionare **SUPPORTO > Strumenti > Metriche**.
 - b. Selezionare **Politica di classificazione del traffico** dalla sezione **Grafana**.
 - c. Selezionare la policy dal menu in alto a sinistra della pagina.
 - d. Posiziona il cursore su un grafico per visualizzare un pop-up che mostra la data e l'ora del campione, le dimensioni degli oggetti aggregati nel conteggio e il numero di richieste al secondo durante quel periodo di tempo.

Le policy di classificazione del traffico sono identificate dal loro ID. Gli ID dei criteri sono elencati nella pagina Criteri di classificazione del traffico.
7. Analizza i grafici per determinare la frequenza con cui la policy limita il traffico e se è necessario modificarla.

Cifrature supportate per le connessioni TLS in uscita

Il sistema StorageGRID supporta un set limitato di suite di crittografia per le connessioni Transport Layer Security (TLS) ai sistemi esterni utilizzati per la federazione delle identità e i pool di archiviazione cloud.

Versioni supportate di TLS

StorageGRID supporta TLS 1.2 e TLS 1.3 per le connessioni a sistemi esterni utilizzati per la federazione delle identità e i pool di archiviazione cloud.

I cifrari TLS supportati per l'uso con sistemi esterni sono stati selezionati per garantire la compatibilità con una vasta gamma di sistemi esterni. L'elenco è più lungo dell'elenco dei cifrari supportati per l'uso con le applicazioni client S3. Per configurare i cifrari, vai su **CONFIGURAZIONE > Sicurezza > Impostazioni di sicurezza** e seleziona **Criteri TLS e SSH**.



Le opzioni di configurazione TLS, quali versioni del protocollo, cifrature, algoritmi di scambio di chiavi e algoritmi MAC, non sono configurabili in StorageGRID. Per richieste specifiche su queste impostazioni, contattare il rappresentante dell'account NetApp.

Vantaggi delle connessioni HTTP attive, inattive e simultanee

La modalità di configurazione delle connessioni HTTP può influire sulle prestazioni del sistema StorageGRID . Le configurazioni variano a seconda che la connessione HTTP sia attiva o inattiva o che ci siano più connessioni simultanee.

È possibile identificare i vantaggi in termini di prestazioni per i seguenti tipi di connessioni HTTP:

- Connessioni HTTP inattive
- Connessioni HTTP attive
- Connessioni HTTP simultanee

Vantaggi di mantenere aperte le connessioni HTTP inattive

È opportuno mantenere aperte le connessioni HTTP anche quando le applicazioni client sono inattive, per consentire alle applicazioni client di eseguire transazioni successive sulla connessione aperta. In base alle misurazioni del sistema e all'esperienza di integrazione, dovresti mantenere aperta una connessione HTTP inattiva per un massimo di 10 minuti. StorageGRID potrebbe chiudere automaticamente una connessione HTTP mantenuta aperta e inattiva per più di 10 minuti.

Le connessioni HTTP aperte e inattive offrono i seguenti vantaggi:

- Latenza ridotta dal momento in cui il sistema StorageGRID determina di dover eseguire una transazione HTTP al momento in cui il sistema StorageGRID può eseguire la transazione

Il vantaggio principale è la latenza ridotta, soprattutto per quanto riguarda il tempo necessario per stabilire connessioni TCP/IP e TLS.

- Aumento della velocità di trasferimento dati mediante l'attivazione dell'algoritmo di avvio lento TCP/IP con trasferimenti eseguiti in precedenza
- Notifica istantanea di diverse classi di condizioni di errore che interrompono la connettività tra l'applicazione client e il sistema StorageGRID

Determinare per quanto tempo mantenere aperta una connessione inattiva è un compromesso tra i vantaggi dell'avvio lento associati alla connessione esistente e l'allocazione ideale della connessione alle risorse di sistema interne.

Vantaggi delle connessioni HTTP attive

Per le connessioni dirette ai nodi di archiviazione, è opportuno limitare la durata di una connessione HTTP attiva a un massimo di 10 minuti, anche se la connessione HTTP esegue continuamente transazioni.

Determinare la durata massima per cui una connessione deve rimanere aperta è un compromesso tra i vantaggi della persistenza della connessione e l'allocazione ideale della connessione alle risorse del sistema interno.

Per le connessioni client ai nodi di archiviazione, la limitazione delle connessioni HTTP attive offre i seguenti vantaggi:

- Consente un bilanciamento ottimale del carico nel sistema StorageGRID .

Nel tempo, una connessione HTTP potrebbe non essere più ottimale poiché cambiano i requisiti di bilanciamento del carico. Il sistema ottiene il miglior bilanciamento del carico quando le applicazioni client stabiliscono una connessione HTTP separata per ogni transazione, ma ciò annulla i vantaggi molto più

preziosi associati alle connessioni persistenti.

- Consente alle applicazioni client di indirizzare le transazioni HTTP ai servizi LDR che dispongono di spazio disponibile.
- Consente l'avvio delle procedure di manutenzione.

Alcune procedure di manutenzione iniziano solo dopo il completamento di tutte le connessioni HTTP in corso.

Per le connessioni client al servizio Load Balancer, limitare la durata delle connessioni aperte può essere utile per consentire l'avvio tempestivo di alcune procedure di manutenzione. Se la durata delle connessioni client non è limitata, potrebbero volerci diversi minuti prima che le connessioni attive vengano terminate automaticamente.

Vantaggi delle connessioni HTTP simultanee

È consigliabile mantenere aperte più connessioni TCP/IP al sistema StorageGRID per consentire il parallelismo, che aumenta le prestazioni. Il numero ottimale di connessioni parallele dipende da diversi fattori.

Le connessioni HTTP simultanee offrono i seguenti vantaggi:

- Latenza ridotta

Le transazioni possono iniziare immediatamente, senza dover attendere il completamento di altre transazioni.

- Aumento della produttività

Il sistema StorageGRID può eseguire transazioni parallele e aumentare la produttività complessiva delle transazioni.

Le applicazioni client devono stabilire più connessioni HTTP. Quando un'applicazione client deve eseguire una transazione, può selezionare e utilizzare immediatamente qualsiasi connessione stabilita che non stia elaborando una transazione.

Ogni topologia del sistema StorageGRID presenta un throughput di picco diverso per transazioni e connessioni simultanee prima che le prestazioni inizino a peggiorare. La velocità massima di elaborazione dipende da fattori quali risorse di elaborazione, risorse di rete, risorse di archiviazione e collegamenti WAN. Anche il numero di server e servizi e il numero di applicazioni supportate dal sistema StorageGRID sono fattori da considerare.

I sistemi StorageGRID spesso supportano più applicazioni client. È opportuno tenerlo presente quando si determina il numero massimo di connessioni simultanee utilizzate da un'applicazione client. Se l'applicazione client è composta da più entità software, ciascuna delle quali stabilisce connessioni al sistema StorageGRID, è necessario sommare tutte le connessioni tra le entità. Potrebbe essere necessario modificare il numero massimo di connessioni simultanee nelle seguenti situazioni:

- La topologia del sistema StorageGRID influisce sul numero massimo di transazioni e connessioni simultanee che il sistema può supportare.
- Le applicazioni client che interagiscono con il sistema StorageGRID su una rete con larghezza di banda limitata potrebbero dover ridurre il grado di concorrenza per garantire che le singole transazioni vengano completate in un tempo ragionevole.
- Quando molte applicazioni client condividono il sistema StorageGRID, potrebbe essere necessario ridurre

il grado di concorrenza per evitare di superare i limiti del sistema.

Separazione dei pool di connessioni HTTP per le operazioni di lettura e scrittura

È possibile utilizzare pool separati di connessioni HTTP per le operazioni di lettura e scrittura e controllare la quantità di pool da utilizzare per ciascuna. Pool separati di connessioni HTTP consentono di controllare meglio le transazioni e bilanciare i carichi.

Le applicazioni client possono creare carichi che sono dominanti nel recupero (lettura) o dominanti nello stoccaggio (scrittura). Grazie a pool separati di connessioni HTTP per le transazioni di lettura e scrittura, è possibile definire la quantità di ciascun pool da dedicare alle transazioni di lettura o scrittura.

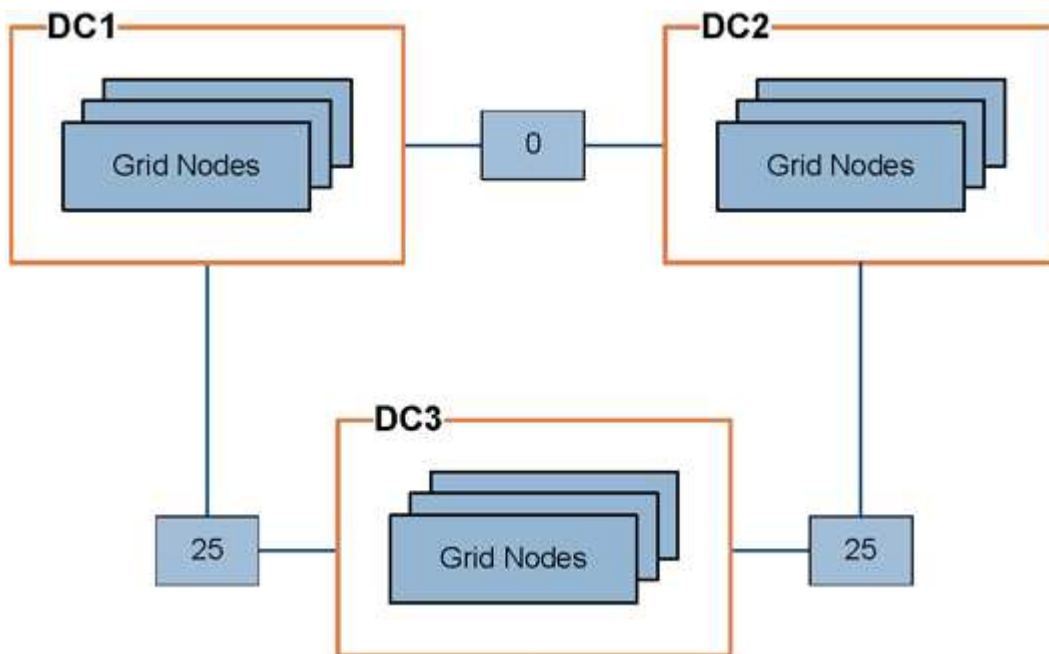
Gestire i costi dei link

I costi di collegamento consentono di stabilire la priorità del sito del data center che fornisce un servizio richiesto quando sono presenti due o più siti del data center. È possibile adattare i costi dei collegamenti in base alla latenza tra i siti.

Quali sono i costi dei link?

- I costi di collegamento vengono utilizzati per stabilire la priorità della copia dell'oggetto da utilizzare per completare i recuperi dell'oggetto.
- I costi dei collegamenti vengono utilizzati dall'API di gestione della griglia e dall'API di gestione dei tenant per determinare quali servizi StorageGRID interni utilizzare.
- I costi di collegamento vengono utilizzati dal servizio Load Balancer sui nodi amministrativi e sui nodi gateway per indirizzare le connessioni client. Vedere ["Considerazioni sul bilanciamento del carico"](#).

Il diagramma mostra una griglia a tre siti in cui sono configurati i costi di collegamento tra i siti:



- Il servizio Load Balancer sui nodi amministrativi e sui nodi gateway distribuisce equamente le connessioni client a tutti i nodi di archiviazione nello stesso sito del data center e a tutti i siti del data center con un costo di collegamento pari a 0.

Nell'esempio, un nodo gateway nel sito del data center 1 (DC1) distribuisce equamente le connessioni

client ai nodi di archiviazione in DC1 e ai nodi di archiviazione in DC2. Un nodo gateway in DC3 invia connessioni client solo ai nodi di archiviazione in DC3.

- Quando si recupera un oggetto che esiste in più copie replicate, StorageGRID recupera la copia nel data center che ha il costo di collegamento più basso.

Nell'esempio, se un'applicazione client su DC2 recupera un oggetto archiviato sia su DC1 che su DC3, l'oggetto viene recuperato da DC1, perché il costo del collegamento da DC1 a DC2 è 0, che è inferiore al costo del collegamento da DC3 a DC2 (25).

I costi dei collegamenti sono numeri relativi arbitrari, senza un'unità di misura specifica. Ad esempio, un costo di collegamento pari a 50 viene utilizzato in modo meno preferenziale rispetto a un costo di collegamento pari a 25. La tabella mostra i costi dei link più comunemente utilizzati.

Collegamento	Costo del collegamento	Note
Tra i siti fisici dei data center	25 (predefinito)	Data center collegati tramite collegamento WAN.
Tra siti di data center logici nella stessa posizione fisica	0	Data center logici nello stesso edificio fisico o campus collegati tramite una LAN.

Aggiorna i costi dei link

È possibile aggiornare i costi di collegamento tra i siti dei data center per riflettere la latenza tra i siti.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Autorizzazione di configurazione della pagina della topologia della griglia"](#) .

Passi

1. Seleziona **SUPPORTO > Altro > Costo del collegamento**.



Link Cost

Updated: 2023-02-15 18:09:28 MST

Site Names (1 - 3 of 3)

Site ID	Site Name	Actions
10	Data Center 1	
20	Data Center 2	
30	Data Center 3	

Show Records Per Page

Previous
« 1 » Next

Link Costs

Link Source	Link Destination			Actions
	10	20	30	
Data Center 1	0	25	25	



- Seleziona un sito in **Origine collegamento** e inserisci un valore di costo compreso tra 0 e 100 in **Destinazione collegamento**.

Non è possibile modificare il costo del collegamento se la sorgente è la stessa della destinazione.

Per annullare le modifiche, selezionare  **Ripristina**.

- Selezionare **Applica modifiche**.

Utilizzare AutoSupport

Che cos'è AutoSupport?

La funzionalità AutoSupport consente a StorageGRID di inviare pacchetti di stato e di integrità al supporto tecnico NetApp .

Utilizzando AutoSupport è possibile velocizzare notevolmente la determinazione e la risoluzione dei problemi. Il supporto tecnico può anche monitorare le esigenze di archiviazione del tuo sistema e aiutarti a stabilire se è necessario aggiungere nuovi nodi o siti. Facoltativamente, è possibile configurare i pacchetti AutoSupport in modo che vengano inviati a un'ulteriore destinazione.

StorageGRID ha due tipi di AutoSupport:

- * StorageGRID AutoSupport* segnala problemi software StorageGRID . Abilitato per impostazione predefinita quando si installa per la prima volta StorageGRID. Puoi [modificare la configurazione predefinita AutoSupport](#) se necessario.



Se StorageGRID AutoSupport non è abilitato, viene visualizzato un messaggio nella dashboard di Grid Manager. Il messaggio include un collegamento alla pagina di configurazione AutoSupport . Se chiudi il messaggio, questo non verrà più visualizzato finché la cache del browser non verrà cancellata, anche se AutoSupport rimane disabilitato.

- **Appliance hardware AutoSupport** segnala problemi relativi all'appliance StorageGRID . Devi ["configurare AutoSupport hardware su ogni appliance"](#) .

Che cos'è il Active IQ?

Active IQ è un consulente digitale basato sul cloud che sfrutta l'analisi predittiva e la saggezza della community basata sulla base installata di NetApp. Le sue valutazioni continue dei rischi, gli avvisi predittivi, le linee guida prescrittive e le azioni automatizzate ti aiutano a prevenire i problemi prima che si verifichino, migliorando lo stato del sistema e aumentandone la disponibilità.

Se si desidera utilizzare le dashboard e le funzionalità Active IQ sul sito di supporto NetApp , è necessario abilitare AutoSupport.

["Documentazione Digital Advisor Active IQ"](#)

Informazioni incluse nel pacchetto AutoSupport

Un pacchetto AutoSupport contiene i seguenti file e dettagli.

Nome del file	Campi	Descrizione
AUTOSUPPORT-HISTORY.XML	Numero di sequenza AutoSupport + Destinazione per questo AutoSupport + Stato di consegna + Tentativi di consegna + Oggetto AutoSupport + URI di consegna + Ultimo errore + Nome file PUT AutoSupport + Ora di generazione + Dimensione compressa AutoSupport + Dimensione decompressa AutoSupport + Tempo totale di raccolta (ms)	File cronologico AutoSupport .
AUTOSUPPORT.XML	Nodo + Protocollo per contattare l'assistenza + URL di supporto per HTTP/HTTPS + Indirizzo di supporto + Stato di AutoSupport OnDemand + URL del server di AutoSupport OnDemand + Intervallo di polling AutoSupport OnDemand	File di stato AutoSupport . Fornisce dettagli sul protocollo utilizzato, URL e indirizzo del supporto tecnico, intervallo di polling e OnDemand AutoSupport , se abilitato o disabilitato.

Nome del file	Campi	Descrizione
BUCKETS.XML	ID bucket + ID account + versione build + configurazione vincolo posizione + conformità abilitata + configurazione conformità + blocco oggetto S3 abilitato + configurazione blocco oggetto S3 + configurazione coerenza + CORS abilitato + configurazione CORS + ora ultimo accesso abilitata + policy abilitata + configurazione policy + notifiche abilitate + configurazione notifiche + cloud mirror abilitato + configurazione cloud mirror + ricerca abilitata + configurazione ricerca + tag bucket abilitato + configurazione tag bucket + configurazione versioning	Fornisce dettagli di configurazione e statistiche a livello di bucket. Esempi di configurazioni dei bucket includono servizi di piattaforma, conformità e coerenza dei bucket.
GRID-CONFIGURATIONS.XML	ID attributo + Nome attributo + Valore + Indice + ID tabella + Nome tabella	File di informazioni sulla configurazione a livello di griglia. Contiene informazioni sui certificati di griglia, spazio riservato ai metadati, impostazioni di configurazione a livello di griglia (conformità, blocco oggetti S3, compressione oggetti, avvisi, syslog e configurazione ILM), dettagli del profilo di codifica di cancellazione, nome DNS e " Nome NMS ".
GRID-SPEC.XML	Specifiche della griglia, XML grezzo	Utilizzato per configurare e distribuire StorageGRID. Contiene le specifiche della griglia, l'IP del server NTP, l'IP del server DNS, la topologia di rete e i profili hardware dei nodi.
GRID-TASKS.XML	Nodo + Percorso del servizio + ID attributo + Nome attributo + Valore + Indice + ID tabella + Nome tabella	File di stato delle attività di griglia (procedure di manutenzione). Fornisce dettagli sulle attività attive, terminate, completate, non riuscite e in sospeso della griglia.
GRID.JSON	Griglia + Revisione + Versione software + Descrizione + Licenza + Password + DNS + NTP + Siti + Nodi	Informazioni sulla griglia.

Nome del file	Campi	Descrizione
ILM-CONFIGURAZIONE.XML	ID attributo + Nome attributo + Valore + Indice + ID tabella + Nome tabella	Elenco degli attributi per le configurazioni ILM.
ILM-STATUS.XML	Nodo + Percorso del servizio + ID attributo + Nome attributo + Valore + Indice + ID tabella + Nome tabella	File di informazioni sulle metriche ILM. Contiene i tassi di valutazione ILM per ciascun nodo e le metriche a livello di griglia.
ILM.XML	XML grezzo ILM	File di policy attiva ILM. Contiene dettagli sui criteri ILM attivi, come ID del pool di archiviazione, comportamento di acquisizione, filtri, regole e descrizione.
LOG.TGZ	<i>n / a</i>	File di registro scaricabile. Contiene <code>broadcast-err.log</code> e <code>servermanager.log</code> da ogni nodo.
MANIFEST.XML	Ordine di raccolta + Nome del file del contenuto AutoSupport per questi dati + Descrizione di questo elemento dati + Numero di byte raccolti + Tempo impiegato per la raccolta + Stato di questo elemento dati + Descrizione dell'errore + Tipo di contenuto AutoSupport per questi dati +	Contiene metadati AutoSupport e brevi descrizioni di tutti i file AutoSupport .
NMS-ENTITIES.XML	Indice attributo + OID entità + ID nodo + ID modello dispositivo + Versione modello dispositivo + Nome entità	Entità di gruppo e di servizio nel " Albero NMS ". Fornisce dettagli sulla topologia della griglia. Il nodo può essere determinato in base ai servizi in esecuzione sul nodo.
OGGETTI-STATO.XML	Nodo + Percorso del servizio + ID attributo + Nome attributo + Valore + Indice + ID tabella + Nome tabella	Stato dell'oggetto, tra cui stato della scansione in background, trasferimento attivo, velocità di trasferimento, trasferimenti totali, velocità di eliminazione, frammenti danneggiati, oggetti persi, oggetti mancanti, tentativi di riparazione, velocità di scansione, periodo di scansione stimato e stato di completamento della riparazione.

Nome del file	Campi	Descrizione
STATO-SERVER.XML	Nodo + Percorso del servizio + ID attributo + Nome attributo + Valore + Indice + ID tabella + Nome tabella	Configurazioni del server. Contiene i seguenti dettagli per ciascun nodo: tipo di piattaforma, sistema operativo, memoria installata, memoria disponibile, connettività di archiviazione, numero di serie dello chassis dell'appliance di archiviazione, numero di unità guaste del controller di archiviazione, temperatura dello chassis del controller di elaborazione, hardware di elaborazione, numero di serie del controller di elaborazione, alimentatore, dimensioni dell'unità e tipo di unità.
STATO-SERVIZIO.XML	Nodo + Percorso del servizio + ID attributo + Nome attributo + Valore + Indice + ID tabella + Nome tabella	File di informazioni sul nodo di servizio. Contiene dettagli quali spazio tabella allocato, spazio tabella libero, metriche Reaper del database, durata della riparazione del segmento, durata del processo di riparazione, riavvii automatici del processo e terminazione automatica del processo.
STORAGE-GRADES.XML	ID grado di archiviazione + Nome grado di archiviazione + ID nodo di archiviazione + Percorso nodo di archiviazione	File di definizione del grado di archiviazione per ciascun nodo di archiviazione.
SUMMARY-ATTRIBUTES.XML	OID gruppo + Percorso gruppo + ID attributo riepilogo + Nome attributo riepilogo + Valore + Indice + ID tabella + Nome tabella	Dati di stato del sistema di alto livello che riepilogano le informazioni sull'utilizzo StorageGRID . Fornisce dettagli quali il nome della griglia, i nomi dei siti, il numero di nodi di archiviazione per griglia e per sito, il tipo di licenza, la capacità e l'utilizzo della licenza, i termini di supporto software e i dettagli delle operazioni S3.
AVVISI DI SISTEMA.XML	Nome + Gravità + Nome nodo + Stato avviso + Nome sito + Ora di attivazione avviso + Ora di risoluzione avviso + ID regola + ID nodo + ID sito + Disattivato + Altre annotazioni + Altre etichette	Avvisi di sistema attuali che indicano potenziali problemi nel sistema StorageGRID .

Nome del file	Campi	Descrizione
USERAGENTS.XML	User agent + Numero di giorni + Richieste HTTP totali + Byte totali ingeriti + Byte totali recuperati + Richieste PUT + Richieste GET + Richieste DELETE + Richieste HEAD + Richieste POST + Richieste OPTIONS + Tempo medio della richiesta (ms) + Tempo medio della richiesta PUT (ms) + Tempo medio della richiesta GET (ms) + Tempo medio della richiesta DELETE (ms) + Tempo medio della richiesta HEAD (ms) + Tempo medio della richiesta POST (ms) + Tempo medio della richiesta OPTIONS (ms)	Statistiche basate sugli user agent dell'applicazione. Ad esempio, il numero di operazioni PUT/GET/DELETE/HEAD per user agent e la dimensione totale in byte di ciascuna operazione.
X-HEADER-DATI	X-Netapp-asup-generato-on + X-Netapp-asup-nome host + X-Netapp-asup-versione-os + X-Netapp-asup-num-seriale + X-Netapp-asup-oggetto + X-Netapp-asup-id-sistema + X-Netapp-asup-nome-modello +	Dati di intestazione AutoSupport .

Configura AutoSupport

Per impostazione predefinita, la funzionalità StorageGRID AutoSupport è abilitata quando si installa StorageGRID per la prima volta. Tuttavia, è necessario configurare AutoSupport hardware su ogni appliance. Se necessario, è possibile modificare la configurazione AutoSupport .

Se si desidera modificare la configurazione di StorageGRID AutoSupport, apportare le modifiche solo sul nodo di amministrazione primario. Devi [configurare l'hardware AutoSupport](#) su ogni elettrodomestico.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Permesso di accesso root"](#) .
- Se utilizzerai HTTPS per l'invio di pacchetti AutoSupport , avrai fornito l'accesso Internet in uscita al nodo di amministrazione primario, direttamente o ["utilizzando un server proxy"](#) (non sono richieste connessioni in entrata).
- Se HTTP è selezionato nella pagina StorageGRID AutoSupport , è necessario ["configurato un server proxy"](#) per inoltrare i pacchetti AutoSupport come HTTPS. I server AutoSupport di NetApp rifiuteranno i pacchetti inviati tramite HTTP.
- Se si utilizzerà SMTP come protocollo per i pacchetti AutoSupport , è stato configurato un server di posta SMTP.

Informazioni su questo compito

È possibile utilizzare una qualsiasi combinazione delle seguenti opzioni per inviare i pacchetti AutoSupport al supporto tecnico:

- **Settimanale:** invia automaticamente i pacchetti AutoSupport una volta alla settimana. Impostazione predefinita: Abilitato.
- **Attivato da evento:** invia automaticamente pacchetti AutoSupport ogni ora o quando si verificano eventi di sistema significativi. Impostazione predefinita: Abilitato.
- **Su richiesta:** consente al supporto tecnico di richiedere che il sistema StorageGRID invii automaticamente pacchetti AutoSupport, il che è utile quando stanno lavorando attivamente a un problema (richiede il protocollo di trasmissione HTTPS AutoSupport). Impostazione predefinita: Disabilitato.
- **Attivato dall'utente:** invia manualmente i pacchetti AutoSupport in qualsiasi momento.

Specifica il protocollo per i pacchetti AutoSupport

Per inviare pacchetti AutoSupport è possibile utilizzare uno qualsiasi dei seguenti protocolli:

- **HTTPS:** Questa è l'impostazione predefinita e consigliata per le nuove installazioni. Questo protocollo utilizza la porta 443. Se lo desideri [abilitare la funzionalità AutoSupport on Demand](#), devi usare HTTPS.
- **HTTP:** Se si seleziona HTTP, è necessario configurare un server proxy per inoltrare i pacchetti AutoSupport come HTTPS. I server AutoSupport di NetApp rifiutano i pacchetti inviati tramite HTTP. Questo protocollo utilizza la porta 80.
- **SMTP:** utilizzare questa opzione se si desidera che i pacchetti AutoSupport vengano inviati tramite e-mail.

Il protocollo impostato viene utilizzato per l'invio di tutti i tipi di pacchetti AutoSupport.

Passi

1. Selezionare **SUPPORTO > Strumenti > * AutoSupport* > Impostazioni**.
2. Seleziona il protocollo che desideri utilizzare per inviare i pacchetti AutoSupport.
3. Se hai selezionato **HTTPS**, seleziona se utilizzare un certificato di supporto NetApp (certificato TLS) per proteggere la connessione al server di supporto tecnico.
 - **Verifica certificato** (predefinito): garantisce che la trasmissione dei pacchetti AutoSupport sia sicura. Il certificato di supporto NetApp è già installato con il software StorageGRID.
 - **Non verificare il certificato:** seleziona questa opzione solo quando hai una buona ragione per non utilizzare la convalida del certificato, ad esempio quando si verifica un problema temporaneo con un certificato.
4. Seleziona **Salva**. Tutti i pacchetti settimanali, attivati dall'utente e attivati da eventi vengono inviati utilizzando il protocollo selezionato.

Disabilita AutoSupport settimanale

Per impostazione predefinita, il sistema StorageGRID è configurato per inviare un pacchetto AutoSupport al supporto tecnico una volta alla settimana.

Per determinare quando verrà inviato il pacchetto AutoSupport settimanale, vai alla scheda *** AutoSupport* > Risultati**. Nella sezione *** AutoSupport settimanale***, osserva il valore per **Prossimo orario pianificato**.

È possibile disattivare in qualsiasi momento l'invio automatico dei pacchetti AutoSupport settimanali.

Passi

1. Selezionare **SUPPORTO > Strumenti > * AutoSupport* > Impostazioni**.
2. Deseleziona la casella di controllo **Abilita AutoSupport settimanale**.
3. Seleziona **Salva**.

Disabilita AutoSupport attivato da eventi

Per impostazione predefinita, il sistema StorageGRID è configurato per inviare un pacchetto AutoSupport al supporto tecnico ogni ora.

È possibile disattivare AutoSupport attivato da eventi in qualsiasi momento.

Passi

1. Selezionare **SUPPORTO > Strumenti > * AutoSupport* > Impostazioni**.
2. Deselezionare la casella di controllo **Abilita AutoSupport attivato da evento**.
3. Seleziona **Salva**.

Abilita AutoSupport su richiesta

AutoSupport on Demand può aiutare a risolvere i problemi su cui il supporto tecnico sta lavorando attivamente.

Per impostazione predefinita, AutoSupport on Demand è disabilitato. Abilitando questa funzionalità, il supporto tecnico potrà richiedere al sistema StorageGRID di inviare automaticamente i pacchetti AutoSupport. Il supporto tecnico può anche impostare l'intervallo di polling per le query AutoSupport on Demand.

Il supporto tecnico non può abilitare o disabilitare AutoSupport on Demand.

Passi

1. Selezionare **SUPPORTO > Strumenti > * AutoSupport* > Impostazioni**.
2. Selezionare **HTTPS** come protocollo.
3. Selezionare la casella di controllo **Abilita AutoSupport settimanale**.
4. Selezionare la casella di controllo **Abilita AutoSupport su richiesta**.
5. Seleziona **Salva**.

AutoSupport on Demand è abilitato e il supporto tecnico può inviare richieste AutoSupport on Demand a StorageGRID.

Disattiva i controlli per gli aggiornamenti software

Per impostazione predefinita, StorageGRID contatta NetApp per determinare se sono disponibili aggiornamenti software per il sistema. Se è disponibile un hotfix o una nuova versione StorageGRID, la nuova versione viene visualizzata nella pagina Aggiornamento StorageGRID.

Se necessario, è possibile disattivare facoltativamente il controllo degli aggiornamenti software. Ad esempio, se il sistema non dispone di accesso WAN, è consigliabile disattivare il controllo per evitare errori di download.

Passi

1. Selezionare **SUPPORTO > Strumenti > * AutoSupport* > Impostazioni**.
2. Deseleziona la casella di controllo **Verifica aggiornamenti software**.
3. Seleziona **Salva**.

Aggiungi una destinazione AutoSupport aggiuntiva

Quando si attiva AutoSupport, i pacchetti di salute e stato vengono inviati al supporto tecnico. È possibile specificare una destinazione aggiuntiva per tutti i pacchetti AutoSupport .

Per verificare o modificare il protocollo utilizzato per inviare i pacchetti AutoSupport , vedere le istruzioni per [specificare il protocollo per i pacchetti AutoSupport](#) .



Non è possibile utilizzare il protocollo SMTP per inviare pacchetti AutoSupport a una destinazione aggiuntiva.

Passi

1. Selezionare **SUPPORTO > Strumenti > * AutoSupport* > Impostazioni**.
2. Selezionare **Abilita destinazione AutoSupport aggiuntiva**.
3. Specificare quanto segue:

Nome host

Il nome host del server o l'indirizzo IP di un server di destinazione AutoSupport aggiuntivo.



È possibile inserire solo una destinazione aggiuntiva.

Porta

Porta utilizzata per connettersi a un server di destinazione AutoSupport aggiuntivo. La porta predefinita è 80 per HTTP o la porta 443 per HTTPS.

Convalida del certificato

Se viene utilizzato un certificato TLS per proteggere la connessione alla destinazione aggiuntiva.

- Selezionare **Verifica certificato** per utilizzare la convalida del certificato.
- Seleziona **Non verificare il certificato** per inviare i pacchetti AutoSupport senza convalida del certificato.

Selezionare questa opzione solo quando si ha una buona ragione per non utilizzare la convalida del certificato, ad esempio quando si verifica un problema temporaneo con un certificato.

4. Se hai selezionato **Verifica certificato**, procedi come segue:
 - a. Passare alla posizione del certificato CA.
 - b. Carica il file del certificato CA.

Vengono visualizzati i metadati del certificato CA.

5. Seleziona **Salva**.

Tutti i futuri pacchetti AutoSupport settimanali, attivati da eventi e attivati dall'utente verranno inviati alla destinazione aggiuntiva.

Configura AutoSupport per gli elettrodomestici

AutoSupport per gli apparecchi segnala problemi hardware StorageGRID , mentre StorageGRID AutoSupport segnala problemi software StorageGRID , con un'eccezione: per SGF6112, StorageGRID AutoSupport

segnala sia problemi hardware che software. È necessario configurare AutoSupport su ogni appliance, ad eccezione di SGF6112, che non richiede alcuna configurazione aggiuntiva. AutoSupport viene implementato in modo diverso per le appliance di servizi e per quelle di storage.

Utilizzare SANtricity per abilitare AutoSupport per ogni appliance di storage. È possibile configurare SANtricity AutoSupport durante la configurazione iniziale dell'appliance o dopo l'installazione dell'appliance:

- Per gli apparecchi SG6000 e SG5700, ["configurare AutoSupport in SANtricity System Manager"](#)

I pacchetti AutoSupport degli appliance E-Series possono essere inclusi in StorageGRID AutoSupport se si configura la distribuzione AutoSupport tramite proxy in ["Gestore del sistema SANtricity"](#).

StorageGRID AutoSupport non segnala problemi hardware, come guasti alla DIMM o alla scheda di interfaccia host (HIC). Tuttavia, alcuni guasti dei componenti potrebbero innescare ["avvisi hardware"](#). Per gli apparecchi StorageGRID dotati di un controller di gestione della scheda base (BMC), è possibile configurare trappole SNMP e e-mail per segnalare guasti hardware:

- ["Imposta notifiche e-mail per gli avvisi BMC"](#)
- ["Configurare le impostazioni SNMP per BMC"](#)

Informazioni correlate

["Supporto NetApp"](#)

Attivare manualmente un pacchetto AutoSupport

Per aiutare il supporto tecnico a risolvere i problemi del sistema StorageGRID, è possibile attivare manualmente l'invio di un pacchetto AutoSupport.

Prima di iniziare

- Devi aver effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- È necessario disporre dell'autorizzazione di accesso Root o di un'altra configurazione della griglia.

Passi

1. Selezionare **SUPPORTO > Strumenti > * AutoSupport***.
2. Nella scheda **Azioni**, seleziona **Invia AutoSupport attivato dall'utente**.

StorageGRID tenta di inviare un pacchetto AutoSupport al sito di supporto NetApp. Se il tentativo ha esito positivo, i valori **Risultato più recente** e **Ultima volta riuscita** nella scheda **Risultati** vengono aggiornati. Se si verifica un problema, il valore **Risultato più recente** viene aggiornato in "Non riuscito" e StorageGRID non tenta più di inviare il pacchetto AutoSupport.



Dopo aver inviato un pacchetto AutoSupport attivato dall'utente, aggiorna la pagina AutoSupport nel browser dopo 1 minuto per accedere ai risultati più recenti.

Risoluzione dei problemi dei pacchetti AutoSupport

Se un tentativo di invio di un pacchetto AutoSupport fallisce, il sistema StorageGRID intraprende azioni diverse a seconda del tipo di pacchetto AutoSupport. È possibile verificare lo stato dei pacchetti AutoSupport selezionando **SUPPORTO > Strumenti > * AutoSupport* > Risultati**.

Se l'invio del pacchetto AutoSupport non riesce, nella scheda **Risultati** della pagina * AutoSupport* viene visualizzato il messaggio "Non riuscito".



Se hai configurato un server proxy per inoltrare i pacchetti AutoSupport a NetApp, dovresti [verificare che le impostazioni di configurazione del server proxy siano corrette](#) .

Errore settimanale del pacchetto AutoSupport

Se un pacchetto AutoSupport settimanale non riesce a essere inviato, il sistema StorageGRID esegue le seguenti azioni:

1. Aggiorna l'attributo Risultato più recente in Nuovo tentativo.
2. Tenta di inviare nuovamente il pacchetto AutoSupport 15 volte ogni quattro minuti per un'ora.
3. Dopo un'ora di errori di invio, aggiorna l'attributo Risultato più recente in Non riuscito.
4. Tenta di inviare nuovamente un pacchetto AutoSupport al successivo orario programmato.
5. Mantiene la normale pianificazione AutoSupport se il pacchetto non riesce perché il servizio NMS non è disponibile e se un pacchetto viene inviato prima che siano trascorsi sette giorni.
6. Quando il servizio NMS è nuovamente disponibile, invia immediatamente un pacchetto AutoSupport se un pacchetto non è stato inviato per sette giorni o più.

Errore del pacchetto AutoSupport attivato dall'utente o dall'evento

Se un pacchetto AutoSupport attivato dall'utente o da un evento non riesce a inviare, il sistema StorageGRID esegue le seguenti azioni:

1. Visualizza un messaggio di errore se l'errore è noto. Ad esempio, se un utente seleziona il protocollo SMTP senza fornire le impostazioni di configurazione e-mail corrette, viene visualizzato il seguente errore:
`AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. Non tenta di inviare nuovamente il pacco.
3. Registra l'errore in `nms.log` .

Se si verifica un errore e SMTP è il protocollo selezionato, verificare che il server di posta elettronica del sistema StorageGRID sia configurato correttamente e che il server di posta elettronica sia in esecuzione (**SUPPORTO > Allarmi (legacy) > Configurazione posta elettronica legacy**). Nella pagina AutoSupport potrebbe apparire il seguente messaggio di errore: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Scopri come ["configurare le impostazioni del server di posta elettronica"](#) .

Correggere un errore del pacchetto AutoSupport

Se si verifica un errore e SMTP è il protocollo selezionato, verificare che il server di posta elettronica del sistema StorageGRID sia configurato correttamente e che il server di posta elettronica sia in esecuzione. Nella pagina AutoSupport potrebbe apparire il seguente messaggio di errore: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Inviare pacchetti E-Series AutoSupport tramite StorageGRID

È possibile inviare i pacchetti E-Series SANtricity System Manager AutoSupport al

supporto tecnico tramite un nodo di amministrazione StorageGRID anziché tramite la porta di gestione dell'appliance di archiviazione.

Vedere ["AutoSupport hardware serie E"](#) per ulteriori informazioni sull'utilizzo di AutoSupport con gli apparecchi della serie E.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager tramite un ["browser web supportato"](#) .
- Tu hai il ["Amministratore dell'appliance di archiviazione o autorizzazione di accesso root"](#) .
- Hai configurato SANtricity AutoSupport:
 - Per gli apparecchi SG6000 e SG5700, ["configurare AutoSupport in SANtricity System Manager"](#)



Per accedere a SANtricity System Manager tramite Grid Manager è necessario disporre del firmware SANtricity 8.70 o superiore.

Informazioni su questo compito

I pacchetti E-Series AutoSupport contengono dettagli sull'hardware di archiviazione e sono più specifici rispetto ad altri pacchetti AutoSupport inviati dal sistema StorageGRID .

È possibile configurare un indirizzo server proxy speciale in SANtricity System Manager per trasmettere i pacchetti AutoSupport tramite un nodo di amministrazione StorageGRID senza utilizzare la porta di gestione dell'appliance. I pacchetti AutoSupport trasmessi in questo modo vengono inviati dal ["mittente preferito Nodo amministratore"](#) e usano qualsiasi ["impostazioni proxy amministratore"](#) che sono stati configurati in Grid Manager.

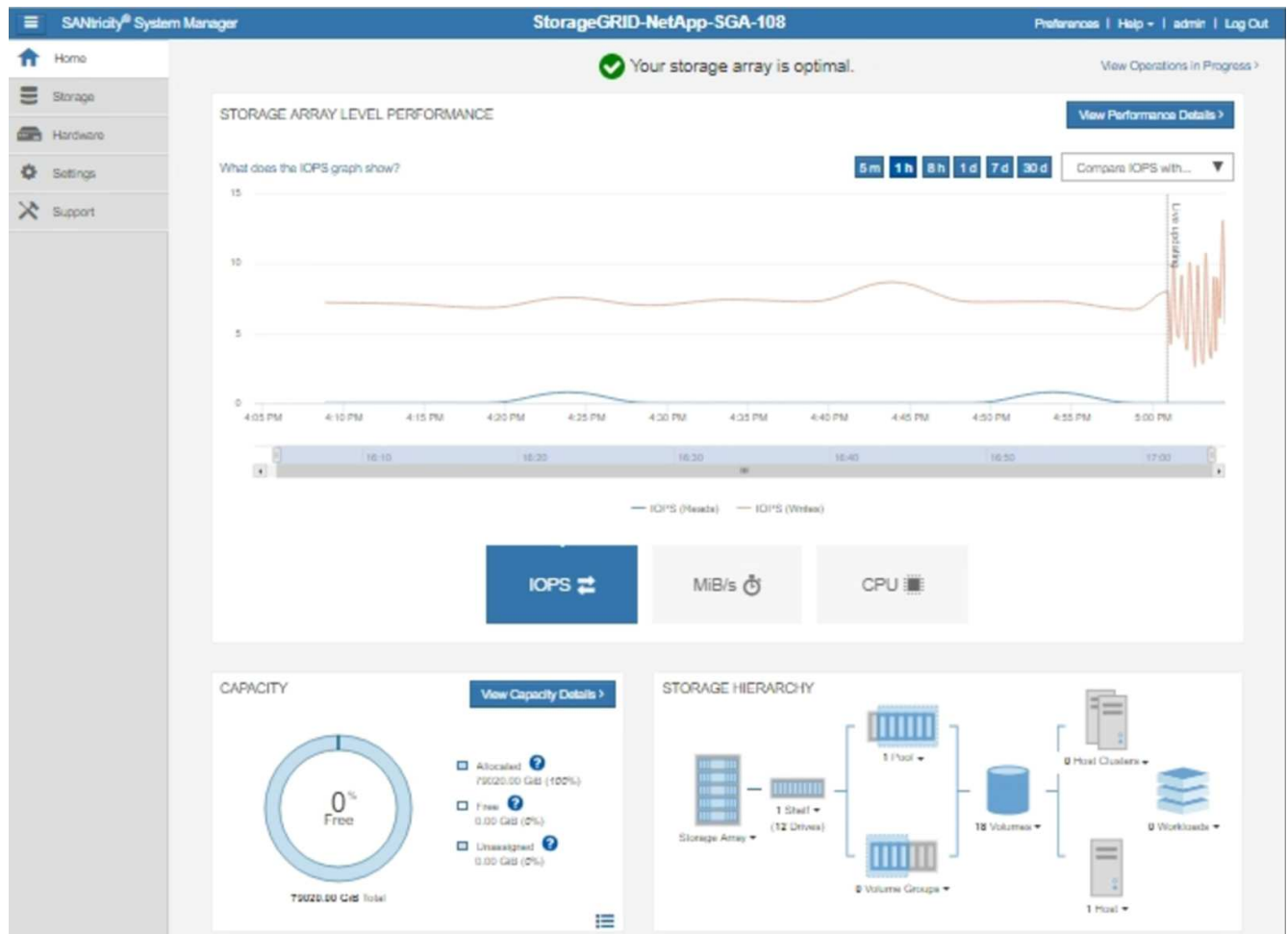


Questa procedura è valida solo per la configurazione di un server proxy StorageGRID per i pacchetti E-Series AutoSupport . Per ulteriori dettagli sulla configurazione di E-Series AutoSupport , vedere ["Documentazione NetApp E-Series e SANtricity"](#) .

Passi

1. Nel Grid Manager, seleziona **NODI**.
2. Dall'elenco dei nodi a sinistra, seleziona il nodo dell'appliance di archiviazione che desideri configurare.
3. Selezionare * SANtricity System Manager*.

Viene visualizzata la home page di SANtricity System Manager.



4. Selezionare **SUPPORTO** > **Centro assistenza** > * AutoSupport*.

Viene visualizzata la pagina delle operazioni di AutoSupport .

Technical Support

Chassis serial number: 031517000693

 [NetApp My Support](#)

US/Canada 888.463.8277

[Other Contacts](#)

Support Resources

Diagnostics

AutoSupport

AutoSupport operations

AutoSupport status: Enabled ?

[Enable/Disable AutoSupport Features](#)

AutoSupport proactively monitors the health of your storage array and automatically sends support data ("dispatches") to the support team.

[Configure AutoSupport Delivery Method](#)

Connect to the support team via HTTPS, HTTP or Mail (SMTP) server delivery methods.

[Schedule AutoSupport Dispatches](#)

AutoSupport dispatches are sent daily at 03:06 PM UTC and weekly at 07:39 AM UTC on Thursday.

[Send AutoSupport Dispatch](#)

Automatically sends the support team a dispatch to troubleshoot system issues without waiting for periodic dispatches.

[View AutoSupport Log](#)

The AutoSupport log provides information about status, dispatch history, and errors encountered during delivery of AutoSupport dispatches.

[Enable AutoSupport Maintenance Window](#)

Enable AutoSupport Maintenance window to allow maintenance activities to be performed on the storage array without generating support cases.

[Disable AutoSupport Maintenance Window](#)

Disable AutoSupport Maintenance window to allow the storage array to generate support cases on component failures and other destructive actions.

5. Selezionare *Configura metodo di consegna AutoSupport*.

Viene visualizzata la pagina Configura metodo di consegna AutoSupport .

6. Selezionare **HTTPS** come metodo di consegna.



Il certificato che abilita HTTPS è preinstallato.

7. Selezionare **tramite server proxy**.

8. Entra `tunnel-host` per l'**Indirizzo host**.

`tunnel-host` è l'indirizzo speciale per utilizzare un nodo di amministrazione per inviare pacchetti E-Series AutoSupport .

9. Entra `10225` per il **Numero di porta**.

`10225` è il numero di porta sul server proxy StorageGRID che riceve i pacchetti AutoSupport dal controller E-Series nell'appliance.

10. Selezionare **Test configurazione** per testare il routing e la configurazione del server proxy AutoSupport .

Se è corretto, viene visualizzato un messaggio in un banner verde: "La configurazione AutoSupport è stata verificata".

Se il test fallisce, viene visualizzato un messaggio di errore in un banner rosso. Controlla le impostazioni DNS e di rete StorageGRID , assicurati che "[mittente preferito](#) [Nodo amministratore](#)" puoi connetterti al sito di supporto NetApp e riprovare il test.

11. Seleziona **Salva**.

La configurazione viene salvata e viene visualizzato un messaggio di conferma: "Il metodo di consegna AutoSupport è stato configurato".

Gestisci nodi di archiviazione

Gestisci nodi di archiviazione

I nodi di archiviazione forniscono capacità e servizi di archiviazione su disco. La gestione dei nodi di archiviazione comporta quanto segue:

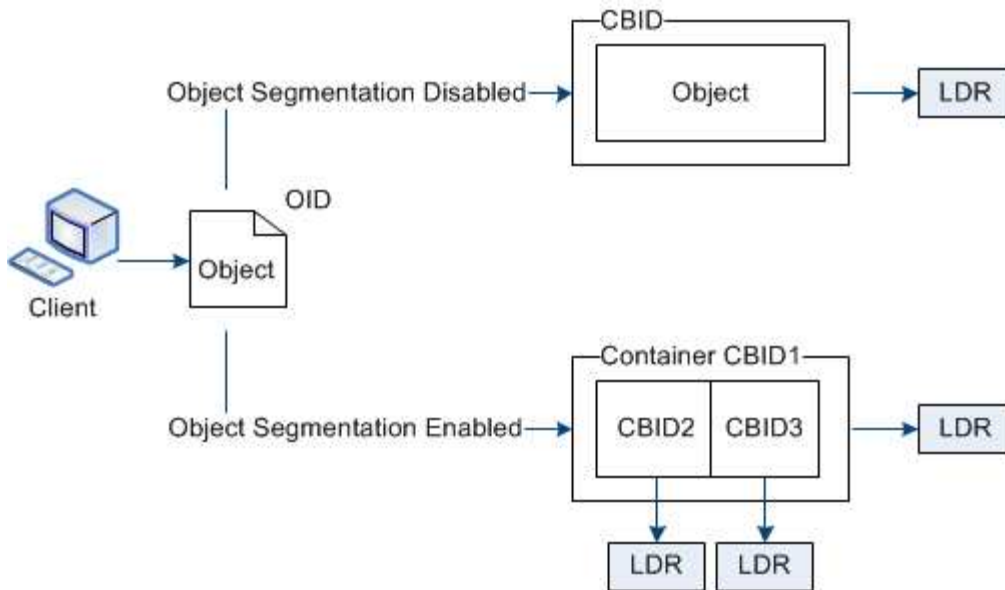
- Gestione delle opzioni di archiviazione
- Comprendere cosa sono le filigrane del volume di archiviazione e come è possibile utilizzare gli override delle filigrane per controllare quando i nodi di archiviazione diventano di sola lettura
- Monitoraggio e gestione dello spazio utilizzato per i metadati degli oggetti
- Configurazione delle impostazioni globali per gli oggetti memorizzati
- Applicazione delle impostazioni di configurazione del nodo di archiviazione
- Gestione di nodi di archiviazione completi

Utilizzare le opzioni di archiviazione

Che cos'è la segmentazione degli oggetti?

La segmentazione degli oggetti è il processo di suddivisione di un oggetto in una raccolta di oggetti più piccoli di dimensioni fisse per ottimizzare l'archiviazione e l'utilizzo delle risorse per oggetti di grandi dimensioni. Il caricamento multiparte di S3 crea anche oggetti segmentati, con un oggetto che rappresenta ogni parte.

Quando un oggetto viene inserito nel sistema StorageGRID , il servizio LDR lo suddivide in segmenti e crea un contenitore di segmenti che elenca le informazioni di intestazione di tutti i segmenti come contenuto.



Al recupero di un contenitore di segmenti, il servizio LDR assembla l'oggetto originale dai suoi segmenti e restituisce l'oggetto al client.

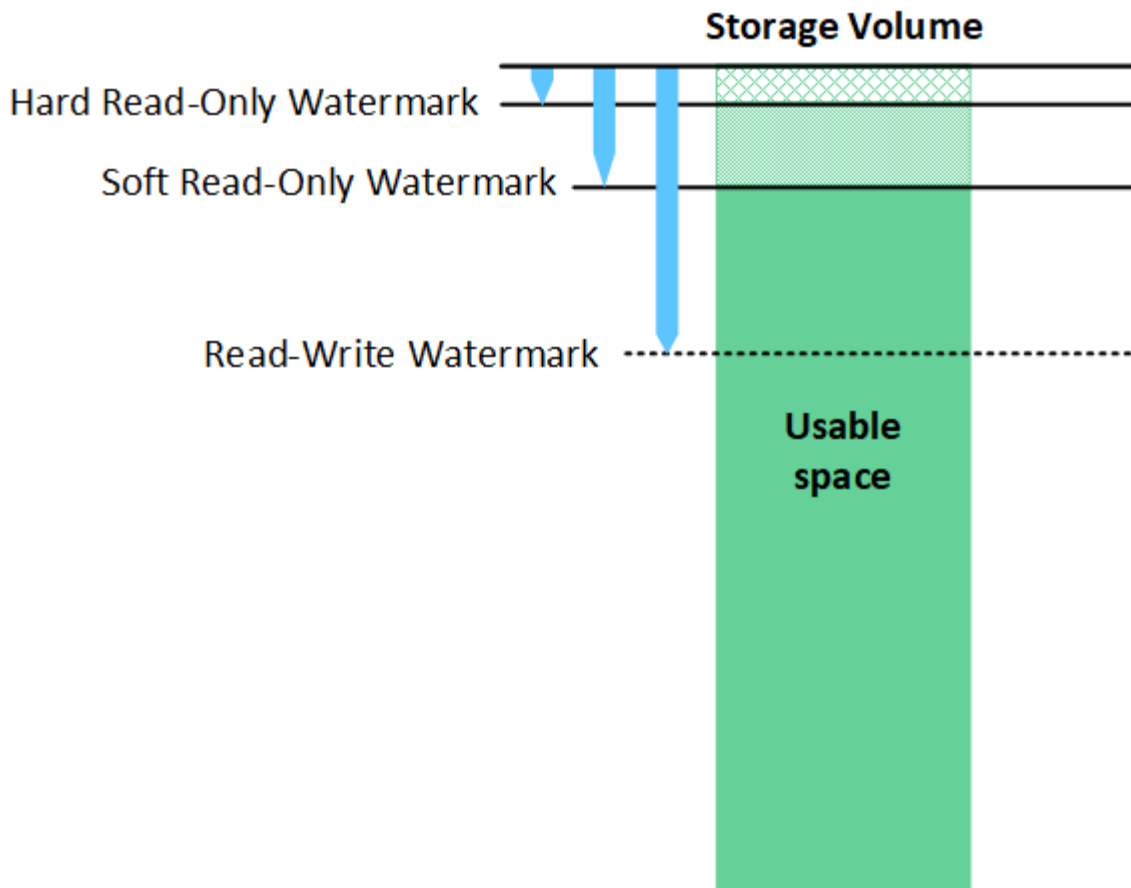
Il contenitore e i segmenti non sono necessariamente archiviati sullo stesso nodo di archiviazione. Il contenitore e i segmenti possono essere archiviati su qualsiasi nodo di archiviazione all'interno del pool di archiviazione specificato nella regola ILM.

Ogni segmento viene trattato in modo indipendente dal sistema StorageGRID e contribuisce al conteggio di attributi quali oggetti gestiti e oggetti archiviati. Ad esempio, se un oggetto archiviato nel sistema StorageGRID viene suddiviso in due segmenti, il valore degli oggetti gestiti aumenta di tre volte al termine dell'acquisizione, come segue:

```
segment container + segment 1 + segment 2 = three stored objects
```

Cosa sono le filigrane del volume di archiviazione?

StorageGRID utilizza tre filigrane di volume di archiviazione per garantire che i nodi di archiviazione vengano trasferiti in modo sicuro a uno stato di sola lettura prima che lo spazio si esaurisca in modo critico e per consentire ai nodi di archiviazione che sono stati trasferiti a uno stato di sola lettura di tornare allo stato di lettura-scrittura.



Le filigrane del volume di archiviazione si applicano solo allo spazio utilizzato per i dati degli oggetti replicati e codificati per la cancellazione. Per informazioni sullo spazio riservato ai metadati degli oggetti sul volume 0, vai a ["Gestire l'archiviazione dei metadati degli oggetti"](#).

Cos'è la filigrana di sola lettura?

La **filigrana di sola lettura software del volume di archiviazione** è la prima filigrana a indicare che lo spazio utilizzabile di un nodo di archiviazione per i dati degli oggetti si sta esaurendo.

Se ogni volume in un nodo di archiviazione ha meno spazio libero rispetto alla filigrana di sola lettura software di quel volume, il nodo di archiviazione passa alla *modalità di sola lettura*. La modalità di sola lettura significa che il nodo di archiviazione pubblicizza servizi di sola lettura al resto del sistema StorageGRID, ma soddisfa tutte le richieste di scrittura in sospeso.

Ad esempio, supponiamo che ogni volume in un nodo di archiviazione abbia una filigrana di sola lettura software di 10 GB. Non appena ogni volume ha meno di 10 GB di spazio libero, il nodo di archiviazione passa alla modalità di sola lettura software.

Cos'è la filigrana di sola lettura?

La **filigrana di sola lettura fissa del volume di archiviazione** è la filigrana successiva che indica che lo spazio utilizzabile di un nodo per i dati degli oggetti si sta riempiendo.

Se lo spazio libero su un volume è inferiore al limite di sola lettura fisso del volume, le scritture sul volume non riusciranno. Tuttavia, le scritture su altri volumi possono continuare finché lo spazio libero su tali volumi non è inferiore alle relative filigrane di sola lettura.

Ad esempio, supponiamo che ogni volume in un nodo di archiviazione abbia una filigrana di sola lettura fissa di 5 GB. Non appena ogni volume ha meno di 5 GB di spazio libero, il nodo di archiviazione non accetta più richieste di scrittura.

La filigrana di sola lettura fissa è sempre inferiore alla filigrana di sola lettura flessibile.

Cos'è la filigrana di lettura-scrittura?

La **filigrana di lettura-scrittura del volume di archiviazione** si applica solo ai nodi di archiviazione che sono passati alla modalità di sola lettura. Determina quando il nodo può tornare ad essere di lettura-scrittura. Quando lo spazio libero su un volume di archiviazione in un nodo di archiviazione è maggiore del limite di lettura-scrittura del volume, il nodo torna automaticamente allo stato di lettura-scrittura.

Supponiamo, ad esempio, che il nodo di archiviazione sia passato alla modalità di sola lettura. Supponiamo inoltre che ogni volume abbia una filigrana di lettura-scrittura di 30 GB. Non appena lo spazio libero per un volume aumenta a 30 GB, il nodo torna ad essere di lettura-scrittura.

La filigrana di lettura-scrittura è sempre più grande sia della filigrana di sola lettura software che di quella di sola lettura hardware.

Visualizza le filigrane del volume di archiviazione

È possibile visualizzare le impostazioni correnti della filigrana e i valori ottimizzati dal sistema. Se non vengono utilizzate filigrane ottimizzate, puoi valutare se puoi o dovresti modificare le impostazioni.

Prima di iniziare

- Hai completato l'aggiornamento a StorageGRID 11.6 o versione successiva.
- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["Permesso di accesso root"](#).

Visualizza le impostazioni correnti della filigrana

È possibile visualizzare le impostazioni correnti della filigrana di archiviazione in Grid Manager.

Passi

1. Selezionare **SUPPORTO > Altro > Filigrane di archiviazione**.
2. Nella pagina Filigrane di archiviazione, controlla la casella di controllo Usa valori ottimizzati.
 - Se la casella di controllo è selezionata, tutte e tre le filigrane vengono ottimizzate per ogni volume di archiviazione su ogni nodo di archiviazione, in base alle dimensioni del nodo di archiviazione e alla capacità relativa del volume.

Questa è l'impostazione predefinita e consigliata. Non aggiornare questi valori. Facoltativamente, puoi [Visualizza le filigrane di archiviazione ottimizzate](#).
 - Se la casella di controllo Usa valori ottimizzati non è selezionata, vengono utilizzate filigrane personalizzate (non ottimizzate). Si sconsiglia di utilizzare impostazioni di filigrana personalizzate. Utilizzare le istruzioni per ["risoluzione dei problemi avvisi di override della filigrana di sola lettura bassa"](#) per determinare se è possibile o opportuno modificare le impostazioni.

Quando si specificano impostazioni di filigrana personalizzate, è necessario immettere valori maggiori di 0.

Visualizza le filigrane di archiviazione ottimizzate

StorageGRID utilizza due metriche Prometheus per mostrare i valori ottimizzati calcolati per la filigrana di sola lettura software del volume di archiviazione. È possibile visualizzare i valori ottimizzati minimi e massimi per ciascun nodo di archiviazione nella griglia.

1. Selezionare **SUPPORTO > Strumenti > Metriche**.
2. Nella sezione Prometheus, seleziona il collegamento per accedere all'interfaccia utente di Prometheus.
3. Per visualizzare il watermark minimo consigliato per la sola lettura software, immettere la seguente metrica Prometheus e selezionare **Esegui**:

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

L'ultima colonna mostra il valore minimo ottimizzato della filigrana di sola lettura software per tutti i volumi di archiviazione su ciascun nodo di archiviazione. Se questo valore è maggiore dell'impostazione personalizzata per la filigrana di sola lettura software del volume di archiviazione, viene attivato l'avviso **Sostituzione filigrana di sola lettura insufficiente** per il nodo di archiviazione.

4. Per visualizzare il limite massimo consigliato per la sola lettura software, immettere la seguente metrica Prometheus e selezionare **Esegui**:

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

L'ultima colonna mostra il valore massimo ottimizzato della filigrana di sola lettura software per tutti i volumi di archiviazione su ciascun nodo di archiviazione.

Gestire l'archiviazione dei metadati degli oggetti

La capacità dei metadati degli oggetti di un sistema StorageGRID controlla il numero massimo di oggetti che possono essere archiviati su quel sistema. Per garantire che il sistema StorageGRID disponga di spazio adeguato per archiviare nuovi oggetti, è necessario comprendere dove e come StorageGRID archivia i metadati degli oggetti.

Cosa sono i metadati degli oggetti?

I metadati di un oggetto sono tutte le informazioni che descrivono un oggetto. StorageGRID utilizza i metadati degli oggetti per tracciare le posizioni di tutti gli oggetti nella griglia e per gestire il ciclo di vita di ciascun oggetto nel tempo.

Per un oggetto in StorageGRID, i metadati dell'oggetto includono i seguenti tipi di informazioni:

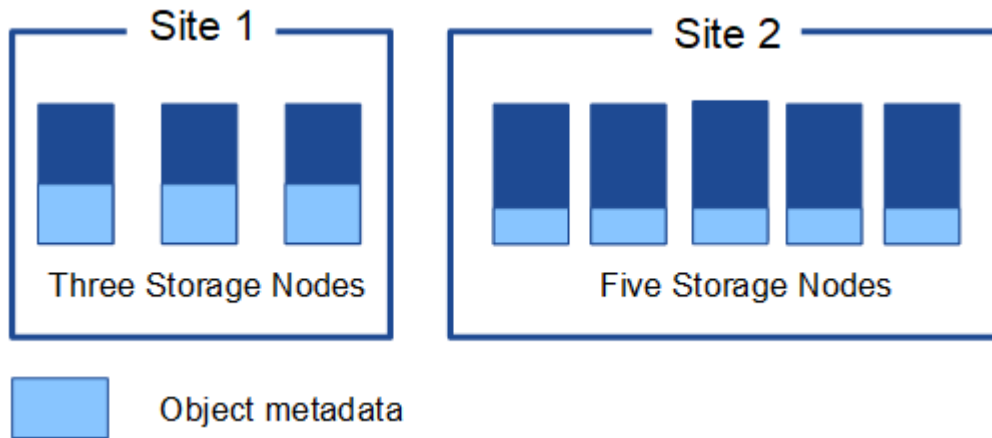
- Metadati di sistema, tra cui un ID univoco per ciascun oggetto (UUID), il nome dell'oggetto, il nome del bucket S3, il nome o l'ID dell'account tenant, la dimensione logica dell'oggetto, la data e l'ora in cui l'oggetto è stato creato per la prima volta e la data e l'ora in cui l'oggetto è stato modificato per l'ultima volta.
- Qualsiasi coppia chiave-valore di metadati utente personalizzati associata all'oggetto.
- Per gli oggetti S3, qualsiasi coppia chiave-valore del tag oggetto associata all'oggetto.
- Per le copie di oggetti replicati, la posizione di archiviazione corrente di ciascuna copia.
- Per le copie di oggetti con codice di cancellazione, la posizione di archiviazione corrente di ciascun frammento.

- Per le copie di oggetti in un Cloud Storage Pool, la posizione dell'oggetto, incluso il nome del bucket esterno e l'identificatore univoco dell'oggetto.
- Per oggetti segmentati e oggetti multiparte, identificatori di segmento e dimensioni dei dati.

Come vengono archiviati i metadati degli oggetti?

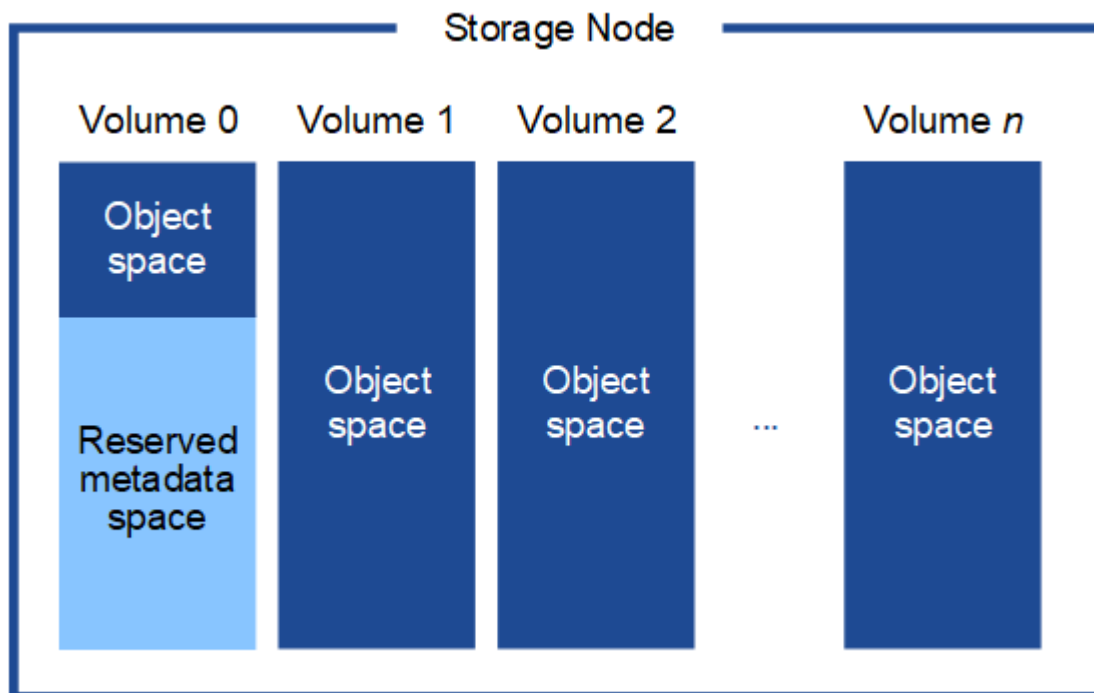
StorageGRID conserva i metadati degli oggetti in un database Cassandra, che viene archiviato indipendentemente dai dati degli oggetti. Per garantire ridondanza e proteggere i metadati degli oggetti dalla perdita, StorageGRID memorizza tre copie dei metadati per tutti gli oggetti nel sistema in ogni sito.

Questa figura rappresenta i nodi di archiviazione in due siti. Ogni sito ha la stessa quantità di metadati degli oggetti e i metadati di ogni sito sono suddivisi tra tutti i nodi di archiviazione di quel sito.



Dove vengono archiviati i metadati degli oggetti?

Questa cifra rappresenta i volumi di archiviazione per un singolo nodo di archiviazione.



Come mostrato nella figura, StorageGRID riserva spazio per i metadati degli oggetti sul volume di archiviazione 0 di ciascun nodo di archiviazione. Utilizza lo spazio riservato per memorizzare i metadati degli

oggetti e per eseguire operazioni essenziali sul database. Tutto lo spazio rimanente sul volume di archiviazione 0 e su tutti gli altri volumi di archiviazione nel nodo di archiviazione viene utilizzato esclusivamente per i dati degli oggetti (copie replicate e frammenti con codice di cancellazione).

La quantità di spazio riservata ai metadati degli oggetti su un particolare nodo di archiviazione dipende da diversi fattori, descritti di seguito.

Impostazione dello spazio riservato ai metadati

Lo *Spazio riservato ai metadati* è un'impostazione a livello di sistema che rappresenta la quantità di spazio che verrà riservata ai metadati sul volume 0 di ogni nodo di archiviazione. Come mostrato nella tabella, il valore predefinito di questa impostazione si basa su:

- La versione del software che stavi utilizzando quando hai installato inizialmente StorageGRID.
- La quantità di RAM su ciascun nodo di archiviazione.

Versione utilizzata per l'installazione iniziale StorageGRID	Quantità di RAM sui nodi di archiviazione	Impostazione predefinita dello spazio riservato ai metadati
da 11,5 a 11,9	128 GB o più su ciascun nodo di archiviazione nella griglia	8 TB (8.000 GB)
	Meno di 128 GB su qualsiasi nodo di archiviazione nella griglia	3 TB (3.000 GB)
11.1 a 11.4	128 GB o più su ciascun nodo di archiviazione in qualsiasi sito	4 TB (4.000 GB)
	Meno di 128 GB su qualsiasi nodo di archiviazione in ogni sito	3 TB (3.000 GB)
11.0 o precedente	Qualsiasi importo	2 TB (2.000 GB)

Visualizza l'impostazione dello spazio riservato ai metadati

Seguire questi passaggi per visualizzare l'impostazione dello spazio riservato ai metadati per il sistema StorageGRID .

Passi

1. Selezionare **CONFIGURAZIONE > Sistema > Impostazioni di archiviazione**.
2. Nella pagina Impostazioni di archiviazione, espandi la sezione **Spazio riservato metadati**.

Per StorageGRID 11.8 o versioni successive, il valore dello spazio riservato ai metadati deve essere almeno 100 GB e non superiore a 1 PB.

L'impostazione predefinita per una nuova installazione StorageGRID 11.6 o versione successiva in cui ogni nodo di archiviazione ha 128 GB o più di RAM è 8.000 GB (8 TB).

Spazio effettivamente riservato per i metadati

Contrariamente all'impostazione dello spazio riservato ai metadati a livello di sistema, lo *spazio riservato effettivo* per i metadati degli oggetti viene determinato per ciascun nodo di archiviazione. Per ogni nodo di archiviazione, lo spazio effettivamente riservato per i metadati dipende dalla dimensione del volume 0 per il nodo e dall'impostazione dello spazio riservato per i metadati a livello di sistema.

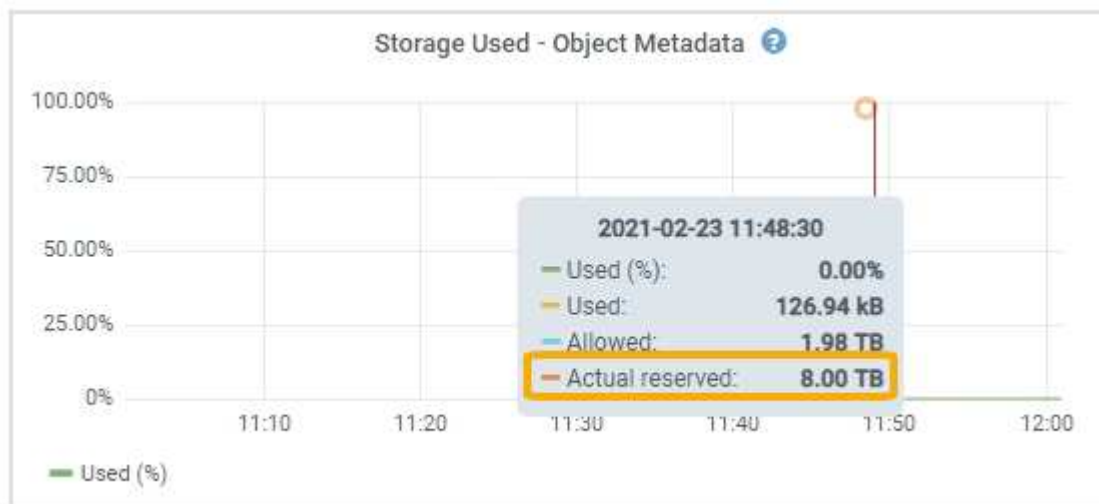
Dimensione del volume 0 per il nodo	Spazio effettivamente riservato per i metadati
Meno di 500 GB (uso non produttivo)	10% del volume 0
500 GB o più + o + Nodi di archiviazione solo metadati	Il più piccolo di questi valori: • Volume 0 • Impostazione dello spazio riservato ai metadati Nota: per i nodi di archiviazione solo metadati è richiesto un solo rangedb.

Visualizza lo spazio effettivamente riservato per i metadati

Per visualizzare lo spazio effettivamente riservato per i metadati su un particolare nodo di archiviazione, seguire questi passaggi.

Passi

1. Da Grid Manager, seleziona **NODI > Nodo di archiviazione**.
2. Selezionare la scheda **Archiviazione**.
3. Posiziona il cursore sul grafico Spazio di archiviazione utilizzato - Metadati oggetto e individua il valore **Riservato effettivo**.



Nello screenshot, il valore **effettivo riservato** è 8 TB. Questa schermata riguarda un nodo di archiviazione di grandi dimensioni in una nuova installazione StorageGRID 11.6. Poiché l'impostazione dello spazio riservato ai metadati a livello di sistema è inferiore al volume 0 per questo nodo di archiviazione, lo spazio riservato effettivo per questo nodo è uguale all'impostazione dello spazio riservato ai metadati.

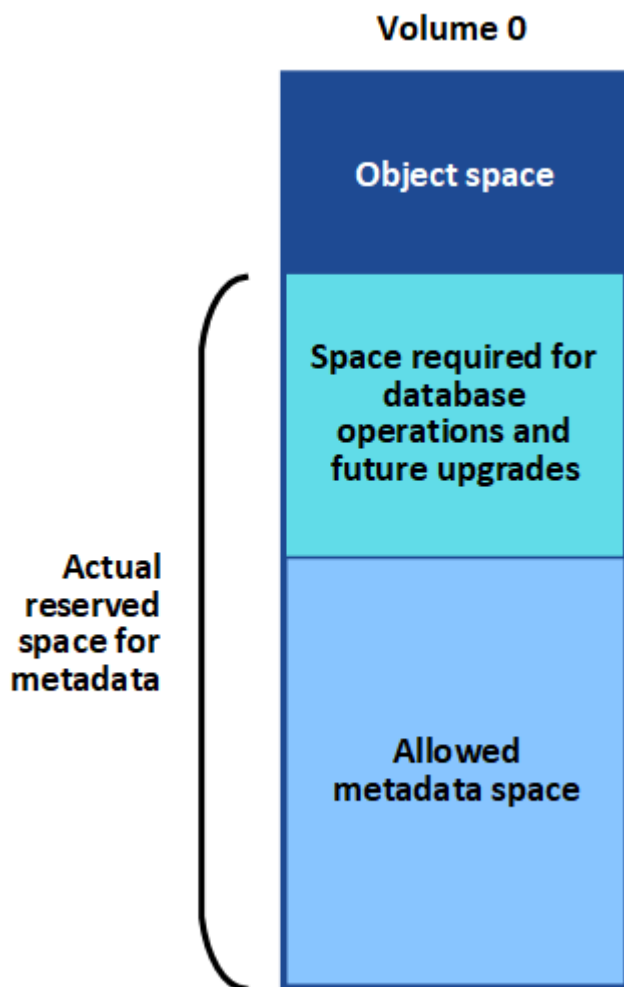
Esempio di spazio metadati effettivamente riservato

Supponiamo di installare un nuovo sistema StorageGRID utilizzando la versione 11.7 o successiva. Per questo esempio, supponiamo che ogni nodo di archiviazione abbia più di 128 GB di RAM e che il volume 0 del nodo di archiviazione 1 (SN1) sia di 6 TB. In base a questi valori:

- Lo **spazio riservato ai metadati** a livello di sistema è impostato su 8 TB. (Questo è il valore predefinito per una nuova installazione StorageGRID 11.6 o versione successiva se ogni nodo di archiviazione ha più di 128 GB di RAM.)
- Lo spazio effettivamente riservato per i metadati per SN1 è di 6 TB. (L'intero volume è riservato perché il volume 0 è più piccolo dell'impostazione **Spazio riservato ai metadati**.)

Spazio metadati consentito

Lo spazio effettivamente riservato per i metadati di ciascun nodo di archiviazione è suddiviso nello spazio disponibile per i metadati degli oggetti (lo *spazio metadati consentito*) e nello spazio richiesto per le operazioni essenziali del database (come la compattazione e la riparazione) e per i futuri aggiornamenti hardware e software. Lo spazio dei metadati consentito regola la capacità complessiva dell'oggetto.



La tabella seguente mostra come StorageGRID calcola lo **spazio metadati consentito** per diversi nodi di archiviazione, in base alla quantità di memoria per il nodo e allo spazio effettivamente riservato per i metadati.

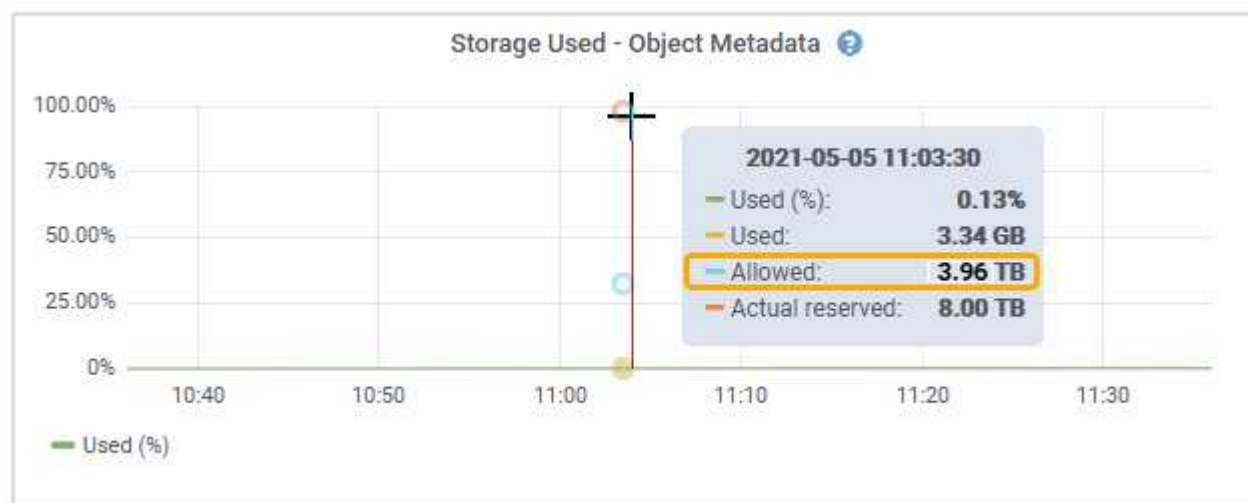
	Quantità di memoria sul nodo di archiviazione		
	< 128 GB	>= 128 GB	Spazio effettivo riservato per i metadati
≤ 4 TB	60% dello spazio effettivamente riservato ai metadati, fino a un massimo di 1,32 TB	60% dello spazio effettivamente riservato ai metadati, fino a un massimo di 1,98 TB	4 TB

Visualizza lo spazio metadati consentito

Per visualizzare lo spazio metadati consentito per un nodo di archiviazione, seguire questi passaggi.

Passi

1. Da Grid Manager, seleziona **NODI**.
2. Selezionare il nodo di archiviazione.
3. Selezionare la scheda **Archiviazione**.
4. Posiziona il cursore sul grafico Metadati oggetto - Spazio di archiviazione utilizzato e individua il valore **Consentito**.



Nello screenshot, il valore **Consentito** è 3,96 TB, che è il valore massimo per un nodo di archiviazione il cui spazio effettivamente riservato per i metadati è superiore a 4 TB.

Il valore **Consentito** corrisponde a questa metrica Prometheus:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Esempio di spazio metadati consentito

Supponiamo di installare un sistema StorageGRID utilizzando la versione 11.6. Per questo esempio, supponiamo che ogni nodo di archiviazione abbia più di 128 GB di RAM e che il volume 0 del nodo di archiviazione 1 (SN1) sia di 6 TB. In base a questi valori:

- Lo **spazio riservato ai metadati** a livello di sistema è impostato su 8 TB. (Questo è il valore predefinito per StorageGRID 11.6 o versioni successive quando ogni nodo di archiviazione ha più di 128 GB di RAM.)
- Lo spazio effettivamente riservato per i metadati per SN1 è di 6 TB. (L'intero volume è riservato perché il volume 0 è più piccolo dell'impostazione **Spazio riservato ai metadati**.)
- Lo spazio consentito per i metadati su SN1 è di 3 TB, in base al calcolo mostrato nella [tabella per lo spazio consentito per i metadati](#) : (Spazio effettivo riservato per i metadati – 1 TB) × 60%, fino a un massimo di 3,96 TB.

Come i nodi di archiviazione di diverse dimensioni influenzano la capacità degli oggetti

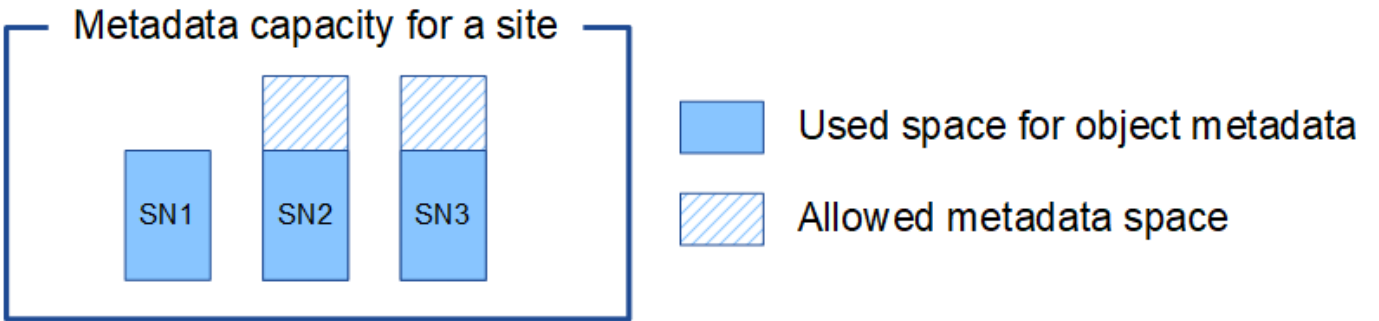
Come descritto sopra, StorageGRID distribuisce uniformemente i metadati degli oggetti tra i nodi di archiviazione in ciascun sito. Per questo motivo, se un sito contiene nodi di archiviazione di dimensioni diverse, il nodo più piccolo del sito determina la capacità dei metadati del sito.

Consideriamo il seguente esempio:

- Si dispone di una griglia a sito singolo contenente tre nodi di archiviazione di dimensioni diverse.
- L'impostazione **Spazio riservato ai metadati** è 4 TB.
- I nodi di archiviazione hanno i seguenti valori per lo spazio metadati effettivamente riservato e lo spazio metadati consentito.

Nodo di archiviazione	Dimensione del volume 0	Spazio metadati effettivamente riservato	Spazio metadati consentito
SN1	2,2 TB	2,2 TB	1,32 TB
SN2	5 TB	4 TB	1,98 TB
SN3	6 TB	4 TB	1,98 TB

Poiché i metadati degli oggetti sono distribuiti uniformemente tra i nodi di archiviazione di un sito, ogni nodo in questo esempio può contenere solo 1,32 TB di metadati. Non è possibile utilizzare gli ulteriori 0,66 TB di spazio metadati consentito per SN2 e SN3.



Analogamente, poiché StorageGRID gestisce tutti i metadati degli oggetti per un sistema StorageGRID in ogni

sito, la capacità complessiva dei metadati di un sistema StorageGRID è determinata dalla capacità dei metadati degli oggetti del sito più piccolo.

E poiché la capacità dei metadati degli oggetti controlla il conteggio massimo degli oggetti, quando un nodo esaurisce la capacità dei metadati, la griglia è di fatto piena.

Informazioni correlate

- Per informazioni su come monitorare la capacità dei metadati degli oggetti per ciascun nodo di archiviazione, consultare le istruzioni per "[Monitoraggio StorageGRID](#)".
- Per aumentare la capacità dei metadati degli oggetti per il tuo sistema, "[espandere una griglia](#)" aggiungendo nuovi nodi di archiviazione.

Aumenta l'impostazione dello spazio riservato ai metadati

Potresti essere in grado di aumentare l'impostazione di sistema Spazio riservato ai metadati se i tuoi nodi di archiviazione soddisfano requisiti specifici per RAM e spazio disponibile.

Cosa ti servirà

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Tu hai il "[Autorizzazione di accesso root o configurazione della pagina topologia griglia e altre autorizzazioni di configurazione griglia](#)".



La pagina Topologia griglia è stata deprecata e verrà rimossa in una versione futura.

Informazioni su questo compito

Potresti essere in grado di aumentare manualmente l'impostazione Spazio riservato metadati a livello di sistema fino a 8 TB.

È possibile aumentare il valore dell'impostazione Spazio riservato metadati a livello di sistema solo se entrambe le seguenti affermazioni sono vere:

- Ogni nodo di archiviazione in qualsiasi sito del sistema dispone di almeno 128 GB di RAM.
- Ciascun nodo di archiviazione in qualsiasi sito del sistema dispone di spazio disponibile sufficiente sul volume di archiviazione 0.

Tieni presente che se aumenti questa impostazione, ridurrai contemporaneamente lo spazio disponibile per l'archiviazione degli oggetti sul volume di archiviazione 0 di tutti i nodi di archiviazione. Per questo motivo, potrebbe essere preferibile impostare lo spazio riservato ai metadati su un valore inferiore a 8 TB, in base ai requisiti previsti per i metadati degli oggetti.



In generale, è meglio usare un valore più alto anziché uno più basso. Se l'impostazione Spazio riservato metadati è troppo grande, è possibile ridurla in seguito. Al contrario, se si aumenta il valore in un secondo momento, il sistema potrebbe dover spostare i dati dell'oggetto per liberare spazio.

Per una spiegazione dettagliata di come l'impostazione Spazio riservato metadati influisce sullo spazio consentito per l'archiviazione dei metadati degli oggetti su un particolare nodo di archiviazione, vedere "[Gestire l'archiviazione dei metadati degli oggetti](#)".

Passi

1. Determina l'impostazione corrente dello spazio riservato ai metadati.
 - a. Selezionare **CONFIGURAZIONE > Sistema > Opzioni di archiviazione**.
 - b. Nella sezione Filigrane di archiviazione, annotare il valore di **Spazio riservato metadati**.
2. Assicurarsi di avere abbastanza spazio disponibile sul volume di archiviazione 0 di ciascun nodo di archiviazione per aumentare questo valore.
 - a. Selezionare **NODES**.
 - b. Selezionare il primo nodo di archiviazione nella griglia.
 - c. Selezionare la scheda Archiviazione.
 - d. Nella sezione Volumi, individuare la voce **/var/local/rangedb/0**.
 - e. Verificare che il valore Disponibile sia uguale o maggiore della differenza tra il nuovo valore che si desidera utilizzare e il valore corrente dello Spazio riservato ai metadati.

Ad esempio, se l'impostazione Spazio riservato metadati è attualmente pari a 4 TB e si desidera aumentarla a 6 TB, il valore Disponibile deve essere pari o superiore a 2 TB.

- f. Ripetere questi passaggi per tutti i nodi di archiviazione.
 - Se uno o più nodi di archiviazione non dispongono di spazio disponibile sufficiente, il valore Spazio riservato ai metadati non può essere aumentato. Non continuare con questa procedura.
 - Se ogni nodo di archiviazione dispone di spazio sufficiente sul volume 0, procedere al passaggio successivo.
3. Assicurati di avere almeno 128 GB di RAM su ogni nodo di archiviazione.
 - a. Selezionare **NODES**.
 - b. Selezionare il primo nodo di archiviazione nella griglia.
 - c. Selezionare la scheda **Hardware**.
 - d. Passa il cursore sul grafico Utilizzo memoria. Assicurarsi che la **Memoria totale** sia almeno 128 GB.
 - e. Ripetere questi passaggi per tutti i nodi di archiviazione.
 - Se uno o più nodi di archiviazione non dispongono di memoria totale disponibile sufficiente, il valore dello spazio riservato ai metadati non può essere aumentato. Non continuare con questa procedura.
 - Se ogni nodo di archiviazione ha almeno 128 GB di memoria totale, passare al passaggio successivo.
4. Aggiorna l'impostazione Spazio riservato ai metadati.
 - a. Selezionare **CONFIGURAZIONE > Sistema > Opzioni di archiviazione**.
 - b. Selezionare la scheda Configurazione.
 - c. Nella sezione Filigrane di archiviazione, seleziona **Spazio riservato metadati**.
 - d. Inserisci il nuovo valore.

Ad esempio, per immettere 8 TB, che è il valore massimo supportato, immettere **8000000000000** (8 seguito da 12 zeri)

Storage Options

Overview

Configuration



Configure Storage Options

Updated: 2021-12-10 13:48:23 MST

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1000000000

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark Override	0
Storage Volume Soft Read-Only Watermark Override	0
Storage Volume Hard Read-Only Watermark Override	0
Metadata Reserved Space	800000000000

Apply Changes 

a. Selezionare **Applica modifiche**.

Comprimi gli oggetti memorizzati

È possibile abilitare la compressione degli oggetti per ridurre le dimensioni degli oggetti archiviati in StorageGRID, in modo che occupino meno spazio di archiviazione.

Prima di iniziare

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

Informazioni su questo compito

Per impostazione predefinita, la compressione degli oggetti è disabilitata. Se si abilita la compressione, StorageGRID tenta di comprimere ogni oggetto durante il salvataggio, utilizzando la compressione senza perdita di dati.



Se si modifica questa impostazione, ci vorrà circa un minuto prima che la nuova impostazione venga applicata. Il valore configurato viene memorizzato nella cache per migliorare le prestazioni e il ridimensionamento.

Prima di abilitare la compressione degli oggetti, tenere presente quanto segue:

- Non selezionare **Comprimi oggetti memorizzati** a meno che non si sia certi che i dati memorizzati siano comprimibili.
- Le applicazioni che salvano oggetti in StorageGRID potrebbero comprimerli prima di salvarli. Se un'applicazione client ha già compresso un oggetto prima di salvarlo in StorageGRID, la selezione di questa opzione non ridurrà ulteriormente le dimensioni dell'oggetto.
- Non selezionare **Comprimi oggetti archiviati** se si utilizza NetApp FabricPool con StorageGRID.
- Se è selezionata l'opzione **Comprimi oggetti archiviati**, le applicazioni client S3 devono evitare di

eseguire operazioni `GetObject` che specificano un intervallo di byte da restituire. Queste operazioni di "lettura di intervallo" sono inefficienti perché StorageGRID deve effettivamente decomprimere gli oggetti per accedere ai byte richiesti. Le operazioni `GetObject` che richiedono un intervallo ridotto di byte da un oggetto molto grande sono particolarmente inefficienti; ad esempio, è inefficiente leggere un intervallo di 10 MB da un oggetto compresso da 50 GB.

Se gli intervalli vengono letti da oggetti compressi, le richieste del client potrebbero scadere.



Se è necessario comprimere oggetti e l'applicazione client deve utilizzare letture di intervallo, aumentare il timeout di lettura per l'applicazione.

Passi

1. Selezionare **CONFIGURAZIONE > Sistema > Impostazioni di archiviazione > Compressione oggetti**.
2. Selezionare la casella di controllo **Comprimi oggetti memorizzati**.
3. Seleziona **Salva**.

Gestisci nodi di archiviazione completi

Quando i nodi di archiviazione raggiungono la capacità massima, è necessario espandere il sistema StorageGRID aggiungendo nuovo spazio di archiviazione. Sono disponibili tre opzioni: aggiunta di volumi di archiviazione, aggiunta di ripiani di espansione dell'archiviazione e aggiunta di nodi di archiviazione.

Aggiungere volumi di archiviazione

Ogni nodo di archiviazione supporta un numero massimo di volumi di archiviazione. Il massimo definito varia a seconda della piattaforma. Se un nodo di archiviazione contiene un numero di volumi di archiviazione inferiore al massimo consentito, è possibile aggiungere volumi per aumentarne la capacità. Vedi le istruzioni per ["espansione di un sistema StorageGRID"](#).

Aggiungere ripiani di espansione per lo stoccaggio

Alcuni nodi di archiviazione dell'appliance StorageGRID, come SG6060 o SG6160, possono supportare ripiani di archiviazione aggiuntivi. Se si dispone di dispositivi StorageGRID con capacità di espansione che non sono ancora stati ampliati alla capacità massima, è possibile aggiungere ripiani di archiviazione per aumentare la capacità. Vedi le istruzioni per ["espansione di un sistema StorageGRID"](#).

Aggiungi nodi di archiviazione

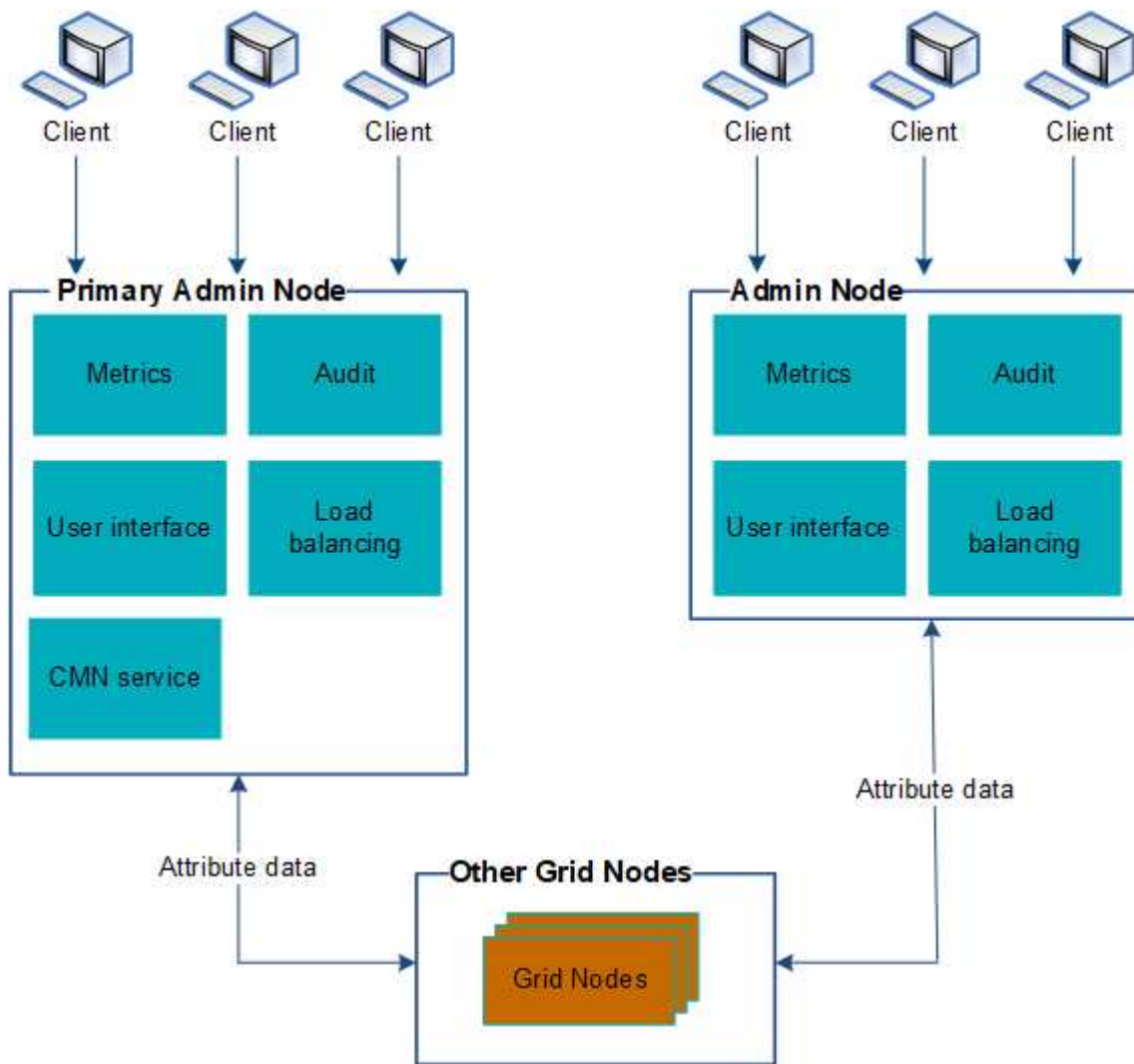
È possibile aumentare la capacità di archiviazione aggiungendo nodi di archiviazione. Quando si aggiunge spazio di archiviazione, è necessario valutare attentamente le regole ILM attualmente attive e i requisiti di capacità. Vedi le istruzioni per ["espansione di un sistema StorageGRID"](#).

Gestisci nodi amministrativi

Utilizzare più nodi di amministrazione

Un sistema StorageGRID può includere più nodi amministrativi per consentirti di monitorare e configurare continuamente il tuo sistema StorageGRID anche in caso di guasto di un nodo amministrativo.

Se un nodo di amministrazione non è più disponibile, l'elaborazione degli attributi continua, gli avvisi vengono comunque attivati e le notifiche e-mail e i pacchetti AutoSupport vengono comunque inviati. Tuttavia, la presenza di più nodi amministrativi non garantisce la protezione dal failover, fatta eccezione per le notifiche e i pacchetti AutoSupport.



Esistono due opzioni per continuare a visualizzare e configurare il sistema StorageGRID in caso di errore di un nodo di amministrazione:

- I client Web possono riconnettersi a qualsiasi altro nodo di amministrazione disponibile.
- Se un amministratore di sistema ha configurato un gruppo ad alta disponibilità di nodi amministrativi, i client Web possono continuare ad accedere a Grid Manager o Tenant Manager utilizzando l'indirizzo IP virtuale del gruppo HA. Vedere ["Gestire gruppi ad alta disponibilità"](#).



Quando si utilizza un gruppo HA, l'accesso viene interrotto se il nodo di amministrazione attivo non funziona. Gli utenti devono effettuare nuovamente l'accesso dopo che l'indirizzo IP virtuale del gruppo HA ha eseguito il failover su un altro nodo di amministrazione nel gruppo.

Alcune attività di manutenzione possono essere eseguite solo tramite il nodo di amministrazione primario. Se il nodo di amministrazione primario si guasta, è necessario ripristinarlo prima che il sistema StorageGRID torni a funzionare correttamente.

Identificare il nodo di amministrazione primario

Il nodo amministrativo primario offre più funzionalità rispetto ai nodi amministrativi non primari. Ad esempio, alcune procedure di manutenzione devono essere eseguite utilizzando il nodo di amministrazione primario.

Per ulteriori informazioni sui nodi di amministrazione, vedere ["Che cos'è un nodo di amministrazione"](#).

Prima di iniziare

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

Passi

1. Selezionare **NODES**.
2. Inserisci **primario** nella casella di ricerca.

Nei risultati della ricerca, identifica il nodo con "Nodo amministratore primario" visualizzato nella colonna Tipo. Dovrebbe essere elencato un nodo di amministrazione primario.

Visualizza lo stato delle notifiche e le code

Il servizio Network Management System (NMS) sui nodi amministrativi invia notifiche al server di posta. È possibile visualizzare lo stato attuale del servizio NMS e la dimensione della coda delle notifiche nella pagina Interface Engine.

Per accedere alla pagina Interface Engine, selezionare **SUPPORTO > Strumenti > Topologia griglia**. Quindi seleziona **site > Admin Node > NMS > Interface Engine**.

Overview	Alarms	Reports	Configuration
Main			
Overview: NMS (170-176) - Interface Engine Updated: 2009-03-09 10:12:17 PDT			
NMS Interface Engine Status:		Connected	
Connected Services:		15	
E-mail Notification Events			
E-mail Notifications Status:		No Errors	
E-mail Notifications Queued:		0	
Database Connection Pool			
Maximum Supported Capacity:		100	
Remaining Capacity:		95 %	
Active Connections:		5	

Le notifiche vengono elaborate tramite la coda delle notifiche e-mail e inviate al server di posta una dopo l'altra nell'ordine in cui vengono attivate. Se si verifica un problema (ad esempio, un errore di connessione di rete) e il server di posta non è disponibile quando si tenta di inviare la notifica, viene effettuato un tentativo di inviare nuovamente la notifica al server di posta per un periodo di 60 secondi. Se la notifica non viene inviata al server di posta entro 60 secondi, viene eliminata dalla coda delle notifiche e viene effettuato un tentativo di inviare la notifica successiva nella coda.

Gestire gli oggetti con ILM

Gestire gli oggetti con ILM

Le regole di gestione del ciclo di vita delle informazioni (ILM) in una policy ILM indicano a StorageGRID come creare e distribuire copie dei dati degli oggetti e come gestire tali copie nel tempo.

Informazioni su queste istruzioni

La progettazione e l'implementazione delle regole e delle politiche ILM richiedono un'attenta pianificazione. È necessario comprendere i requisiti operativi, la topologia del sistema StorageGRID, le esigenze di protezione degli oggetti e i tipi di storage disponibili. Quindi, è necessario stabilire come si desidera che i diversi tipi di oggetti vengano copiati, distribuiti e archiviati.

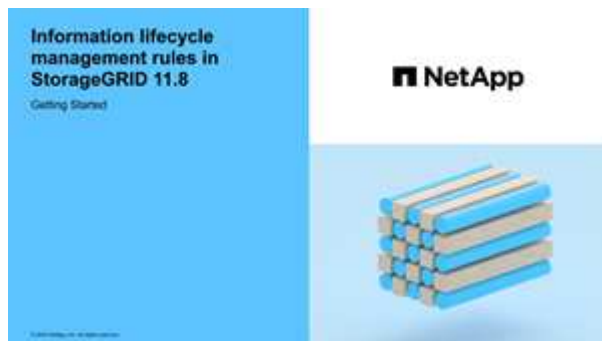
Utilizzare queste istruzioni per:

- Scopri di più su StorageGRID ILM, incluso ["come funziona l'ILM durante tutta la vita di un oggetto"](#).
- Scopri come configurare ["pool di stoccaggio"](#), ["Pool di archiviazione cloud"](#), e ["Regole ILM"](#).
- Impara come ["creare, simulare e attivare una politica ILM"](#) che proteggerà i dati degli oggetti su uno o più siti.
- Impara come ["gestire gli oggetti con S3 Object Lock"](#), che aiuta a garantire che gli oggetti in bucket S3 specifici non vengano eliminati o sovrascritti per un periodo di tempo specificato.

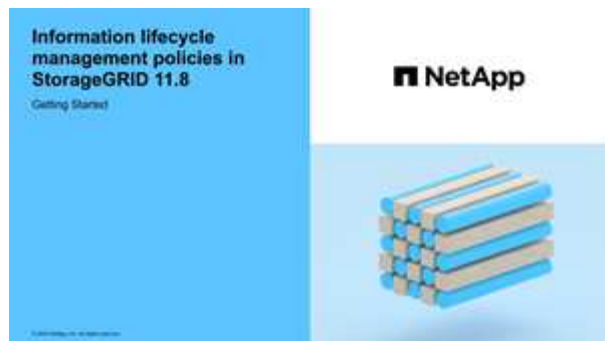
Saperne di più

Per saperne di più, guarda questi video:

- ["Video: panoramica delle regole ILM"](#).



- ["Video: Panoramica delle politiche ILM"](#)



ILM e ciclo di vita degli oggetti

Come funziona l'ILM durante la vita di un oggetto

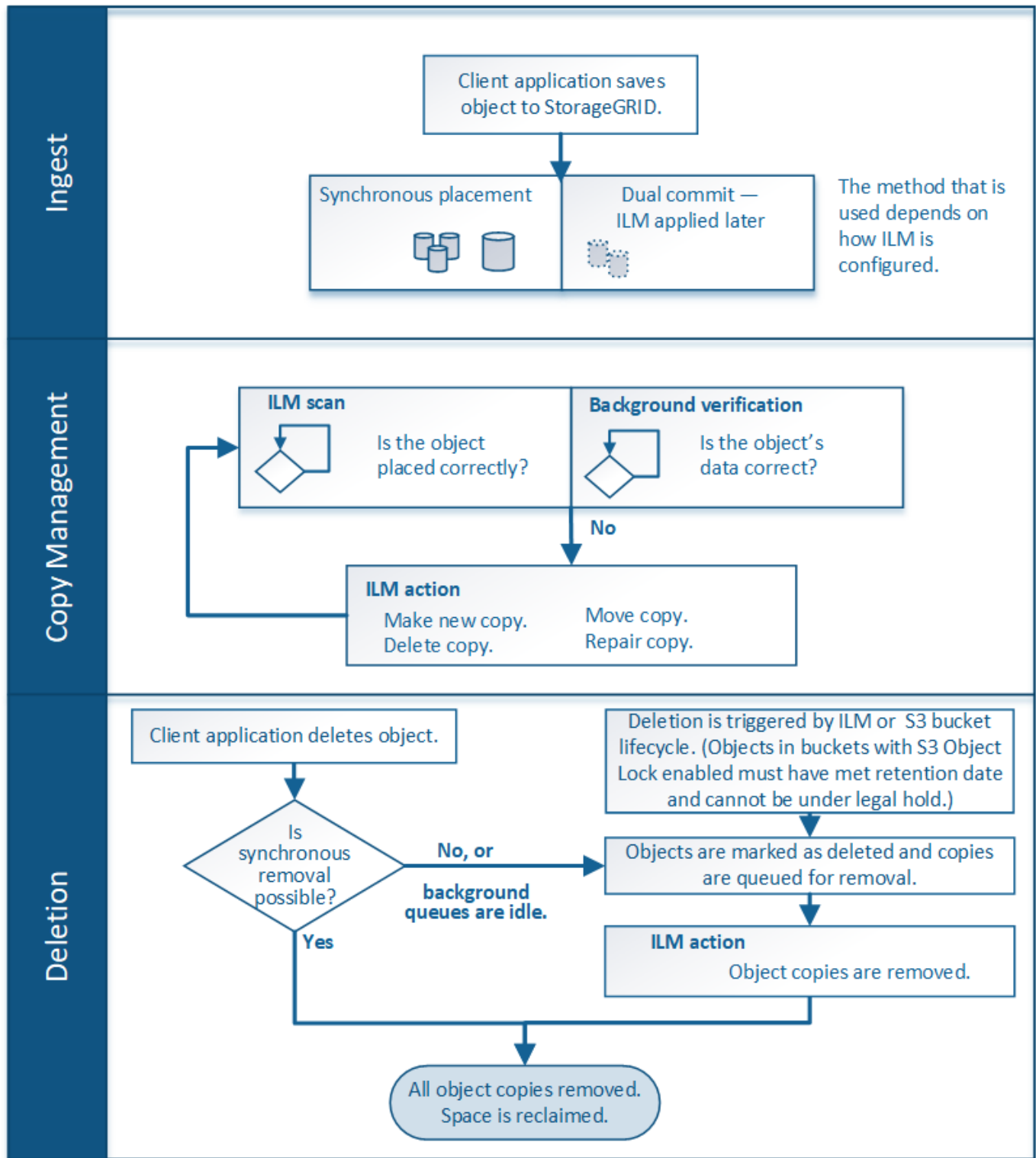
Comprendere come StorageGRID utilizza ILM per gestire gli oggetti in ogni fase del loro ciclo di vita può aiutarti a progettare una policy più efficace.

- **Ingest:** l'ingestione inizia quando un'applicazione client S3 stabilisce una connessione per salvare un oggetto nel sistema StorageGRID e termina quando StorageGRID restituisce al client un messaggio di "ingest riuscito". I dati degli oggetti vengono protetti durante l'acquisizione applicando immediatamente le istruzioni ILM (posizionamento sincrono) oppure creando copie provvisorie e applicando ILM in un secondo momento (doppio commit), a seconda di come sono stati specificati i requisiti ILM.
- **Gestione delle copie:** dopo aver creato il numero e il tipo di copie degli oggetti specificati nelle istruzioni di posizionamento dell'ILM, StorageGRID gestisce le posizioni degli oggetti e li protegge dalla perdita.
 - **Scansione e valutazione ILM:** StorageGRID esegue continuamente la scansione dell'elenco degli oggetti archiviati nella griglia e verifica se le copie correnti soddisfano i requisiti ILM. Quando sono necessari tipi, numeri o posizioni diverse di copie di oggetti, StorageGRID crea, elimina o sposta le copie in base alle necessità.
 - **Verifica in background:** StorageGRID esegue costantemente la verifica in background per controllare l'integrità dei dati degli oggetti. Se viene rilevato un problema, StorageGRID crea automaticamente una nuova copia dell'oggetto o un frammento di oggetto sostitutivo con codice di cancellazione in una posizione che soddisfa i requisiti ILM correnti. Vedere "[Verificare l'integrità dell'oggetto](#)".
- **Eliminazione oggetto:** la gestione di un oggetto termina quando tutte le copie vengono rimosse dal sistema StorageGRID. Gli oggetti possono essere rimossi a seguito di una richiesta di eliminazione da parte di un client, oppure a seguito di un'eliminazione da parte di ILM o causata dalla scadenza del ciclo di vita di un bucket S3.



Gli oggetti in un bucket in cui è abilitato il blocco degli oggetti S3 non possono essere eliminati se sono soggetti a conservazione legale o se è stata specificata una data di conservazione fino a quando non è stata ancora rispettata.

Il diagramma riassume il funzionamento dell'ILM durante l'intero ciclo di vita di un oggetto.



Come vengono ingeriti gli oggetti

Opzioni di acquisizione

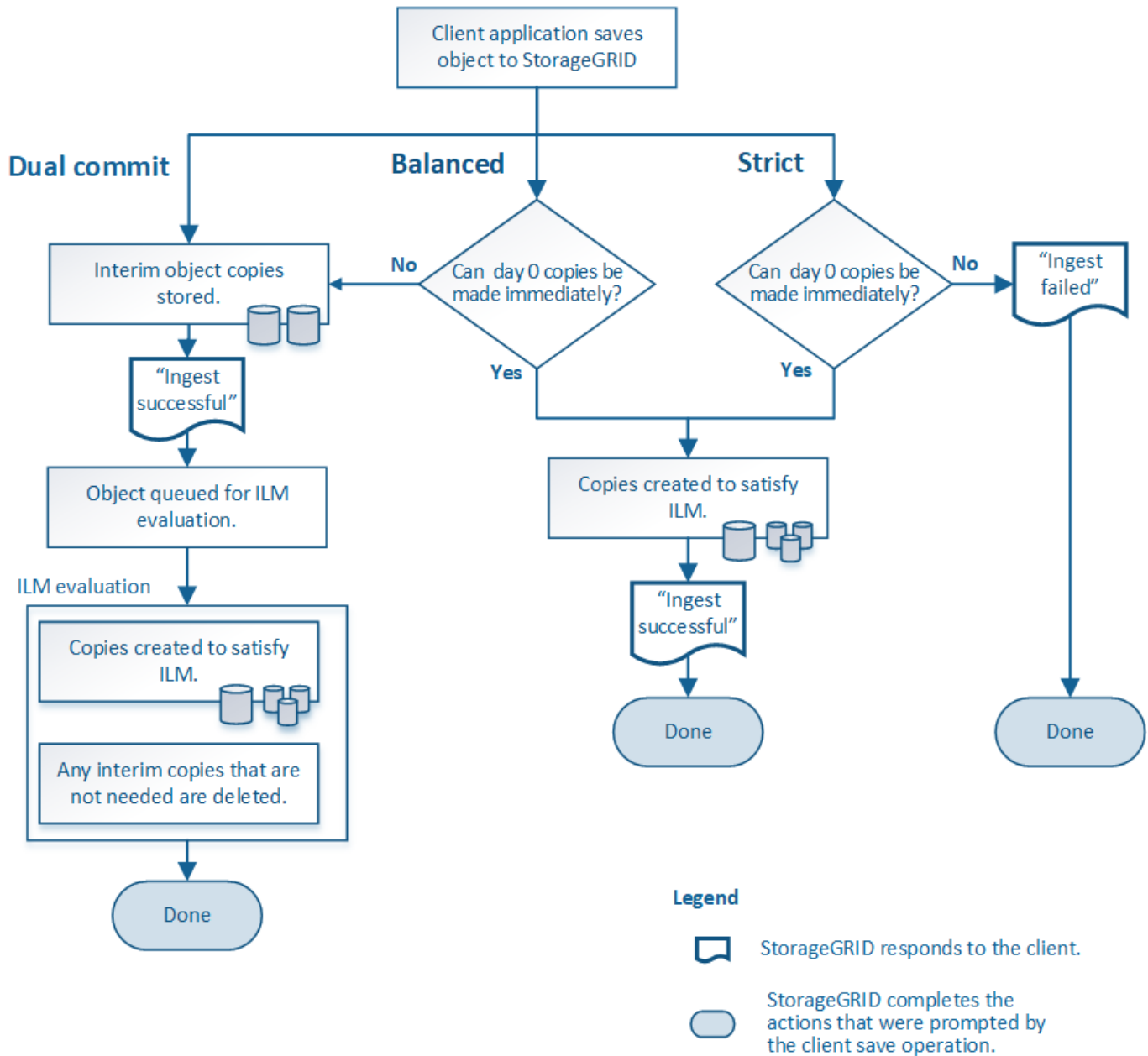
Quando si crea una regola ILM, si specifica una delle tre opzioni per la protezione degli oggetti in fase di acquisizione: Doppio commit, Rigoroso o Bilanciato.

A seconda della scelta, StorageGRID esegue copie provvisorie e mette in coda gli oggetti per una successiva

valutazione ILM, oppure utilizza il posizionamento sincrono ed esegue immediatamente copie per soddisfare i requisiti ILM.

Diagramma di flusso delle opzioni di acquisizione

Il diagramma di flusso mostra cosa accade quando gli oggetti vengono abbinati da una regola ILM che utilizza ciascuna delle tre opzioni di acquisizione.



Doppio impegno

Quando si seleziona l'opzione Dual commit, StorageGRID esegue immediatamente copie provvisorie degli oggetti su due diversi nodi di archiviazione e restituisce al client un messaggio di "ingest riuscito". L'oggetto viene messo in coda per la valutazione ILM e in seguito vengono create copie che soddisfano le istruzioni di posizionamento della regola. Se la policy ILM non può essere elaborata immediatamente dopo il doppio commit, la protezione contro la perdita del sito potrebbe richiedere del tempo.

Utilizzare l'opzione Dual commit in uno di questi casi:

- Stai utilizzando regole ILM multi-sito e la latenza di acquisizione del client è la tua considerazione principale. Quando si utilizza il Dual commit, è necessario assicurarsi che la griglia possa eseguire il lavoro aggiuntivo di creazione e rimozione delle copie dual-commit se non soddisfano ILM. Nello specifico:
 - Il carico sulla rete deve essere sufficientemente basso da evitare un arretrato ILM.
 - La griglia deve disporre di risorse hardware in eccesso (IOPS, CPU, memoria, larghezza di banda di rete e così via).
- Si utilizzano regole ILM multi-sito e la connessione WAN tra i siti presenta solitamente un'elevata latenza o una larghezza di banda limitata. In questo scenario, l'utilizzo dell'opzione Dual commit può aiutare a prevenire i timeout del client. Prima di scegliere l'opzione Dual commit, è opportuno testare l'applicazione client con carichi di lavoro realistici.

Bilanciato (predefinito)

Quando si seleziona l'opzione Bilanciato, StorageGRID utilizza anche il posizionamento sincrono durante l'acquisizione ed esegue immediatamente tutte le copie specificate nelle istruzioni di posizionamento della regola. A differenza dell'opzione Strict, se StorageGRID non riesce a effettuare immediatamente tutte le copie, utilizza invece Dual commit. Se la policy ILM utilizza posizionamenti su più siti e non è possibile ottenere una protezione immediata contro la perdita del sito, viene attivato l'avviso **Posizionamento ILM non realizzabile**.

Utilizzare l'opzione Bilanciata per ottenere la migliore combinazione di protezione dei dati, prestazioni della griglia e successo dell'acquisizione. Bilanciato è l'opzione predefinita nella procedura guidata Crea regola ILM.

Rigorous

Quando si seleziona l'opzione Rigorosa, StorageGRID utilizza il posizionamento sincrono durante l'acquisizione ed esegue immediatamente tutte le copie degli oggetti specificate nelle istruzioni di posizionamento della regola. L'acquisizione non riesce se StorageGRID non riesce a creare tutte le copie, ad esempio perché una posizione di archiviazione richiesta non è temporaneamente disponibile. Il client deve riprovare l'operazione.

Utilizzare l'opzione Rigorosa se si ha un requisito operativo o normativo che impone di archiviare immediatamente gli oggetti solo nelle posizioni indicate nella regola ILM. Ad esempio, per soddisfare un requisito normativo, potrebbe essere necessario utilizzare l'opzione Rigorosa e un filtro avanzato Vincolo di posizione per garantire che gli oggetti non vengano mai archiviati in determinati data center.

Vedere ["Esempio 5: regole e policy ILM per un comportamento di acquisizione rigoroso"](#).

Vantaggi, svantaggi e limitazioni delle opzioni di ingestione

Comprendere i vantaggi e gli svantaggi di ciascuna delle tre opzioni per la protezione dei dati in fase di acquisizione (Balanced, Strict o Dual commit) può aiutarti a decidere quale selezionare per una regola ILM.

Per una panoramica delle opzioni di acquisizione, vedere ["Opzioni di acquisizione"](#).

Vantaggi delle opzioni Bilanciata e Rigorosa

Rispetto al Dual commit, che crea copie provvisorie durante l'acquisizione, le due opzioni di posizionamento sincrono possono offrire i seguenti vantaggi:

- **Maggiore sicurezza dei dati:** i dati degli oggetti vengono immediatamente protetti come specificato nelle istruzioni di posizionamento della regola ILM, che possono essere configurate per proteggere da un'ampia gamma di condizioni di errore, incluso l'errore di più di una posizione di archiviazione. Il doppio commit può

proteggere solo dalla perdita di una singola copia locale.

- **Funzionamento della griglia più efficiente:** ogni oggetto viene elaborato una sola volta, quando viene acquisito. Poiché il sistema StorageGRID non ha bisogno di tracciare o eliminare copie provvisorie, il carico di elaborazione è inferiore e viene consumato meno spazio nel database.
- **(Bilanciato) Consigliato:** l'opzione Bilanciata garantisce un'efficienza ILM ottimale. Si consiglia di utilizzare l'opzione Bilanciata, a meno che non sia richiesto un comportamento di ingestione rigoroso o che la griglia soddisfi tutti i criteri per l'utilizzo del commit doppio.
- **(Rigorosa) Certezza sulla posizione degli oggetti:** l'opzione Rigorosa garantisce che gli oggetti vengano immediatamente archiviati secondo le istruzioni di posizionamento nella regola ILM.

Svantaggi delle opzioni Bilanciata e Rigorosa

Rispetto al Dual commit, le opzioni Balanced e Strict presentano alcuni svantaggi:

- **Ingestione client più lunga:** le latenze di acquisizione client potrebbero essere più lunghe. Quando si utilizzano le opzioni Bilanciato o Rigoroso, il messaggio "ingest riuscito" non viene restituito al client finché non vengono creati e archiviati tutti i frammenti codificati in modo da essere cancellati o le copie replicate. Tuttavia, è molto probabile che i dati degli oggetti raggiungano la loro collocazione finale molto più rapidamente.
- **(Rigoroso) Maggiori tassi di errore di acquisizione:** con l'opzione Rigorosa, l'acquisizione fallisce ogni volta che StorageGRID non riesce a effettuare immediatamente tutte le copie specificate nella regola ILM. Si potrebbero verificare alti tassi di errore di acquisizione se una posizione di archiviazione richiesta è temporaneamente offline o se problemi di rete causano ritardi nella copia di oggetti tra siti.
- **(Rigoroso) In alcune circostanze, i posizionamenti dei carichi multiparte S3 potrebbero non essere quelli previsti:** con Rigoroso, ci si aspetta che gli oggetti vengano posizionati come descritto dalla regola ILM oppure che l'acquisizione non vada a buon fine. Tuttavia, con un caricamento multiparte S3, l'ILM viene valutato per ogni parte dell'oggetto mentre viene acquisito e per l'oggetto nel suo complesso quando il caricamento multiparte viene completato. Nelle seguenti circostanze, ciò potrebbe comportare posizionamenti diversi da quelli previsti:
 - **Se ILM cambia mentre è in corso un caricamento multiparte S3:** poiché ogni parte viene posizionata in base alla regola attiva al momento dell'acquisizione della parte, alcune parti dell'oggetto potrebbero non soddisfare i requisiti ILM correnti al termine del caricamento multiparte. In questi casi l'acquisizione dell'oggetto non fallisce. Invece, qualsiasi parte non posizionata correttamente viene messa in coda per la rivalutazione ILM e successivamente spostata nella posizione corretta.
 - **Quando le regole ILM filtrano in base alle dimensioni:** quando si valuta ILM per una parte, StorageGRID filtra in base alle dimensioni della parte, non in base alle dimensioni dell'oggetto. Ciò significa che parti di un oggetto possono essere archiviate in posizioni che non soddisfano i requisiti ILM per l'oggetto nel suo complesso. Ad esempio, se una regola specifica che tutti gli oggetti da 10 GB o più grandi vengono archiviati in DC1 mentre tutti gli oggetti più piccoli vengono archiviati in DC2, al momento dell'acquisizione ogni parte da 1 GB di un caricamento multiparte da 10 parti viene archiviata in DC2. Quando l'ILM viene valutato per l'oggetto, tutte le parti dell'oggetto vengono spostate in DC1.
- **(Rigoroso) L'inserimento non fallisce quando i tag degli oggetti o i metadati vengono aggiornati e non è possibile effettuare nuovi posizionamenti richiesti:** con Rigoroso, ci si aspetta che gli oggetti vengano posizionati come descritto dalla regola ILM oppure che l'inserimento fallisca. Tuttavia, quando si aggiornano i metadati o i tag per un oggetto già archiviato nella griglia, l'oggetto non viene reinserito. Ciò significa che le modifiche al posizionamento degli oggetti attivate dall'aggiornamento non vengono apportate immediatamente. Le modifiche al posizionamento vengono apportate quando l'ILM viene rivalutato tramite i normali processi ILM in background. Se non è possibile apportare le modifiche di posizionamento richieste (ad esempio perché una posizione appena richiesta non è disponibile), l'oggetto aggiornato mantiene la sua posizione attuale finché non saranno possibili le modifiche di posizionamento.

Limitazioni sul posizionamento degli oggetti con le opzioni Bilanciato e Rigoroso

Le opzioni Bilanciato o Rigoroso non possono essere utilizzate per le regole ILM che hanno una qualsiasi di queste istruzioni di posizionamento:

- Posizionamento in un Cloud Storage Pool al giorno 0.
- Posizionamenti in un pool di archiviazione cloud quando la regola ha un orario di creazione definito dall'utente come orario di riferimento.

Queste restrizioni esistono perché StorageGRID non può creare copie sincrone su un Cloud Storage Pool e un orario di creazione definito dall'utente potrebbe essere risolto nel presente.

Come le regole e la coerenza ILM interagiscono per influenzare la protezione dei dati

Sia la regola ILM che la scelta della coerenza influiscono sul modo in cui gli oggetti vengono protetti. Queste impostazioni possono interagire.

Ad esempio, il comportamento di acquisizione selezionato per una regola ILM influisce sul posizionamento iniziale delle copie degli oggetti, mentre la coerenza utilizzata quando un oggetto viene archiviato influisce sul posizionamento iniziale dei metadati degli oggetti. Poiché StorageGRID richiede l'accesso sia ai dati che ai metadati di un oggetto per soddisfare le richieste dei client, la selezione di livelli di protezione corrispondenti per la coerenza e il comportamento di acquisizione può garantire una migliore protezione iniziale dei dati e risposte di sistema più prevedibili.

Ecco un breve riepilogo dei valori di coerenza disponibili in StorageGRID:

- **Tutti:** tutti i nodi ricevono immediatamente i metadati dell'oggetto, altrimenti la richiesta non andrà a buon fine.
- **Strong-global:** i metadati degli oggetti vengono distribuiti immediatamente a tutti i siti. Garantisce la coerenza di lettura e scrittura per tutte le richieste dei clienti su tutti i siti.
- **Strong-site:** i metadati degli oggetti vengono immediatamente distribuiti agli altri nodi del sito. Garantisce la coerenza di lettura e scrittura per tutte le richieste dei client all'interno di un sito.
- **Lettura dopo nuova scrittura:** garantisce coerenza di lettura dopo scrittura per i nuovi oggetti e coerenza finale per gli aggiornamenti degli oggetti. Offre elevate garanzie di disponibilità e protezione dei dati. Consigliato nella maggior parte dei casi.
- **Disponibile:** fornisce coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono letti raramente o per operazioni HEAD o GET su chiavi inesistenti). Non supportato per i bucket S3 FabricPool.



Prima di selezionare un valore di coerenza, [leggi la descrizione completa della coerenza](#).
Prima di modificare il valore predefinito, è necessario comprenderne i vantaggi e le limitazioni.

Esempio di come la coerenza e le regole ILM possono interagire

Supponiamo di avere una griglia a due siti con la seguente regola ILM e la seguente coerenza:

- **Regola ILM:** creare due copie dell'oggetto, una nel sito locale e una in un sito remoto. Utilizzare un comportamento di acquisizione rigoroso.
- **coerenza:** Strong-global (i metadati degli oggetti vengono distribuiti immediatamente a tutti i siti).

Quando un client memorizza un oggetto nella griglia, StorageGRID esegue entrambe le copie dell'oggetto e

distribuisce i metadati a entrambi i siti prima di restituire l'esito positivo al client.

L'oggetto è completamente protetto contro la perdita al momento dell'acquisizione corretta del messaggio. Ad esempio, se il sito locale viene perso poco dopo l'acquisizione, copie sia dei dati dell'oggetto sia dei metadati dell'oggetto sono ancora presenti nel sito remoto. L'oggetto è completamente recuperabile.

Se invece si utilizzasse la stessa regola ILM e la coerenza del sito forte, il client potrebbe ricevere un messaggio di successo dopo che i dati dell'oggetto sono stati replicati sul sito remoto, ma prima che i metadati dell'oggetto vengano distribuiti lì. In questo caso, il livello di protezione dei metadati degli oggetti non corrisponde al livello di protezione dei dati degli oggetti. Se il sito locale viene perso subito dopo l'acquisizione, anche i metadati dell'oggetto vengono persi. L'oggetto non può essere recuperato.

L'interrelazione tra coerenza e regole ILM può essere complessa. Se hai bisogno di assistenza, contatta NetApp .

Informazioni correlate

["Esempio 5: regole e policy ILM per un comportamento di acquisizione rigoroso"](#)

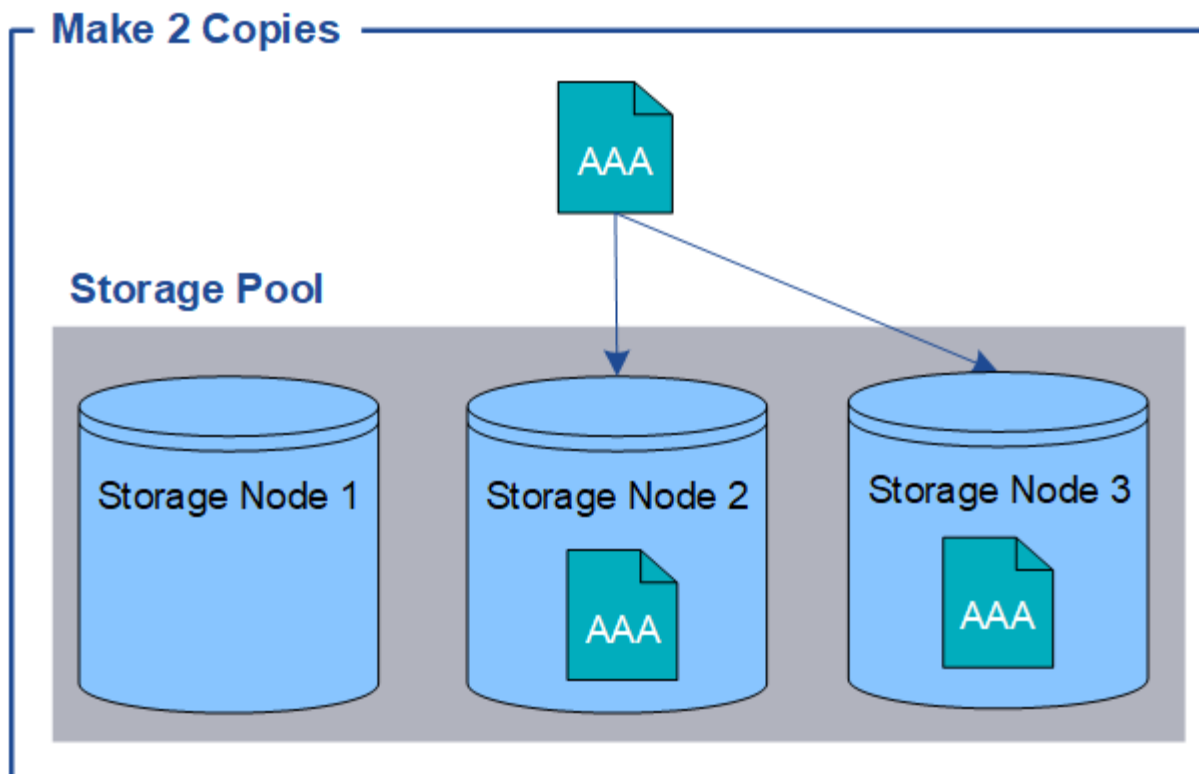
Come vengono memorizzati gli oggetti (codifica di replicazione o cancellazione)

Che cosa è la replicazione?

La replica è uno dei due metodi utilizzati da StorageGRID per archiviare i dati degli oggetti (l'altro metodo è la codifica di cancellazione). Quando gli oggetti corrispondono a una regola ILM che utilizza la replica, il sistema crea copie esatte dei dati dell'oggetto e memorizza le copie sui nodi di archiviazione.

Quando si configura una regola ILM per creare copie replicate, si specifica quante copie devono essere create, dove devono essere posizionate e per quanto tempo devono essere conservate in ogni posizione.

Nell'esempio seguente, la regola ILM specifica che due copie replicate di ciascun oggetto devono essere posizionate in un pool di archiviazione contenente tre nodi di archiviazione.



Quando StorageGRID abbina gli oggetti a questa regola, crea due copie dell'oggetto, posizionando ciascuna copia su un diverso nodo di archiviazione nel pool di archiviazione. Le due copie possono essere posizionate su due qualsiasi dei tre nodi di archiviazione disponibili. In questo caso, la regola ha posizionato copie degli oggetti sui nodi di archiviazione 2 e 3. Poiché sono presenti due copie, l'oggetto può essere recuperato se uno qualsiasi dei nodi nel pool di archiviazione si guasta.



StorageGRID può archiviare solo una copia replicata di un oggetto su un dato nodo di archiviazione. Se la griglia include tre nodi di archiviazione e si crea una regola ILM a 4 copie, verranno create solo tre copie: una copia per ciascun nodo di archiviazione. L'avviso **Posizionamento ILM non realizzabile** viene attivato per indicare che la regola ILM non può essere applicata completamente.

Informazioni correlate

- ["Che cosa è la codifica di cancellazione"](#)
- ["Che cos'è un pool di archiviazione"](#)
- ["Abilita la protezione contro la perdita del sito utilizzando la codifica di replicazione e cancellazione"](#)

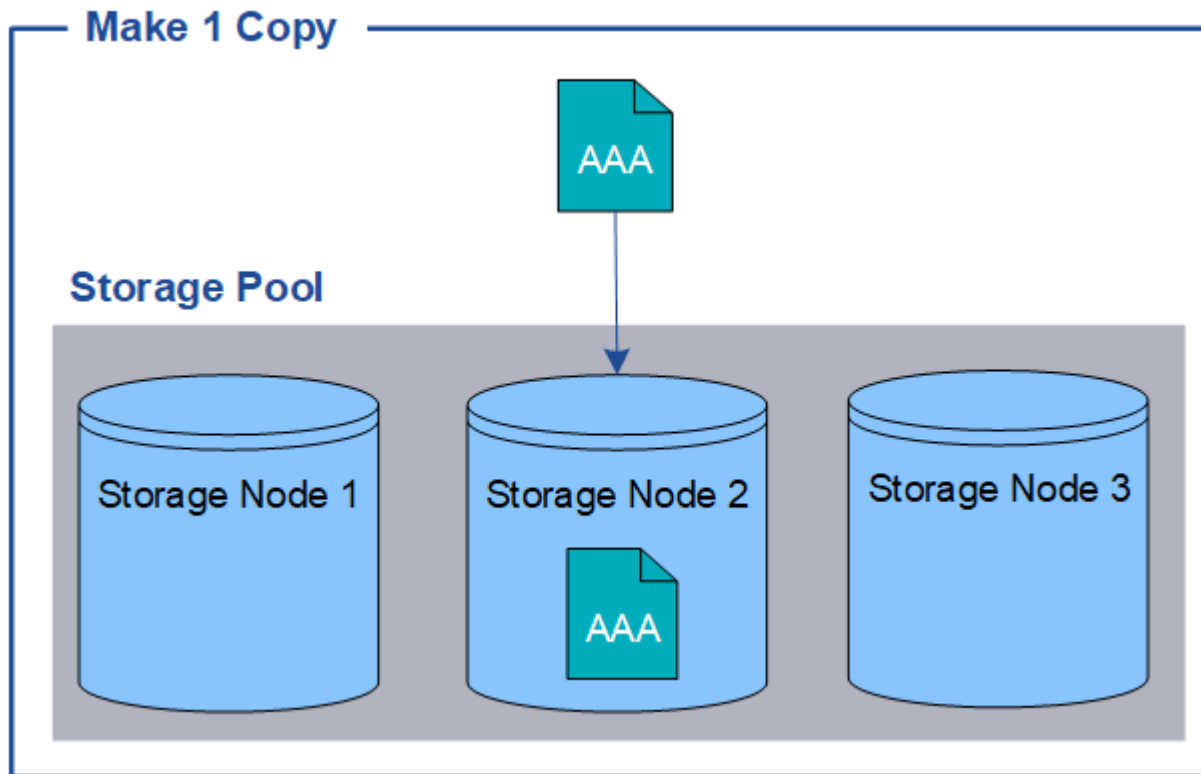
Perché non dovresti usare la replicazione a copia singola

Quando si crea una regola ILM per creare copie replicate, è necessario specificare sempre almeno due copie per qualsiasi periodo di tempo nelle istruzioni di posizionamento.

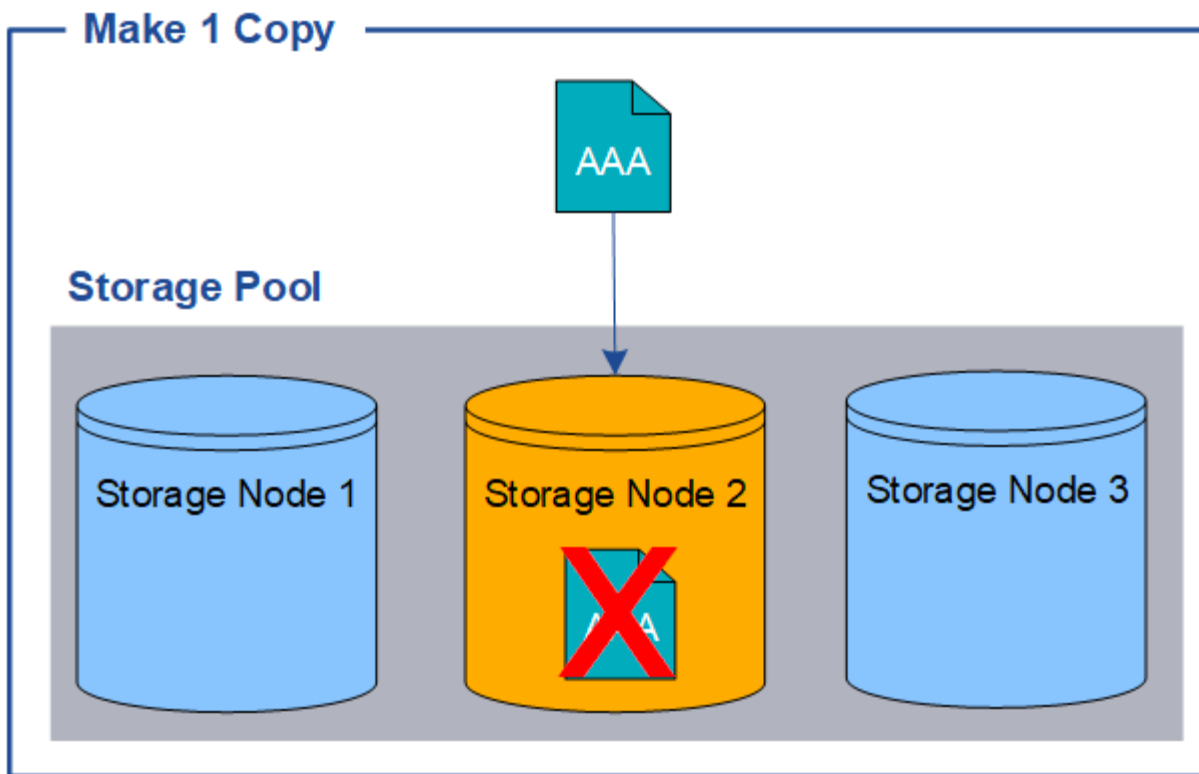


Non utilizzare una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo. Se esiste una sola copia replicata di un oggetto, tale oggetto viene perso se un nodo di archiviazione si guasta o presenta un errore significativo. Inoltre, durante le procedure di manutenzione, come gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

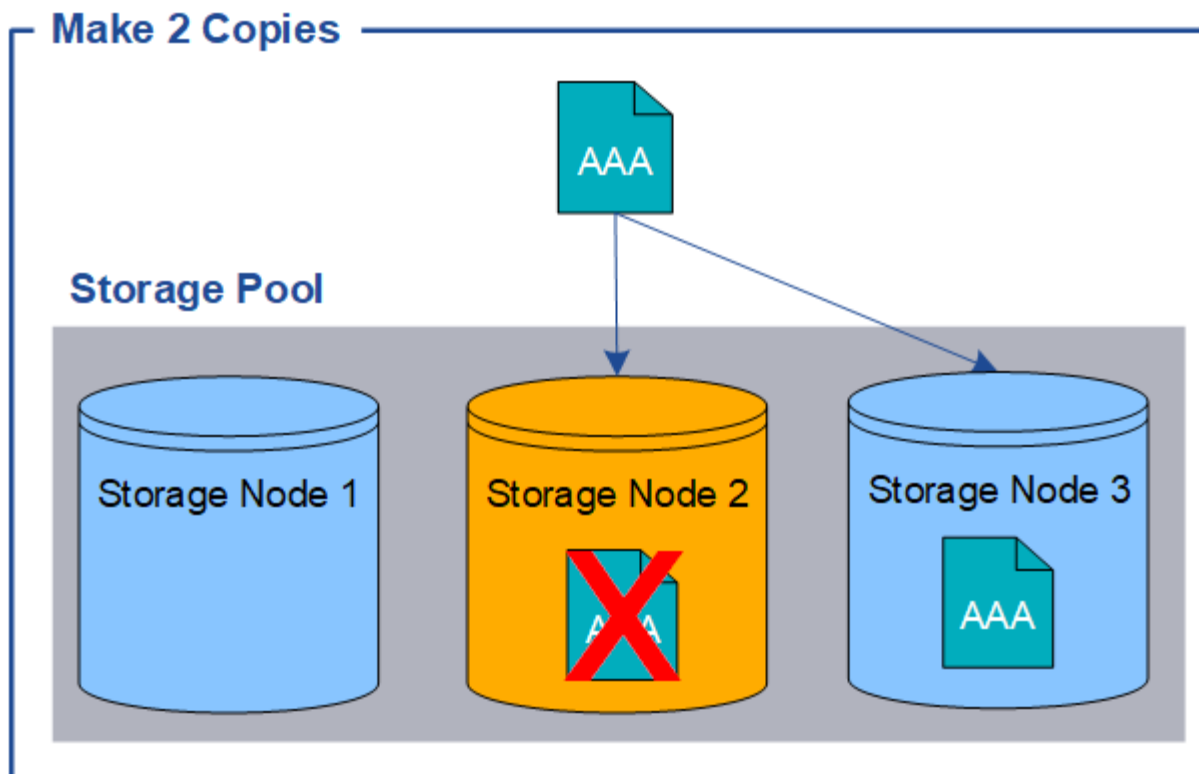
Nell'esempio seguente, la regola ILM Make 1 Copy specifica che una copia replicata di un oggetto venga inserita in un pool di archiviazione contenente tre nodi di archiviazione. Quando viene acquisito un oggetto che corrisponde a questa regola, StorageGRID ne posiziona una singola copia su un solo nodo di archiviazione.



Quando una regola ILM crea una sola copia replicata di un oggetto, l'oggetto diventa inaccessibile quando il nodo di archiviazione non è disponibile. In questo esempio, si perderà temporaneamente l'accesso all'oggetto AAA ogni volta che Storage Node 2 è offline, ad esempio durante un aggiornamento o un'altra procedura di manutenzione. Se il nodo di archiviazione 2 si guasta, l'oggetto AAA verrà perso completamente.



Per evitare di perdere i dati degli oggetti, è consigliabile effettuare sempre almeno due copie di tutti gli oggetti che si desidera proteggere con la replica. Se esistono due o più copie, è comunque possibile accedere all'oggetto se un nodo di archiviazione si guasta o va offline.



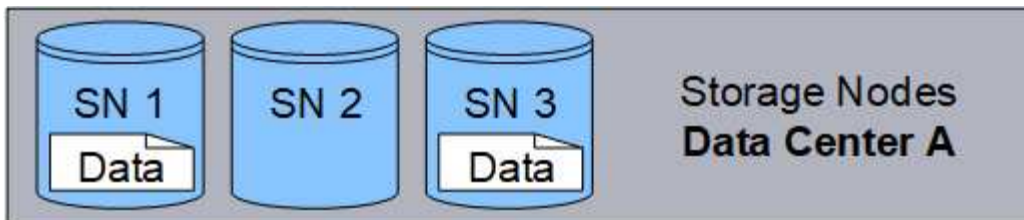
Che cos'è la codifica di cancellazione?

La codifica di cancellazione è uno dei due metodi utilizzati StorageGRID per archiviare i dati degli oggetti (l'altro metodo è la replica). Quando gli oggetti corrispondono a una regola ILM che utilizza la codifica di cancellazione, tali oggetti vengono suddivisi in frammenti di dati, vengono calcolati frammenti di parità aggiuntivi e ogni frammento viene archiviato su un diverso nodo di archiviazione.

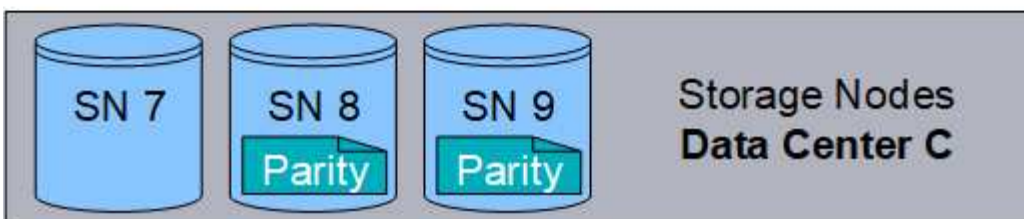
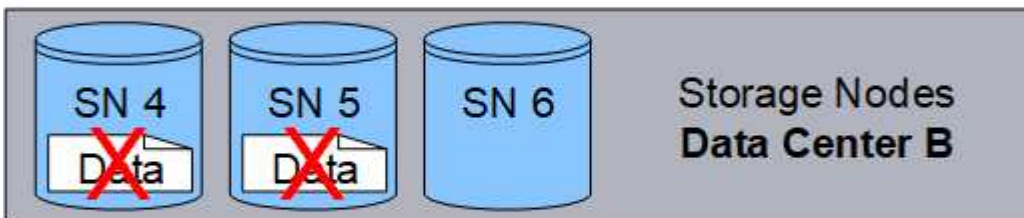
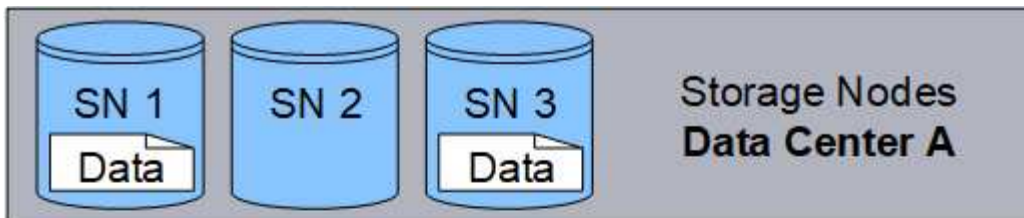
Quando si accede a un oggetto, questo viene riassembleato utilizzando i frammenti memorizzati. Se un dato o un frammento di parità si danneggia o viene perso, l'algoritmo di codifica di cancellazione può ricreare quel frammento utilizzando un sottoinsieme dei dati e dei frammenti di parità rimanenti.

Quando si creano regole ILM, StorageGRID crea profili di codifica di cancellazione che supportano tali regole. È possibile visualizzare un elenco di profili di codifica di cancellazione, ["rinominare un profilo di codifica di cancellazione"](#), o ["disattivare un profilo di codifica di cancellazione se non è attualmente utilizzato in nessuna regola ILM"](#).

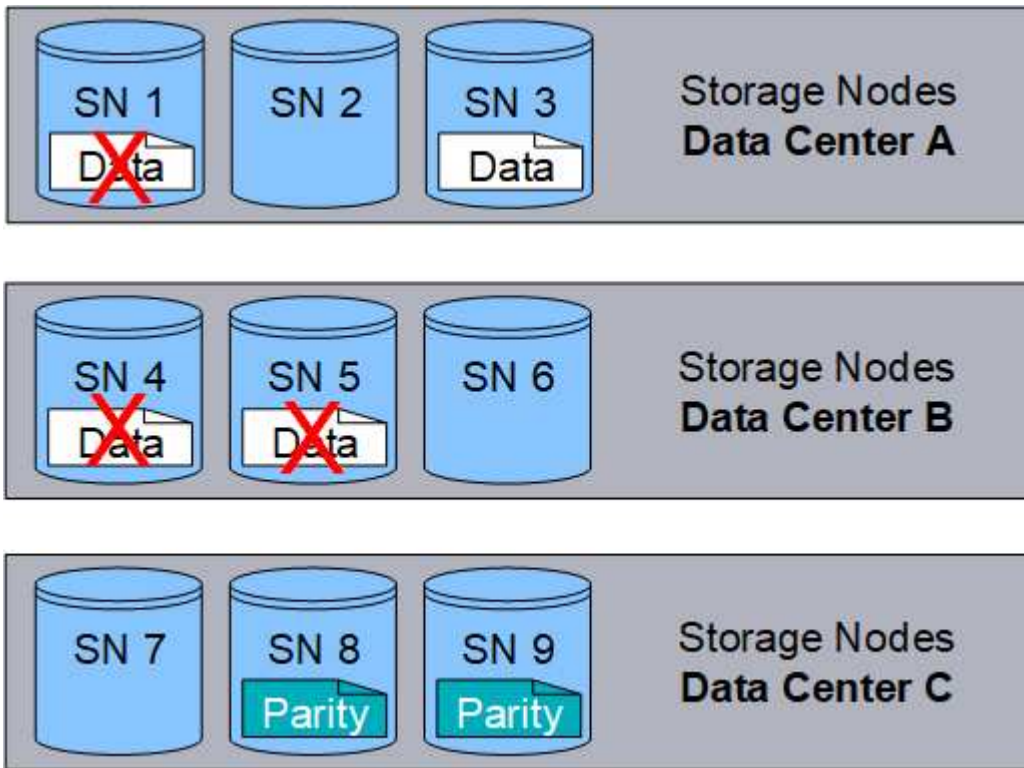
L'esempio seguente illustra l'uso di un algoritmo di codifica di cancellazione sui dati di un oggetto. In questo esempio, la regola ILM utilizza uno schema di codifica di cancellazione 4+2. Ogni oggetto viene suddiviso in quattro frammenti di dati uguali e dai dati dell'oggetto vengono calcolati due frammenti di parità. Ciascuno dei sei frammenti viene archiviato su un nodo diverso in tre siti di data center per garantire la protezione dei dati in caso di guasti dei nodi o perdite del sito.



Lo schema di codifica a cancellazione 4+2 può essere configurato in vari modi. Ad esempio, è possibile configurare un pool di archiviazione a sito singolo contenente sei nodi di archiviazione. Per ["protezione contro la perdita del sito"](#), è possibile utilizzare un pool di archiviazione contenente tre siti con tre nodi di archiviazione in ciascun sito. Un oggetto può essere recuperato finché rimangono disponibili quattro dei sei frammenti (dati o parità). È possibile perdere fino a due frammenti senza perdere i dati dell'oggetto. Se un intero sito viene perso, l'oggetto può comunque essere recuperato o riparato, a patto che tutti gli altri frammenti rimangano accessibili.



Se vengono persi più di due nodi di archiviazione, l'oggetto non sarà recuperabile.



Informazioni correlate

- ["Che cosa è la replicazione"](#)
- ["Che cos'è un pool di archiviazione"](#)
- ["Cosa sono gli schemi di codifica di cancellazione"](#)
- ["Rinominare un profilo di codifica di cancellazione"](#)
- ["Disattivare un profilo di codifica di cancellazione"](#)

Cosa sono gli schemi di codifica di cancellazione?

Gli schemi di codifica di cancellazione controllano quanti frammenti di dati e quanti frammenti di parità vengono creati per ciascun oggetto.

Quando si crea o si modifica una regola ILM, si seleziona uno schema di codifica di cancellazione disponibile. StorageGRID crea automaticamente schemi di codifica di cancellazione in base al numero di nodi di archiviazione e siti che compongono il pool di archiviazione che si intende utilizzare.

Protezione dei dati

Il sistema StorageGRID utilizza l'algoritmo di codifica della cancellazione Reed-Solomon. L'algoritmo divide un oggetto in k frammenti di dati e calcoli m frammenti di parità.

IL $k + m = n$ i frammenti sono sparsi n Nodi di archiviazione per garantire la protezione dei dati come segue:

- Per recuperare o riparare un oggetto, k sono necessari frammenti.
- Un oggetto può sostenere fino a m frammenti persi o corrotti. Più alto è il valore di m , maggiore è la tolleranza al guasto.

La migliore protezione dei dati è fornita dallo schema di codifica di cancellazione con la più alta tolleranza ai guasti del nodo o del volume all'interno di un pool di archiviazione.

Spese di archiviazione generali

Il sovraccarico di archiviazione di uno schema di codifica di cancellazione viene calcolato dividendo il numero di frammenti di parità(m) dal numero di frammenti di dati(k). È possibile utilizzare il sovraccarico di archiviazione per calcolare la quantità di spazio su disco richiesta da ciascun oggetto con codice di cancellazione:

$$\text{disk space} = \text{object size} + (\text{object size} * \text{storage overhead})$$

Ad esempio, se si archivia un oggetto da 10 MB utilizzando lo schema 4+2 (che ha un overhead di archiviazione del 50%), l'oggetto consuma 15 MB di spazio di archiviazione della griglia. Se si memorizza lo stesso oggetto da 10 MB utilizzando lo schema 6+2 (che ha un overhead di archiviazione del 33%), l'oggetto consuma circa 13,3 MB.

Selezionare lo schema di codifica di cancellazione con il valore totale più basso di $k+m$ che soddisfa le tue esigenze. Gli schemi di codifica di cancellazione con un numero inferiore di frammenti sono più efficienti dal punto di vista computazionale perché:

- Vengono creati e distribuiti (o recuperati) meno frammenti per oggetto
- Hanno prestazioni migliori perché la dimensione del frammento è maggiore
- Possono richiedere che vengano aggiunti meno nodi in un'[espansione quando è necessario più spazio di archiviazione](#)

Linee guida per i pool di stoccaggio

Quando si seleziona il pool di archiviazione da utilizzare per una regola che creerà una copia con codice di cancellazione, attenersi alle seguenti linee guida per i pool di archiviazione:

- Il pool di archiviazione deve includere tre o più siti oppure esattamente un sito.



Non è possibile utilizzare la codifica di cancellazione se il pool di archiviazione include due siti.

- [Schemi di codifica di cancellazione per pool di archiviazione contenenti tre o più siti](#)
- [Schemi di codifica di cancellazione per pool di archiviazione monosito](#)
- Non utilizzare un pool di archiviazione che includa il sito Tutti i siti.
- Il pool di archiviazione dovrebbe includere almeno $k+m + 1$ Nodi di archiviazione in grado di archiviare dati di oggetti.



Durante l'installazione, è possibile configurare i nodi di archiviazione in modo che contengano solo metadati degli oggetti e non dati degli oggetti. Per ulteriori informazioni, consultare ["Tipi di nodi di archiviazione"](#).

Il numero minimo di nodi di archiviazione richiesti è $k+m$. Tuttavia, avere almeno un nodo di archiviazione aggiuntivo può aiutare a prevenire errori di acquisizione o arretrati ILM se un nodo di archiviazione necessario non è temporaneamente disponibile.

Schemi di codifica di cancellazione per pool di archiviazione contenenti tre o più siti

Nella tabella seguente vengono descritti gli schemi di codifica di cancellazione attualmente supportati da StorageGRID per i pool di archiviazione che includono tre o più siti. Tutti questi schemi garantiscono una protezione contro le perdite del sito. Anche se un sito può andare perso, l'oggetto sarà comunque accessibile.

Per gli schemi di codifica di cancellazione che forniscono protezione contro la perdita del sito, il numero consigliato di nodi di archiviazione nel pool di archiviazione supera $k+m + 1$ perché ogni sito richiede un minimo di tre nodi di archiviazione.

Schema di codifica di cancellazione ($k+m$)	Numero minimo di siti distribuiti	Numero consigliato di nodi di archiviazione in ogni sito	Numero totale consigliato di nodi di archiviazione	Protezione contro le perdite del sito?	Spese di archiviazione generali
4+2	3	3	9	Sì	50%
6+2	4	3	12	Sì	33%
8+2	5	3	15	Sì	25%
6+3	3	4	12	Sì	50%
9+3	4	4	16	Sì	33%
2+1	3	3	9	Sì	50%
4+1	5	3	15	Sì	25%
6+1	7	3	21	Sì	17%
7+5	3	5	15	Sì	71%



StorageGRID richiede un minimo di tre nodi di archiviazione per sito. Per utilizzare lo schema 7+5, ogni sito richiede un minimo di quattro nodi di archiviazione. Si consiglia di utilizzare cinque nodi di archiviazione per sito.

Quando si seleziona uno schema di codifica di cancellazione che garantisca la protezione del sito, è necessario valutare l'importanza relativa dei seguenti fattori:

- **Numero di frammenti:** le prestazioni e la flessibilità di espansione sono generalmente migliori quando il numero totale di frammenti è inferiore.
- **Tolleranza ai guasti:** la tolleranza ai guasti aumenta avendo più segmenti di parità (ovvero, quando m ha un valore più alto.)
- **Traffico di rete:** durante il ripristino da guasti, utilizzando uno schema con più frammenti (ovvero, un totale più elevato per $k+m$) crea più traffico di rete.
- **Sovraccarico di archiviazione:** gli schemi con sovraccarico più elevato richiedono più spazio di archiviazione per oggetto.

Ad esempio, quando si decide tra uno schema 4+2 e uno schema 6+3 (entrambi con un overhead di archiviazione del 50%), selezionare lo schema 6+3 se è richiesta una tolleranza agli errori aggiuntiva. Selezionare lo schema 4+2 se le risorse di rete sono limitate. Se tutti gli altri fattori sono uguali, seleziona 4+2 perché ha un numero totale di frammenti inferiore.



Se non sei sicuro di quale schema utilizzare, seleziona 4+2 o 6+3 oppure contatta l'assistenza tecnica.

Schemi di codifica di cancellazione per pool di archiviazione monosito

Un pool di archiviazione con un solo sito supporta tutti gli schemi di codifica di cancellazione definiti per tre o più siti, a condizione che il sito disponga di un numero sufficiente di nodi di archiviazione.

Il numero minimo di nodi di archiviazione richiesti è $k+m$, ma un pool di archiviazione con $k+m + 1$ Si consiglia l'uso di Storage Nodes. Ad esempio, lo schema di codifica di cancellazione 2+1 richiede un pool di archiviazione con un minimo di tre nodi di archiviazione, ma si consigliano quattro nodi di archiviazione.

Schema di codifica di cancellazione ($k+m$)	Numero minimo di nodi di archiviazione	Numero consigliato di nodi di archiviazione	Spese di archiviazione generali
4+2	6	7	50%
6+2	8	9	33%
8+2	10	11	25%
6+3	9	10	50%
9+3	12	13	33%
2+1	3	4	50%
4+1	5	6	25%
6+1	7	8	17%
7+5	12	13	71%

Vantaggi, svantaggi e requisiti della codifica di cancellazione

Prima di decidere se utilizzare la codifica di replicazione o di cancellazione per proteggere i dati degli oggetti dalla perdita, è necessario comprendere i vantaggi, gli svantaggi e i requisiti della codifica di cancellazione.

Vantaggi della codifica di cancellazione

Rispetto alla replicazione, la codifica di cancellazione offre maggiore affidabilità, disponibilità ed efficienza di archiviazione.

- **Affidabilità:** l'affidabilità viene misurata in termini di tolleranza ai guasti, ovvero il numero di guasti simultanei che possono essere sostenuti senza perdita di dati. Con la replicazione, più copie identiche vengono archiviate su nodi diversi e in più siti. Con la codifica di cancellazione, un oggetto viene codificato in frammenti di dati e parità e distribuito su molti nodi e siti. Questa dispersione garantisce protezione contro i guasti sia del sito che del nodo. Rispetto alla replicazione, la codifica di cancellazione garantisce una maggiore affidabilità a costi di archiviazione comparabili.
- **Disponibilità:** la disponibilità può essere definita come la capacità di recuperare oggetti se i nodi di archiviazione falliscono o diventano inaccessibili. Rispetto alla replicazione, la codifica di cancellazione garantisce una maggiore disponibilità a costi di archiviazione comparabili.
- **Efficienza di archiviazione:** per livelli simili di disponibilità e affidabilità, gli oggetti protetti tramite codifica di cancellazione consumano meno spazio su disco rispetto a quanto farebbero se protetti tramite replica. Ad esempio, un oggetto da 10 MB replicato su due siti consuma 20 MB di spazio su disco (due copie), mentre un oggetto codificato con cancellazione su tre siti con uno schema di codifica con cancellazione 6+3 consuma solo 15 MB di spazio su disco.



Lo spazio su disco per gli oggetti con codice di cancellazione viene calcolato sommando le dimensioni dell'oggetto al sovraccarico di archiviazione. La percentuale di sovraccarico di archiviazione è il numero di frammenti di parità diviso per il numero di frammenti di dati.

Svantaggi della codifica di cancellazione

Rispetto alla replicazione, la codifica a cancellazione presenta i seguenti svantaggi:

- Si consiglia un numero maggiore di nodi e siti di archiviazione, a seconda dello schema di codifica di cancellazione. Al contrario, se si replicano i dati degli oggetti, è necessario un solo nodo di archiviazione per ogni copia. Vedere ["Schemi di codifica di cancellazione per pool di archiviazione contenenti tre o più siti"](#) E ["Schemi di codifica di cancellazione per pool di archiviazione monosito"](#) .
- Aumento dei costi e della complessità delle espansioni di storage. Per espandere una distribuzione che utilizza la replica, è necessario aggiungere capacità di archiviazione in ogni posizione in cui vengono eseguite le copie degli oggetti. Per espandere una distribuzione che utilizza la codifica di cancellazione, è necessario considerare sia lo schema di codifica di cancellazione in uso sia il livello di riempimento dei nodi di archiviazione esistenti. Ad esempio, se si attende che i nodi esistenti siano pieni al 100%, è necessario aggiungere almeno $k+m$ Nodi di archiviazione, ma se si espande quando i nodi esistenti sono pieni al 70%, è possibile aggiungere due nodi per sito e continuare a massimizzare la capacità di archiviazione utilizzabile. Per ulteriori informazioni, consultare ["Aggiungere capacità di archiviazione per oggetti con codice di cancellazione"](#) .
- Quando si utilizza la codifica di cancellazione su siti distribuiti geograficamente, si verificano latenze di recupero maggiori. I frammenti di un oggetto codificato in modo da essere cancellato e distribuito su siti remoti richiedono più tempo per essere recuperati tramite connessioni WAN rispetto a un oggetto replicato e disponibile localmente (lo stesso sito a cui si connette il client).
- Quando si utilizza la codifica di cancellazione su siti distribuiti geograficamente, si verifica un utilizzo maggiore del traffico di rete WAN per recuperi e riparazioni, in particolare per oggetti recuperati frequentemente o per riparazioni di oggetti su connessioni di rete WAN.
- Quando si utilizza la codifica di cancellazione su più siti, la velocità massima di elaborazione degli oggetti diminuisce drasticamente all'aumentare della latenza di rete tra i siti. Questa diminuzione è dovuta alla corrispondente diminuzione della velocità di trasmissione della rete TCP, che influisce sulla velocità con cui il sistema StorageGRID può archiviare e recuperare frammenti di oggetti.
- Maggiore utilizzo delle risorse di elaborazione.

Quando utilizzare la codifica di cancellazione

La codifica di cancellazione è più adatta ai seguenti requisiti:

- Oggetti di dimensioni superiori a 1 MB.



La codifica di cancellazione è più adatta per oggetti di dimensioni superiori a 1 MB. Non utilizzare la codifica di cancellazione per oggetti di dimensioni inferiori a 200 KB per evitare il sovraccarico dovuto alla gestione di frammenti molto piccoli con codifica di cancellazione.

- Archiviazione a lungo termine o a freddo per contenuti recuperati raramente.
- Elevata disponibilità e affidabilità dei dati.
- Protezione contro guasti completi del sito e del nodo.
- Efficienza di archiviazione.
- Distribuzioni in un unico sito che richiedono una protezione efficiente dei dati con una sola copia con codice di cancellazione anziché più copie replicate.
- Distribuzioni multi-sito in cui la latenza tra i siti è inferiore a 100 ms.

Come viene determinata la ritenzione dell'oggetto

StorageGRID offre opzioni sia agli amministratori della griglia sia ai singoli utenti tenant per specificare per quanto tempo archiviare gli oggetti. In generale, tutte le istruzioni di conservazione fornite da un utente tenant hanno la precedenza sulle istruzioni di conservazione fornite dall'amministratore della griglia.

Come gli utenti tenant controllano la conservazione degli oggetti

Gli utenti tenant possono utilizzare questi metodi per controllare per quanto tempo i loro oggetti vengono archiviati in StorageGRID:

- Se l'impostazione globale Blocco oggetti S3 è abilitata per la griglia, gli utenti del tenant S3 possono creare bucket con Blocco oggetti S3 abilitato e quindi selezionare un **Periodo di conservazione predefinito** per ciascun bucket.
- Se l'impostazione globale S3 Object Lock è abilitata per la griglia, gli utenti del tenant S3 possono creare bucket con S3 Object Lock abilitato e quindi utilizzare l'API REST S3 per specificare le impostazioni di conservazione fino alla data di scadenza e di conservazione legale per ogni versione dell'oggetto aggiunta a tale bucket.
 - Una versione di un oggetto sottoposta a conservazione legale non può essere eliminata con alcun metodo.
 - Prima che venga raggiunta la data di conservazione di una versione di un oggetto, tale versione non può essere eliminata con alcun metodo.
 - Gli oggetti nei bucket con S3 Object Lock abilitato vengono conservati da ILM "per sempre". Tuttavia, una volta raggiunta la data di conservazione, una versione dell'oggetto può essere eliminata da una richiesta del client o dalla scadenza del ciclo di vita del bucket. Vedere ["Gestisci gli oggetti con S3 Object Lock"](#).
- Gli utenti del tenant S3 possono aggiungere ai propri bucket una configurazione del ciclo di vita che specifica un'azione di scadenza. Se esiste un ciclo di vita del bucket, StorageGRID archivia un oggetto finché non viene raggiunta la data o il numero di giorni specificati nell'azione Scadenza, a meno che il client non elimini prima l'oggetto. Vedere ["Crea la configurazione del ciclo di vita S3"](#).

- Un client S3 può inviare una richiesta di eliminazione di un oggetto. StorageGRID dà sempre priorità alle richieste di eliminazione del client rispetto al ciclo di vita del bucket S3 o all'ILM quando decide se eliminare o conservare un oggetto.

Come gli amministratori della griglia controllano la conservazione degli oggetti

Gli amministratori della griglia possono utilizzare questi metodi per controllare la conservazione degli oggetti:

- Imposta un periodo massimo di conservazione del blocco degli oggetti S3 per ciascun tenant. Quindi, gli utenti tenant possono impostare un periodo di conservazione predefinito per ciascuno dei loro bucket. Il periodo di conservazione massimo viene applicato anche a tutti gli oggetti appena acquisiti per quel bucket (data di conservazione dell'oggetto).
- Creare istruzioni di posizionamento ILM per controllare per quanto tempo gli oggetti vengono conservati. Quando gli oggetti corrispondono a una regola ILM, StorageGRID li memorizza finché non è trascorso l'ultimo periodo di tempo nella regola ILM. Gli oggetti vengono conservati indefinitamente se nelle istruzioni di posizionamento è specificato "per sempre".
- Indipendentemente da chi controlla per quanto tempo gli oggetti vengono conservati, le impostazioni ILM controllano quali tipi di copie degli oggetti (replicate o con codice di cancellazione) vengono archiviate e dove si trovano le copie (nodi di archiviazione o pool di archiviazione cloud).

Come interagiscono il ciclo di vita del bucket S3 e ILM

Quando viene configurato un ciclo di vita del bucket S3, le azioni di scadenza del ciclo di vita sovrascrivono il criterio ILM per gli oggetti che corrispondono al filtro del ciclo di vita. Di conseguenza, un oggetto potrebbe essere mantenuto sulla griglia anche dopo che sono scadute tutte le istruzioni ILM per il posizionamento dell'oggetto.

Esempi di conservazione degli oggetti

Per comprendere meglio le interazioni tra S3 Object Lock, impostazioni del ciclo di vita del bucket, richieste di eliminazione client e ILM, prendere in considerazione i seguenti esempi.

Esempio 1: il ciclo di vita del bucket S3 conserva gli oggetti più a lungo di ILM

ILM

Conservare due copie per 1 anno (365 giorni)

Ciclo di vita del bucket

Scadenza degli oggetti in 2 anni (730 giorni)

Risultato

StorageGRID memorizza l'oggetto per 730 giorni. StorageGRID utilizza le impostazioni del ciclo di vita del bucket per determinare se eliminare o conservare un oggetto.



Se il ciclo di vita del bucket specifica che gli oggetti devono essere conservati più a lungo di quanto specificato da ILM, StorageGRID continua a utilizzare le istruzioni di posizionamento ILM quando determina il numero e il tipo di copie da archiviare. In questo esempio, due copie dell'oggetto continueranno a essere archiviate in StorageGRID dal giorno 366 al giorno 730.

Esempio 2: il ciclo di vita del bucket S3 fa scadere gli oggetti prima di ILM

ILM

Conservare due copie per 2 anni (730 giorni)

Ciclo di vita del bucket

Scadenza degli oggetti in 1 anno (365 giorni)

Risultato

StorageGRID elimina entrambe le copie dell'oggetto dopo il giorno 365.

Esempio 3: l'eliminazione del client sovrascrive il ciclo di vita del bucket e ILM

ILM

Conserva due copie sui nodi di archiviazione "per sempre"

Ciclo di vita del bucket

Scadenza degli oggetti in 2 anni (730 giorni)

Richiesta di eliminazione del cliente

Emesso il giorno 400

Risultato

StorageGRID elimina entrambe le copie dell'oggetto il giorno 400 in risposta alla richiesta di eliminazione del client.

Esempio 4: S3 Object Lock sovrascrive la richiesta di eliminazione del client

Blocco oggetto S3

La data di conservazione per una versione dell'oggetto è il 31/03/2026. Non è in vigore alcun blocco legale.

Regola ILM conforme

Conserva due copie sui nodi di archiviazione "per sempre"

Richiesta di eliminazione del cliente

Pubblicato il 31/03/2024

Risultato

StorageGRID non eliminerà la versione dell'oggetto perché la data di conservazione è ancora lontana 2 anni.

Come vengono eliminati gli oggetti

StorageGRID può eliminare oggetti in risposta diretta a una richiesta del client oppure automaticamente in seguito alla scadenza del ciclo di vita di un bucket S3 o ai requisiti della policy ILM. Comprendere i diversi modi in cui gli oggetti possono essere eliminati e il modo in cui StorageGRID gestisce le richieste di eliminazione può aiutarti a gestire gli oggetti in modo più efficace.

StorageGRID può utilizzare uno dei due metodi per eliminare gli oggetti:

- Eliminazione sincrona: quando StorageGRID riceve una richiesta di eliminazione da parte del client, tutte le copie degli oggetti vengono rimosse immediatamente. Dopo aver rimosso le copie, il cliente viene

informato che l'eliminazione è avvenuta con successo.

- Gli oggetti vengono messi in coda per l'eliminazione: quando StorageGRID riceve una richiesta di eliminazione, l'oggetto viene messo in coda per l'eliminazione e il client viene immediatamente informato che l'eliminazione è avvenuta correttamente. Le copie degli oggetti vengono rimosse in seguito tramite l'elaborazione ILM in background.

Quando si eliminano oggetti, StorageGRID utilizza il metodo che ottimizza le prestazioni di eliminazione, riduce al minimo i potenziali backlog di eliminazione e libera spazio più rapidamente.

La tabella riepiloga quando StorageGRID utilizza ciascun metodo.

Metodo di esecuzione dell'eliminazione	Quando utilizzato
Gli oggetti vengono messi in coda per l'eliminazione	Quando una delle seguenti condizioni è vera: • L'eliminazione automatica degli oggetti è stata attivata da uno dei seguenti eventi: ◦ È stata raggiunta la data di scadenza o il numero di giorni nella configurazione del ciclo di vita per un bucket S3. ◦ Trascorre l'ultimo periodo di tempo specificato in una regola ILM. • Un client S3 richiede l'eliminazione e una o più di queste condizioni sono vere: ◦ Le copie non possono essere eliminate entro 30 secondi perché, ad esempio, la posizione di un oggetto non è temporaneamente disponibile. ◦ Le code di eliminazione in background sono inattive. Nota: gli oggetti in un bucket in cui è abilitato il blocco degli oggetti S3 non possono essere eliminati se sono sottoposti a conservazione legale o se è stata specificata una data di conservazione fino a quando non è stata ancora rispettata.
Gli oggetti vengono rimossi immediatamente (eliminazione sincrona)	Quando un client S3 effettua una richiesta di eliminazione e tutte le seguenti condizioni sono soddisfatte: • Tutte le copie possono essere rimosse entro 30 secondi. • Le code di eliminazione in background contengono oggetti da elaborare.

Quando i client S3 effettuano richieste di eliminazione, StorageGRID inizia aggiungendo oggetti alla coda di eliminazione. Quindi passa all'esecuzione dell'eliminazione sincrona. Assicurandosi che la coda di eliminazione in background abbia oggetti da elaborare, StorageGRID può elaborare le eliminazioni in modo più efficiente, soprattutto per i client con bassa concorrenza, contribuendo al contempo a prevenire gli arretrati di eliminazione dei client.

Tempo necessario per eliminare gli oggetti

Il modo in cui StorageGRID elimina gli oggetti può influire sulle prestazioni apparenti del sistema:

- Quando StorageGRID esegue l'eliminazione sincrona, potrebbero essere necessari fino a 30 secondi prima che StorageGRID restituisca un risultato al client. Ciò significa che l'eliminazione può sembrare più

lenta, anche se in realtà le copie vengono rimosse più rapidamente rispetto a quando StorageGRID mette in coda gli oggetti per l'eliminazione.

- Se si monitorano attentamente le prestazioni di eliminazione durante un'eliminazione in blocco, si potrebbe notare che la velocità di eliminazione sembra essere lenta dopo l'eliminazione di un certo numero di oggetti. Questa modifica si verifica quando StorageGRID passa dalla messa in coda degli oggetti per l'eliminazione all'esecuzione dell'eliminazione sincrona. L'apparente riduzione del tasso di eliminazione non significa che le copie degli oggetti vengano rimosse più lentamente. Al contrario, indica che, in media, lo spazio viene ora liberato più rapidamente.

Se si eliminano un gran numero di oggetti e la priorità è liberare spazio rapidamente, si può prendere in considerazione l'utilizzo di una richiesta client per eliminare gli oggetti anziché eliminarli tramite ILM o altri metodi. In generale, lo spazio viene liberato più rapidamente quando l'eliminazione viene eseguita dai client, perché StorageGRID può utilizzare l'eliminazione sincrona.

Il tempo necessario per liberare spazio dopo l'eliminazione di un oggetto dipende da diversi fattori:

- Se le copie degli oggetti vengono rimosse in modo sincrono o messe in coda per essere rimosse in un secondo momento (per le richieste di eliminazione del client).
- Altri fattori, come il numero di oggetti nella griglia o la disponibilità di risorse della griglia quando le copie degli oggetti vengono messe in coda per la rimozione (sia per le eliminazioni client che per altri metodi).

Come vengono eliminati gli oggetti con versione S3

Quando il controllo delle versioni è abilitato per un bucket S3, StorageGRID segue il comportamento di Amazon S3 quando risponde alle richieste di eliminazione, indipendentemente dal fatto che tali richieste provengano da un client S3, dalla scadenza del ciclo di vita di un bucket S3 o dai requisiti della policy ILM.

Quando gli oggetti sono sottoposti a controllo di versione, le richieste di eliminazione degli oggetti non eliminano la versione corrente dell'oggetto e non liberano spazio. Al contrario, una richiesta di eliminazione di un oggetto crea un marcatore di eliminazione di zero byte come versione corrente dell'oggetto, il che rende la versione precedente dell'oggetto "non corrente". Un marcatore di eliminazione di un oggetto diventa un marcatore di eliminazione di un oggetto scaduto quando è la versione corrente e non ci sono versioni non correnti.

Anche se l'oggetto non è stato rimosso, StorageGRID si comporta come se la versione corrente dell'oggetto non fosse più disponibile. Le richieste a tale oggetto restituiscono 404 Not Found. Tuttavia, poiché i dati dell'oggetto non corrente non sono stati rimossi, le richieste che specificano una versione non corrente dell'oggetto possono avere esito positivo.

Per liberare spazio durante l'eliminazione di oggetti sottoposti a controllo di versione o per rimuovere i marcatori di eliminazione, utilizzare una delle seguenti opzioni:

- **Richiesta client S3:** specificare l'ID della versione dell'oggetto nella richiesta S3 DELETE Object(DELETE /object?versionId=ID). Tieni presente che questa richiesta rimuove solo le copie degli oggetti per la versione specificata (le altre versioni continuano a occupare spazio).
- **Ciclo di vita del bucket:** utilizzare il `NoncurrentVersionExpiration` azione nella configurazione del ciclo di vita del bucket. Quando viene raggiunto il numero di `NoncurrentDays` specificato, StorageGRID rimuove definitivamente tutte le copie delle versioni non correnti degli oggetti. Queste versioni degli oggetti non possono essere recuperate.

IL `NewerNoncurrentVersions` l'azione nella configurazione del ciclo di vita del bucket specifica il numero di versioni non correnti conservate in un bucket S3 con versione. Se ci sono più versioni non correnti di `NewerNoncurrentVersions` specifica che StorageGRID rimuove le versioni precedenti

quando è trascorso il valore `NoncurrentDays`. IL `NewerNoncurrentVersions` la soglia sovrascrive le regole del ciclo di vita fornite da ILM, il che significa che un oggetto non corrente con una versione all'interno di `NewerNoncurrentVersions` la soglia viene mantenuta se ILM ne richiede l'eliminazione.

Per rimuovere i marcatori di eliminazione degli oggetti scaduti utilizzare `Expiration` azione con uno dei seguenti tag: `ExpiredObjectDeleteMarker`, `Days`, `O Date`.

- **ILM:** ["Clonare una policy attiva"](#) e aggiungere due regole ILM alla nuova policy:
 - Prima regola: utilizzare "Tempo non corrente" come tempo di riferimento per far corrispondere le versioni non correnti dell'oggetto. In ["Passaggio 1 \(Immissione dei dettagli\) della procedura guidata Crea una regola ILM"](#), seleziona **Sì** alla domanda "Applicare questa regola solo alle versioni precedenti degli oggetti (nei bucket S3 con controllo delle versioni abilitato)?"
 - Seconda regola: utilizzare **Tempo di acquisizione** in modo che corrisponda alla versione corrente. La regola "Tempo non corrente" deve comparire nella policy sopra la regola **Tempo di inserimento**.

Per rimuovere i marcatori di eliminazione degli oggetti scaduti, utilizzare una regola **Tempo di acquisizione** che corrisponda ai marcatori di eliminazione correnti. I marcatori di eliminazione vengono rimossi solo quando è trascorso un **periodo di tempo di giorni** e l'attuale marcatore di eliminazione è scaduto (non ci sono versioni non correnti).

- **Elimina oggetti nel bucket:** usa il gestore tenant per ["elimina tutte le versioni dell'oggetto"](#), compresi i marcatori di eliminazione, da un bucket.

Quando un oggetto con versione viene eliminato, StorageGRID crea un marcatore di eliminazione a zero byte come versione corrente dell'oggetto. Prima di poter eliminare un bucket con versione, è necessario rimuovere tutti gli oggetti e i marcatori di eliminazione.

- I marcatori di eliminazione creati in StorageGRID 11.7 o versioni precedenti possono essere rimossi solo tramite richieste client S3; non vengono rimossi da ILM, dalle regole del ciclo di vita del bucket o dagli oggetti di eliminazione nelle operazioni del bucket.
- I marcatori di eliminazione da un bucket creato in StorageGRID 11.8 o versione successiva possono essere rimossi tramite ILM, regole del ciclo di vita del bucket, operazioni di eliminazione degli oggetti nelle bucket o un'eliminazione esplicita del client S3.

Informazioni correlate

- ["Utilizzare l'API REST S3"](#)
- ["Esempio 4: regole e policy ILM per oggetti con versione S3"](#)

Creare e assegnare gradi di archiviazione

I gradi di archiviazione identificano il tipo di archiviazione utilizzato da un nodo di archiviazione. È possibile creare gradi di archiviazione se si desidera che le regole ILM posizionino determinati oggetti su determinati nodi di archiviazione.

Prima di iniziare

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

Informazioni su questo compito

Quando installi StorageGRID per la prima volta, il livello di archiviazione **Predefinito** viene assegnato automaticamente a ogni nodo di archiviazione nel tuo sistema. Se necessario, è possibile definire gradi di

archiviazione personalizzati e assegnarli a diversi nodi di archiviazione.

Utilizzando gradi di archiviazione personalizzati è possibile creare pool di archiviazione ILM che contengono solo un tipo specifico di nodo di archiviazione. Ad esempio, potresti voler archiviare determinati oggetti sui nodi di archiviazione più veloci, come gli storage appliance all-flash StorageGRID .



Durante l'installazione, è possibile configurare i nodi di archiviazione in modo che contengano solo metadati degli oggetti e non dati degli oggetti. Ai nodi di archiviazione solo metadati non può essere assegnato un grado di archiviazione. Per ulteriori informazioni, consultare "[Tipi di nodi di archiviazione](#)".

Se il grado di archiviazione non è un problema (ad esempio, tutti i nodi di archiviazione sono identici), è possibile saltare questa procedura e utilizzare la selezione **include tutti i gradi di archiviazione** per il grado di archiviazione quando si "[creare pool di archiviazione](#)". Utilizzando questa selezione si garantisce che il pool di archiviazione includa tutti i nodi di archiviazione del sito, indipendentemente dal loro grado di archiviazione.



Non creare più livelli di archiviazione del necessario. Ad esempio, non creare un grado di archiviazione per ogni nodo di archiviazione. Assegna invece ogni grado di archiviazione a due o più nodi. I gradi di archiviazione assegnati a un solo nodo possono causare arretrati ILM se il nodo in questione non è più disponibile.

Passi

1. Selezionare **ILM > Gradi di archiviazione**.
2. Definisci gradi di archiviazione personalizzati:
 - a. Per ogni grado di archiviazione personalizzato che desideri aggiungere, seleziona *Inserisci*  per aggiungere una riga.
 - b. Inserisci un'etichetta descrittiva.



Storage Grades

Updated: 2017-05-26 11:22:39 MDT

Storage Grade Definitions

Storage Grade	Label	Actions
0	Default	
1	disk	

Storage Grades

LDR	Storage Grade	Actions
Data Center 1/DC1-S1/LDR	Default	
Data Center 1/DC1-S2/LDR	Default	
Data Center 1/DC1-S3/LDR	Default	
Data Center 2/DC2-S1/LDR	Default	
Data Center 2/DC2-S2/LDR	Default	
Data Center 2/DC2-S3/LDR	Default	
Data Center 3/DC3-S1/LDR	Default	
Data Center 3/DC3-S2/LDR	Default	
Data Center 3/DC3-S3/LDR	Default	

Apply Changes

c. Selezionare **Applica modifiche**.

d. Facoltativamente, se devi modificare un'etichetta salvata, seleziona **Modifica*** e seleziona ***Applica modifiche**.



Non è possibile eliminare i gradi di archiviazione.

3. Assegna nuovi gradi di archiviazione ai nodi di archiviazione:

a. Individuare il nodo di archiviazione nell'elenco LDR e selezionare la relativa icona ***Modifica*** .

b. Selezionare dall'elenco il grado di conservazione appropriato.



LDR	Storage Grade	Actions
Data Center 1/DC1-S1/LDR	Default	
Data Center 1/DC1-S2/LDR	Default disk	
Data Center 1/DC1-S3/LDR	Default	
Data Center 2/DC2-S1/LDR	Default	
Data Center 2/DC2-S2/LDR	Default	
Data Center 2/DC2-S3/LDR	Default	
Data Center 3/DC3-S1/LDR	Default	
Data Center 3/DC3-S2/LDR	Default	
Data Center 3/DC3-S3/LDR	Default	

Apply Changes



Assegnare un grado di archiviazione a un determinato nodo di archiviazione una sola volta. Un nodo di archiviazione ripristinato dopo un errore mantiene il grado di archiviazione assegnato in precedenza. Non modificare questa assegnazione dopo l'attivazione della policy ILM. Se l'assegnazione viene modificata, i dati vengono archiviati in base al nuovo grado di archiviazione.

a. Selezionare **Applica modifiche**.

Utilizzare pool di archiviazione

Che cos'è un pool di archiviazione?

Un pool di archiviazione è un raggruppamento logico di nodi di archiviazione.

Quando si installa StorageGRID, viene creato automaticamente un pool di archiviazione per sito. È possibile configurare pool di archiviazione aggiuntivi in base alle proprie esigenze di archiviazione.



Durante l'installazione, è possibile configurare i nodi di archiviazione in modo che contengano dati e metadati degli oggetti oppure solo metadati degli oggetti. I nodi di archiviazione solo metadati non possono essere utilizzati nei pool di archiviazione. Per ulteriori informazioni, consultare ["Tipi di nodi di archiviazione"](#).

I pool di archiviazione hanno due attributi:

- **Livello di archiviazione:** per i nodi di archiviazione, le prestazioni relative dell'archiviazione di supporto.
- **Sito:** Il centro dati in cui verranno archiviati gli oggetti.

I pool di archiviazione vengono utilizzati nelle regole ILM per determinare dove vengono archiviati i dati degli oggetti e il tipo di archiviazione utilizzato. Quando si configurano le regole ILM per la replica, si selezionano uno o più pool di archiviazione.

Linee guida per la creazione di pool di archiviazione

Configurare e utilizzare pool di archiviazione per proteggersi dalla perdita di dati distribuendo i dati su più siti. Le copie replicate e le copie con codice di cancellazione richiedono configurazioni di pool di archiviazione diverse.

Vedere ["Esempi di abilitazione della protezione contro la perdita del sito mediante la codifica di replicazione e cancellazione"](#) .

Linee guida per tutti i pool di archiviazione

- Mantenere le configurazioni dei pool di archiviazione il più semplici possibile. Non creare più pool di archiviazione del necessario.
- Creare pool di archiviazione con il maggior numero possibile di nodi. Ogni pool di archiviazione dovrebbe contenere due o più nodi. Un pool di archiviazione con nodi insufficienti può causare arretrati ILM se un nodo diventa non disponibile.
- Evitare di creare o utilizzare pool di archiviazione sovrapposti (che contengono uno o più nodi uguali). Se i pool di archiviazione si sovrappongono, è possibile che più copie dei dati degli oggetti vengano salvate sullo stesso nodo.
- In generale, non utilizzare il pool di archiviazione All Storage Nodes (StorageGRID 11.6 e versioni precedenti) o il sito All Sites. Questi elementi vengono aggiornati automaticamente per includere tutti i nuovi siti aggiunti in un'espansione, il che potrebbe non essere il comportamento desiderato.

Linee guida per i pool di archiviazione utilizzati per le copie replicate

- Per la protezione contro la perdita del sito utilizzando ["replicazione"](#) , specificare uno o più pool di archiviazione specifici del sito in ["istruzioni di posizionamento per ogni regola ILM"](#) .

Durante l'installazione StorageGRID viene creato automaticamente un pool di archiviazione per ogni sito.

L'utilizzo di un pool di archiviazione per ogni sito garantisce che le copie degli oggetti replicati vengano posizionate esattamente dove previsto (ad esempio, una copia di ogni oggetto in ogni sito per la protezione contro la perdita del sito).

- Se si aggiunge un sito in un'espansione, creare un nuovo pool di archiviazione che contenga solo il nuovo sito. Poi, ["aggiornare le regole ILM"](#) per controllare quali oggetti vengono archiviati nel nuovo sito.
- Se il numero di copie è inferiore al numero di pool di archiviazione, il sistema distribuisce le copie per bilanciare l'utilizzo del disco tra i pool.
- Se i pool di archiviazione si sovrappongono (contengono gli stessi nodi di archiviazione), tutte le copie dell'oggetto potrebbero essere salvate in un solo sito. È necessario assicurarsi che i pool di archiviazione selezionati non contengano gli stessi nodi di archiviazione.

Linee guida per i pool di archiviazione utilizzati per le copie con codice di cancellazione

- Per la protezione contro la perdita del sito utilizzando ["codifica di cancellazione"](#) , creare pool di archiviazione costituiti da almeno tre siti. Se un pool di archiviazione include solo due siti, non è possibile utilizzare tale pool di archiviazione per la codifica di cancellazione. Non sono disponibili schemi di codifica di cancellazione per un pool di archiviazione con due siti.
- Il numero di nodi di archiviazione e siti contenuti nel pool di archiviazione determina quali ["schemi di codifica di cancellazione"](#) sono disponibili.
- Se possibile, un pool di archiviazione dovrebbe includere un numero di nodi di archiviazione superiore a

quello minimo richiesto per lo schema di codifica di cancellazione selezionato. Ad esempio, se si utilizza uno schema di codifica di cancellazione 6+3, è necessario disporre di almeno nove nodi di archiviazione. Tuttavia, si consiglia di avere almeno un nodo di archiviazione aggiuntivo per sito.

- Distribuire i nodi di archiviazione tra i siti nel modo più uniforme possibile. Ad esempio, per supportare uno schema di codifica di cancellazione 6+3, configurare un pool di archiviazione che includa almeno tre nodi di archiviazione in tre siti.
- Se si hanno requisiti di throughput elevati, non è consigliabile utilizzare un pool di archiviazione che includa più siti se la latenza di rete tra i siti è superiore a 100 ms. Con l'aumentare della latenza, la velocità con cui StorageGRID può creare, posizionare e recuperare frammenti di oggetti diminuisce drasticamente a causa della diminuzione della velocità di trasmissione della rete TCP.

La riduzione della produttività influisce sulle velocità massime raggiungibili di acquisizione e recupero degli oggetti (quando come comportamento di acquisizione è selezionato Bilanciato o Rigoroso) o potrebbe causare arretrati nella coda ILM (quando come comportamento di acquisizione è selezionato Doppio commit). Vedere ["Comportamento di acquisizione delle regole ILM"](#).



Se la griglia include un solo sito, non è possibile utilizzare il pool di archiviazione All Storage Nodes (StorageGRID 11.6 e versioni precedenti) o il sito All Sites in un profilo di codifica di cancellazione. Questo comportamento impedisce che il profilo diventi non valido se viene aggiunto un secondo sito.

Abilita la protezione contro la perdita del sito

Se la distribuzione StorageGRID include più di un sito, è possibile utilizzare la replicazione e la codifica di cancellazione con pool di archiviazione opportunamente configurati per abilitare la protezione contro la perdita del sito.

La replicazione e la codifica di cancellazione richiedono configurazioni di pool di archiviazione diverse:

- Per utilizzare la replica per la protezione contro la perdita del sito, utilizzare i pool di archiviazione specifici del sito creati automaticamente durante l'installazione StorageGRID. Quindi crea regole ILM con ["istruzioni per il posizionamento"](#) che specificano più pool di archiviazione in modo che una copia di ciascun oggetto venga posizionata in ogni sito.
- Per utilizzare la codifica di cancellazione per la protezione dalla perdita del sito, ["creare pool di archiviazione costituiti da più siti"](#). Quindi creare regole ILM che utilizzino un pool di archiviazione composto da più siti e qualsiasi schema di codifica di cancellazione disponibile.



Quando si configura la distribuzione StorageGRID per la protezione dalle perdite del sito, è necessario tenere conto anche degli effetti di ["opzioni di ingestione"](#) e ["coerenza"](#).

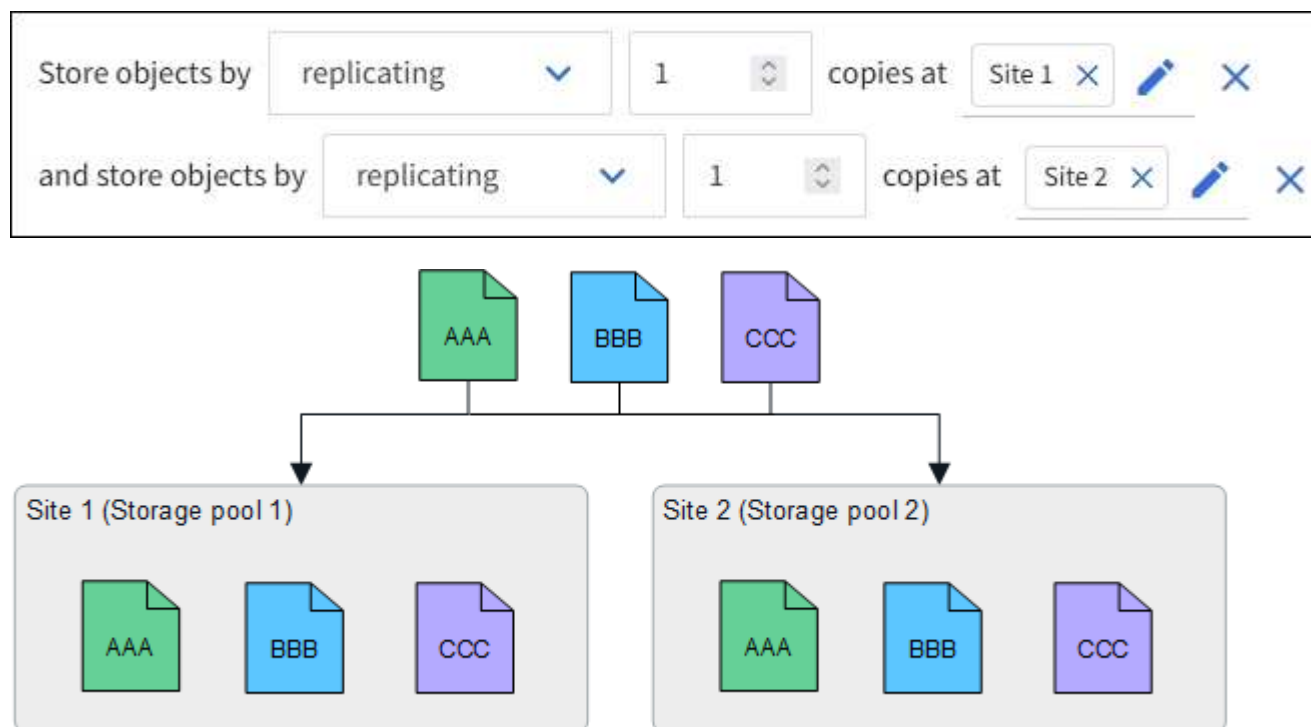
Esempio di replicazione

Per impostazione predefinita, durante l'installazione StorageGRID viene creato un pool di archiviazione per ogni sito. Disporre di pool di archiviazione costituiti da un solo sito consente di configurare regole ILM che utilizzano la replica per la protezione dalle perdite del sito. In questo esempio:

- Il pool di archiviazione 1 contiene il sito 1
- Il pool di archiviazione 2 contiene il sito 2
- La regola ILM contiene due posizionamenti:
 - Memorizza gli oggetti replicandone 1 copia nel Sito 1

- Memorizza gli oggetti replicandone 1 copia nel sito 2

Posizionamenti delle regole ILM:



Se un sito viene perso, copie degli oggetti sono disponibili nell'altro sito.

Esempio di codifica di cancellazione

Disporre di pool di archiviazione composti da più di un sito per pool di archiviazione consente di configurare regole ILM che utilizzano la codifica di cancellazione per la protezione dalla perdita del sito. In questo esempio:

- Il pool di archiviazione 1 contiene i siti da 1 a 3
- La regola ILM contiene un posizionamento: memorizzare gli oggetti tramite codifica di cancellazione utilizzando uno schema EC 4+2 nel pool di archiviazione 1, che contiene tre siti

Posizionamenti delle regole ILM:



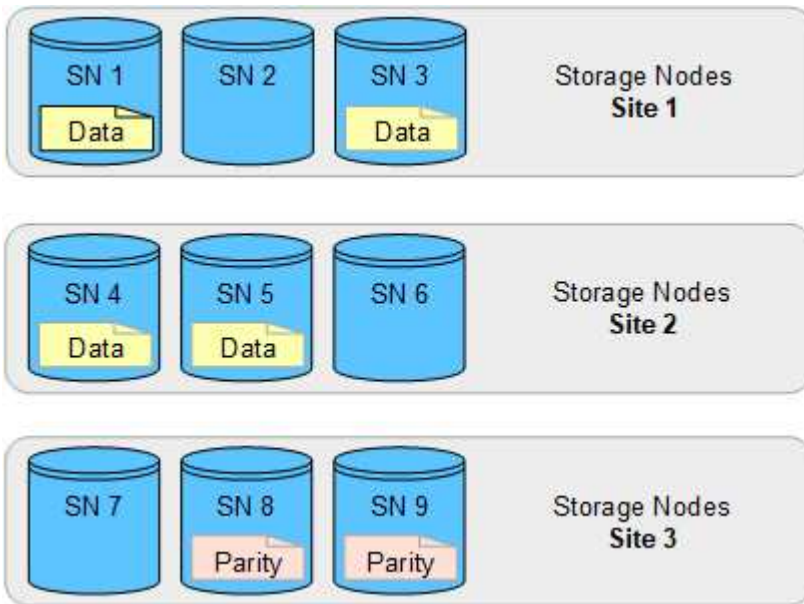
In questo esempio:

- La regola ILM utilizza uno schema di codifica a cancellazione 4+2.
- Ogni oggetto viene suddiviso in quattro frammenti di dati uguali e dai dati dell'oggetto vengono calcolati due frammenti di parità.
- Ciascuno dei sei frammenti viene archiviato su un nodo diverso in tre siti di data center per garantire la protezione dei dati in caso di guasti dei nodi o perdite del sito.

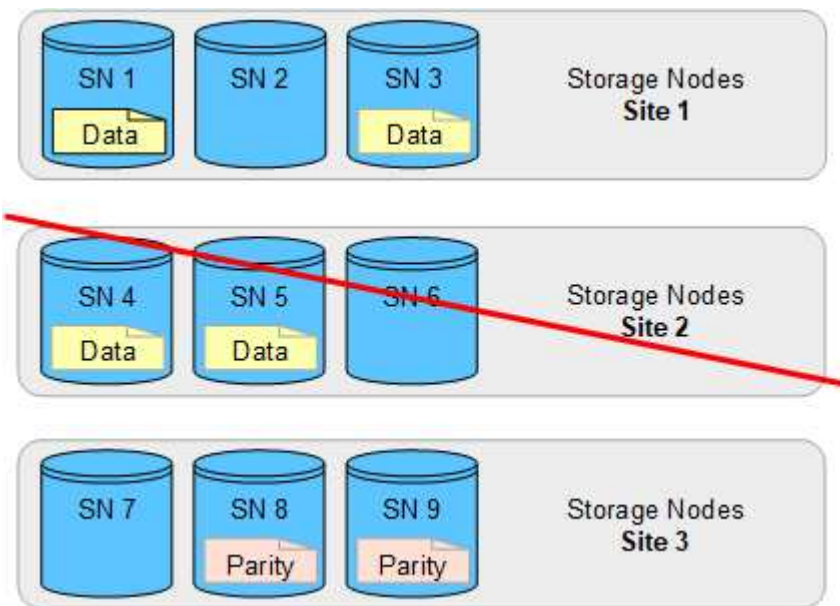


La codifica di cancellazione è consentita nei pool di archiviazione contenenti un numero qualsiasi di siti, *tranne* due siti.

Regola ILM che utilizza lo schema di codifica a cancellazione 4+2:



Se un sito viene perso, i dati possono comunque essere recuperati:



Creare un pool di archiviazione

È possibile creare pool di archiviazione per determinare dove il sistema StorageGRID archivia i dati degli oggetti e il tipo di archiviazione utilizzato. Ogni pool di archiviazione include uno o più siti e uno o più gradi di archiviazione.



Quando si installa StorageGRID 11.9 su una nuova griglia, vengono creati automaticamente pool di archiviazione per ciascun sito. Tuttavia, se inizialmente hai installato StorageGRID 11.6 o una versione precedente, i pool di archiviazione non vengono creati automaticamente per ogni sito.

Se si desidera creare pool di archiviazione cloud per archiviare dati di oggetti al di fuori del sistema

StorageGRID , vedere ["informazioni sull'utilizzo dei pool di archiviazione cloud"](#) .

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Hai ["autorizzazioni di accesso specifiche"](#) .
- Hai esaminato le linee guida per la creazione di pool di archiviazione.

Informazioni su questo compito

I pool di archiviazione determinano dove vengono archiviati i dati degli oggetti. Il numero di pool di archiviazione necessari dipende dal numero di siti nella griglia e dal tipo di copie desiderate: replicate o con codice di cancellazione.

- Per la replicazione e la codifica di cancellazione a sito singolo, creare un pool di archiviazione per ciascun sito. Ad esempio, se si desidera archiviare copie di oggetti replicati in tre siti, creare tre pool di archiviazione.
- Per la codifica di cancellazione in tre o più siti, creare un pool di archiviazione che includa una voce per ciascun sito. Ad esempio, se si desidera eliminare oggetti di codice in tre siti, creare un pool di archiviazione.



Non includere il sito Tutti i siti in un pool di archiviazione che verrà utilizzato in un profilo di codifica di cancellazione. Aggiungere invece una voce separata al pool di archiviazione per ogni sito in cui verranno archiviati i dati con codice di cancellazione. Vedere [questo passo](#) per fare un esempio.

- Se si dispone di più di un livello di archiviazione, non creare un pool di archiviazione che includa diversi livelli di archiviazione in un singolo sito. Vedi il ["Linee guida per la creazione di pool di archiviazione"](#) .

Passi

1. Selezionare **ILM > Pool di archiviazione**.

Nella scheda Pool di archiviazione sono elencati tutti i pool di archiviazione definiti.



Per le nuove installazioni di StorageGRID 11.6 o versioni precedenti, il pool di archiviazione All Storage Nodes viene aggiornato automaticamente ogni volta che si aggiungono nuovi siti di data center. Non utilizzare questo pool nelle regole ILM.

2. Per creare un nuovo pool di archiviazione, selezionare **Crea**.
3. Immettere un nome univoco per il pool di archiviazione. Utilizzare un nome che sia facile da identificare quando si configurano i profili di codifica di cancellazione e le regole ILM.
4. Dall'elenco a discesa **Sito**, selezionare un sito per questo pool di archiviazione.

Quando si seleziona un sito, il numero di nodi di archiviazione nella tabella viene aggiornato automaticamente.

In generale, non utilizzare il sito Tutti i siti in nessun pool di archiviazione. Le regole ILM che utilizzano un pool di archiviazione All Sites posizionano gli oggetti in qualsiasi sito disponibile, riducendo il controllo sul posizionamento degli oggetti. Inoltre, un pool di archiviazione All Sites utilizza immediatamente i nodi di archiviazione in un nuovo sito, il che potrebbe non essere il comportamento previsto.

5. Dall'elenco a discesa **Livello di archiviazione**, selezionare il tipo di archiviazione che verrà utilizzato se una regola ILM utilizza questo pool di archiviazione.

Il grado di archiviazione, *include tutti i gradi di archiviazione*, include tutti i nodi di archiviazione nel sito selezionato. Se hai creato gradi di archiviazione aggiuntivi per i nodi di archiviazione nella tua griglia, questi vengono elencati nel menu a discesa.

6. Se si desidera utilizzare il pool di archiviazione in un profilo di codifica di cancellazione multi-sito, selezionare **Aggiungi altri nodi** per aggiungere una voce per ciascun sito al pool di archiviazione.



Se aggiungi più di una voce con diversi gradi di archiviazione per un sito, verrai avvisato.

Per rimuovere una voce, seleziona l'icona Elimina .

7. Quando sei soddisfatto delle tue selezioni, seleziona **Salva**.

Il nuovo pool di archiviazione viene aggiunto all'elenco.

Visualizza i dettagli del pool di archiviazione

È possibile visualizzare i dettagli di un pool di archiviazione per determinare dove viene utilizzato e per vedere quali nodi e livelli di archiviazione sono inclusi.

Prima di iniziare

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

Passi

1. Selezionare **ILM > Pool di archiviazione**.

La tabella Pool di archiviazione include le seguenti informazioni per ogni pool di archiviazione che include nodi di archiviazione:

- **Nome:** nome visualizzato univoco del pool di archiviazione.
- **Conteggio nodi:** numero di nodi nel pool di archiviazione.
- **Utilizzo dello spazio di archiviazione:** la percentuale dello spazio utilizzabile totale che è stata utilizzata per i dati degli oggetti su questo nodo. Questo valore non include i metadati dell'oggetto.
- **Capacità totale:** la dimensione del pool di archiviazione, che equivale alla quantità totale di spazio utilizzabile per i dati degli oggetti per tutti i nodi nel pool di archiviazione.
- **Utilizzo ILM:** modalità di utilizzo attuale del pool di archiviazione. Un pool di archiviazione potrebbe non essere utilizzato oppure potrebbe essere utilizzato in una o più regole ILM, profili di codifica di cancellazione o entrambi.

2. Per visualizzare i dettagli di uno specifico pool di archiviazione, selezionarne il nome.

Viene visualizzata la pagina dei dettagli del pool di archiviazione.

3. Visualizza la scheda **Nodi** per informazioni sui nodi di archiviazione inclusi nel pool di archiviazione.

La tabella include le seguenti informazioni per ciascun nodo:

- Nome del nodo
- Nome del sito

- Grado di conservazione
- Utilizzo dello spazio di archiviazione: percentuale dello spazio totale utilizzabile per i dati degli oggetti che è stato utilizzato per il nodo di archiviazione.



Lo stesso valore di utilizzo dello storage (%) viene visualizzato anche nel grafico Storage Used - Object Data per ciascun Storage Node (selezionare **NODES > Storage Node > Storage**).

4. Visualizzare la scheda **Utilizzo ILM** per determinare se il pool di archiviazione è attualmente utilizzato in regole ILM o profili di codifica di cancellazione.
5. Facoltativamente, vai alla **pagina delle regole ILM** per scoprire e gestire tutte le regole che utilizzano il pool di archiviazione.

Vedi il "[istruzioni per lavorare con le regole ILM](#)".

Modifica pool di archiviazione

È possibile modificare un pool di archiviazione per cambiarne il nome o per aggiornare i siti e i livelli di archiviazione.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Hai "[autorizzazioni di accesso specifiche](#)".
- Hai esaminato il "[linee guida per la creazione di pool di archiviazione](#)".
- Se si prevede di modificare un pool di archiviazione utilizzato da una regola nel criterio ILM attivo, è necessario considerare in che modo le modifiche influiranno sul posizionamento dei dati degli oggetti.

Informazioni su questo compito

Se si aggiunge un nuovo sito o un nuovo livello di archiviazione a un pool di archiviazione utilizzato nella policy ILM attiva, tenere presente che i nodi di archiviazione nel nuovo sito o livello di archiviazione non verranno utilizzati automaticamente. Per forzare StorageGRID a utilizzare un nuovo sito o un nuovo livello di archiviazione, è necessario attivare un nuovo criterio ILM dopo aver salvato il pool di archiviazione modificato.

Passi

1. Selezionare **ILM > Pool di archiviazione**.
2. Selezionare la casella di controllo per il pool di archiviazione che si desidera modificare.

Non è possibile modificare il pool di archiviazione All Storage Nodes (StorageGRID 11.6 e versioni precedenti).

3. Selezionare **Modifica**.
4. Se necessario, modificare il nome del pool di archiviazione.
5. Se necessario, selezionare altri siti e gradi di stoccaggio.

Non è possibile modificare il sito o il grado di archiviazione se il pool di archiviazione viene utilizzato in un profilo di codifica di cancellazione e la modifica renderebbe non valido lo schema di codifica di cancellazione. Ad esempio, se un pool di archiviazione utilizzato in un profilo di codifica di cancellazione include attualmente un grado di archiviazione con un solo sito, non è possibile utilizzare un grado di archiviazione con due siti perché la modifica renderebbe non valido lo schema di codifica di cancellazione.



L'aggiunta o la rimozione di siti da un pool di archiviazione esistente non sposterà alcun dato codificato per la cancellazione esistente. Se si desidera spostare i dati esistenti dal sito, è necessario creare un nuovo pool di archiviazione e un profilo EC per ricodificare i dati.

6. Seleziona **Salva**.

Dopo aver finito

Se hai aggiunto un nuovo sito o un nuovo livello di archiviazione a un pool di archiviazione utilizzato nel criterio ILM attivo, attiva un nuovo criterio ILM per forzare StorageGRID a utilizzare il nuovo sito o livello di archiviazione. Ad esempio, clona la tua policy ILM esistente e poi attiva il clone. Vedere "[Lavorare con le regole e le politiche ILM](#)".

Rimuovere un pool di archiviazione

È possibile rimuovere un pool di archiviazione non utilizzato.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Tu hai il "[autorizzazioni di accesso richieste](#)".

Passi

1. Selezionare **ILM > Pool di archiviazione**.
2. Esaminare la colonna relativa all'utilizzo di ILM nella tabella per determinare se è possibile rimuovere il pool di archiviazione.

Non è possibile rimuovere un pool di archiviazione se è utilizzato in una regola ILM o in un profilo di codifica di cancellazione. Se necessario, selezionare **nome pool di archiviazione > Utilizzo ILM** per determinare dove viene utilizzato il pool di archiviazione.

3. Se il pool di archiviazione che si desidera rimuovere non è in uso, selezionare la casella di controllo.
4. Seleziona **Rimuovi**.
5. Selezionare **OK**.

Utilizzare i pool di archiviazione cloud

Che cos'è un Cloud Storage Pool?

Un Cloud Storage Pool consente di utilizzare ILM per spostare i dati degli oggetti all'esterno del sistema StorageGRID. Ad esempio, potresti voler spostare gli oggetti a cui si accede raramente su un archivio cloud più economico, come Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud o il livello di accesso Archive nell'archivio BLOB di Microsoft Azure. In alternativa, potresti voler mantenere un backup cloud degli oggetti StorageGRID per migliorare il ripristino in caso di emergenza.

Dal punto di vista ILM, un Cloud Storage Pool è simile a un pool di archiviazione. Per archiviare gli oggetti in una delle due posizioni, selezionare il pool durante la creazione delle istruzioni di posizionamento per una regola ILM. Tuttavia, mentre i pool di archiviazione sono costituiti da nodi di archiviazione all'interno del sistema StorageGRID, un pool di archiviazione cloud è costituito da un bucket esterno (S3) o da un contenitore (archiviazione BLOB di Azure).

La tabella confronta i pool di archiviazione con i pool di archiviazione cloud e mostra le principali somiglianze e differenze.

	Pool di stoccaggio	Pool di archiviazione cloud
Come viene creato?	Utilizzando l'opzione ILM > Pool di archiviazione in Grid Manager.	Utilizzando l'opzione ILM > Pool di archiviazione > Pool di archiviazione cloud in Grid Manager. È necessario configurare il bucket o il contenitore esterno prima di poter creare il Cloud Storage Pool.
Quante piscine puoi creare?	Illimitato.	Fino a 10.
Dove vengono conservati gli oggetti?	Su uno o più nodi di archiviazione all'interno StorageGRID.	In un bucket Amazon S3, in un contenitore di archiviazione BLOB di Azure o in un Google Cloud esterno al sistema StorageGRID . Se il Cloud Storage Pool è un bucket Amazon S3: • Facoltativamente, è possibile configurare un ciclo di vita del bucket per trasferire gli oggetti in un archivio a basso costo e a lungo termine, come Amazon S3 Glacier o S3 Glacier Deep Archive. Il sistema di archiviazione esterno deve supportare la classe di archiviazione Glacier e l'API S3 RestoreObject. • È possibile creare pool di archiviazione cloud da utilizzare con AWS Commercial Cloud Services (C2S), che supporta la regione segreta AWS. Se il Cloud Storage Pool è un contenitore di archiviazione BLOB di Azure, StorageGRID trasferisce l'oggetto al livello Archivio. Nota: in generale, non configurare la gestione del ciclo di vita dell'archiviazione BLOB di Azure per il contenitore utilizzato per un pool di archiviazione cloud. Le operazioni di RestoreObject sugli oggetti nel Cloud Storage Pool possono essere influenzate dal ciclo di vita configurato.
Cosa controlla il posizionamento degli oggetti?	Una regola ILM nelle policy ILM attive.	Una regola ILM nelle policy ILM attive.
Quale metodo di protezione dei dati viene utilizzato?	Codifica di replicazione o cancellazione.	Replicazione.

	Pool di stoccaggio	Pool di archiviazione cloud
Quante copie di ciascun oggetto sono consentite?	Multiplo.	Una copia nel Cloud Storage Pool e, facoltativamente, una o più copie in StorageGRID. Nota: non è possibile archiviare un oggetto in più di un Cloud Storage Pool contemporaneamente.
Quali sono i vantaggi?	Gli oggetti sono rapidamente accessibili in qualsiasi momento.	Archiviazione a basso costo. Nota: i dati FabricPool non possono essere suddivisi in livelli nei Cloud Storage Pool.

Ciclo di vita di un oggetto Cloud Storage Pool

Prima di implementare i Cloud Storage Pool, esaminare il ciclo di vita degli oggetti archiviati in ciascun tipo di Cloud Storage Pool.

S3: Ciclo di vita di un oggetto Cloud Storage Pool

I passaggi descrivono le fasi del ciclo di vita di un oggetto archiviato in un pool di archiviazione cloud S3.



"Glacier" si riferisce sia alla classe di archiviazione Glacier sia alla classe di archiviazione Glacier Deep Archive, con un'eccezione: la classe di archiviazione Glacier Deep Archive non supporta il livello di ripristino accelerato. È supportato solo il recupero in blocco o standard.



Google Cloud Platform (GCP) supporta il recupero di oggetti da archivi a lungo termine senza richiedere un'operazione di ripristino POST.

1. Oggetto memorizzato in StorageGRID

Per avviare il ciclo di vita, un'applicazione client memorizza un oggetto in StorageGRID.

2. Oggetto spostato nel pool di archiviazione cloud S3

- Quando l'oggetto corrisponde a una regola ILM che utilizza un pool di archiviazione cloud S3 come posizione di posizionamento, StorageGRID sposta l'oggetto nel bucket S3 esterno specificato dal pool di archiviazione cloud.
- Quando l'oggetto è stato spostato nel pool di archiviazione cloud S3, l'applicazione client può recuperarlo utilizzando una richiesta S3 GetObject da StorageGRID, a meno che l'oggetto non sia stato trasferito nello storage Glacier.

3. Oggetto trasferito a Glacier (stato non recuperabile)

- Facoltativamente, l'oggetto può essere trasferito nello storage Glacier. Ad esempio, il bucket S3 esterno potrebbe utilizzare la configurazione del ciclo di vita per trasferire un oggetto allo storage Glacier immediatamente o dopo un certo numero di giorni.



Se si desidera effettuare la transizione degli oggetti, è necessario creare una configurazione del ciclo di vita per il bucket S3 esterno e utilizzare una soluzione di archiviazione che implementi la classe di archiviazione Glacier e supporti l'API S3 RestoreObject.

- Durante la transizione, l'applicazione client può utilizzare una richiesta S3 HeadObject per monitorare lo stato dell'oggetto.

4. Oggetto ripristinato dal deposito Glacier

Se un oggetto è stato trasferito nello storage Glacier, l'applicazione client può inviare una richiesta S3 RestoreObject per ripristinare una copia recuperabile nello storage pool S3 Cloud. La richiesta specifica per quanti giorni la copia deve essere disponibile nel Cloud Storage Pool e il livello di accesso ai dati da utilizzare per l'operazione di ripristino (Expedited, Standard o Bulk). Quando viene raggiunta la data di scadenza della copia recuperabile, la copia torna automaticamente allo stato non recuperabile.



Se una o più copie dell'oggetto sono presenti anche sui nodi di archiviazione all'interno di StorageGRID, non è necessario ripristinare l'oggetto da Glacier inviando una richiesta RestoreObject. In alternativa, è possibile recuperare direttamente la copia locale, utilizzando una richiesta GetObject.

5. Oggetto recuperato

Una volta ripristinato un oggetto, l'applicazione client può inviare una richiesta GetObject per recuperare l'oggetto ripristinato.

Azure: ciclo di vita di un oggetto Cloud Storage Pool

I passaggi descrivono le fasi del ciclo di vita di un oggetto archiviato in un pool di Azure Cloud Storage.

1. Oggetto memorizzato in StorageGRID

Per avviare il ciclo di vita, un'applicazione client memorizza un oggetto in StorageGRID.

2. Oggetto spostato nel pool di archiviazione cloud di Azure

Quando l'oggetto corrisponde a una regola ILM che utilizza un pool di archiviazione cloud di Azure come posizione di posizionamento, StorageGRID sposta l'oggetto nel contenitore di archiviazione BLOB di Azure esterno specificato dal pool di archiviazione cloud.

3. Oggetto trasferito al livello Archivio (stato non recuperabile)

Subito dopo aver spostato l'oggetto nel pool di archiviazione cloud di Azure, StorageGRID trasferisce automaticamente l'oggetto al livello di archivio di archiviazione BLOB di Azure.

4. Oggetto ripristinato dal livello Archivio

Se un oggetto è stato trasferito al livello Archivio, l'applicazione client può inviare una richiesta S3 RestoreObject per ripristinare una copia recuperabile nel pool di archiviazione cloud di Azure.

Quando StorageGRID riceve RestoreObject, trasferisce temporaneamente l'oggetto al livello Cool di archiviazione BLOB di Azure. Non appena viene raggiunta la data di scadenza nella richiesta RestoreObject, StorageGRID riporta l'oggetto al livello Archivio.



Se una o più copie dell'oggetto sono presenti anche sui nodi di archiviazione all'interno di StorageGRID, non è necessario ripristinare l'oggetto dal livello di accesso all'archivio inviando una richiesta RestoreObject. In alternativa, è possibile recuperare direttamente la copia locale, utilizzando una richiesta GetObject.

5. Oggetto recuperato

Una volta ripristinato un oggetto nel pool di archiviazione cloud di Azure, l'applicazione client può inviare una richiesta GetObject per recuperare l'oggetto ripristinato.

Informazioni correlate

["Utilizzare l'API REST S3"](#)

Quando utilizzare i pool di archiviazione cloud

Utilizzando i Cloud Storage Pool, è possibile eseguire il backup o suddividere i dati in livelli in una posizione esterna. Inoltre, è possibile eseguire il backup o suddividere i dati in più cloud.

Eseguire il backup dei dati StorageGRID in una posizione esterna

È possibile utilizzare un Cloud Storage Pool per eseguire il backup degli oggetti StorageGRID in una posizione esterna.

Se le copie in StorageGRID non sono accessibili, i dati degli oggetti nel Cloud Storage Pool possono essere utilizzati per soddisfare le richieste dei client. Tuttavia, potrebbe essere necessario inviare una richiesta S3 RestoreObject per accedere alla copia dell'oggetto di backup nel Cloud Storage Pool.

I dati degli oggetti in un Cloud Storage Pool possono essere utilizzati anche per recuperare i dati persi da StorageGRID a causa di un errore del volume di archiviazione o del nodo di archiviazione. Se l'unica copia rimanente di un oggetto si trova in un Cloud Storage Pool, StorageGRID ripristina temporaneamente l'oggetto e crea una nuova copia sul nodo di archiviazione recuperato.

Per implementare una soluzione di backup:

1. Crea un singolo Cloud Storage Pool.
2. Configurare una regola ILM che memorizzi simultaneamente copie di oggetti su nodi di archiviazione (come copie replicate o con codice di cancellazione) e una singola copia di oggetti nel pool di archiviazione cloud.
3. Aggiungi la regola alla tua policy ILM. Quindi, simulare e attivare la policy.

Dati di livello da StorageGRID alla posizione esterna

È possibile utilizzare un Cloud Storage Pool per archiviare oggetti al di fuori del sistema StorageGRID. Supponiamo, ad esempio, di avere un gran numero di oggetti che devi conservare, ma che prevedi di accedervi raramente, se non mai. È possibile utilizzare un Cloud Storage Pool per suddividere gli oggetti in livelli di archiviazione più economici e liberare spazio in StorageGRID.

Per implementare una soluzione a livelli:

1. Crea un singolo Cloud Storage Pool.

2. Configura una regola ILM che sposta gli oggetti raramente utilizzati dai nodi di archiviazione al pool di archiviazione cloud.
3. Aggiungi la regola alla tua policy ILM. Quindi, simulare e attivare la policy.

Gestisci più endpoint cloud

È possibile configurare più endpoint del Cloud Storage Pool se si desidera suddividere in livelli o eseguire il backup dei dati degli oggetti su più cloud. I filtri nelle regole ILM consentono di specificare quali oggetti vengono archiviati in ciascun Cloud Storage Pool. Ad esempio, potresti voler archiviare oggetti da alcuni tenant o bucket in Amazon S3 Glacier e oggetti da altri tenant o bucket nell'archiviazione BLOB di Azure. Oppure potresti voler spostare i dati tra Amazon S3 Glacier e Azure Blob Storage.



Quando si utilizzano più endpoint Cloud Storage Pool, tenere presente che un oggetto può essere archiviato in un solo Cloud Storage Pool alla volta.

Per implementare più endpoint cloud:

1. Crea fino a 10 pool di archiviazione cloud.
2. Configurare le regole ILM per archiviare i dati degli oggetti appropriati al momento opportuno in ogni Cloud Storage Pool. Ad esempio, archivia gli oggetti dal bucket A nel Cloud Storage Pool A e archivia gli oggetti dal bucket B nel Cloud Storage Pool B. Oppure, archivia gli oggetti nel Cloud Storage Pool A per un certo periodo di tempo e poi spostali nel Cloud Storage Pool B.
3. Aggiungi le regole alla tua policy ILM. Quindi, simulare e attivare la policy.

Considerazioni sui pool di archiviazione cloud

Se si prevede di utilizzare un Cloud Storage Pool per spostare oggetti fuori dal sistema StorageGRID , è necessario esaminare le considerazioni per la configurazione e l'utilizzo dei Cloud Storage Pool.

Considerazioni generali

- In generale, l'archiviazione cloud, come Amazon S3 Glacier o Azure Blob Storage, è un modo economico per archiviare dati di oggetti. Tuttavia, i costi per recuperare i dati dall'archiviazione cloud sono relativamente elevati. Per ottenere il costo complessivo più basso, è necessario considerare quando e con quale frequenza si accederà agli oggetti nel Cloud Storage Pool. Si consiglia di utilizzare un pool di archiviazione cloud solo per i contenuti a cui si prevede di accedere raramente.
- L'utilizzo di Cloud Storage Pool con FabricPool non è supportato a causa della latenza aggiuntiva necessaria per recuperare un oggetto dalla destinazione di Cloud Storage Pool.
- Gli oggetti con S3 Object Lock abilitato non possono essere inseriti nei Cloud Storage Pool.
- Se il bucket S3 di destinazione per un Cloud Storage Pool ha abilitato il blocco degli oggetti S3, il tentativo di configurare la replica del bucket (PutBucketReplication) fallirà con un errore AccessDenied.
- Le seguenti combinazioni di piattaforma, autenticazione e protocollo con blocco oggetto S3 non sono supportate per i pool di archiviazione cloud:
 - **Piattaforme:** Google Cloud Platform e Azure
 - **Tipi di autenticazione:** ruoli IAM ovunque e accesso anonimo
 - **Protocollo:** HTTP

Considerazioni sulle porte utilizzate per i pool di archiviazione cloud

Per garantire che le regole ILM possano spostare oggetti da e verso il Cloud Storage Pool specificato, è necessario configurare la rete o le reti che contengono i nodi di archiviazione del sistema. È necessario assicurarsi che le seguenti porte possano comunicare con il Cloud Storage Pool.

Per impostazione predefinita, i pool di archiviazione cloud utilizzano le seguenti porte:

- **80**: Per gli URI degli endpoint che iniziano con http
- **443**: Per gli URI degli endpoint che iniziano con https

È possibile specificare una porta diversa quando si crea o si modifica un Cloud Storage Pool.

Se si utilizza un server proxy non trasparente, è necessario anche ["configurare un proxy di archiviazione"](#) per consentire l'invio di messaggi a endpoint esterni, ad esempio un endpoint su Internet.

Considerazioni sui costi

Per accedere allo storage nel cloud tramite un Cloud Storage Pool è necessaria la connettività di rete al cloud. È necessario considerare il costo dell'infrastruttura di rete che verrà utilizzata per accedere al cloud e predisporla in modo appropriato, in base alla quantità di dati che si prevede di spostare tra StorageGRID e il cloud utilizzando il Cloud Storage Pool.

Quando StorageGRID si connette all'endpoint esterno del Cloud Storage Pool, invia varie richieste per monitorare la connettività e garantire che possa eseguire le operazioni richieste. Sebbene a queste richieste siano associati alcuni costi aggiuntivi, il costo del monitoraggio di un Cloud Storage Pool dovrebbe rappresentare solo una piccola frazione del costo complessivo dell'archiviazione degli oggetti in S3 o Azure.

Potrebbero essere sostenuti costi più significativi se è necessario spostare oggetti da un endpoint Cloud Storage Pool esterno a StorageGRID. Gli oggetti potrebbero essere spostati nuovamente su StorageGRID in uno dei seguenti casi:

- L'unica copia dell'oggetto si trova in un Cloud Storage Pool e si decide di archiviare l'oggetto in StorageGRID. In questo caso, è necessario riconfigurare le regole e i criteri ILM. Quando si verifica la valutazione ILM, StorageGRID invia più richieste per recuperare l'oggetto dal Cloud Storage Pool. StorageGRID crea quindi localmente il numero specificato di copie replicate o con codice di cancellazione. Dopo che l'oggetto viene spostato nuovamente su StorageGRID, la copia nel Cloud Storage Pool viene eliminata.
- Gli oggetti vengono persi a causa di un errore del nodo di archiviazione. Se l'unica copia rimanente di un oggetto si trova in un Cloud Storage Pool, StorageGRID ripristina temporaneamente l'oggetto e crea una nuova copia sul nodo di archiviazione recuperato.



Quando gli oggetti vengono spostati nuovamente su StorageGRID da un Cloud Storage Pool, StorageGRID invia più richieste all'endpoint del Cloud Storage Pool per ciascun oggetto. Prima di spostare un gran numero di oggetti, contattare l'assistenza tecnica per ottenere assistenza nella stima dei tempi e dei costi associati.

S3: Autorizzazioni richieste per il bucket Cloud Storage Pool

I criteri per il bucket S3 esterno utilizzato per un Cloud Storage Pool devono concedere a StorageGRID l'autorizzazione per spostare un oggetto nel bucket, ottenere lo stato di un oggetto, ripristinare un oggetto dallo storage Glacier quando necessario e altro ancora. Idealmente, StorageGRID dovrebbe avere accesso completo al bucket(`s3 : *`); tuttavia, se ciò non è possibile, la policy del bucket deve concedere le seguenti autorizzazioni S3 a StorageGRID:

- s3:AbortMultipartUpload
- s3:DeleteObject
- s3:GetObject
- s3:ListBucket
- s3:ListBucketMultipartUploads
- s3:ListMultipartUploadParts
- s3:PutObject
- s3:RestoreObject

S3: Considerazioni sul ciclo di vita del bucket esterno

Lo spostamento degli oggetti tra StorageGRID e il bucket S3 esterno specificato nel Cloud Storage Pool è controllato dalle regole ILM e dai criteri ILM attivi in StorageGRID. Al contrario, la transizione degli oggetti dal bucket S3 esterno specificato nel Cloud Storage Pool ad Amazon S3 Glacier o S3 Glacier Deep Archive (o a una soluzione di archiviazione che implementa la classe di archiviazione Glacier) è controllata dalla configurazione del ciclo di vita di quel bucket.

Se si desidera trasferire oggetti dal Cloud Storage Pool, è necessario creare la configurazione del ciclo di vita appropriata sul bucket S3 esterno e utilizzare una soluzione di archiviazione che implementi la classe di archiviazione Glacier e supporti l'API S3 RestoreObject.

Ad esempio, supponiamo di voler trasferire immediatamente tutti gli oggetti spostati da StorageGRID al Cloud Storage Pool allo storage Amazon S3 Glacier. Dovresti creare una configurazione del ciclo di vita sul bucket S3 esterno che specifica una singola azione (**Transizione**) come segue:

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
      <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Questa regola trasferirà tutti gli oggetti bucket ad Amazon S3 Glacier il giorno in cui sono stati creati (ovvero il giorno in cui sono stati spostati da StorageGRID al Cloud Storage Pool).



Quando si configura il ciclo di vita del bucket esterno, non utilizzare mai azioni **Scadenza** per definire quando scadono gli oggetti. Le azioni di scadenza determinano l'eliminazione degli oggetti scaduti da parte del sistema di archiviazione esterno. Se in seguito si tenta di accedere a un oggetto scaduto da StorageGRID, l'oggetto eliminato non verrà trovato.

Se si desidera trasferire gli oggetti nel Cloud Storage Pool a S3 Glacier Deep Archive (anziché ad Amazon S3 Glacier), specificare `<StorageClass>DEEP_ARCHIVE</StorageClass>` nel ciclo di vita del bucket. Tuttavia, tieni presente che non puoi utilizzare il Expedited livello per ripristinare gli oggetti dall'archivio profondo del ghiacciaio S3.

Azure: considerazioni sul livello di accesso

Quando si configura un account di archiviazione di Azure, è possibile impostare il livello di accesso predefinito su Accesso frequente o Accesso sporadico. Quando si crea un account di archiviazione da utilizzare con un Cloud Storage Pool, è consigliabile utilizzare il livello Hot come livello predefinito. Anche se StorageGRID imposta immediatamente il livello su Archivio quando sposta gli oggetti nel Cloud Storage Pool, l'utilizzo di un'impostazione predefinita su Caldo garantisce che non verrà addebitata alcuna commissione per l'eliminazione anticipata degli oggetti rimossi dal livello Freddo prima del minimo di 30 giorni.

Azure: gestione del ciclo di vita non supportata

Non utilizzare la gestione del ciclo di vita dell'archiviazione BLOB di Azure per il contenitore utilizzato con un pool di archiviazione cloud. Le operazioni del ciclo di vita potrebbero interferire con le operazioni del Cloud Storage Pool.

Informazioni correlate

["Creare un pool di archiviazione cloud"](#)

Confronta i pool di archiviazione cloud e la replica di CloudMirror

Quando si inizia a utilizzare Cloud Storage Pools, potrebbe essere utile comprendere le somiglianze e le differenze tra Cloud Storage Pools e il servizio di replica StorageGRID CloudMirror.

	Pool di archiviazione cloud	Servizio di replica CloudMirror
Qual è lo scopo principale?	Funziona come destinazione di archivio. La copia dell'oggetto nel Cloud Storage Pool può essere l'unica copia dell'oggetto oppure una copia aggiuntiva. Ciò significa che, invece di conservare due copie in loco, è possibile conservarne una copia in StorageGRID e inviarne una copia al Cloud Storage Pool.	Consente a un tenant di replicare automaticamente gli oggetti da un bucket in StorageGRID (origine) a un bucket S3 esterno (destinazione). Crea una copia indipendente di un oggetto in un'infrastruttura S3 indipendente.
Come è impostato?	Definiti allo stesso modo dei pool di archiviazione, utilizzando Grid Manager o Grid Management API. Può essere selezionato come posizione di posizionamento in una regola ILM. Mentre un pool di archiviazione è costituito da un gruppo di nodi di archiviazione, un pool di archiviazione cloud viene definito utilizzando un endpoint S3 o Azure remoto (indirizzo IP, credenziali e così via).	Un utente tenant "configura la replica di CloudMirror" definendo un endpoint CloudMirror (indirizzo IP, credenziali e così via) tramite Tenant Manager o l'API S3. Dopo aver configurato l'endpoint CloudMirror, qualsiasi bucket di proprietà di quell'account tenant può essere configurato in modo che punti all'endpoint CloudMirror.

	Pool di archiviazione cloud	Servizio di replica CloudMirror
Chi è responsabile della sua istituzione?	In genere, un amministratore di rete	In genere, un utente tenant
Qual è la destinazione?	• Qualsiasi infrastruttura S3 compatibile (incluso Amazon S3) • Livello di archivio BLOB di Azure • Piattaforma Google Cloud (GCP)	• Qualsiasi infrastruttura S3 compatibile (incluso Amazon S3) • Piattaforma Google Cloud (GCP)
Cosa determina lo spostamento degli oggetti verso la destinazione?	Una o più regole ILM nelle policy ILM attive. Le regole ILM definiscono quali oggetti StorageGRID sposta nel Cloud Storage Pool e quando gli oggetti vengono spostati.	L'atto di ingerire un nuovo oggetto in un bucket di origine configurato con un endpoint CloudMirror. Gli oggetti presenti nel bucket di origine prima che il bucket fosse configurato con l'endpoint CloudMirror non vengono replicati, a meno che non vengano modificati.
Come vengono recuperati gli oggetti?	Le applicazioni devono inviare richieste a StorageGRID per recuperare gli oggetti che sono stati spostati in un Cloud Storage Pool. Se l'unica copia di un oggetto è stata trasferita in un archivio, StorageGRID gestisce il processo di ripristino dell'oggetto in modo che possa essere recuperato.	Poiché la copia speculare nel bucket di destinazione è una copia indipendente, le applicazioni possono recuperare l'oggetto inviando richieste a StorageGRID o alla destinazione S3. Supponiamo, ad esempio, di utilizzare la replica CloudMirror per eseguire il mirroring degli oggetti su un'organizzazione partner. Il partner può utilizzare le proprie applicazioni per leggere o aggiornare gli oggetti direttamente dalla destinazione S3. Non è obbligatorio utilizzare StorageGRID.
Riesci a leggere direttamente dalla destinazione?	No. Gli oggetti spostati in un Cloud Storage Pool vengono gestiti da StorageGRID. Le richieste di lettura devono essere indirizzate a StorageGRID (e StorageGRID sarà responsabile del recupero da Cloud Storage Pool).	Sì, perché la copia speculare è una copia indipendente.
Cosa succede se un oggetto viene eliminato dalla sorgente?	L'oggetto viene eliminato anche dal Cloud Storage Pool.	L'azione di eliminazione non viene replicata. Un oggetto eliminato non esiste più nel bucket StorageGRID, ma continua a esistere nel bucket di destinazione. Allo stesso modo, gli oggetti nel bucket di destinazione possono essere eliminati senza influire sulla sorgente.

	Pool di archiviazione cloud	Servizio di replica CloudMirror
Come si accede agli oggetti dopo un disastro (sistema StorageGRID non operativo)?	I nodi StorageGRID non riusciti devono essere ripristinati. Durante questo processo, le copie degli oggetti replicati potrebbero essere ripristinate utilizzando le copie presenti nel Cloud Storage Pool.	Le copie degli oggetti nella destinazione CloudMirror sono indipendenti da StorageGRID, quindi è possibile accedervi direttamente prima che i nodi StorageGRID vengano ripristinati.

Creare un pool di archiviazione cloud

Un Cloud Storage Pool specifica un singolo bucket Amazon S3 esterno o un altro provider compatibile con S3 oppure un contenitore di archiviazione BLOB di Azure.

Quando si crea un Cloud Storage Pool, si specifica il nome e la posizione del bucket o del contenitore esterno che StorageGRID utilizzerà per archiviare gli oggetti, il tipo di provider cloud (Amazon S3/GCP o Azure Blob Storage) e le informazioni necessarie a StorageGRID per accedere al bucket o al contenitore esterno.

StorageGRID convalida il Cloud Storage Pool non appena lo salvi, quindi devi assicurarti che il bucket o il contenitore specificato nel Cloud Storage Pool esista e sia raggiungibile.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["autorizzazioni di accesso richieste"](#).
- Hai esaminato il ["considerazioni per i pool di archiviazione cloud"](#).
- Il bucket o contenitore esterno a cui fa riferimento il Cloud Storage Pool esiste già e si dispone di [informazioni sull'endpoint del servizio](#).
- Per accedere al secchio o al contenitore, hai il [informazioni sull'account per il tipo di autenticazione](#) sceglierai tu.

Passi

1. Selezionare **ILM > Pool di archiviazione > Pool di archiviazione cloud**.
2. Seleziona **Crea**, quindi inserisci le seguenti informazioni:

Campo	Descrizione
Nome del pool di archiviazione cloud	Un nome che descrive brevemente il Cloud Storage Pool e il suo scopo. Utilizzare un nome che sia facile da identificare quando si configurano le regole ILM.
Tipo di fornitore	Quale provider cloud utilizzerai per questo Cloud Storage Pool: • Amazon S3/GCP: seleziona questa opzione per un provider Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) o un altro provider compatibile con S3. • Archiviazione BLOB di Azure

Campo	Descrizione
Secchio o contenitore	Nome del bucket S3 esterno o del contenitore di Azure. Non è possibile modificare questo valore dopo aver salvato il Cloud Storage Pool.

3. In base alla selezione del tipo di provider, immettere le informazioni sull'endpoint del servizio.

Amazon S3/GCP

- a. Per il protocollo, selezionare HTTPS o HTTP.



Non utilizzare connessioni HTTP per dati sensibili.

- b. Inserisci il nome host. Esempio:

`s3-aws-region.amazonaws.com`

- c. Seleziona lo stile URL:

Opzione	Descrizione
Rilevamento automatico	Tenta di rilevare automaticamente quale stile URL utilizzare, in base alle informazioni fornite. Ad esempio, se si specifica un indirizzo IP, StorageGRID utilizzerà un URL in stile percorso. Seleziona questa opzione solo se non sai quale stile specifico utilizzare.
Stile ospitato virtuale	Utilizzare un URL in stile virtual-hosted per accedere al bucket. Gli URL in stile virtual-hosted includono il nome del bucket come parte del nome di dominio. Esempio: <code>https://bucket-name.s3.company.com/key-name</code>
Stile percorso	Utilizzare un URL in stile percorso per accedere al bucket. Gli URL in stile percorso includono il nome del bucket alla fine. Esempio: <code>https://s3.company.com/bucket-name/key-name</code> Nota: l'opzione URL in stile percorso non è consigliata e verrà deprecata in una futura versione di StorageGRID.

- d. Facoltativamente, immettere il numero di porta oppure utilizzare la porta predefinita: 443 per HTTPS o 80 per HTTP.

Archiviazione BLOB di Azure

- a. Utilizzando uno dei seguenti formati, immettere l'URI per l'endpoint del servizio.

- `https://host:port`
- `http://host:port`

Esempio: `https://myaccount.blob.core.windows.net:443`

Se non si specifica una porta, per impostazione predefinita viene utilizzata la porta 443 per HTTPS e la porta 80 per HTTP.

4. Seleziona **Continua**. Quindi seleziona il tipo di autenticazione e inserisci le informazioni richieste per l'endpoint del Cloud Storage Pool:

Chiave di accesso

Per Amazon S3/GCP o altri provider compatibili con S3

- a. **ID chiave di accesso:** immettere l'ID chiave di accesso per l'account proprietario del bucket esterno.
- b. **Chiave di accesso segreta:** Inserisci la chiave di accesso segreta.

Ruoli IAM ovunque

Per il servizio AWS IAM Roles Anywhere

StorageGRID utilizza AWS Security Token Service (STS) per generare dinamicamente un token di breve durata per accedere alle risorse AWS.

- a. **Regione AWS IAM Roles Anywhere:** seleziona la regione per il Cloud Storage Pool. Ad esempio, `us-east-1`.
- b. **URN dell'ancora di trust:** immettere l'URN dell'ancora di trust che convalida le richieste di credenziali STS di breve durata. Può essere una CA radice o intermedia.
- c. **URN del profilo:** immettere l'URN del profilo IAM Roles Anywhere che elenca i ruoli che possono essere assunti da chiunque sia considerato attendibile.
- d. **URN del ruolo:** immettere l'URN del ruolo IAM che può essere assunto da chiunque sia considerato attendibile.
- e. **Durata sessione:** immettere la durata delle credenziali di sicurezza temporanee e della sessione del ruolo. Inserisci almeno 15 minuti e non più di 12 ore.
- f. **Certificato CA del server** (facoltativo): uno o più certificati CA attendibili, in formato PEM, per la verifica del server IAM Roles Anywhere. Se omissso, il server non verrà verificato.
- g. **Certificato dell'entità finale:** la chiave pubblica, in formato PEM, del certificato X509 firmato dal trust anchor. AWS IAM Roles Anywhere utilizza questa chiave per emettere un token STS.
- h. **Chiave privata dell'entità finale:** la chiave privata per il certificato dell'entità finale.

CAP (portale di accesso C2S)

Per il servizio S3 dei servizi cloud commerciali (C2S)

- a. **URL delle credenziali temporanee:** immettere l'URL completo che StorageGRID utilizzerà per ottenere le credenziali temporanee dal server CAP, inclusi tutti i parametri API obbligatori e facoltativi assegnati al proprio account C2S.
- b. **Certificato CA del server:** seleziona **Sfogliala** e carica il certificato CA che StorageGRID utilizzerà per verificare il server CAP. Il certificato deve essere codificato PEM ed emesso da un'autorità di certificazione governativa (CA) appropriata.
- c. **Certificato client:** seleziona **Sfogliala** e carica il certificato che StorageGRID utilizzerà per identificarsi sul server CAP. Il certificato client deve essere codificato PEM, rilasciato da un'autorità di certificazione governativa (CA) appropriata e deve consentire l'accesso al tuo account C2S.
- d. **Chiave privata client:** selezionare **Sfogliala** e caricare la chiave privata codificata PEM per il certificato client.
- e. Se la chiave privata del client è crittografata, immettere la passphrase per decrittografare la chiave privata del client. In caso contrario, lasciare vuoto il campo **Passphrase della chiave privata del client**.



Se il certificato client verrà crittografato, utilizzare il formato tradizionale per la crittografia. Il formato crittografato PKCS #8 non è supportato.

Archiviazione BLOB di Azure

Per Azure Blob Storage, solo chiave condivisa

- Nome account:** immettere il nome dell'account di archiviazione proprietario del contenitore esterno
- Chiave account:** inserisci la chiave segreta per l'account di archiviazione

È possibile utilizzare il portale di Azure per trovare questi valori.

Anonimo

Non sono richieste ulteriori informazioni.

5. Selezionare **Continua**. Quindi scegli il tipo di verifica del server che desideri utilizzare:

Opzione	Descrizione
Utilizzare i certificati CA radice nel sistema operativo Storage Node	Utilizzare i certificati Grid CA installati sul sistema operativo per proteggere le connessioni.
Utilizza un certificato CA personalizzato	Utilizzare un certificato CA personalizzato. Selezionare Sfoglia e caricare il certificato codificato PEM.
Non verificare il certificato	Selezionando questa opzione le connessioni TLS al Cloud Storage Pool non saranno sicure.

6. Seleziona **Salva**.

Quando si salva un Cloud Storage Pool, StorageGRID esegue le seguenti operazioni:

- Verifica che il bucket o il contenitore e l'endpoint del servizio esistano e che possano essere raggiunti utilizzando le credenziali specificate.
- Scrive un file marcatore nel bucket o nel contenitore per identificarlo come Cloud Storage Pool. Non rimuovere mai questo file, che si chiama `x-ntap-sgws-cloud-pool-uuid`.

Se la convalida del Cloud Storage Pool non riesce, viene visualizzato un messaggio di errore che spiega il motivo per cui la convalida non è riuscita. Ad esempio, potrebbe essere segnalato un errore se si verifica un errore del certificato o se il bucket o il contenitore specificato non esiste già.

7. Se si verifica un errore, vedere il ["Istruzioni per la risoluzione dei problemi dei pool di archiviazione cloud"](#), risolvere eventuali problemi e quindi provare a salvare nuovamente il Cloud Storage Pool.

Visualizza i dettagli del Cloud Storage Pool

È possibile visualizzare i dettagli di un Cloud Storage Pool per determinare dove viene utilizzato e vedere quali nodi e livelli di archiviazione sono inclusi.

Prima di iniziare

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

Passi

1. Selezionare **ILM > Pool di archiviazione > Pool di archiviazione cloud**.

La tabella Cloud Storage Pools include le seguenti informazioni per ogni Cloud Storage Pool che include nodi di archiviazione:

- **Nome:** il nome visualizzato univoco del pool.
- **URI:** Uniform Resource Identifier del Cloud Storage Pool.
- **Tipo di provider:** quale provider cloud viene utilizzato per questo Cloud Storage Pool.
- **Contenitore:** il nome del bucket utilizzato per il Cloud Storage Pool.
- **Utilizzo ILM:** modalità di utilizzo attuale del pool. Un Cloud Storage Pool potrebbe non essere utilizzato oppure potrebbe essere utilizzato in una o più regole ILM, profili di codifica di cancellazione o entrambi.
- **Ultimo errore:** l'ultimo errore rilevato durante un controllo dello stato di questo Cloud Storage Pool.

2. Per visualizzare i dettagli di uno specifico Cloud Storage Pool, selezionarne il nome.

Viene visualizzata la pagina dei dettagli del pool.

3. Visualizza la scheda **Autenticazione** per informazioni sul tipo di autenticazione per questo Cloud Storage Pool e per modificare i dettagli di autenticazione.
4. Visualizza la scheda **Verifica del server** per conoscere i dettagli della verifica, modificare la verifica, scaricare un nuovo certificato o copiare il certificato PEM.
5. Visualizzare la scheda **Utilizzo ILM** per determinare se il Cloud Storage Pool è attualmente utilizzato in regole ILM o profili di codifica di cancellazione.
6. Facoltativamente, vai alla **pagina delle regole ILM** per ["conoscere e gestire tutte le regole"](#) che utilizzano il Cloud Storage Pool.

Modifica un pool di archiviazione cloud

È possibile modificare un Cloud Storage Pool per cambiarne il nome, l'endpoint del servizio o altri dettagli; tuttavia, non è possibile modificare il bucket S3 o il contenitore di Azure per un Cloud Storage Pool.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Hai ["autorizzazioni di accesso specifiche"](#) .
- Hai esaminato il ["considerazioni per i pool di archiviazione cloud"](#) .

Passi

1. Selezionare **ILM > Pool di archiviazione > Pool di archiviazione cloud**.

Nella tabella Cloud Storage Pools sono elencati i Cloud Storage Pool esistenti.

2. Seleziona la casella di controllo per il Cloud Storage Pool che desideri modificare, quindi seleziona **Azioni > Modifica**.

In alternativa, seleziona il nome del Cloud Storage Pool, quindi seleziona **Modifica**.

3. Se necessario, modificare il nome del Cloud Storage Pool, l'endpoint del servizio, le credenziali di autenticazione o il metodo di verifica del certificato.



Non è possibile modificare il tipo di provider, il bucket S3 o il contenitore di Azure per un pool di archiviazione cloud.

Se in precedenza hai caricato un certificato server o client, puoi espandere la voce **Dettagli certificato** per esaminare il certificato attualmente in uso.

4. Seleziona **Salva**.

Quando si salva un Cloud Storage Pool, StorageGRID verifica che il bucket o il contenitore e l'endpoint del servizio esistano e che possano essere raggiunti utilizzando le credenziali specificate.

Se la convalida del Cloud Storage Pool fallisce, viene visualizzato un messaggio di errore. Ad esempio, potrebbe essere segnalato un errore se si verifica un errore nel certificato.

Vedi le istruzioni per "[risoluzione dei problemi dei pool di archiviazione cloud](#)", risolvere il problema e quindi provare a salvare nuovamente il Cloud Storage Pool.

Rimuovere un pool di archiviazione cloud

È possibile rimuovere un Cloud Storage Pool se non è utilizzato in una regola ILM e non contiene dati di oggetti.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Tu hai il "[autorizzazioni di accesso richieste](#)".

Se necessario, utilizzare ILM per spostare i dati dell'oggetto

Se il Cloud Storage Pool che si desidera rimuovere contiene dati di oggetti, è necessario utilizzare ILM per spostare i dati in una posizione diversa. Ad esempio, puoi spostare i dati sui nodi di archiviazione nella tua griglia o su un pool di archiviazione cloud diverso.

Passi

1. Selezionare **ILM > Pool di archiviazione > Pool di archiviazione cloud**.
2. Esaminare la colonna relativa all'utilizzo di ILM nella tabella per determinare se è possibile rimuovere il Cloud Storage Pool.

Non è possibile rimuovere un Cloud Storage Pool se è utilizzato in una regola ILM o in un profilo di codifica di cancellazione.

3. Se si utilizza il Cloud Storage Pool, selezionare **nome del cloud storage pool > Utilizzo ILM**.
4. "[Clona ogni regola ILM](#)" che attualmente posiziona gli oggetti nel Cloud Storage Pool che desideri rimuovere.
5. Determina dove vuoi spostare gli oggetti esistenti gestiti da ciascuna regola clonata.

È possibile utilizzare uno o più pool di archiviazione oppure un diverso Cloud Storage Pool.

6. Modifica ciascuna delle regole che hai clonato.

Per il passaggio 2 della procedura guidata Crea regola ILM, selezionare la nuova posizione dal campo **copie in**.

7. ["Crea una nuova policy ILM"](#) e sostituire ciascuna delle vecchie regole con una regola clonata.

8. Attiva la nuova politica.

9. Attendi che ILM rimuova gli oggetti dal Cloud Storage Pool e li posizioni nella nuova posizione.

Elimina pool di archiviazione cloud

Quando il Cloud Storage Pool è vuoto e non viene utilizzato in alcuna regola ILM, è possibile eliminarlo.

Prima di iniziare

- Sono state rimosse tutte le regole ILM che potrebbero aver utilizzato il pool.
- Hai confermato che il bucket S3 o il contenitore di Azure non contiene alcun oggetto.

Si verifica un errore se si tenta di rimuovere un Cloud Storage Pool che contiene oggetti. Vedere ["Risoluzione dei problemi dei pool di archiviazione cloud"](#).



Quando si crea un Cloud Storage Pool, StorageGRID scrive un file marcatore nel bucket o nel contenitore per identificarlo come Cloud Storage Pool. Non rimuovere questo file, che si chiama `x-ntap-sgws-cloud-pool-uuid`.

Passi

1. Selezionare **ILM > Pool di archiviazione > Pool di archiviazione cloud**.
2. Se la colonna Utilizzo ILM indica che Cloud Storage Pool non è in uso, selezionare la casella di controllo.
3. Selezionare **Azioni > Rimuovi**.
4. Selezionare **OK**.

Risoluzione dei problemi dei pool di archiviazione cloud

Utilizza questi passaggi per la risoluzione dei problemi per risolvere gli errori che potresti riscontrare durante la creazione, la modifica o l'eliminazione di un Cloud Storage Pool.

Determina se si è verificato un errore

StorageGRID esegue un semplice controllo dello stato di salute su ogni Cloud Storage Pool leggendo l'oggetto noto `x-ntap-sgws-cloud-pool-uuid` per garantire che il Cloud Storage Pool sia accessibile e funzioni correttamente. Quando StorageGRID rileva un errore sull'endpoint, esegue un controllo dello stato ogni minuto da ciascun nodo di archiviazione. Una volta risolto l'errore, i controlli di integrità si interrompono. Se un controllo dello stato rileva un problema, viene visualizzato un messaggio nella colonna Ultimo errore della tabella Cloud Storage Pools nella pagina Storage Pools.

La tabella mostra l'errore più recente rilevato per ciascun Cloud Storage Pool e indica da quanto tempo si è verificato l'errore.

Inoltre, viene attivato un avviso di **Errore di connettività del Cloud Storage Pool** se il controllo dello stato rileva che si sono verificati uno o più nuovi errori del Cloud Storage Pool negli ultimi 5 minuti. Se ricevi una notifica via e-mail per questo avviso, vai alla pagina Pool di archiviazione (seleziona **ILM > Pool di**

archiviazione), esamina i messaggi di errore nella colonna Ultimo errore e fai riferimento alle linee guida per la risoluzione dei problemi riportate di seguito.

Controlla se un errore è stato risolto

Dopo aver risolto eventuali problemi di fondo, è possibile determinare se l'errore è stato risolto. Dalla pagina Cloud Storage Pool, seleziona l'endpoint e seleziona **Cancella errore**. Un messaggio di conferma indica che StorageGRID ha eliminato l'errore per il Cloud Storage Pool.

Se il problema di fondo è stato risolto, il messaggio di errore non viene più visualizzato. Tuttavia, se il problema di fondo non è stato risolto (o se si verifica un errore diverso), il messaggio di errore verrà visualizzato nella colonna Ultimo errore entro pochi minuti.

Errore: controllo dello stato di integrità non riuscito. Errore dall'endpoint

Potresti riscontrare questo errore quando abiliti S3 Object Lock con conservazione predefinita per il tuo bucket Amazon S3 dopo aver iniziato a utilizzare questo bucket per un Cloud Storage Pool. Questo errore si verifica quando l'operazione PUT non ha un'intestazione HTTP con un valore di checksum del payload come Content-MD5 . Questo valore di intestazione è richiesto da AWS per le operazioni PUT nei bucket con S3 Object Lock abilitato.

Per correggere questo problema, seguire i passaggi in ["Modifica un pool di archiviazione cloud"](#) senza apportare alcuna modifica. Questa azione attiva la convalida della configurazione del Cloud Storage Pool che rileva e aggiorna automaticamente il flag S3 Object Lock su una configurazione dell'endpoint del Cloud Storage Pool.

Errore: questo pool di archiviazione cloud contiene contenuti inaspettati

Potresti riscontrare questo errore quando provi a creare, modificare o eliminare un Cloud Storage Pool. Questo errore si verifica se il bucket o il contenitore include x-ntap-sgws-cloud-pool-uuid file marker, ma quel file non ha il campo metadati con l'UUID previsto.

In genere, questo errore viene visualizzato solo se si sta creando un nuovo Cloud Storage Pool e un'altra istanza di StorageGRID sta già utilizzando lo stesso Cloud Storage Pool.

Prova uno di questi passaggi per correggere il problema:

- Se si sta configurando un nuovo Cloud Storage Pool e il bucket contiene x-ntap-sgws-cloud-pool-uuid file e chiavi di oggetti aggiuntivi simili all'esempio seguente, crea un nuovo bucket e usalo al suo posto.

Esempio di una chiave oggetto aggiuntiva: my-bucket.3E64CF2C-B74D-4B7D-AFE7-AD28BC18B2F6.1727326606730410

- Se il x-ntap-sgws-cloud-pool-uuid file è l'unico oggetto nel bucket, elimina questo file.

Se questi passaggi non si applicano al tuo scenario, contatta l'assistenza.

Errore: impossibile creare o aggiornare il Cloud Storage Pool. Errore dall'endpoint

Questo errore potrebbe verificarsi nelle seguenti circostanze:

- Quando si tenta di creare o modificare un Cloud Storage Pool.
- Quando si seleziona una combinazione di piattaforma, autenticazione o protocollo non supportata con S3 Object Lock durante la configurazione di un nuovo Cloud Storage Pool. Vedere ["Considerazioni sui pool di"](#)

Questo errore indica che un problema di connettività o di configurazione impedisce a StorageGRID di scrivere sul Cloud Storage Pool.

Per correggere il problema, rivedere il messaggio di errore dall'endpoint.

- Se il messaggio di errore contiene `Get url: EOF`, verificare che l'endpoint del servizio utilizzato per Cloud Storage Pool non utilizzi HTTP per un contenitore o un bucket che richiede HTTPS.
- Se il messaggio di errore contiene `Get url: net/http: request canceled while waiting for connection`, verificare che la configurazione di rete consenta ai nodi di archiviazione di accedere all'endpoint del servizio utilizzato per il pool di archiviazione cloud.
- Se l'errore è dovuto a una piattaforma, un'autenticazione o un protocollo non supportati, passare a una configurazione supportata con S3 Object Lock e provare a salvare nuovamente il nuovo Cloud Storage Pool.
- Per tutti gli altri messaggi di errore dell'endpoint, provare una o più delle seguenti soluzioni:
 - Crea un contenitore o un bucket esterno con lo stesso nome immesso per il Cloud Storage Pool e prova a salvare nuovamente il nuovo Cloud Storage Pool.
 - Correggi il nome del contenitore o del bucket specificato per il Cloud Storage Pool e prova a salvare nuovamente il nuovo Cloud Storage Pool.

Errore: impossibile analizzare il certificato CA

Potresti riscontrare questo errore quando provi a creare o modificare un Cloud Storage Pool. L'errore si verifica se StorageGRID non è riuscito ad analizzare il certificato immesso durante la configurazione del Cloud Storage Pool.

Per correggere il problema, controlla il certificato CA fornito per eventuali problemi.

Errore: non è stato trovato un pool di archiviazione cloud con questo ID

Potresti riscontrare questo errore quando provi a modificare o eliminare un Cloud Storage Pool. Questo errore si verifica se l'endpoint restituisce una risposta 404, che può significare uno dei seguenti:

- Le credenziali utilizzate per Cloud Storage Pool non dispongono dell'autorizzazione di lettura per il bucket.
- Il bucket utilizzato per il Cloud Storage Pool non include `x-ntap-sgws-cloud-pool-uuid` file marcatore.

Prova uno o più di questi passaggi per correggere il problema:

- Verificare che l'utente associato alla chiave di accesso configurata disponga delle autorizzazioni richieste.
- Modificare il Cloud Storage Pool con credenziali che dispongono delle autorizzazioni richieste.
- Se le autorizzazioni sono corrette, contattare l'assistenza.

Errore: impossibile controllare il contenuto del Cloud Storage Pool. Errore dall'endpoint

Potresti riscontrare questo errore quando provi a eliminare un Cloud Storage Pool. Questo errore indica che un problema di connettività o di configurazione impedisce a StorageGRID di leggere il contenuto del bucket Cloud Storage Pool.

Per correggere il problema, rivedere il messaggio di errore dall'endpoint.

Errore: gli oggetti sono già stati inseriti in questo bucket

Potresti riscontrare questo errore quando provi a eliminare un Cloud Storage Pool. Non è possibile eliminare un Cloud Storage Pool se contiene dati spostati lì da ILM, dati presenti nel bucket prima della configurazione del Cloud Storage Pool o dati inseriti nel bucket da un'altra origine dopo la creazione del Cloud Storage Pool.

Prova uno o più di questi passaggi per correggere il problema:

- Seguire le istruzioni per spostare nuovamente gli oggetti su StorageGRID in "Ciclo di vita di un oggetto Cloud Storage Pool".
- Se sei certo che gli oggetti rimanenti non siano stati inseriti nel Cloud Storage Pool da ILM, eliminali manualmente dal bucket.



Non eliminare mai manualmente oggetti da un Cloud Storage Pool che potrebbero essere stati inseriti lì da ILM. Se in seguito si tenta di accedere a un oggetto eliminato manualmente da StorageGRID, l'oggetto eliminato non verrà trovato.

Errore: il proxy ha riscontrato un errore esterno durante il tentativo di raggiungere il Cloud Storage Pool

Questo errore potrebbe verificarsi se è stato configurato un proxy di archiviazione non trasparente tra i nodi di archiviazione e l'endpoint S3 esterno utilizzato per il pool di archiviazione cloud. Questo errore si verifica se il server proxy esterno non riesce a raggiungere l'endpoint del Cloud Storage Pool. Ad esempio, il server DNS potrebbe non essere in grado di risolvere il nome host oppure potrebbe esserci un problema di rete esterna.

Prova uno o più di questi passaggi per correggere il problema:

- Controllare le impostazioni per il Cloud Storage Pool (**ILM > Storage pool**).
- Controllare la configurazione di rete del server proxy di archiviazione.

Errore: il certificato X.509 è scaduto nel periodo di validità

Potresti riscontrare questo errore quando provi a eliminare un Cloud Storage Pool. Questo errore si verifica quando l'autenticazione richiede un certificato X.509 per garantire che venga convalidato il corretto Cloud Storage Pool esterno e che il pool esterno sia vuoto prima che la configurazione del Cloud Storage Pool venga eliminata.

Per risolvere il problema, prova a seguire questi passaggi:

- Aggiornare il certificato configurato per l'autenticazione nel Cloud Storage Pool.
- Assicurarsi che tutti gli avvisi di scadenza dei certificati su questo Cloud Storage Pool siano stati risolti.

Informazioni correlate

["Ciclo di vita di un oggetto Cloud Storage Pool"](#)

Gestisci i profili di codifica di cancellazione

È possibile visualizzare i dettagli di un profilo di codifica di cancellazione e, se necessario, rinominare un profilo. È possibile disattivare un profilo di codifica di cancellazione se non è attualmente utilizzato in alcuna regola ILM.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Tu hai il "[autorizzazioni di accesso richieste](#)".

Visualizza i dettagli del profilo di codifica di cancellazione

È possibile visualizzare i dettagli di un profilo di codifica di cancellazione per determinarne lo stato, lo schema di codifica di cancellazione utilizzato e altre informazioni.

Passi

1. Selezionare **CONFIGURAZIONE > Sistema > Codifica di cancellazione**.
2. Seleziona il profilo. Viene visualizzata la pagina dei dettagli del profilo.
3. Facoltativamente, visualizza la scheda Regole ILM per un elenco delle regole ILM che utilizzano il profilo e i criteri ILM che utilizzano tali regole.
4. Facoltativamente, visualizza la scheda Nodi di archiviazione per i dettagli su ciascun nodo di archiviazione nel pool di archiviazione del profilo, ad esempio il sito in cui si trova e l'utilizzo dello spazio di archiviazione.

Rinominare un profilo di codifica di cancellazione

Potresti voler rinominare un profilo di codifica di cancellazione per rendere più evidente la sua funzione.

Passi

1. Selezionare **CONFIGURAZIONE > Sistema > Codifica di cancellazione**.
2. Seleziona il profilo che vuoi rinominare.
3. Selezionare **Rinomina**.
4. Immettere un nome univoco per il profilo di codifica di cancellazione.

Il nome del profilo di codifica di cancellazione viene aggiunto al nome del pool di archiviazione nelle istruzioni di posizionamento per una regola ILM.



I nomi dei profili di codifica di cancellazione devono essere univoci. Si verifica un errore di convalida se si utilizza il nome di un profilo esistente, anche se tale profilo è stato disattivato.

5. Seleziona **Salva**.

Disattivare un profilo di codifica di cancellazione

È possibile disattivare un profilo di codifica di cancellazione se non si prevede più di utilizzarlo e se il profilo non è attualmente utilizzato in alcuna regola ILM.



Verificare che non siano in corso operazioni di riparazione di dati codificati tramite cancellazione o procedure di disattivazione. Se si tenta di disattivare un profilo di codifica di cancellazione mentre è in corso una di queste operazioni, viene visualizzato un messaggio di errore.

Informazioni su questo compito

StorageGRID impedisce la disattivazione di un profilo di codifica di cancellazione se si verifica una delle seguenti condizioni:

- Il profilo di codifica della cancellazione è attualmente utilizzato in una regola ILM.

- Il profilo di codifica della cancellazione non è più utilizzato in nessuna regola ILM, ma i dati degli oggetti e i frammenti di parità per il profilo esistono ancora.

Passi

1. Selezionare **CONFIGURAZIONE > Sistema > Codifica di cancellazione**.
2. Nella scheda Attivo, rivedere la colonna **Stato** per confermare che il profilo di codifica di cancellazione che si desidera disattivare non sia utilizzato in alcuna regola ILM.

Non è possibile disattivare un profilo di codifica di cancellazione se è utilizzato in una regola ILM. Nell'esempio, il profilo 2+1 Data Center 1 viene utilizzato in almeno una regola ILM.

☐	Profile name ?	Status ?	Storage pool ?	Erasure-coding scheme ?
☐	2+1 Data Center 1	Used in 5 rules	Data Center 1	2+1
☐	New profile	Deactivated	Data Center 1	2+1

3. Se il profilo viene utilizzato in una regola ILM, attenersi alla seguente procedura:
 - a. Selezionare **ILM > Regole**.
 - b. Selezionare ciascuna regola e rivedere il diagramma di conservazione per determinare se la regola utilizza il profilo di codifica di cancellazione che si desidera disattivare.
 - c. Se la regola ILM utilizza il profilo di codifica di cancellazione che si desidera disattivare, determinare se la regola viene utilizzata in un criterio ILM.
 - d. Completare i passaggi aggiuntivi nella tabella, in base al punto in cui viene utilizzato il profilo di codifica di cancellazione.

Dove è stato utilizzato il profilo?	Ulteriori passaggi da eseguire prima di disattivare il profilo	Fare riferimento a queste istruzioni aggiuntive
Mai utilizzato in nessuna regola ILM	Non sono richiesti passaggi aggiuntivi. Continuare con questa procedura.	Nessuno
In una regola ILM che non è mai stata utilizzata in nessuna politica ILM	i. Modifica o elimina tutte le regole ILM interessate. Se modifichi la regola, rimuovi tutti i posizionamenti che utilizzano il profilo di codifica di cancellazione. ii. Continuare con questa procedura.	"Lavorare con le regole e le politiche ILM"

Dove è stato utilizzato il profilo?	Ulteriori passaggi da eseguire prima di disattivare il profilo	Fare riferimento a queste istruzioni aggiuntive
In una regola ILM che è attualmente in una policy ILM attiva	i. Clonare la policy. ii. Rimuovere la regola ILM che utilizza il profilo di codifica di cancellazione. iii. Aggiungere una o più nuove regole ILM per garantire la protezione degli oggetti. iv. Salva, simula e attiva la nuova policy. v. Attendi che la nuova policy venga applicata e che gli oggetti esistenti vengano spostati in nuove posizioni in base alle nuove regole aggiunte. Nota: a seconda del numero di oggetti e delle dimensioni del sistema StorageGRID , potrebbero essere necessarie settimane o addirittura mesi prima che le operazioni ILM spostino gli oggetti in nuove posizioni, in base alle nuove regole ILM. Sebbene sia possibile tentare in tutta sicurezza di disattivare un profilo di codifica di cancellazione mentre è ancora associato ai dati, l'operazione di disattivazione non andrà a buon fine. Un messaggio di errore ti informerà se il profilo non è ancora pronto per essere disattivato. vi. Modifica o elimina la regola rimossa dal criterio. Se modifichi la regola, rimuovi tutti i posizionamenti che utilizzano il profilo di codifica di cancellazione. vii. Continuare con questa procedura.	"Creare una policy ILM" "Lavorare con le regole e le politiche ILM"
In una regola ILM che è attualmente in una politica ILM	i. Modifica la politica. ii. Rimuovere la regola ILM che utilizza il profilo di codifica di cancellazione. iii. Aggiungere una o più nuove regole ILM per garantire che tutti gli oggetti siano protetti. iv. Salva la polizza. v. Modifica o elimina la regola rimossa dal criterio. Se modifichi la regola, rimuovi tutti i posizionamenti che utilizzano il profilo di codifica di cancellazione. vi. Continuare con questa procedura.	"Creare una policy ILM" "Lavorare con le regole e le politiche ILM"

e. Aggiornare la pagina Profili di codifica di cancellazione per assicurarsi che il profilo non venga utilizzato in una regola ILM.

4. Se il profilo non viene utilizzato in una regola ILM, selezionare il pulsante di opzione e scegliere **Disattiva**.

Viene visualizzata la finestra di dialogo Disattiva profilo di codifica di cancellazione.



È possibile selezionare più profili da disattivare contemporaneamente, a condizione che ciascun profilo non venga utilizzato in alcuna regola.

5. Se sei sicuro di voler disattivare il profilo, seleziona **Disattiva**.

Risultati

- Se StorageGRID è in grado di disattivare il profilo di codifica di cancellazione, il suo stato è Disattivato. Non è più possibile selezionare questo profilo per nessuna regola ILM. Non è possibile riattivare un profilo disattivato.
- Se StorageGRID non riesce a disattivare il profilo, viene visualizzato un messaggio di errore. Ad esempio, viene visualizzato un messaggio di errore se i dati dell'oggetto sono ancora associati a questo profilo. Potrebbe essere necessario attendere diverse settimane prima di provare nuovamente la procedura di disattivazione.

Configurare le regioni (facoltativo e solo S3)

Le regole ILM possono filtrare gli oggetti in base alle regioni in cui vengono creati i bucket S3, consentendo di archiviare oggetti provenienti da regioni diverse in posizioni di archiviazione diverse.

Se si desidera utilizzare una regione bucket S3 come filtro in una regola, è necessario prima creare le regioni che possono essere utilizzate dai bucket nel sistema.



Non è possibile modificare la regione di un bucket dopo averlo creato.

Prima di iniziare

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

Informazioni su questo compito

Quando si crea un bucket S3, è possibile specificare che il bucket venga creato in una regione specifica. Specificando una regione, il bucket può essere geograficamente vicino ai suoi utenti, il che può aiutare a ottimizzare la latenza, ridurre al minimo i costi e soddisfare i requisiti normativi.

Quando si crea una regola ILM, potrebbe essere opportuno utilizzare la regione associata a un bucket S3 come filtro avanzato. Ad esempio, è possibile progettare una regola che si applica solo agli oggetti nei bucket S3 creati in `us-west-2` regione. È quindi possibile specificare che copie di tali oggetti vengano posizionate su nodi di archiviazione in un sito di data center all'interno di quella regione per ottimizzare la latenza.

Quando si configurano le regioni, seguire queste linee guida:

- Per impostazione predefinita, tutti i bucket sono considerati appartenenti a `us-east-1` regione.
- È necessario creare le regioni utilizzando Grid Manager prima di poter specificare una regione non predefinita quando si creano bucket utilizzando Tenant Manager o Tenant Management API oppure con l'elemento di richiesta LocationConstraint per le richieste S3 PUT Bucket API. Si verifica un errore se una richiesta PUT Bucket utilizza una regione non definita in StorageGRID.
- Quando si crea il bucket S3, è necessario utilizzare il nome esatto della regione. I nomi delle regioni sono sensibili alle maiuscole e alle minuscole. I caratteri validi sono numeri, lettere e trattini.



EU non è considerato un alias di eu-west-1. Se si desidera utilizzare la regione EU o eu-west-1, è necessario utilizzare il nome esatto.

- Non è possibile eliminare o modificare una regione se è utilizzata in una regola assegnata a un criterio (attivo o inattivo).
- Se si utilizza una regione non valida come filtro avanzato in una regola ILM, non è possibile aggiungere tale regola a un criterio.

Una regione non valida può verificarsi se si utilizza una regione come filtro avanzato in una regola ILM ma in seguito si elimina tale regione oppure se si utilizza l'API di gestione della griglia per creare una regola e si specifica una regione che non è stata definita.

- Se elimini una regione dopo averla utilizzata per creare un bucket S3, dovrai aggiungere nuovamente la regione se desideri utilizzare il filtro avanzato Vincolo di posizione per trovare oggetti in quel bucket.

Passi

1. Selezionare **ILM > Regioni**.

Viene visualizzata la pagina Regioni, in cui sono elencate le regioni attualmente definite. **Regione 1** mostra la regione predefinita, `us-east-1`, che non può essere modificato o rimosso.

2. Per aggiungere una regione:

- a. Seleziona **Aggiungi un'altra regione**.
- b. Inserisci il nome della regione che desideri utilizzare durante la creazione dei bucket S3.

Quando si crea il bucket S3 corrispondente, è necessario utilizzare questo nome di regione esatto come elemento di richiesta LocationConstraint.

3. Per rimuovere una regione non utilizzata, seleziona l'icona Elimina .

Se si tenta di rimuovere una regione attualmente utilizzata in un criterio (attivo o inattivo), viene visualizzato un messaggio di errore.

4. Una volta completate le modifiche, seleziona **Salva**.

Ora puoi selezionare queste regioni dalla sezione Filtri avanzati nel passaggio 1 della procedura guidata Crea regola ILM. Vedere ["Utilizzare filtri avanzati nelle regole ILM"](#).

Crea regola ILM

Utilizzare le regole ILM per gestire gli oggetti

Per gestire gli oggetti, è necessario creare un set di regole di gestione del ciclo di vita delle informazioni (ILM) e organizzarle in una policy ILM.

Ogni oggetto inserito nel sistema viene valutato in base alla policy attiva. Quando una regola nella policy corrisponde ai metadati di un oggetto, le istruzioni nella regola determinano quali azioni intraprende StorageGRID per copiare e archiviare quell'oggetto.



I metadati degli oggetti non sono gestiti dalle regole ILM. I metadati degli oggetti vengono invece archiviati in un database Cassandra, in quello che è noto come archivio di metadati. In ogni sito vengono conservate automaticamente tre copie dei metadati degli oggetti per proteggere i dati da eventuali perdite.

Elementi di una regola ILM

Una regola ILM è composta da tre elementi:

- **Criteri di filtraggio:** i filtri di base e avanzati di una regola definiscono a quali oggetti si applica la regola. Se un oggetto corrisponde a tutti i filtri, StorageGRID applica la regola e crea le copie dell'oggetto specificate nelle istruzioni di posizionamento della regola.
- **Istruzioni di posizionamento:** le istruzioni di posizionamento di una regola definiscono il numero, il tipo e la posizione delle copie dell'oggetto. Ogni regola può includere una sequenza di istruzioni di posizionamento per modificare nel tempo il numero, il tipo e la posizione delle copie dell'oggetto. Quando scade il periodo di tempo per un tirocinio, le istruzioni del tirocinio successivo vengono applicate automaticamente dalla successiva valutazione ILM.
- **Comportamento di acquisizione:** il comportamento di acquisizione di una regola consente di scegliere in che modo gli oggetti filtrati dalla regola vengono protetti durante l'acquisizione (quando un client S3 salva un oggetto nella griglia).

Filtraggio delle regole ILM

Quando si crea una regola ILM, si specificano i filtri per identificare gli oggetti a cui si applica la regola.

Nel caso più semplice, una regola potrebbe non utilizzare alcun filtro. Qualsiasi regola che non utilizza filtri si applica a tutti gli oggetti, quindi deve essere l'ultima regola (predefinita) in un criterio ILM. La regola predefinita fornisce istruzioni di archiviazione per gli oggetti che non corrispondono ai filtri di un'altra regola.

- I filtri di base consentono di applicare regole diverse a gruppi di oggetti ampi e distinti. Questi filtri consentono di applicare una regola a specifici account tenant, a specifici bucket S3 o a entrambi.

I filtri di base offrono un modo semplice per applicare regole diverse a un gran numero di oggetti. Ad esempio, potrebbe essere necessario archiviare i registri finanziari della tua azienda per soddisfare i requisiti normativi, mentre i dati del reparto marketing potrebbero dover essere archiviati per facilitare le operazioni quotidiane. Dopo aver creato account tenant separati per ciascun reparto o dopo aver suddiviso i dati dei diversi reparti in bucket S3 separati, è possibile creare facilmente una regola che si applica a tutti i record finanziari e una seconda regola che si applica a tutti i dati di marketing.

- I filtri avanzati ti offrono un controllo granulare. È possibile creare filtri per selezionare gli oggetti in base alle seguenti proprietà:
 - Tempo di ingestione
 - Ultimo orario di accesso
 - Tutto o parte del nome dell'oggetto (Chiave)
 - Vincolo di posizione (solo S3)
 - Dimensione dell'oggetto
 - Metadati utente
 - Tag oggetto (solo S3)

È possibile filtrare gli oggetti in base a criteri molto specifici. Ad esempio, gli oggetti archiviati dal reparto di

diagnostica per immagini di un ospedale potrebbero essere utilizzati frequentemente quando hanno meno di 30 giorni e raramente in seguito, mentre gli oggetti che contengono informazioni sulle visite dei pazienti potrebbero dover essere copiati nel reparto di fatturazione presso la sede centrale della rete sanitaria. È possibile creare filtri che identificano ogni tipo di oggetto in base al nome dell'oggetto, alle dimensioni, ai tag dell'oggetto S3 o a qualsiasi altro criterio rilevante, quindi creare regole separate per archiviare in modo appropriato ogni set di oggetti.

È possibile combinare i filtri in base alle proprie esigenze in un'unica regola. Ad esempio, il reparto marketing potrebbe voler archiviare file di immagini di grandi dimensioni in modo diverso rispetto ai record dei fornitori, mentre il reparto delle risorse umane potrebbe dover archiviare i record del personale in una specifica area geografica e le informazioni sulle politiche in modo centralizzato. In questo caso è possibile creare regole che filtrano in base all'account del tenant per separare i record da ciascun reparto, utilizzando al contempo filtri in ogni regola per identificare il tipo specifico di oggetti a cui si applica la regola.

Istruzioni per il posizionamento delle regole ILM

Le istruzioni di posizionamento determinano dove, quando e come vengono archiviati i dati degli oggetti. Una regola ILM può includere una o più istruzioni di posizionamento. Ogni istruzione di posizionamento si applica a un singolo periodo di tempo.

Quando si creano istruzioni di posizionamento:

- Si inizia specificando l'ora di riferimento, che determina quando iniziano le istruzioni di posizionamento. Il momento di riferimento potrebbe essere il momento in cui un oggetto viene acquisito, quando si accede a un oggetto, quando un oggetto con versione diventa non corrente o un momento definito dall'utente.
- Successivamente, si specifica quando verrà applicato il posizionamento, in relazione all'orario di riferimento. Ad esempio, un posizionamento potrebbe iniziare il giorno 0 e continuare per 365 giorni, in relazione al momento in cui l'oggetto è stato acquisito.
- Infine, si specifica il tipo di copie (codifica di replicazione o di cancellazione) e la posizione in cui vengono archiviate le copie. Ad esempio, potresti voler archiviare due copie replicate in due siti diversi.

Ogni regola può definire più posizionamenti per un singolo periodo di tempo e posizionamenti diversi per periodi di tempo diversi.

- Per posizionare oggetti in più posizioni durante un singolo periodo di tempo, seleziona **Aggiungi altro tipo o posizione** per aggiungere più di una riga per quel periodo di tempo.
- Per posizionare oggetti in posizioni diverse in periodi di tempo diversi, seleziona **Aggiungi un altro periodo di tempo** per aggiungere il periodo di tempo successivo. Quindi, specificare una o più righe all'interno del periodo di tempo.

L'esempio mostra due istruzioni di posizionamento nella pagina Definisci posizionamenti della procedura guidata Crea regola ILM.

Time period and placements Sort by start date

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1
From Day 0 store for 365 days

Store objects by replicating 2 copies at Data Center 1 , Data Center 2

and store objects by erasure coding using 6+3 EC scheme at all sites

1

Add other type or location

Time period 2
From Day 365 store forever

Store objects by replicating 2 copies at Data Center 3

2

Add other type or location

Le prime istruzioni di posizionamento **1** ha due linee per il primo anno:

- La prima riga crea due copie replicate dell'oggetto in due siti di data center.
- La seconda riga crea una copia con codice di cancellazione 6+3 utilizzando tutti i siti del data center.

La seconda istruzione di posizionamento **2** ne crea due copie dopo un anno e le conserva per sempre.

Quando si definisce il set di istruzioni di posizionamento per una regola, è necessario assicurarsi che almeno un'istruzione di posizionamento inizi al giorno 0, che non vi siano intervalli tra i periodi di tempo definiti e che l'istruzione di posizionamento finale continui per sempre o finché non saranno più necessarie copie dell'oggetto.

Alla scadenza di ogni periodo di tempo previsto dalla regola, vengono applicate le istruzioni di posizionamento dei contenuti per il periodo di tempo successivo. Vengono create nuove copie dell'oggetto e quelle non necessarie vengono eliminate.

Comportamento di acquisizione delle regole ILM

Il comportamento di acquisizione controlla se le copie degli oggetti vengono posizionate immediatamente in base alle istruzioni della regola oppure se vengono create copie provvisorie e le istruzioni di posizionamento vengono applicate in un secondo momento. Per le regole ILM sono disponibili i seguenti comportamenti di acquisizione:

- **Bilanciato:** StorageGRID tenta di effettuare tutte le copie specificate nella regola ILM al momento dell'acquisizione; se ciò non è possibile, vengono effettuate copie provvisorie e il client riceve un messaggio di conferma dell'operazione riuscita. Quando possibile, vengono effettuate le copie specificate nella norma ILM.
- **Rigoroso:** tutte le copie specificate nella regola ILM devono essere eseguite prima che il risultato positivo venga restituito al client.

- **Doppio commit:** StorageGRID crea immediatamente copie provvisorie dell'oggetto e restituisce il risultato positivo al client. Quando possibile, vengono effettuate le copie specificate nella norma ILM.

Informazioni correlate

- ["Opzioni di acquisizione"](#)
- ["Vantaggi, svantaggi e limitazioni delle opzioni di ingestione"](#)
- ["Come la coerenza e le regole ILM interagiscono per influenzare la protezione dei dati"](#)

Esempio di regola ILM

Ad esempio, una regola ILM potrebbe specificare quanto segue:

- Si applica solo agli oggetti appartenenti all'inquilino A.
- Realizza due copie replicate di quegli oggetti e conserva ciascuna copia in un luogo diverso.
- Conservare le due copie "per sempre", il che significa che StorageGRID non le eliminerà automaticamente. StorageGRID conserverà invece questi oggetti finché non verranno eliminati da una richiesta di eliminazione del client o dalla scadenza del ciclo di vita di un bucket.
- Utilizzare l'opzione Bilanciato per il comportamento di acquisizione: l'istruzione di posizionamento su due siti viene applicata non appena il Tenant A salva un oggetto in StorageGRID, a meno che non sia possibile effettuare immediatamente entrambe le copie richieste.

Ad esempio, se il sito 2 non è raggiungibile quando il tenant A salva un oggetto, StorageGRID eseguirà due copie provvisorie sui nodi di archiviazione del sito 1. Non appena il Sito 2 sarà disponibile, StorageGRID effettuerà la copia richiesta in quel sito.

Informazioni correlate

- ["Che cos'è un pool di archiviazione"](#)
- ["Che cos'è un Cloud Storage Pool"](#)

Accedi alla procedura guidata Crea una regola ILM

Le regole ILM consentono di gestire il posizionamento dei dati degli oggetti nel tempo. Per creare una regola ILM, utilizzare la procedura guidata Crea una regola ILM.

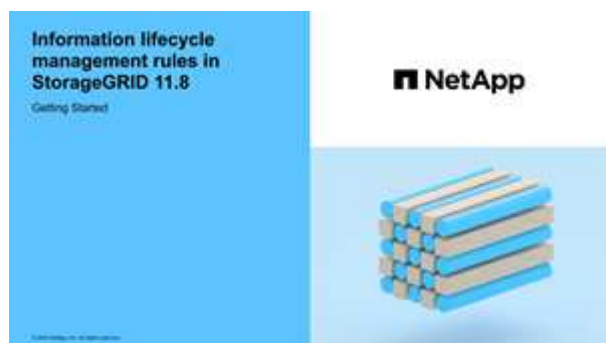


Se si desidera creare la regola ILM predefinita per una policy, seguire la procedura ["istruzioni per la creazione di una regola ILM predefinita"](#) Invece.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Hai ["autorizzazioni di accesso specifiche"](#) .
- Se si desidera specificare a quali account tenant si applica questa regola, è necessario ["Autorizzazione degli account degli inquilini"](#) oppure conosci l'ID account per ogni account.
- Se si desidera che la regola filtri gli oggetti in base ai metadati dell'ora dell'ultimo accesso, gli aggiornamenti dell'ora dell'ultimo accesso devono essere abilitati dal bucket S3.
- Hai configurato tutti i Cloud Storage Pool che intendi utilizzare. Vedere ["Crea un pool di archiviazione cloud"](#) .
- Hai familiarità con il ["opzioni di ingestione"](#) .

- Se è necessario creare una regola conforme da utilizzare con S3 Object Lock, è necessario avere familiarità con ["requisiti per S3 Object Lock"](#) .
- Facoltativamente, hai guardato il video: ["Video: panoramica delle regole ILM"](#) .



Informazioni su questo compito

Durante la creazione delle regole ILM:

- Prendiamo in considerazione la topologia e le configurazioni di archiviazione del sistema StorageGRID .
- Considera quali tipi di copie di oggetti vuoi realizzare (replicate o con codice di cancellazione) e il numero di copie necessarie per ciascun oggetto.
- Determinare quali tipi di metadati degli oggetti vengono utilizzati nelle applicazioni che si connettono al sistema StorageGRID . Le regole ILM filtrano gli oggetti in base ai loro metadati.
- Considera dove vuoi che vengano posizionate le copie degli oggetti nel tempo.
- Decidi quale opzione di gestione utilizzare (Bilanciata, Rigorosa o Doppio commit).

Passi

1. Selezionare **ILM > Regole**.
2. Seleziona **Crea**. ["Passaggio 1 \(Inserisci i dettagli\)"](#) viene visualizzata la procedura guidata Crea una regola ILM.

Passaggio 1 di 3: Inserisci i dettagli

Il passaggio **Inserisci dettagli** della procedura guidata Crea una regola ILM consente di immettere un nome e una descrizione per la regola e di definire i filtri per la regola.

L'inserimento di una descrizione e la definizione dei filtri per la regola sono facoltativi.

Informazioni su questo compito

Quando si valuta un oggetto rispetto a un ["Regola ILM"](#) StorageGRID confronta i metadati dell'oggetto con i filtri della regola. Se i metadati dell'oggetto corrispondono a tutti i filtri, StorageGRID utilizza la regola per posizionare l'oggetto. È possibile progettare una regola da applicare a tutti gli oggetti oppure specificare filtri di base, come uno o più account tenant o nomi di bucket, oppure filtri avanzati, come le dimensioni dell'oggetto o i metadati dell'utente.

Passi

1. Immettere un nome univoco per la regola nel campo **Nome**.
2. Facoltativamente, inserisci una breve descrizione della regola nel campo **Descrizione**.

Dovresti descrivere lo scopo o la funzione della regola in modo da poterla riconoscere in seguito.

3. Facoltativamente, seleziona uno o più account tenant S3 a cui si applica questa regola. Se questa regola si applica a tutti gli inquilini, lasciare vuoto questo campo.

Se non si dispone né dell'autorizzazione di accesso Root né dell'autorizzazione Account tenant, non è possibile selezionare i tenant dall'elenco. In alternativa, immettere l'ID tenant oppure più ID come stringa delimitata da virgole.

4. Facoltativamente, specificare i bucket S3 a cui si applica questa regola.

Se è selezionata l'opzione **si applica a tutti i bucket** (impostazione predefinita), la regola si applica a tutti i bucket S3.

5. Per i tenant S3, selezionare facoltativamente **Sì** per applicare la regola solo alle versioni precedenti degli oggetti nei bucket S3 in cui è abilitato il controllo delle versioni.

Se selezioni **Sì**, "Tempo non corrente" verrà automaticamente selezionato per il tempo di riferimento in ["Passaggio 2 della procedura guidata Crea una regola ILM"](#).



Il tempo non corrente si applica solo agli oggetti S3 nei bucket abilitati al controllo delle versioni. Vedere ["Operazioni sui bucket, PutBucketVersioning"](#) E ["Gestisci gli oggetti con S3 Object Lock"](#).

È possibile utilizzare questa opzione per ridurre l'impatto sull'archiviazione degli oggetti sottoposti a controllo delle versioni, filtrando le versioni degli oggetti non correnti. Vedere ["Esempio 4: regole e policy ILM per oggetti con versione S3"](#).

6. Facoltativamente, seleziona **Aggiungi un filtro avanzato** per specificare filtri aggiuntivi.

Se non si configura il filtro avanzato, la regola si applica a tutti gli oggetti che corrispondono ai filtri di base. Per ulteriori informazioni sul filtraggio avanzato, vedere [Utilizzare filtri avanzati nelle regole ILM](#) E [Specificare più tipi e valori di metadati](#).

7. Selezionare **Continua**. ["Fase 2 \(Definire i posizionamenti\)"](#) viene visualizzata la procedura guidata Crea una regola ILM.

Utilizzare filtri avanzati nelle regole ILM

Il filtraggio avanzato consente di creare regole ILM che si applicano solo a oggetti specifici in base ai loro metadati. Quando si imposta un filtro avanzato per una regola, si seleziona il tipo di metadati che si desidera abbinare, si seleziona un operatore e si specifica un valore per i metadati. Quando gli oggetti vengono valutati, la regola ILM viene applicata solo agli oggetti che hanno metadati corrispondenti al filtro avanzato.

Nella tabella sono indicati i tipi di metadati che è possibile specificare nei filtri avanzati, gli operatori che è possibile utilizzare per ciascun tipo di metadati e i valori dei metadati previsti.

Tipo di metadati	Operatori supportati	Valore dei metadati
Tempo di ingestione	• È • non è • è prima • è acceso o prima • è dopo • è acceso o dopo	Ora e data in cui l'oggetto è stato ingerito. Nota: per evitare problemi di risorse durante l'attivazione di un nuovo criterio ILM, è possibile utilizzare il filtro avanzato Tempo di acquisizione in qualsiasi regola che potrebbe modificare la posizione di un gran numero di oggetti esistenti. Impostare il tempo di acquisizione su un valore maggiore o uguale al momento approssimativo in cui la nuova policy entrerà in vigore, per garantire che gli oggetti esistenti non vengano spostati inutilmente.
Chiave	• è uguale • non è uguale • contiene • non contiene • inizia con • non inizia con • finisce con • non finisce con	Tutta o parte di una chiave univoca dell'oggetto S3. Ad esempio, potresti voler abbinare oggetti che terminano con <code>.txt</code> o inizia con <code>test-object/</code>.
Ultimo orario di accesso	• È • non è • è prima • è acceso o prima • è dopo • è acceso o dopo	Ora e data dell'ultimo recupero (lettura o visualizzazione) dell'oggetto. Nota: se hai intenzione di "usa l'ultimo orario di accesso" come filtro avanzato, gli aggiornamenti dell'ora dell'ultimo accesso devono essere abilitati per il bucket S3.
Vincolo di posizione (solo S3)	• è uguale • non è uguale	La regione in cui è stato creato un bucket S3. Utilizzare ILM > Regioni per definire le regioni visualizzate. Nota: il valore <code>us-east-1</code> corrisponderà agli oggetti nei bucket creati nella regione <code>us-east-1</code> e agli oggetti nei bucket per i quali non è specificata alcuna regione. Vedere "Configurare le regioni (facoltativo e solo S3)".

Tipo di metadati	Operatori supportati	Valore dei metadati
Dimensione dell'oggetto	• è uguale • non è uguale • meno di • minore o uguale a • maggiore di • maggiore o uguale a	Le dimensioni dell'oggetto. La codifica di cancellazione è più adatta per oggetti di dimensioni superiori a 1 MB. Non utilizzare la codifica di cancellazione per oggetti di dimensioni inferiori a 200 KB per evitare il sovraccarico dovuto alla gestione di frammenti molto piccoli con codifica di cancellazione.
Metadati utente	• contiene • finisce con • è uguale • esiste • inizia con • non contiene • non finisce con • non è uguale • non esiste • non inizia con	Coppia chiave-valore, dove Nome metadati utente è la chiave e Valore metadati è il valore. Ad esempio, per filtrare gli oggetti che hanno metadati utente di <code>color=blue</code>, specificare <code>color</code> per Nome metadati utente, <code>equals</code> per l'operatore, e <code>blue</code> per Valore metadati. Nota: i nomi dei metadati utente non sono sensibili alle maiuscole e alle minuscole; lo sono invece i valori dei metadati utente.
Tag oggetto (solo S3)	• contiene • finisce con • è uguale • esiste • inizia con • non contiene • non finisce con • non è uguale • non esiste • non inizia con	Coppia chiave-valore, dove Nome tag oggetto è la chiave e Valore tag oggetto è il valore. Ad esempio, per filtrare gli oggetti che hanno un tag oggetto di <code>Image=True</code>, specificare <code>Image</code> per nome tag oggetto, <code>equals</code> per l'operatore, e <code>True</code> per valore tag oggetto. Nota: i nomi e i valori dei tag degli oggetti sono sensibili alle maiuscole e alle minuscole. È necessario immettere questi elementi esattamente come sono stati definiti per l'oggetto.

Specificare più tipi e valori di metadati

Quando si definisce un filtro avanzato, è possibile specificare più tipi di metadati e più valori di metadati. Ad esempio, se si desidera che una regola corrisponda a oggetti di dimensioni comprese tra 10 MB e 100 MB, è necessario selezionare il tipo di metadati **Dimensione oggetto** e specificare due valori di metadati.

- Il primo valore dei metadati specifica oggetti maggiori o uguali a 10 MB.
- Il secondo valore dei metadati specifica oggetti di dimensioni inferiori o uguali a 100 MB.

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ✕

Object size	greater than or equal to	10	MB	✕
and				
Object size	less than or equal to	100	MB	✕

Utilizzando più voci è possibile avere un controllo preciso sugli oggetti da abbinare. Nell'esempio seguente, la regola si applica agli oggetti che hanno Brand A o Brand B come valore dei metadati utente camera_type. Tuttavia, la regola si applica solo agli oggetti Brand B di dimensioni inferiori a 10 MB.

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ✕

User metadata	camera_type	equals	Brand A	✕

[Add another advanced filter](#)

or **Filter group 2** Objects with all of following metadata will be evaluated by this rule: ✕

User metadata	camera_type	equals	Brand B	✕
and				
Object size	less than or equal to	10	MB	✕

[Add another advanced filter](#)

Fase 2 di 3: definire i posizionamenti

Il passaggio **Definisci posizionamenti** della procedura guidata Crea regola ILM consente di definire le istruzioni di posizionamento che determinano per quanto tempo gli oggetti vengono archiviati, il tipo di copie (replicate o con codice di cancellazione), la posizione di archiviazione e il numero di copie.



Gli screenshot mostrati sono esempi. I risultati potrebbero variare a seconda della versione StorageGRID .

Informazioni su questo compito

Una regola ILM può includere una o più istruzioni di posizionamento. Ogni istruzione di posizionamento si applica a un singolo periodo di tempo. Quando si utilizzano più istruzioni, i periodi di tempo devono essere contigui e almeno un'istruzione deve iniziare il giorno 0. Le istruzioni possono continuare all'infinito oppure finché non avrai più bisogno di copie dell'oggetto.

Ogni istruzione di posizionamento può avere più righe se si desidera creare diversi tipi di copie o utilizzare posizioni diverse durante quel periodo di tempo.

In questo esempio, la regola ILM memorizza una copia replicata nel Sito 1 e una copia replicata nel Sito 2 per il primo anno. Dopo un anno, viene realizzata una copia con codice di cancellazione 2+1 e salvata in un solo sito.

Time period 1
From Day
0
store
for
365
days

Store objects by
replicating
1
copies at
Site 1

and store objects by
replicating
1
copies at
Site 2

Add other type or location

Time period 2
From Day
365
store
forever

Store objects by
erasure coding
using
2+1 EC scheme at Site 3

Add other type or location

Passi

1. Per **Tempo di riferimento**, seleziona il tipo di tempo da utilizzare per calcolare l'ora di inizio di un'istruzione di tirocinio.

Opzione	Descrizione
Tempo di ingestione	Il momento in cui l'oggetto è stato ingerito.
Ultimo orario di accesso	Ora dell'ultima volta in cui l'oggetto è stato recuperato (letto o visualizzato). Per utilizzare questa opzione, è necessario abilitare gli aggiornamenti all'ora dell'ultimo accesso per il bucket S3. Fare riferimento a "Utilizzare l'orario dell'ultimo accesso nelle regole ILM" .
Ora di creazione definita dall'utente	Un orario specificato nei metadati definiti dall'utente.
Tempo non corrente	"Tempo non corrente" viene selezionato automaticamente se hai selezionato Sì per la domanda "Applicare questa regola solo alle versioni precedenti degli oggetti (nei bucket S3 con controllo delle versioni abilitato)?" in "Passaggio 1 della procedura guidata Crea una regola ILM" .

Se vuoi creare una regola *conforme*, devi selezionare **Ora di inserimento**. Fare riferimento a ["Gestisci gli oggetti con S3 Object Lock"](#) .

2. Nella sezione **Periodo di tempo e posizionamenti**, inserisci un orario di inizio e una durata per il primo periodo di tempo.

Ad esempio, potresti voler specificare dove archiviare gli oggetti per il primo anno (*Dal giorno 0 archivia per 365 giorni*). Almeno un'istruzione deve iniziare al giorno 0.

3. Se si desidera creare copie replicate:

- a. Dall'elenco a discesa **Memorizza oggetti per**, seleziona **replica**.
- b. Seleziona il numero di copie che desideri effettuare.

Se si modifica il numero di copie in 1, viene visualizzato un avviso. Una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo espone i dati al rischio di perdita permanente. Fare riferimento a ["Perché non dovresti usare la replicazione a copia singola"](#).

Per evitare il rischio, eseguire una o più delle seguenti operazioni:

- Aumentare il numero di copie per il periodo di tempo.
- Aggiungere copie ad altri pool di archiviazione o a un pool di archiviazione cloud.
- Selezionare **codifica di cancellazione** invece di **replicazione**.

È possibile ignorare tranquillamente questo avviso se questa regola crea già più copie per tutti i periodi di tempo.

- c. Nel campo **copie in**, seleziona i pool di archiviazione che desideri aggiungere.

Se si specifica un solo pool di archiviazione, tenere presente che StorageGRID può archiviare solo una copia replicata di un oggetto su un dato nodo di archiviazione. Se la griglia include tre nodi di archiviazione e si seleziona 4 come numero di copie, verranno effettuate solo tre copie, una copia per ciascun nodo di archiviazione.

L'avviso **Posizionamento ILM non realizzabile** viene attivato per indicare che la regola ILM non può essere applicata completamente.

Se si specifica più di un pool di archiviazione, tenere a mente queste regole:

- Il numero di copie non può essere maggiore del numero di pool di archiviazione.
- Se il numero di copie è uguale al numero di pool di archiviazione, una copia dell'oggetto viene archiviata in ciascun pool di archiviazione.
- Se il numero di copie è inferiore al numero di pool di archiviazione, una copia viene archiviata nel sito di acquisizione, quindi il sistema distribuisce le copie rimanenti per mantenere bilanciato l'utilizzo del disco tra i pool, garantendo al contempo che nessun sito riceva più di una copia di un oggetto.
- Se i pool di archiviazione si sovrappongono (contengono gli stessi nodi di archiviazione), tutte le copie dell'oggetto potrebbero essere salvate in un solo sito. Per questo motivo, non specificare il pool di archiviazione All Storage Nodes (StorageGRID 11.6 e versioni precedenti) e un altro pool di archiviazione.

4. Se vuoi creare una copia con codice di cancellazione:

- a. Dall'elenco a discesa **Memorizza oggetti per**, seleziona **codifica di cancellazione**.



La codifica di cancellazione è più adatta per oggetti di dimensioni superiori a 1 MB. Non utilizzare la codifica di cancellazione per oggetti di dimensioni inferiori a 200 KB per evitare il sovraccarico dovuto alla gestione di frammenti molto piccoli con codifica di cancellazione.

- b. Se non hai aggiunto un filtro Dimensione oggetto per un valore superiore a 200 KB, seleziona **Precedente** per tornare al passaggio 1. Quindi, seleziona **Aggiungi un filtro avanzato** e imposta un

filtro **Dimensione oggetto** su un valore maggiore di 200 KB.

- c. Selezionare il pool di archiviazione che si desidera aggiungere e lo schema di codifica di cancellazione che si desidera utilizzare.

La posizione di archiviazione per una copia con codice di cancellazione include il nome dello schema di codifica di cancellazione, seguito dal nome del pool di archiviazione.

Gli schemi di codifica di cancellazione disponibili sono limitati dal numero di nodi di archiviazione nel pool di archiviazione selezionato. UN Recommended Il badge appare accanto agli schemi che forniscono entrambi i ["migliore protezione o il minimo sovraccarico di archiviazione"](#).

5. Facoltativamente:

- a. Seleziona **Aggiungi altro tipo o posizione** per creare copie aggiuntive in posizioni diverse.
- b. Seleziona **Aggiungi un altro periodo di tempo** per aggiungere periodi di tempo diversi.



L'eliminazione degli oggetti avviene in base alle seguenti impostazioni:

- Gli oggetti vengono eliminati automaticamente alla fine del periodo di tempo finale, a meno che un altro periodo di tempo non termini con **per sempre**.
- A seconda di ["impostazioni del periodo di conservazione del bucket e del tenant"](#), gli oggetti potrebbero non essere eliminati anche se termina il periodo di conservazione ILM.

6. Se si desidera archiviare oggetti in un Cloud Storage Pool:

- a. Nell'elenco a discesa **Archivia oggetti per**, seleziona **replica**.
- b. Selezionare il campo **copie in**, quindi selezionare un Cloud Storage Pool.

Quando si utilizzano i Cloud Storage Pool, tenere a mente queste regole:

- Non è possibile selezionare più di un Cloud Storage Pool in una singola istruzione di posizionamento. Allo stesso modo, non è possibile selezionare un Cloud Storage Pool e un pool di archiviazione nella stessa istruzione di posizionamento.
- È possibile archiviare solo una copia di un oggetto in un determinato Cloud Storage Pool. Se si imposta **Copie** su 2 o più, viene visualizzato un messaggio di errore.
- Non è possibile archiviare più di una copia dell'oggetto contemporaneamente in un Cloud Storage Pool. Viene visualizzato un messaggio di errore se più posizionamenti che utilizzano un Cloud Storage Pool hanno date sovrapposte o se più righe nello stesso posizionamento utilizzano un Cloud Storage Pool.
- È possibile archiviare un oggetto in un Cloud Storage Pool nello stesso momento in cui l'oggetto viene archiviato come copie replicate o con codice di cancellazione in StorageGRID. Tuttavia, è necessario includere più di una riga nelle istruzioni di posizionamento per il periodo di tempo, in modo da poter specificare il numero e il tipo di copie per ogni posizione.

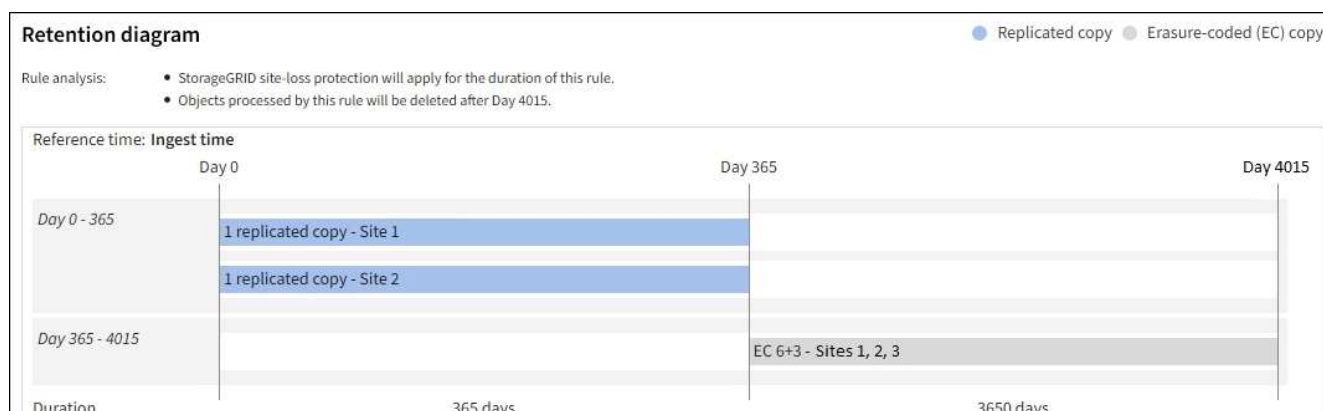
7. Nel diagramma di ritenzione, conferma le istruzioni di posizionamento.

In questo esempio, la regola ILM memorizza una copia replicata nel Sito 1 e una copia replicata nel Sito 2 per il primo anno. Dopo un anno e per altri 10 anni, una copia con codice di cancellazione 6+3 verrà salvata in tre siti. Dopo 11 anni totali, gli oggetti verranno eliminati da StorageGRID.

La sezione Analisi delle regole del diagramma di conservazione afferma:

- La protezione contro le perdite del sito StorageGRID sarà valida per tutta la durata di questa regola.
- Gli oggetti elaborati da questa regola verranno eliminati dopo il giorno 4015.

Fare riferimento a ["Abilita la protezione contro la perdita del sito."](#)



- Selezionare **Continua**. ["Passaggio 3 \(selezionare il comportamento di acquisizione\)"](#) viene visualizzata la procedura guidata Crea una regola ILM.

Utilizzare l'orario dell'ultimo accesso nelle regole ILM

È possibile utilizzare l'orario dell'ultimo accesso come orario di riferimento in una regola ILM. Ad esempio, potresti voler lasciare gli oggetti visualizzati negli ultimi tre mesi sui nodi di archiviazione locali, spostando invece gli oggetti non visualizzati di recente in una posizione esterna. È anche possibile utilizzare l'ora dell'ultimo accesso come filtro avanzato se si desidera che una regola ILM venga applicata solo agli oggetti a cui si è effettuato l'ultimo accesso in una data specifica.

Informazioni su questo compito

Prima di utilizzare l'orario dell'ultimo accesso in una regola ILM, esaminare le seguenti considerazioni:

- Quando si utilizza l'orario dell'ultimo accesso come orario di riferimento, tenere presente che la modifica dell'orario dell'ultimo accesso per un oggetto non attiva una valutazione ILM immediata. Al contrario, vengono valutati i posizionamenti dell'oggetto e l'oggetto viene spostato secondo necessità quando l'ILM in background valuta l'oggetto. Potrebbero volerci due settimane o più dopo l'accesso all'oggetto.

Tieni conto di questa latenza quando crei regole ILM basate sull'orario dell'ultimo accesso ed evita posizionamenti che utilizzano periodi di tempo brevi (meno di un mese).

- Quando si utilizza l'orario dell'ultimo accesso come filtro avanzato o come orario di riferimento, è necessario abilitare gli aggiornamenti dell'orario dell'ultimo accesso per i bucket S3. Puoi usare il ["Responsabile degli inquilini"](#) o il ["API di gestione degli inquilini"](#).



Per impostazione predefinita, gli aggiornamenti dell'orario dell'ultimo accesso sono disabilitati per i bucket S3.



Tieni presente che l'abilitazione degli aggiornamenti dell'ora dell'ultimo accesso può ridurre le prestazioni, soprattutto nei sistemi con oggetti di piccole dimensioni. L'impatto sulle prestazioni si verifica perché StorageGRID deve aggiornare gli oggetti con nuovi timestamp ogni volta che vengono recuperati.

La tabella seguente riassume se l'orario dell'ultimo accesso viene aggiornato per tutti gli oggetti nel bucket per diversi tipi di richieste.

Tipo di richiesta	Se l'orario dell'ultimo accesso viene aggiornato quando gli aggiornamenti dell'orario dell'ultimo accesso sono disabilitati	Se l'orario dell'ultimo accesso viene aggiornato quando sono abilitati gli aggiornamenti dell'orario dell'ultimo accesso
Richiesta di recupero di un oggetto, del suo elenco di controllo di accesso o dei suoi metadati	NO	Sì
Richiesta di aggiornamento dei metadati di un oggetto	Sì	Sì
Richiesta di copiare un oggetto da un bucket all'altro	• No, per la copia sorgente • Sì, per la copia di destinazione	• Sì, per la copia sorgente • Sì, per la copia di destinazione
Richiesta di completamento di un caricamento multiparte	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato

Passaggio 3 di 3: seleziona il comportamento di acquisizione

Il passaggio **Seleziona comportamento di acquisizione** della procedura guidata Crea regola ILM consente di scegliere in che modo gli oggetti filtrati da questa regola vengono protetti durante l'acquisizione.

Informazioni su questo compito

StorageGRID può creare copie provvisorie e mettere in coda gli oggetti per una successiva valutazione ILM, oppure può creare copie per soddisfare immediatamente le istruzioni di posizionamento della regola.

Passi

1. Seleziona il ["comportamento di ingestione"](#) da usare.

Per ulteriori informazioni, consultare ["Vantaggi, svantaggi e limitazioni delle opzioni di ingestione"](#).



Non è possibile utilizzare l'opzione Bilanciato o Rigoroso se la regola utilizza uno di questi posizionamenti:

- Un pool di archiviazione cloud al giorno 0
- Un pool di archiviazione cloud quando la regola utilizza un orario di creazione definito dall'utente come orario di riferimento

Vedere ["Esempio 5: regole e policy ILM per un comportamento di acquisizione rigoroso"](#).

2. Seleziona **Crea**.

Viene creata la regola ILM. La regola non diventa attiva finché non viene aggiunta a un ["Politica ILM"](#) e tale politica viene attivata.

Per visualizzare i dettagli della regola, seleziona il nome della regola nella pagina delle regole ILM.

Crea una regola ILM predefinita

Prima di creare un criterio ILM, è necessario creare una regola predefinita per posizionare nel criterio tutti gli oggetti non corrispondenti a un'altra regola. La regola predefinita non può utilizzare alcun filtro. Deve essere applicato a tutti i tenant, a tutti i bucket e a tutte le versioni degli oggetti.

Prima di iniziare

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

Informazioni su questo compito

La regola predefinita è l'ultima regola da valutare in un criterio ILM, quindi non può utilizzare alcun filtro. Le istruzioni di posizionamento per la regola predefinita vengono applicate a tutti gli oggetti che non corrispondono a un'altra regola nel criterio.

In questo esempio di policy, la prima regola si applica solo agli oggetti appartenenti a test-tenant-1. La regola predefinita, che è l'ultima, si applica agli oggetti appartenenti a tutti gli altri account tenant.

Proposed policy name

Example ILM policy

Reason for change

Example

Manage rules

1. Select the rules you want to add to the policy.

2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

Select rules

Rule order	Rule name	Filters
1	EC for test-tenant-1	Tenant is test-tenant-1
Default	Default rule	—

Quando crei la regola predefinita, tieni a mente questi requisiti:

- La regola predefinita verrà automaticamente posizionata come ultima regola quando la aggiungi a un criterio.
- La regola predefinita non può utilizzare filtri di base o avanzati.
- La regola predefinita deve essere applicata a tutte le versioni dell'oggetto.

- La regola predefinita dovrebbe creare copie replicate.



Non utilizzare una regola che crea copie con codice di cancellazione come regola predefinita per una policy. Le regole di codifica di cancellazione dovrebbero utilizzare un filtro avanzato per impedire che gli oggetti più piccoli vengano codificati in modo errato.

- In generale, la regola predefinita dovrebbe conservare gli oggetti per sempre.
- Se si utilizza (o si prevede di abilitare) l'impostazione globale S3 Object Lock, la regola predefinita deve essere conforme.

Passi

1. Selezionare **ILM > Regole**.
2. Seleziona **Crea**.

Viene visualizzato il passaggio 1 (Immissione dei dettagli) della procedura guidata Crea regola ILM.

3. Immettere un nome univoco per la regola nel campo **Nome regola**.
4. Facoltativamente, inserisci una breve descrizione della regola nel campo **Descrizione**.
5. Lasciare vuoto il campo **Account inquilino**.

La regola predefinita deve essere applicata a tutti gli account tenant.

6. Lasciare la selezione a discesa Nome bucket come **applicabile a tutti i bucket**.

La regola predefinita deve essere applicata a tutti i bucket S3.

7. Mantenere la risposta predefinita, **No**, per la domanda "Applicare questa regola solo alle versioni precedenti degli oggetti (nei bucket S3 con controllo delle versioni abilitato)?"
8. Non aggiungere filtri avanzati.

La regola predefinita non può specificare alcun filtro.

9. Selezionare **Avanti**.

Viene visualizzato il passaggio 2 (Definizione dei posizionamenti).

10. Per Tempo di riferimento, selezionare un'opzione qualsiasi.

Se hai mantenuto la risposta predefinita, **No**, alla domanda "Applicare questa regola solo alle versioni precedenti dell'oggetto?" Il tempo non corrente non verrà incluso nell'elenco a discesa. La regola predefinita deve essere applicata a tutte le versioni dell'oggetto.

11. Specificare le istruzioni di posizionamento per la regola predefinita.
 - La regola predefinita dovrebbe conservare gli oggetti per sempre. Quando si attiva un nuovo criterio, viene visualizzato un avviso se la regola predefinita non conserva gli oggetti per sempre. Devi confermare che questo è il comportamento che ti aspetti.
 - La regola predefinita dovrebbe creare copie replicate.



Non utilizzare una regola che crea copie con codice di cancellazione come regola predefinita per una policy. Le regole di codifica di cancellazione dovrebbero includere il filtro avanzato **Dimensione oggetto (MB) maggiore di 200 KB** per impedire che oggetti più piccoli vengano codificati in modo da essere cancellati.

- Se si utilizza (o si prevede di abilitare) l'impostazione globale S3 Object Lock, la regola predefinita deve essere conforme:
 - Deve creare almeno due copie replicate dell'oggetto o una copia con codice di cancellazione.
 - Queste copie devono essere presenti sui nodi di archiviazione per l'intera durata di ciascuna riga nelle istruzioni di posizionamento.
 - Le copie degli oggetti non possono essere salvate in un Cloud Storage Pool.
 - Almeno una riga delle istruzioni di posizionamento deve iniziare dal giorno 0, utilizzando l'ora di acquisizione come ora di riferimento.
 - Almeno una riga delle istruzioni di posizionamento deve essere "per sempre".

12. Consultare il diagramma di ritenzione per confermare le istruzioni di posizionamento.

13. Selezionare **Continua**.

Viene visualizzato il passaggio 3 (Seleziona comportamento di acquisizione).

14. Seleziona l'opzione di acquisizione da utilizzare e seleziona **Crea**.

Gestire le policy ILM

Utilizzare le policy ILM

Una policy di gestione del ciclo di vita delle informazioni (ILM) è un insieme ordinato di regole ILM che determinano il modo in cui il sistema StorageGRID gestisce i dati degli oggetti nel tempo.



Una policy ILM configurata in modo errato può comportare una perdita di dati irrecuperabile. Prima di attivare una policy ILM, esaminare attentamente la policy ILM e le relative regole ILM, quindi simulare la policy ILM. Verificare sempre che la politica ILM funzioni come previsto.

Criterio ILM predefinito

Quando si installa StorageGRID e si aggiungono siti, viene creato automaticamente un criterio ILM predefinito, come segue:

- Se la griglia contiene un sito, il criterio predefinito contiene una regola predefinita che replica due copie di ciascun oggetto in quel sito.
- Se la griglia contiene più di un sito, la regola predefinita replica una copia di ciascun oggetto in ogni sito.

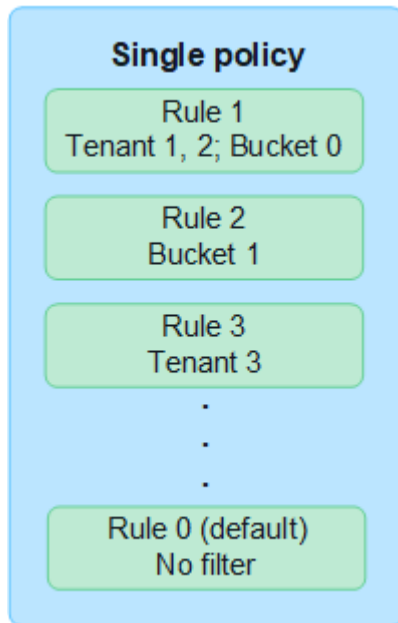
Se la policy predefinita non soddisfa i requisiti di archiviazione, è possibile creare regole e policy personalizzate. Vedere ["Crea una regola ILM"](#) E ["Creare una policy ILM"](#) .

Una o più polizze ILM attive?

È possibile avere una o più polizze ILM attive contemporaneamente.

Una politica

Se la griglia utilizzerà uno schema di protezione dei dati semplice con poche regole specifiche per tenant e bucket, utilizzare un singolo criterio ILM attivo. Le regole ILM possono contenere filtri per gestire diversi bucket o tenant.



Quando si dispone di una sola policy e i requisiti di un tenant cambiano, è necessario creare una nuova policy ILM o clonare la policy esistente per applicare le modifiche, simulare e quindi attivare la nuova policy ILM. Le modifiche alla policy ILM potrebbero comportare spostamenti di oggetti che potrebbero richiedere molti giorni e causare latenza del sistema.

Politiche multiple

Per offrire agli inquilini diverse opzioni di qualità del servizio, è possibile avere più di una polizza attiva contemporaneamente. Ogni policy può gestire tenant, bucket S3 e oggetti specifici. Quando si applica o si modifica una policy per un set specifico di tenant o oggetti, le policy applicate ad altri tenant e oggetti non vengono modificate.

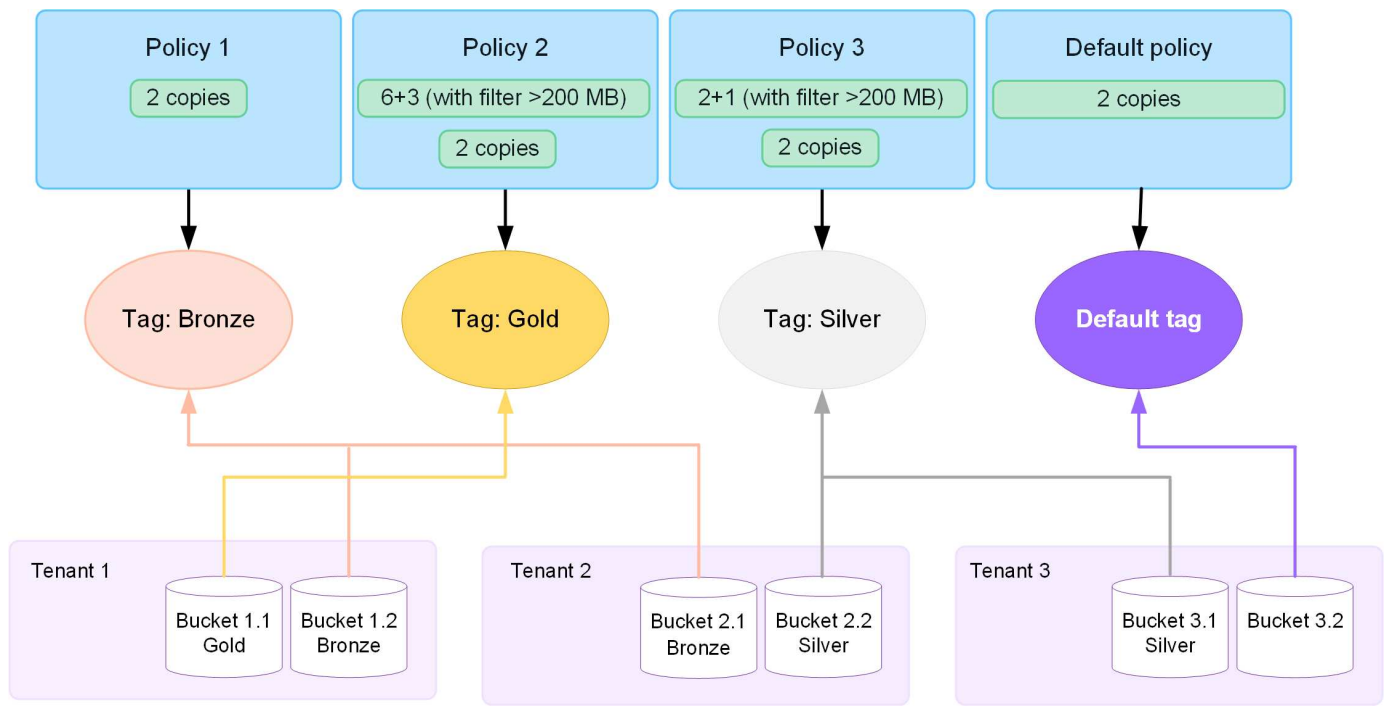
Tag di policy ILM

Se si desidera consentire ai tenant di passare facilmente da una policy di protezione dei dati all'altra per ogni bucket, utilizzare più policy ILM con *tag policy ILM*. Si assegna ogni policy ILM a un tag, quindi i tenant taggano un bucket per applicare la policy a quel bucket. È possibile impostare i tag dei criteri ILM solo sui bucket S3.

Ad esempio, potresti avere tre tag denominati Oro, Argento e Bronzo. È possibile assegnare un criterio ILM a ciascun tag, in base alla durata e alla posizione in cui tale criterio archivia gli oggetti. Gli inquilini possono scegliere quale policy utilizzare etichettando i propri bucket. Un bucket contrassegnato come Gold è gestito dalla policy Gold e riceve il livello Gold di protezione dei dati e prestazioni.

Tag di policy ILM predefinito

Un tag di policy ILM predefinito viene creato automaticamente quando si installa StorageGRID. Ogni griglia deve avere una policy attiva assegnata al tag Default. Il criterio predefinito si applica a tutti i bucket S3 non taggati.



In che modo una policy ILM valuta gli oggetti?

Una policy ILM attiva controlla il posizionamento, la durata e la protezione dei dati degli oggetti.

Quando i client salvano oggetti in StorageGRID, gli oggetti vengono valutati in base al set ordinato di regole ILM nella policy, come segue:

1. Se i filtri per la prima regola nel criterio corrispondono a un oggetto, l'oggetto viene acquisito in base al comportamento di acquisizione di quella regola e archiviato in base alle istruzioni di posizionamento di quella regola.
2. Se i filtri per la prima regola non corrispondono all'oggetto, l'oggetto viene valutato rispetto a ogni regola successiva nel criterio finché non viene trovata una corrispondenza.
3. Se nessuna regola corrisponde a un oggetto, vengono applicate le istruzioni di posizionamento e comportamento di acquisizione per la regola predefinita nel criterio. La regola predefinita è l'ultima regola di una policy. La regola predefinita deve essere applicata a tutti i tenant, a tutti i bucket S3 e a tutte le versioni degli oggetti e non può utilizzare filtri avanzati.

Esempio di politica ILM

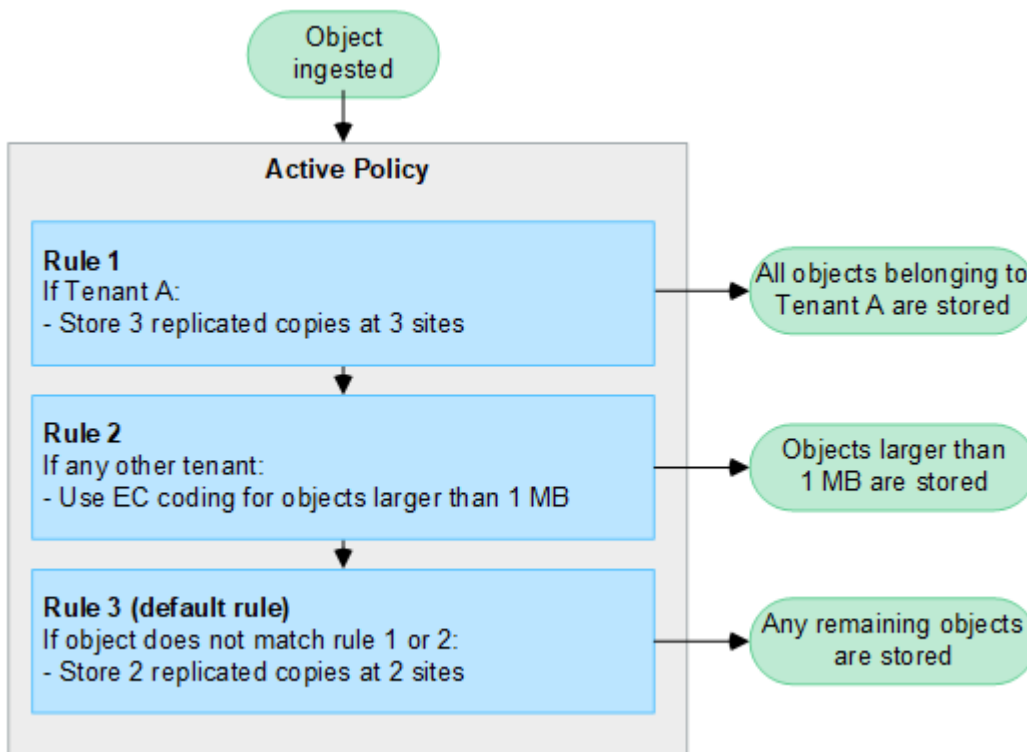
Ad esempio, una policy ILM potrebbe contenere tre regole ILM che specificano quanto segue:

- **Regola 1: Copie replicate per l'inquilino A**
 - Abbina tutti gli oggetti appartenenti all'inquilino A.
 - Conservare questi oggetti in tre copie replicate in tre siti.
 - Gli oggetti appartenenti ad altri tenant non sono soggetti alla Regola 1, pertanto vengono valutati in base alla Regola 2.
- **Regola 2: Codifica di cancellazione per oggetti di dimensioni superiori a 1 MB**
 - Corrisponde a tutti gli oggetti degli altri tenant, ma solo se sono maggiori di 1 MB. Questi oggetti di grandi dimensioni vengono memorizzati utilizzando la codifica di cancellazione 6+3 in tre siti.
 - Non corrisponde a oggetti di dimensioni pari o inferiori a 1 MB, pertanto questi oggetti vengono valutati

in base alla Regola 3.

- **Regola 3: 2 copie 2 data center** (predefinita)

- È l'ultima regola predefinita della policy. Non utilizza filtri.
- Eseguire due copie replicate di tutti gli oggetti non corrispondenti alla Regola 1 o alla Regola 2 (oggetti non appartenenti al Tenant A di dimensioni pari o inferiori a 1 MB).



Cosa sono le politiche attive e inattive?

Ogni sistema StorageGRID deve avere almeno una policy ILM attiva. Se si desidera avere più di un criterio ILM attivo, è possibile creare tag di criteri ILM e assegnare un criterio a ciascun tag. I tenant applicano quindi i tag ai bucket S3. Il criterio predefinito viene applicato a tutti gli oggetti nei bucket a cui non è assegnato un tag di criterio.

Quando si crea per la prima volta un criterio ILM, si selezionano una o più regole ILM e le si dispone in un ordine specifico. Dopo aver simulato la policy per confermarne il comportamento, attivarla.

Quando si attiva un criterio ILM, StorageGRID utilizza tale criterio per gestire tutti gli oggetti, compresi quelli esistenti e quelli appena acquisiti. Gli oggetti esistenti potrebbero essere spostati in nuove posizioni quando verranno implementate le regole ILM nella nuova policy.

Se si attivano più policy ILM contemporaneamente e i tenant applicano tag policy ai bucket S3, gli oggetti in ciascun bucket vengono gestiti in base alla policy assegnata al tag.

Un sistema StorageGRID tiene traccia della cronologia delle policy attivate o disattivate.

Considerazioni per la creazione di una politica ILM

- Nei sistemi di test utilizzare solo la policy fornita dal sistema, ovvero la policy delle copie Baseline 2. Per StorageGRID 11.6 e versioni precedenti, la regola Crea 2 copie in questo criterio utilizza il pool di archiviazione Tutti i nodi di archiviazione, che contiene tutti i siti. Se il sistema StorageGRID ha più di un sito, è possibile che due copie di un oggetto siano posizionate sullo stesso sito.



Il pool di archiviazione All Storage Nodes viene creato automaticamente durante l'installazione di StorageGRID 11.6 e versioni precedenti. Se si esegue l'aggiornamento a una versione successiva di StorageGRID, il pool All Storage Nodes continuerà a esistere. Se si installa StorageGRID 11.7 o versione successiva come nuova installazione, il pool. Tutti i nodi di archiviazione non viene creato.

- Quando si progetta una nuova policy, bisogna considerare tutti i diversi tipi di oggetti che potrebbero essere inseriti nella griglia. Assicurarsi che la policy includa regole per abbinare e posizionare questi oggetti come richiesto.
- Mantenere la politica ILM il più semplice possibile. In questo modo si evitano situazioni potenzialmente pericolose in cui i dati degli oggetti non sono protetti come previsto quando nel tempo vengono apportate modifiche al sistema StorageGRID .
- Assicuratevi che le regole della policy siano nell'ordine corretto. Quando la policy viene attivata, gli oggetti nuovi ed esistenti vengono valutati dalle regole nell'ordine elencato, iniziando dall'alto. Ad esempio, se la prima regola di un criterio corrisponde a un oggetto, tale oggetto non verrà valutato da nessun'altra regola.
- L'ultima regola in ogni policy ILM è la regola ILM predefinita, che non può utilizzare alcun filtro. Se un oggetto non è stato abbinato a un'altra regola, la regola predefinita controlla dove viene posizionato l'oggetto e per quanto tempo viene conservato.
- Prima di attivare una nuova policy, esaminare tutte le modifiche apportate dalla policy al posizionamento degli oggetti esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi temporanei di risorse quando i nuovi posizionamenti vengono valutati e implementati.

Creare policy ILM

Crea una o più policy ILM per soddisfare i tuoi requisiti di qualità del servizio.

Avere un criterio ILM attivo consente di applicare le stesse regole ILM a tutti i tenant e bucket.

Disporre di più policy ILM attive consente di applicare le regole ILM appropriate a tenant e bucket specifici per soddisfare più requisiti di qualità del servizio.

Creare una policy ILM

Informazioni su questo compito

Prima di creare la tua politica, verifica che ["politica ILM predefinita"](#) non soddisfa i tuoi requisiti di archiviazione.



Nei sistemi di test, utilizzare solo le policy fornite dal sistema, ovvero 2 copie della policy (per griglie a un sito) o 1 copia per sito (per griglie a più siti). Per StorageGRID 11.6 e versioni precedenti, la regola predefinita in questo criterio utilizza il pool di archiviazione All Storage Nodes, che contiene tutti i siti. Se il sistema StorageGRID ha più di un sito, è possibile che due copie di un oggetto siano posizionate sullo stesso sito.



Se il ["l'impostazione globale S3 Object Lock è stata abilitata"](#) , è necessario assicurarsi che la policy ILM sia conforme ai requisiti dei bucket in cui è abilitato S3 Object Lock. In questa sezione, seguire le istruzioni che indicano di aver abilitato S3 Object Lock.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["autorizzazioni di accesso richieste"](#) .

- Hai ["regole ILM create"](#) in base all'abilitazione o meno del blocco oggetti S3.

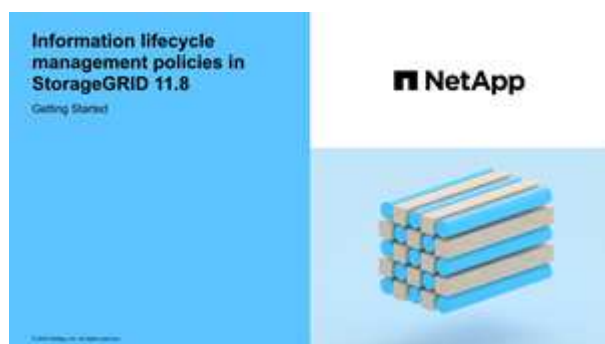
Blocco oggetto S3 non abilitato

- Hai ["ha creato le regole ILM"](#) che vuoi aggiungere alla polizza. Se necessario, è possibile salvare una policy, creare regole aggiuntive e quindi modificare la policy per aggiungere le nuove regole.
- Hai ["ha creato una regola ILM predefinita"](#) che non contiene alcun filtro.

Blocco oggetto S3 abilitato

- IL ["l'impostazione globale di blocco degli oggetti S3 è già abilitata"](#) per il sistema StorageGRID .
- Hai ["ha creato le regole ILM conformi e non conformi"](#) che vuoi aggiungere alla polizza. Se necessario, è possibile salvare una policy, creare regole aggiuntive e quindi modificare la policy per aggiungere le nuove regole.
- Hai ["ha creato una regola ILM predefinita"](#) per la politica conforme.

- Facoltativamente, hai guardato il video: ["Video: Panoramica delle politiche ILM"](#)



Vedere anche ["Utilizzare le policy ILM"](#) .

Passi

1. Selezionare **ILM > Criteri**.

Se l'impostazione globale Blocco oggetti S3 è abilitata, la pagina Criteri ILM indica quali regole ILM sono conformi.

2. Determina come desideri creare la policy ILM.

Crea una nuova politica

- a. Selezionare **Crea policy**.

Clona la politica esistente

- a. Seleziona la casella di controllo relativa al criterio da cui vuoi iniziare, quindi seleziona **Clona**.

Modifica la policy esistente

- a. Se una policy è inattiva, puoi modificarla. Seleziona la casella di controllo per il criterio inattivo da cui vuoi iniziare, quindi seleziona **Modifica**.

3. Nel campo **Nome policy**, immettere un nome univoco per la policy.

4. Facoltativamente, nel campo **Motivo della modifica**, inserisci il motivo per cui stai creando una nuova policy.
5. Per aggiungere regole al criterio, selezionare **Seleziona regole**. Selezionare il nome di una regola per visualizzarne le impostazioni.

Se stai clonando una policy:

- Vengono selezionate le regole utilizzate dalla policy che stai clonando.
- Se il criterio che stai clonando utilizzava regole senza filtri che non erano la regola predefinita, ti verrà chiesto di rimuovere tutte le regole tranne una.
- Se la regola predefinita utilizza un filtro, ti verrà chiesto di selezionare una nuova regola predefinita.
- Se la regola predefinita non era l'ultima regola, è possibile spostarla alla fine del nuovo criterio.

Blocco oggetto S3 non abilitato

- a. Selezionare una regola predefinita per il criterio. Per creare una nuova regola predefinita, seleziona **Pagina regole ILM**.

La regola predefinita si applica a tutti gli oggetti che non corrispondono a un'altra regola nel criterio. La regola predefinita non può utilizzare alcun filtro e viene sempre valutata per ultima.



Non utilizzare la regola Crea 2 copie come regola predefinita per una policy. La regola Crea 2 copie utilizza un singolo pool di archiviazione, Tutti i nodi di archiviazione, che contiene tutti i siti. Se il sistema StorageGRID ha più di un sito, è possibile che due copie di un oggetto siano posizionate sullo stesso sito.

Blocco oggetto S3 abilitato

- a. Selezionare una regola predefinita per il criterio. Per creare una nuova regola predefinita, seleziona **Pagina regole ILM**.

L'elenco delle regole contiene solo le regole conformi e non utilizzano alcun filtro.



Non utilizzare la regola Crea 2 copie come regola predefinita per una policy. La regola Crea 2 copie utilizza un singolo pool di archiviazione, Tutti i nodi di archiviazione, che contiene tutti i siti. Se si utilizza questa regola, è possibile che più copie di un oggetto vengano posizionate nello stesso sito.

- b. Se è necessaria una regola "predefinita" diversa per gli oggetti nei bucket S3 non conformi, selezionare **Includi una regola senza filtri per i bucket S3 non conformi** e selezionare una regola non conforme che non utilizzi un filtro.

Ad esempio, potresti voler utilizzare un Cloud Storage Pool per archiviare oggetti in bucket in cui non è abilitato il blocco degli oggetti S3.



È possibile selezionare solo una regola non conforme che non utilizzi un filtro.

Vedere anche ["Esempio 7: Politica ILM conforme per S3 Object Lock"](#).

6. Dopo aver selezionato la regola predefinita, seleziona **Continua**.

7. Per il passaggio Altre regole, seleziona tutte le altre regole che desideri aggiungere al criterio. Queste regole utilizzano almeno un filtro (account tenant, nome bucket, filtro avanzato o ora di riferimento non corrente). Quindi seleziona **Seleziona**.

Nella finestra Crea un criterio sono ora elencate le regole selezionate. La regola predefinita è alla fine, mentre le altre regole sono sopra.

Se è abilitato il blocco degli oggetti S3 e si è selezionata anche una regola "predefinita" non conforme, tale regola viene aggiunta come penultima regola nel criterio.



Se una regola non conserva gli oggetti per sempre, viene visualizzato un avviso. Quando si attiva questo criterio, è necessario confermare che si desidera che StorageGRID elimini gli oggetti quando scadono le istruzioni di posizionamento per la regola predefinita (a meno che un ciclo di vita del bucket non conservi gli oggetti per un periodo di tempo più lungo).

8. Trascinare le righe delle regole non predefinite per determinare l'ordine in cui tali regole verranno valutate.

Non è possibile spostare la regola predefinita. Se è abilitato il Blocco oggetto S3, non è possibile spostare la regola "predefinita" non conforme, se ne è stata selezionata una.



È necessario confermare che le regole ILM siano nell'ordine corretto. Quando la policy viene attivata, gli oggetti nuovi ed esistenti vengono valutati dalle regole nell'ordine elencato, iniziando dall'alto.

9. Se necessario, selezionare **Seleziona regole** per aggiungere o rimuovere regole.
10. Al termine, seleziona **Salva**.
11. Ripetere questi passaggi per creare ulteriori policy ILM.
12. [Simulare una politica ILM](#) . Dovresti sempre simulare una policy prima di attivarla per assicurarti che funzioni come previsto.

Simulare una politica

Simulare una policy sugli oggetti di prova prima di attivarla e applicarla ai dati di produzione.

Prima di iniziare

- Conosci il bucket S3/chiave oggetto per ogni oggetto che vuoi testare.

Passi

1. Utilizzando un client S3 o "[Console S3](#)" , ingerire gli oggetti necessari per testare ciascuna regola.
2. Nella pagina Criteri ILM, seleziona la casella di controllo per il criterio, quindi seleziona **Simula**.
3. Nel campo **Oggetto**, immettere S3 bucket/object-key per un oggetto di prova. Ad esempio, bucket-01/filename.png .
4. Se è abilitato il controllo delle versioni S3, è possibile immettere facoltativamente un ID versione per l'oggetto nel campo **ID versione**.
5. Selezionare **Simula**.
6. Nella sezione Risultati della simulazione, verificare che a ciascun oggetto sia stata applicata la regola corretta.
7. Per determinare quale pool di archiviazione o profilo di codifica di cancellazione è attivo, selezionare il nome della regola corrispondente per accedere alla pagina dei dettagli della regola.



Esaminare eventuali modifiche al posizionamento degli oggetti replicati e codificati con cancellazione esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi temporanei di risorse quando i nuovi posizionamenti vengono valutati e implementati.

Risultati

Eventuali modifiche alle regole della policy verranno riflesse nei risultati della simulazione e mostreranno la nuova corrispondenza e quella precedente. La finestra Criterio di simulazione conserva gli oggetti testati finché non selezioni **Cancella tutto** o l'icona di rimozione  per ogni oggetto nell'elenco dei risultati della simulazione.

Informazioni correlate

["Esempio di simulazioni di policy ILM"](#)

Attiva una politica

Quando si attiva una nuova policy ILM, gli oggetti esistenti e quelli appena acquisiti vengono gestiti da tale policy. Quando si attivano più policy, i tag delle policy ILM assegnati ai bucket determinano gli oggetti da gestire.

Prima di attivare una nuova polizza:

1. Simula la policy per verificare che si comporti come previsto.
2. Esaminare eventuali modifiche al posizionamento degli oggetti replicati e codificati con cancellazione esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi temporanei di risorse quando i nuovi posizionamenti vengono valutati e implementati.



Gli errori in una policy ILM possono causare una perdita di dati irrecuperabile.

Informazioni su questo compito

Quando si attiva una policy ILM, il sistema distribuisce la nuova policy a tutti i nodi. Tuttavia, la nuova policy attiva potrebbe non avere effetto finché tutti i nodi della griglia non saranno disponibili a riceverla. In alcuni casi, il sistema attende di implementare una nuova policy attiva per garantire che gli oggetti della griglia non vengano rimossi accidentalmente. Nello specifico:

- Se si apportano modifiche ai criteri che **aumentano la ridondanza o la durabilità dei dati**, tali modifiche vengono implementate immediatamente. Ad esempio, se si attiva una nuova policy che include una regola a tre copie anziché a due copie, tale policy verrà implementata immediatamente perché aumenta la ridondanza dei dati.
- Se si apportano modifiche ai criteri che **potrebbero ridurre la ridondanza o la durabilità dei dati**, tali modifiche non verranno implementate finché tutti i nodi della griglia non saranno disponibili. Ad esempio, se si attiva una nuova policy che utilizza una regola a due copie anziché una regola a tre copie, la nuova policy verrà visualizzata nella scheda Policy attiva, ma non avrà effetto finché tutti i nodi non saranno online e disponibili.

Passi

Seguire i passaggi per attivare una o più policy:

Attiva una politica

Se si desidera avere una sola polizza attiva, seguire questi passaggi. Se hai già una o più policy attive e stai attivando policy aggiuntive, segui i passaggi per l'attivazione di più policy.

1. Quando sei pronto ad attivare una policy, seleziona **ILM > Policy**.

In alternativa, è possibile attivare una singola policy dalla pagina **ILM > Tag policy**.

2. Nella scheda Criteri, seleziona la casella di controllo per il criterio che desideri attivare, quindi seleziona **Attiva**.
3. Seguire il passaggio appropriato:
 - Se un messaggio di avviso richiede di confermare l'attivazione del criterio, selezionare **OK**.
 - Se viene visualizzato un messaggio di avviso contenente dettagli sulla policy:
 - i. Esaminare i dettagli per assicurarsi che la policy gestisca i dati come previsto.
 - ii. Se la regola predefinita memorizza gli oggetti per un numero limitato di giorni, rivedere il diagramma di conservazione e digitare tale numero di giorni nella casella di testo.
 - iii. Se la regola predefinita memorizza gli oggetti per sempre, ma una o più altre regole hanno una conservazione limitata, digitare **sì** nella casella di testo.
 - iv. Seleziona **Attiva policy**.

Attiva più policy

Per attivare più policy, è necessario creare dei tag e assegnare una policy a ciascun tag.



Quando vengono utilizzati più tag, se i tenant riassegnano frequentemente i tag dei criteri ai bucket, le prestazioni della griglia potrebbero risentirne. Se hai tenant non attendibili, valuta la possibilità di utilizzare solo il tag Default.

1. Selezionare **ILM > Tag policy**.
2. Seleziona **Crea**.
3. Nella finestra di dialogo Crea tag criterio, digitare un nome per il tag e, facoltativamente, una descrizione per il tag.



I nomi e le descrizioni dei tag sono visibili agli inquilini. Scegli valori che aiuteranno i tenant a prendere una decisione informata quando selezionano i tag dei criteri da assegnare ai loro bucket. Ad esempio, se la policy assegnata eliminerà gli oggetti dopo un certo periodo di tempo, è possibile comunicarlo nella descrizione. Non includere informazioni sensibili in questi campi.

4. Seleziona **Crea tag**.
5. Nella tabella dei tag dei criteri ILM, utilizzare il menu a discesa per selezionare un criterio da assegnare al tag.
6. Se nella colonna Limitazioni della policy vengono visualizzati degli avvisi, selezionare **Visualizza dettagli policy** per rivedere la policy.
7. Assicurarsi che ogni policy gestisca i dati come previsto.
8. Selezionare **Attiva policy assegnate**. Oppure seleziona **Cancella modifiche** per rimuovere l'assegnazione del criterio.

9. Nella finestra di dialogo Attiva criteri con nuovi tag, rivedere le descrizioni di come ciascun tag, criterio e regola gestirà gli oggetti. Apportare le modifiche necessarie per garantire che i criteri gestiscano gli oggetti come previsto.
10. Quando sei sicuro di voler attivare i criteri, digita **si** nella casella di testo, quindi seleziona **Attiva criteri**.

Informazioni correlate

["Esempio 6: Modifica di una policy ILM"](#)

Esempio di simulazioni di policy ILM

Gli esempi di simulazioni di policy ILM forniscono linee guida per strutturare e modificare le simulazioni per il tuo ambiente.

Esempio 1: verificare le regole durante la simulazione di una policy ILM

Questo esempio descrive come verificare le regole durante la simulazione di una policy.

In questo esempio, la **politica ILM di esempio** viene simulata sugli oggetti acquisiti in due bucket. La politica comprende tre regole, come segue:

- La prima regola, **Due copie, due anni per il bucket-a**, si applica solo agli oggetti nel bucket-a.
- La seconda regola, **Oggetti EC > 1 MB**, si applica a tutti i bucket ma filtra gli oggetti di dimensioni superiori a 1 MB.
- La terza regola, **Due copie, due data center**, è la regola predefinita. Non include alcun filtro e non utilizza il tempo di riferimento non corrente.

Dopo aver simulato la policy, verificare che a ciascun oggetto corrisponda la regola corretta.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all ?				
Object	Version ID	Rule matched	Previous match	Actions
bucket-a/bucket-a object.pdf	—	Two copies, two years for bucket-a	—	
bucket-b/test object greater than 1 MB.pdf	—	EC objects > 1 MB	—	
bucket-b/test object less than 1 MB.pdf	—	Two copies, two data centers	—	

In questo esempio:

- bucket-a/bucket-a object.pdf`ha abbinato correttamente la prima regola, che filtra gli oggetti in `bucket-a`.
- bucket-b/test object greater than 1 MB.pdf`è dentro `bucket-b`, quindi non corrispondeva alla prima regola. Invece, è stato correttamente abbinato dalla seconda regola, che filtra gli oggetti di dimensioni superiori a 1 MB.

- `bucket-b/test object less than 1 MB.pdf` non corrisponde ai filtri nelle prime due regole, quindi verrà inserito dalla regola predefinita, che non include filtri.

Esempio 2: riordinare le regole durante la simulazione di una policy ILM

Questo esempio mostra come è possibile riordinare le regole per modificare i risultati durante la simulazione di una policy.

In questo esempio viene simulata la policy **Demo**. Questa politica, che ha lo scopo di trovare oggetti che hanno metadati utente `series=x-men`, include tre regole, come segue:

- La prima regola, **PNG**, filtra i nomi delle chiavi che terminano in `.png`.
- La seconda regola, **X-men**, si applica solo agli oggetti per l'inquilino A e ai filtri per `series=x-men` metadati dell'utente.
- L'ultima regola, **Due copie due data center**, è la regola predefinita, che corrisponde a tutti gli oggetti che non corrispondono alle prime due regole.

Passi

1. Dopo aver aggiunto le regole e salvato il criterio, seleziona **Simula**.
2. Nel campo **Oggetto**, immettere il bucket S3/chiave oggetto per un oggetto di prova e selezionare **Simula**.

Vengono visualizzati i risultati della simulazione, che mostrano che `Havok.png` l'oggetto è stato abbinato dalla regola **PNG**.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all ?				
Object	Version ID	Rule matched	Previous match	Actions
photos/Havok.png	—	PNGs	—	X

Tuttavia, `Havok.png` aveva lo scopo di testare la regola degli **X-men**.

3. Per risolvere il problema, riordina le regole.
 - a. Selezionare **Fine** per chiudere la finestra Simula criterio ILM.
 - b. Selezionare **Modifica** per modificare la policy.
 - c. Trascina la regola **X-men** in cima all'elenco.
 - d. Seleziona **Salva**.
4. Selezionare **Simula**.

Gli oggetti precedentemente testati vengono rivalutati in base alla policy aggiornata e vengono mostrati i nuovi risultati della simulazione. Nell'esempio, la colonna Regola corrispondente mostra che `Havok.png` l'oggetto ora corrisponde alla regola dei metadati degli X-men, come previsto. La colonna Corrispondenza precedente mostra che la regola PNG corrispondeva all'oggetto nella simulazione precedente.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all				
Object	Version ID	Rule matched	Previous match	Actions
photos/Havok.png	—	X-men	PNGs	X

Esempio 3: correggere una regola durante la simulazione di una policy ILM

Questo esempio mostra come simulare una policy, correggere una regola nella policy e continuare la simulazione.

In questo esempio viene simulata la policy **Demo**. Questa politica ha lo scopo di trovare oggetti che hanno `series=x-men` metadati dell'utente. Tuttavia, si sono verificati risultati inaspettati quando si è simulata questa politica contro il `Beast.jpg` oggetto. Invece di corrispondere alla regola dei metadati degli X-Men, l'oggetto corrispondeva alla regola predefinita: due copie di due data center.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all				
Object	Version ID	Rule matched	Previous match	Actions
photos/Beast.jpg	—	Two copies two data centers	—	X

Quando un oggetto di prova non corrisponde alla regola prevista nel criterio, è necessario esaminare ogni regola nel criterio e correggere eventuali errori.

Passi

1. Selezionare **Fine** per chiudere la finestra di dialogo Simula criterio. Nella pagina dei dettagli della policy, seleziona **Diagramma di conservazione**. Quindi seleziona **Espandi tutto** o **Visualizza dettagli** per ogni regola, a seconda delle necessità.
2. Esaminare l'account tenant della regola, l'ora di riferimento e i criteri di filtraggio.

Ad esempio, supponiamo che i metadati per la regola X-men siano stati inseriti come "x-men01" anziché "x-men".

3. Per risolvere l'errore, correggere la regola come segue:
 - Se la regola fa parte della policy, puoi clonarla o rimuoverla dalla policy e poi modificarla.
 - Se la regola fa parte della policy attiva, è necessario clonarla. Non è possibile modificare o rimuovere una regola dal criterio attivo.
4. Eseguire nuovamente la simulazione.

In questo esempio, la regola corretta degli X-men ora corrisponde a `Beast.jpg` oggetto basato su `series=x-men` metadati dell'utente, come previsto.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all				
Object	Version ID	Rule matched	Previous match	Actions
photos/Beast.jpg	—	X-men	—	✕

Gestisci i tag dei criteri ILM

È possibile visualizzare i dettagli dei tag dei criteri ILM, modificare un tag o rimuovere un tag.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["autorizzazioni di accesso richieste"](#).

Visualizza i dettagli del tag della policy ILM

Per visualizzare i dettagli di un tag:

1. Selezionare **ILM > Tag policy**.
2. Selezionare il nome della policy dalla tabella. Viene visualizzata la pagina dei dettagli del tag.
3. Nella pagina dei dettagli, visualizza la cronologia precedente delle policy assegnate.
4. Visualizza una policy selezionandola.

Modifica tag policy ILM



I nomi e le descrizioni dei tag sono visibili agli inquilini. Scegli valori che aiuteranno i tenant a prendere una decisione informata quando selezionano i tag dei criteri da assegnare ai loro bucket. Ad esempio, se la policy assegnata eliminerà gli oggetti dopo un certo periodo di tempo, è possibile comunicarlo nella descrizione. Non includere informazioni sensibili in questi campi.

Per modificare la descrizione di un tag esistente:

1. Selezionare **ILM > Tag policy**.
2. Seleziona la casella di controllo per il tag, quindi seleziona **Modifica**.

In alternativa, seleziona il nome del tag. Viene visualizzata la pagina dei dettagli del tag, in cui puoi selezionare **Modifica**.

3. Modificare la descrizione del tag secondo necessità
4. Seleziona **Salva**.

Rimuovi il tag della policy ILM

Quando si rimuove un tag di policy, a tutti i bucket a cui è assegnato quel tag verrà applicata la policy predefinita.

Per rimuovere un tag:

1. Selezionare **ILM > Tag policy**.
2. Seleziona la casella di controllo per il tag, quindi seleziona **Rimuovi**. Viene visualizzata una finestra di dialogo di conferma.

In alternativa, seleziona il nome del tag. Viene visualizzata la pagina dei dettagli del tag, in cui puoi selezionare **Rimuovi**.

3. Selezionare **Sì** per eliminare il tag.

Verifica una policy ILM con la ricerca dei metadati degli oggetti

Dopo aver attivato un criterio ILM, importare oggetti di prova rappresentativi nel sistema StorageGRID , quindi eseguire una ricerca dei metadati degli oggetti per confermare che le copie vengano eseguite come previsto e posizionate nelle posizioni corrette.

Prima di iniziare

Hai un identificatore di oggetto, che può essere uno dei seguenti: * **UUID**: l'identificatore univoco universale dell'oggetto. * **CBID**: Identificatore univoco dell'oggetto all'interno StorageGRID. È possibile ottenere il CBID di un oggetto dal registro di controllo. Inserire il CBID in maiuscolo. * **Chiave oggetto e bucket S3**: quando un oggetto viene acquisito tramite l'interfaccia S3, l'applicazione client utilizza una combinazione di chiave oggetto e bucket per archiviare e identificare l'oggetto. Se il bucket S3 è sottoposto a controllo di versione e si desidera cercare una versione specifica di un oggetto S3 utilizzando il bucket e la chiave dell'oggetto, si ottiene l'**ID versione**.

Passi

1. Ingerire l'oggetto.
2. Selezionare **ILM > Ricerca metadati oggetto**.
3. Digitare l'identificatore dell'oggetto nel campo **Identificatore**. È possibile immettere un UUID, un CBID o un bucket/chiave oggetto S3.
4. Facoltativamente, immettere un ID versione per l'oggetto (solo S3).
5. Seleziona **Cerca**.

Vengono visualizzati i risultati della ricerca dei metadati dell'oggetto. In questa pagina sono elencati i seguenti tipi di informazioni:

- Metadati di sistema, come ID oggetto (UUID), tipo di risultato (oggetto, marcatore di eliminazione, bucket S3) e dimensione logica dell'oggetto. Per maggiori dettagli, fare riferimento allo screenshot di esempio riportato di seguito.
- Qualsiasi coppia chiave-valore di metadati utente personalizzati associata all'oggetto.
- Per gli oggetti S3, qualsiasi coppia chiave-valore del tag oggetto associata all'oggetto.
- Per le copie di oggetti replicati, la posizione di archiviazione corrente di ciascuna copia.
- Per le copie di oggetti con codice di cancellazione, la posizione di archiviazione corrente di ciascun frammento.
- Per le copie di oggetti in un Cloud Storage Pool, la posizione dell'oggetto, incluso il nome del bucket esterno e l'identificatore univoco dell'oggetto.
- Per oggetti segmentati e oggetti multiparte, un elenco di segmenti di oggetti, inclusi gli identificatori di

segmento e le dimensioni dei dati. Per gli oggetti con più di 100 segmenti, vengono mostrati solo i primi 100 segmenti.

- Tutti i metadati degli oggetti nel formato di archiviazione interna non elaborato. Questi metadati grezzi includono metadati di sistema interni la cui persistenza da una versione all'altra non è garantita.

6. Verificare che l'oggetto sia archiviato nella posizione o nelle posizioni corrette e che si tratti del tipo di copia corretto.

Se l'opzione Audit è abilitata, è anche possibile monitorare il registro di audit per il messaggio ORLM Object Rules Met. Il messaggio di controllo ORLM può fornire maggiori informazioni sullo stato del processo di valutazione ILM, ma non può fornire informazioni sulla correttezza del posizionamento dei dati dell'oggetto o sulla completezza della policy ILM. Devi valutarlo tu stesso. Per maggiori dettagli, vedere ["Esaminare i registri di controllo"](#).

L'esempio seguente mostra i risultati della ricerca dei metadati dell'oggetto per un oggetto di test S3 archiviato come due copie replicate.



La seguente schermata è un esempio. I risultati varieranno a seconda della versione StorageGRID .

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H\$ TFbnQQ} CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H\$ TFboW28 CXG%

Raw Metadata

```
{
  "TYPE": "CTNT",
  "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
  "NAME": "testobject",
  "CBID": "0x8823DE7EC7C10416",
  "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAWS": "2",

```

Informazioni correlate

["Utilizzare l'API REST S3"](#)

Lavorare con le policy e le regole ILM

Man mano che cambiano i requisiti di archiviazione, potrebbe essere necessario implementare policy aggiuntive o modificare le regole ILM associate a una policy. È possibile visualizzare le metriche ILM per determinare le prestazioni del sistema.

Prima di iniziare

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

Visualizza le policy ILM

Per visualizzare le policy ILM attive e inattive e la cronologia delle attivazioni delle policy:

1. Selezionare **ILM > Criteri**.
2. Selezionare **Criteri** per visualizzare un elenco dei criteri attivi e inattivi. Nella tabella sono elencati il nome di ciascun criterio, i tag a cui è assegnato e se il criterio è attivo o inattivo.
3. Selezionare **Cronologia attivazioni** per visualizzare un elenco delle date di inizio e fine dell'attivazione delle polizze.
4. Selezionare il nome di una policy per visualizzarne i dettagli.



Se si visualizzano i dettagli di una policy il cui stato è Modificato o Eliminato, viene visualizzato un messaggio che spiega che si sta visualizzando la versione della policy che era attiva per l'intervallo di tempo specificato e che da allora è stata modificata o eliminata.

Modifica una policy ILM

È possibile modificare solo una policy inattiva. Se si desidera modificare una policy attiva, è possibile disattivarla oppure creare un clone e modificarlo.

Per modificare una policy:

1. Selezionare **ILM > Criteri**.
2. Seleziona la casella di controllo relativa alla policy che desideri modificare, quindi seleziona **Modifica**.
3. Modifica la policy seguendo le istruzioni in "[Creare policy ILM](#)".
4. Simulare la policy prima di riattivarla.



Una policy ILM configurata in modo errato può comportare una perdita di dati irrecuperabile. Prima di attivare una policy ILM, esaminare attentamente la policy ILM e le relative regole ILM, quindi simulare la policy ILM. Verificare sempre che la politica ILM funzioni come previsto.

Clonare una policy ILM

Per clonare una policy ILM:

1. Selezionare **ILM > Criteri**.
2. Seleziona la casella di controllo relativa alla policy che desideri clonare, quindi seleziona **Clona**.
3. Crea una nuova policy partendo dalla policy che hai clonato seguendo le istruzioni in "[Creare policy ILM](#)".



Una policy ILM configurata in modo errato può comportare una perdita di dati irrecuperabile. Prima di attivare una policy ILM, esaminare attentamente la policy ILM e le relative regole ILM, quindi simulare la policy ILM. Verificare sempre che la politica ILM funzioni come previsto.

Rimuovere una policy ILM

È possibile rimuovere un criterio ILM solo se è inattivo. Per rimuovere una policy:

1. Selezionare **ILM > Criteri**.
2. Seleziona la casella di controllo relativa al criterio inattivo che desideri rimuovere.
3. Seleziona **Rimuovi**.

Visualizza i dettagli della regola ILM

Per visualizzare i dettagli di una regola ILM, inclusi il diagramma di conservazione e le istruzioni di posizionamento per la regola:

1. Selezionare **ILM > Regole**.
2. Seleziona il nome della regola di cui vuoi visualizzare i dettagli. Esempio:

The screenshot shows the '2 copies 2 data centers' rule details page. At the top, it displays the rule name and three tabs: 'Rule detail' (selected), 'Used in policies', and 'Retention diagram'. Below the tabs, there are settings for 'Compliant: No', 'Ingest behavior: Strict', and 'Reference time: Noncurrent time'. There are buttons for 'Clone', 'Edit', and 'Remove'. A section titled 'Time period and placements' contains a 'Retention diagram' tab and a 'Placement instructions' tab. The 'Retention diagram' tab shows a timeline from 'Day 0' to 'Forever' with two bars: '2 replicated copies - Data Center 1' (blue) and 'EC 2+1 - Data Center 1' (grey). A legend indicates that blue represents 'Replicated copy' and grey represents 'Erasure-coded (EC) copy'. A 'Rule analysis' section states: 'Objects processed by this rule will not be deleted by ILM.'

Inoltre, puoi utilizzare la pagina dei dettagli per clonare, modificare o rimuovere una regola. Non è possibile modificare o rimuovere una regola se è utilizzata in una policy.

Clona una regola ILM

È possibile clonare una regola esistente se si desidera creare una nuova regola che utilizzi alcune delle impostazioni della regola esistente. Se è necessario modificare una regola utilizzata in una policy, è sufficiente clonare la regola e apportare le modifiche al clone. Dopo aver apportato modifiche al clone, è possibile rimuovere la regola originale dal criterio e sostituirla con la versione modificata, se necessario.



Non è possibile clonare una regola ILM se è stata creata utilizzando StorageGRID versione 10.2 o precedente.

Passi

1. Selezionare **ILM > Regole**.
2. Seleziona la casella di controllo relativa alla regola che desideri clonare, quindi seleziona **Clona**. In alternativa, seleziona il nome della regola, quindi seleziona **Clona** dalla pagina dei dettagli della regola.
3. Aggiorna la regola clonata seguendo i passaggi per [modifica di una regola ILM E"utilizzo di filtri avanzati nelle regole ILM"](#).

Quando si clona una regola ILM, è necessario immettere un nuovo nome.

Modifica una regola ILM

Potrebbe essere necessario modificare una regola ILM per cambiare un filtro o un'istruzione di posizionamento.

Non è possibile modificare una regola se è utilizzata in una policy ILM. Invece, puoi [clonare la regola](#) e apportare tutte le modifiche necessarie alla copia clonata.



Una policy ILM configurata in modo errato può comportare una perdita di dati irrecuperabile. Prima di attivare una policy ILM, esaminare attentamente la policy ILM e le relative regole ILM, quindi simulare la policy ILM. Verificare sempre che la politica ILM funzioni come previsto.

Passi

1. Selezionare **ILM > Regole**.
2. Verificare che la regola che si desidera modificare non sia utilizzata in alcuna policy ILM.
3. Se la regola che vuoi modificare non è in uso, seleziona la casella di controllo per la regola e seleziona **Azioni > Modifica**. In alternativa, seleziona il nome della regola, quindi seleziona **Modifica** nella pagina dei dettagli della regola.
4. Completare i passaggi della procedura guidata Modifica regola ILM. Se necessario, seguire i passaggi per "[creazione di una regola ILM](#)" E "[utilizzo di filtri avanzati nelle regole ILM](#)".

Quando si modifica una regola ILM, non è possibile modificarne il nome.

Rimuovere una regola ILM

Per mantenere gestibile l'elenco delle regole ILM correnti, rimuovi tutte le regole ILM che probabilmente non utilizzerai.

Passi

Per rimuovere una regola ILM attualmente utilizzata in un criterio attivo:

1. Clonare la policy.
2. Rimuovere la regola ILM dal clone della policy.
3. Salvare, simulare e attivare la nuova policy per assicurarsi che gli oggetti siano protetti come previsto.
4. Vai ai passaggi per rimuovere una regola ILM attualmente utilizzata in un criterio inattivo.

Per rimuovere una regola ILM attualmente utilizzata in un criterio inattivo:

1. Selezionare la policy inattiva.
2. Rimuovere la regola ILM dalla policy [rimuovere la politica](#).
3. Vai ai passaggi per rimuovere una regola ILM attualmente non utilizzata.

Per rimuovere una regola ILM attualmente non utilizzata:

1. Selezionare **ILM > Regole**.
2. Verificare che la regola che si desidera rimuovere non sia utilizzata in alcun criterio.

3. Se la regola che vuoi rimuovere non è in uso, selezionala e seleziona **Azioni > Rimuovi**. È possibile selezionare più regole e rimuoverle tutte contemporaneamente.
4. Selezionare **Sì** per confermare che si desidera rimuovere la regola ILM.

Visualizza le metriche ILM

È possibile visualizzare le metriche per ILM, come il numero di oggetti nella coda e la frequenza di valutazione. È possibile monitorare queste metriche per determinare le prestazioni del sistema. Una coda o una frequenza di valutazione elevate potrebbero indicare che il sistema non è in grado di tenere il passo con la frequenza di acquisizione, che il carico delle applicazioni client è eccessivo o che si è verificata una condizione anomala.

Passi

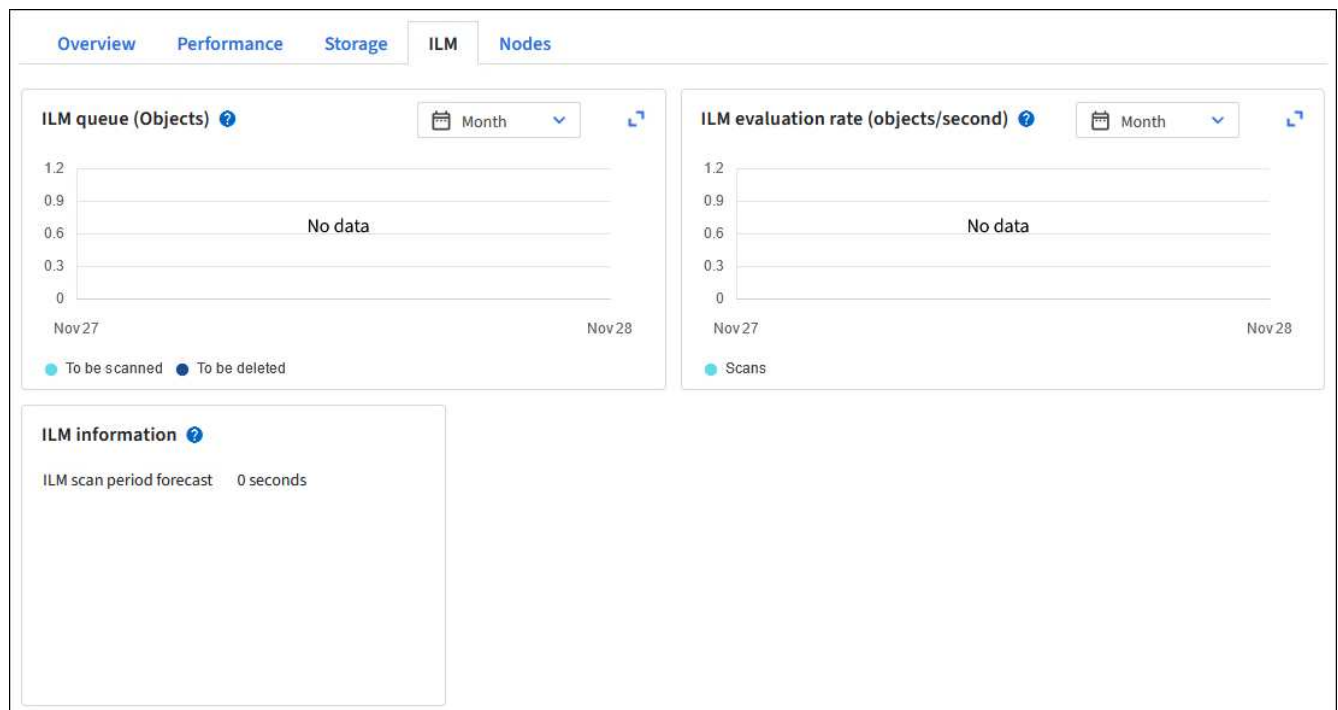
1. Selezionare **Dashboard > ILM**.



Poiché la dashboard può essere personalizzata, la scheda ILM potrebbe non essere disponibile.

2. Monitorare le metriche nella scheda ILM.

Puoi selezionare il punto interrogativo per visualizzare una descrizione degli elementi nella scheda ILM.



Utilizzare il blocco oggetto S3

Gestisci gli oggetti con S3 Object Lock

In qualità di amministratore della griglia, puoi abilitare S3 Object Lock per il tuo sistema StorageGRID e implementare una policy ILM conforme per garantire che gli oggetti in bucket S3 specifici non vengano eliminati o sovrascritti per un periodo di tempo specificato.

Che cos'è S3 Object Lock?

La funzionalità StorageGRID S3 Object Lock è una soluzione di protezione degli oggetti equivalente a S3 Object Lock in Amazon Simple Storage Service (Amazon S3).

Quando l'impostazione globale S3 Object Lock è abilitata per un sistema StorageGRID, un account tenant S3 può creare bucket con o senza S3 Object Lock abilitato. Se in un bucket è abilitato S3 Object Lock, è necessario il controllo delle versioni del bucket, che viene abilitato automaticamente.

Un bucket senza S3 Object Lock può contenere solo oggetti per i quali non sono specificate impostazioni di conservazione. Nessun oggetto ingerito avrà impostazioni di conservazione.

Un bucket con S3 Object Lock può contenere oggetti con e senza impostazioni di conservazione specificate dalle applicazioni client S3. Alcuni oggetti acquisiti avranno impostazioni di conservazione.

Un bucket con S3 Object Lock e conservazione predefinita configurata può contenere oggetti caricati con impostazioni di conservazione specificate e nuovi oggetti senza impostazioni di conservazione. I nuovi oggetti utilizzano l'impostazione predefinita, perché l'impostazione di conservazione non è stata configurata a livello di oggetto.

Di fatto, tutti gli oggetti appena acquisiti hanno impostazioni di conservazione quando è configurata la conservazione predefinita. Gli oggetti esistenti senza impostazioni di conservazione degli oggetti rimangono inalterati.

Modalità di conservazione

La funzionalità StorageGRID S3 Object Lock supporta due modalità di conservazione per applicare diversi livelli di protezione agli oggetti. Queste modalità sono equivalenti alle modalità di conservazione di Amazon S3.

- In modalità conformità:
 - L'oggetto non può essere eliminato finché non viene raggiunta la data di conservazione.
 - La data di conservazione dell'oggetto può essere aumentata, ma non diminuita.
 - La data di conservazione dell'oggetto non può essere rimossa finché non viene raggiunta tale data.
- In modalità di governance:
 - Gli utenti con autorizzazioni speciali possono utilizzare un'intestazione di bypass nelle richieste per modificare determinate impostazioni di conservazione.
 - Questi utenti possono eliminare una versione di un oggetto prima che venga raggiunta la data di conservazione.
 - Questi utenti possono aumentare, diminuire o rimuovere la data di conservazione di un oggetto.

Impostazioni di conservazione per le versioni degli oggetti

Se viene creato un bucket con S3 Object Lock abilitato, gli utenti possono utilizzare l'applicazione client S3 per specificare facoltativamente le seguenti impostazioni di conservazione per ciascun oggetto aggiunto al bucket:

- **Modalità di conservazione:** conformità o governance.
- **Retain-until-date:** se la retain-until-date di una versione di un oggetto è futura, l'oggetto può essere recuperato, ma non eliminato.
- **Sospensione legale:** l'applicazione di una sospensione legale a una versione di un oggetto blocca immediatamente quell'oggetto. Ad esempio, potrebbe essere necessario applicare un blocco legale a un oggetto correlato a un'indagine o a una controversia legale. Una sospensione legale non ha una data di

scadenza, ma rimane in vigore finché non viene rimossa esplicitamente. Le sospensioni legali sono indipendenti dalla data di conservazione fino alla data di scadenza.



Se un oggetto è sottoposto a conservazione legale, nessuno può eliminarlo, indipendentemente dalla sua modalità di conservazione.

Per i dettagli sulle impostazioni dell'oggetto, vedere ["Utilizzare l'API REST S3 per configurare S3 Object Lock"](#).

Impostazione di conservazione predefinita per i bucket

Se viene creato un bucket con S3 Object Lock abilitato, gli utenti possono facoltativamente specificare le seguenti impostazioni predefinite per il bucket:

- **Modalità di conservazione predefinita:** conformità o governance.
- **Periodo di conservazione predefinito:** per quanto tempo devono essere conservate le nuove versioni degli oggetti aggiunte a questo bucket, a partire dal giorno in cui vengono aggiunte.

Le impostazioni predefinite del bucket si applicano solo ai nuovi oggetti che non dispongono di impostazioni di conservazione proprie. Gli oggetti bucket esistenti non vengono modificati quando si aggiungono o si modificano queste impostazioni predefinite.

Vedere ["Crea un bucket S3"](#) e ["Aggiorna la conservazione predefinita del blocco degli oggetti S3"](#).

Confronto tra S3 Object Lock e la conformità legacy

S3 Object Lock sostituisce la funzionalità Compliance disponibile nelle versioni precedenti StorageGRID. Poiché la funzionalità S3 Object Lock è conforme ai requisiti di Amazon S3, essa rende obsoleta la funzionalità proprietaria StorageGRID Compliance, ora denominata "legacy Compliance".



L'impostazione Conformità globale è obsoleta. Se hai abilitato questa impostazione utilizzando una versione precedente di StorageGRID, l'impostazione Blocco oggetto S3 viene abilitata automaticamente. È possibile continuare a utilizzare StorageGRID per gestire le impostazioni dei bucket conformi esistenti; tuttavia, non è possibile creare nuovi bucket conformi. Per i dettagli, vedere ["Knowledge Base di NetApp : come gestire i bucket Compliant legacy in StorageGRID 11.5"](#).

Se hai utilizzato la funzionalità Conformità legacy in una versione precedente di StorageGRID, fai riferimento alla tabella seguente per scoprire come si confronta con la funzionalità Blocco oggetti S3 in StorageGRID.

	Blocco oggetto S3	Conformità (legacy)
Come viene abilitata la funzionalità a livello globale?	Da Grid Manager, seleziona CONFIGURAZIONE > Sistema > Blocco oggetto S3 .	Non più supportato.
Come si abilita la funzionalità per un bucket?	Gli utenti devono abilitare S3 Object Lock quando creano un nuovo bucket utilizzando Tenant Manager, Tenant Management API o S3 REST API.	Non più supportato.

	Blocco oggetto S3	Conformità (legacy)
È supportato il controllo delle versioni dei bucket?	Sì. Il controllo delle versioni del bucket è obbligatorio e viene abilitato automaticamente quando S3 Object Lock è abilitato per il bucket.	NO.
Come viene impostata la conservazione degli oggetti?	Gli utenti possono impostare una data di conservazione per ogni versione dell'oggetto oppure possono impostare un periodo di conservazione predefinito per ogni bucket.	Gli utenti devono impostare un periodo di conservazione per l'intero bucket. Il periodo di conservazione si applica a tutti gli oggetti nel bucket.
È possibile modificare il periodo di conservazione?	• In modalità di conformità, la data di conservazione per una versione di un oggetto può essere aumentata ma mai diminuita. • In modalità di governance, gli utenti con autorizzazioni speciali possono ridurre o addirittura rimuovere le impostazioni di conservazione di un oggetto.	Il periodo di conservazione di un bucket può essere aumentato, ma mai diminuito.
Dove viene controllata la conservazione legale?	Gli utenti possono applicare o rimuovere una sospensione legale per qualsiasi versione dell'oggetto nel bucket.	Viene applicata una sospensione legale al bucket che interessa tutti gli oggetti al suo interno.
Quando è possibile eliminare gli oggetti?	• In modalità di conformità, una versione dell'oggetto può essere eliminata dopo aver raggiunto la data di conservazione, a condizione che l'oggetto non sia soggetto a conservazione legale. • In modalità di governance, gli utenti con autorizzazioni speciali possono eliminare un oggetto prima che venga raggiunta la data di conservazione, a condizione che l'oggetto non sia soggetto a conservazione legale.	Un oggetto può essere eliminato dopo la scadenza del periodo di conservazione, a condizione che il bucket non sia sottoposto a conservazione legale. Gli oggetti possono essere eliminati automaticamente o manualmente.
La configurazione del ciclo di vita del bucket è supportata?	Sì	NO

Attività di blocco degli oggetti S3

In qualità di amministratore della griglia, devi coordinarti strettamente con gli utenti tenant per garantire che gli oggetti siano protetti in modo da soddisfare i loro requisiti di conservazione.



L'applicazione delle impostazioni del tenant sulla griglia potrebbe richiedere 15 minuti o più, a seconda della connettività di rete, dello stato del nodo e delle operazioni di Cassandra.

Gli elenchi seguenti per gli amministratori della griglia e gli utenti tenant contengono le attività di alto livello per l'utilizzo della funzionalità S3 Object Lock.

Amministratore di rete

- Abilita l'impostazione globale di blocco degli oggetti S3 per l'intero sistema StorageGRID .
- Garantire che le politiche di gestione del ciclo di vita delle informazioni (ILM) siano *conformi*; ovvero, che soddisfino i ["requisiti dei bucket con S3 Object Lock abilitato"](#) .
- Se necessario, consentire a un tenant di utilizzare Conformità come modalità di conservazione. In caso contrario, è consentita solo la modalità Governance.
- Se necessario, impostare un periodo massimo di conservazione per un tenant.

Utente inquilino

- Esaminare le considerazioni relative a bucket e oggetti con S3 Object Lock.
- Se necessario, contattare l'amministratore della griglia per abilitare l'impostazione globale di blocco degli oggetti S3 e impostare le autorizzazioni.
- Crea bucket con S3 Object Lock abilitato.
- Facoltativamente, configura le impostazioni di conservazione predefinite per un bucket:
 - Modalità di conservazione predefinita: Governance o Conformità, se consentita dall'amministratore della rete.
 - Periodo di conservazione predefinito: deve essere inferiore o uguale al periodo di conservazione massimo impostato dall'amministratore della griglia.
- Utilizzare l'applicazione client S3 per aggiungere oggetti e, facoltativamente, impostare la conservazione specifica dell'oggetto:
 - Modalità di conservazione. Governance o conformità, se consentito dall'amministratore della rete.
 - Conserva fino alla data: deve essere inferiore o uguale a quanto consentito dal periodo di conservazione massimo impostato dall'amministratore della griglia.

Requisiti per S3 Object Lock

È necessario esaminare i requisiti per abilitare l'impostazione globale S3 Object Lock, i requisiti per creare regole ILM e policy ILM conformi e le restrizioni che StorageGRID impone ai bucket e agli oggetti che utilizzano S3 Object Lock.

Requisiti per l'utilizzo dell'impostazione globale S3 Object Lock

- È necessario abilitare l'impostazione globale S3 Object Lock tramite Grid Manager o Grid Management API prima che un tenant S3 possa creare un bucket con S3 Object Lock abilitato.
- Abilitando l'impostazione globale S3 Object Lock, tutti gli account tenant S3 potranno creare bucket con S3

Object Lock abilitato.

- Dopo aver abilitato l'impostazione globale Blocco oggetti S3, non è possibile disabilitarla.
- Non è possibile abilitare il blocco oggetti S3 globale a meno che la regola predefinita in tutti i criteri ILM attivi non sia *conforme* (ovvero, la regola predefinita deve essere conforme ai requisiti dei bucket con blocco oggetti S3 abilitato).
- Quando l'impostazione globale Blocco oggetti S3 è abilitata, non è possibile creare un nuovo criterio ILM o attivarne uno esistente, a meno che la regola predefinita nel criterio non sia conforme. Dopo aver abilitato l'impostazione globale S3 Object Lock, le pagine Regole ILM e Criteri ILM indicano quali regole ILM sono conformi.

Requisiti per le regole ILM conformi

Se si desidera abilitare l'impostazione globale S3 Object Lock, è necessario assicurarsi che la regola predefinita in tutti i criteri ILM attivi sia conforme. Una regola conforme soddisfa i requisiti di entrambi i bucket con S3 Object Lock abilitato e di tutti i bucket esistenti con la conformità legacy abilitata:

- Deve creare almeno due copie replicate dell'oggetto o una copia con codice di cancellazione.
- Queste copie devono essere presenti sui nodi di archiviazione per l'intera durata di ciascuna riga nelle istruzioni di posizionamento.
- Le copie degli oggetti non possono essere salvate in un Cloud Storage Pool.
- Almeno una riga delle istruzioni di posizionamento deve iniziare dal giorno 0, utilizzando **Ingest time** come orario di riferimento.
- Almeno una riga delle istruzioni di posizionamento deve essere "per sempre".

Requisiti per le politiche ILM

Quando l'impostazione globale Blocco oggetti S3 è abilitata, i criteri ILM attivi e inattivi possono includere sia regole conformi che non conformi.

- La regola predefinita in una policy ILM attiva o inattiva deve essere conforme.
- Le regole non conformi si applicano solo agli oggetti nei bucket in cui non è abilitato S3 Object Lock o in cui non è abilitata la funzionalità legacy Compliance.
- Le regole conformi possono essere applicate agli oggetti in qualsiasi bucket; non è necessario abilitare S3 Object Lock o la conformità legacy per il bucket.

"Esempio di una policy ILM conforme per S3 Object Lock"

Requisiti per i bucket con S3 Object Lock abilitato

- Se l'impostazione globale S3 Object Lock è abilitata per il sistema StorageGRID, è possibile utilizzare Tenant Manager, Tenant Management API o S3 REST API per creare bucket con S3 Object Lock abilitato.
- Se si prevede di utilizzare S3 Object Lock, è necessario abilitarlo quando si crea il bucket. Non è possibile abilitare S3 Object Lock per un bucket esistente.
- Quando S3 Object Lock è abilitato per un bucket, StorageGRID abilita automaticamente il controllo delle versioni per quel bucket. Non è possibile disattivare S3 Object Lock o sospendere il controllo delle versioni per il bucket.
- Facoltativamente, è possibile specificare una modalità di conservazione predefinita e un periodo di conservazione per ciascun bucket utilizzando Tenant Manager, Tenant Management API o S3 REST API. Le impostazioni di conservazione predefinite del bucket si applicano solo ai nuovi oggetti aggiunti al bucket.

che non dispongono di impostazioni di conservazione proprie. È possibile ignorare queste impostazioni predefinite specificando una modalità di conservazione e una data di conservazione per ogni versione dell'oggetto quando viene caricata.

- La configurazione del ciclo di vita del bucket è supportata per i bucket con S3 Object Lock abilitato.
- La replica CloudMirror non è supportata per i bucket con S3 Object Lock abilitato.

Requisiti per gli oggetti nei bucket con S3 Object Lock abilitato

- Per proteggere una versione dell'oggetto, è possibile specificare le impostazioni di conservazione predefinite per il bucket oppure specificare le impostazioni di conservazione per ciascuna versione dell'oggetto. Le impostazioni di conservazione a livello di oggetto possono essere specificate tramite l'applicazione client S3 o l'API REST S3.
- Le impostazioni di conservazione si applicano alle singole versioni degli oggetti. Una versione di un oggetto può avere sia un'impostazione di conservazione fino alla data di scadenza che un'impostazione di conservazione legale, una ma non l'altra, oppure nessuna delle due. Specificando un'impostazione di conservazione fino a data o di conservazione legale per un oggetto, si protegge solo la versione specificata nella richiesta. È possibile creare nuove versioni dell'oggetto, mentre la versione precedente rimane bloccata.

Ciclo di vita degli oggetti nei bucket con S3 Object Lock abilitato

Ogni oggetto salvato in un bucket con S3 Object Lock abilitato attraversa queste fasi:

1. Ingestione di oggetti

Quando una versione di un oggetto viene aggiunta a un bucket in cui è abilitato il blocco degli oggetti S3, le impostazioni di conservazione vengono applicate come segue:

- Se per l'oggetto sono specificate impostazioni di conservazione, vengono applicate le impostazioni a livello di oggetto. Tutte le impostazioni predefinite del bucket vengono ignorate.
- Se non vengono specificate impostazioni di conservazione per l'oggetto, vengono applicate le impostazioni predefinite del bucket, se presenti.
- Se non vengono specificate impostazioni di conservazione per l'oggetto o il bucket, l'oggetto non è protetto da S3 Object Lock.

Se vengono applicate le impostazioni di conservazione, vengono protetti sia l'oggetto sia tutti i metadati S3 definiti dall'utente.

2. Conservazione ed eliminazione degli oggetti

StorageGRID memorizza più copie di ciascun oggetto protetto per il periodo di conservazione specificato. Il numero e il tipo esatti di copie degli oggetti e le posizioni di archiviazione sono determinati dalle regole conformi nelle policy ILM attive. La possibilità di eliminare un oggetto protetto prima che venga raggiunta la data di conservazione dipende dalla sua modalità di conservazione.

- Se un oggetto è sottoposto a conservazione legale, nessuno può eliminarlo, indipendentemente dalla sua modalità di conservazione.

Informazioni correlate

- ["Crea un bucket S3"](#)
- ["Aggiorna la conservazione predefinita del blocco degli oggetti S3"](#)
- ["Utilizzare l'API REST S3 per configurare S3 Object Lock"](#)

- ["Esempio 7: Politica ILM conforme per S3 Object Lock"](#)

Abilita il blocco oggetti S3 a livello globale

Se un account tenant S3 deve rispettare i requisiti normativi durante il salvataggio dei dati degli oggetti, è necessario abilitare S3 Object Lock per l'intero sistema StorageGRID . Abilitando l'impostazione globale S3 Object Lock, qualsiasi utente tenant S3 può creare e gestire bucket e oggetti con S3 Object Lock.

Prima di iniziare

- Tu hai il ["Permesso di accesso root"](#) .
- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Hai esaminato il flusso di lavoro di S3 Object Lock e ne hai compreso le considerazioni.
- Hai confermato che la regola predefinita nel criterio ILM attivo è conforme. Vedere ["Crea una regola ILM predefinita"](#) per i dettagli.

Informazioni su questo compito

Un amministratore di griglia deve abilitare l'impostazione globale S3 Object Lock per consentire agli utenti tenant di creare nuovi bucket con S3 Object Lock abilitato. Una volta abilitata, questa impostazione non può essere disabilitata.

Dopo aver abilitato l'impostazione globale Blocco oggetti S3, rivedere le impostazioni di conformità dei tenant esistenti. Quando si abilita questa impostazione, le impostazioni di S3 Object Lock per tenant dipendono dalla versione StorageGRID al momento della creazione del tenant.



L'impostazione Conformità globale è obsoleta. Se hai abilitato questa impostazione utilizzando una versione precedente di StorageGRID, l'impostazione Blocco oggetto S3 viene abilitata automaticamente. È possibile continuare a utilizzare StorageGRID per gestire le impostazioni dei bucket conformi esistenti; tuttavia, non è possibile creare nuovi bucket conformi. Per i dettagli, vedere ["Knowledge Base di NetApp : come gestire i bucket Compliant legacy in StorageGRID 11.5"](#) .

Passi

1. Selezionare **CONFIGURAZIONE > Sistema > Blocco oggetto S3**.

Viene visualizzata la pagina Impostazioni blocco oggetti S3.

2. Selezionare **Abilita blocco oggetto S3**.

3. Selezionare **Applica**.

Viene visualizzata una finestra di dialogo di conferma che ricorda che non è possibile disattivare S3 Object Lock dopo averlo attivato.

4. Se sei sicuro di voler abilitare in modo permanente S3 Object Lock per l'intero sistema, seleziona **OK**.

Quando selezioni **OK**:

- Se la regola predefinita nel criterio ILM attivo è conforme, S3 Object Lock è ora abilitato per l'intera griglia e non può essere disabilitato.
- Se la regola predefinita non è conforme, viene visualizzato un errore. È necessario creare e attivare

una nuova policy ILM che includa una regola conforme come regola predefinita. Selezionare **OK**. Quindi, crea una nuova policy, simulala e attivala. Vedere "[Crea policy ILM](#)" per istruzioni.

Risolvi gli errori di coerenza durante l'aggiornamento del blocco degli oggetti S3 o della configurazione di conformità legacy

Se un sito del data center o più nodi di archiviazione in un sito diventano non disponibili, potrebbe essere necessario aiutare gli utenti del tenant S3 ad applicare le modifiche al blocco degli oggetti S3 o alla configurazione di conformità legacy.

Gli utenti tenant che dispongono di bucket con S3 Object Lock (o legacy Compliance) abilitato possono modificare determinate impostazioni. Ad esempio, un utente tenant che utilizza S3 Object Lock potrebbe dover mettere una versione dell'oggetto in conservazione legale.

Quando un utente tenant aggiorna le impostazioni per un bucket S3 o una versione di oggetto, StorageGRID tenta di aggiornare immediatamente i metadati del bucket o dell'oggetto in tutta la griglia. Se il sistema non riesce ad aggiornare i metadati perché un sito del data center o più nodi di archiviazione non sono disponibili, restituisce un errore:

```
503: Service Unavailable
Unable to update compliance settings because the settings can't be
consistently applied on enough storage services. Contact your grid
administrator for assistance.
```

Per risolvere questo errore, segui questi passaggi:

1. Tentare di rendere nuovamente disponibili tutti i nodi o siti di archiviazione il prima possibile.
2. Se non riesci a rendere disponibili sufficienti nodi di archiviazione in ogni sito, contatta l'assistenza tecnica, che può aiutarti a ripristinare i nodi e a garantire che le modifiche vengano applicate in modo coerente in tutta la griglia.
3. Una volta risolto il problema di fondo, ricorda all'utente tenant di riprovare ad apportare le modifiche alla configurazione.

Informazioni correlate

- "[Utilizzare un account tenant](#)"
- "[Utilizzare l'API REST S3](#)"
- "[Recuperare e mantenere](#)"

Esempio di regole e policy ILM

Esempio 1: regole e policy ILM per l'archiviazione degli oggetti

È possibile utilizzare le seguenti regole e policy di esempio come punto di partenza per definire una policy ILM che soddisfi i requisiti di protezione e conservazione degli oggetti.



Le seguenti regole e policy ILM sono solo esempi. Esistono molti modi per configurare le regole ILM. Prima di attivare una nuova policy, simulala per verificare che funzioni come previsto per proteggere i contenuti dalla perdita.

Regola ILM 1 per l'esempio 1: Copia i dati dell'oggetto in due siti

Questa regola ILM di esempio copia i dati degli oggetti nei pool di archiviazione in due siti.

Definizione della regola	Valore di esempio
Pool di archiviazione monosito	Due pool di archiviazione, ciascuno contenente siti diversi, denominati Sito 1 e Sito 2.
Nome della regola	Due copie due siti
Tempo di riferimento	Tempo di ingestione
Posizionamenti	Dal giorno 0 all'infinito, conserva una copia replicata nel sito 1 e una copia replicata nel sito 2.

La sezione Analisi delle regole del diagramma di conservazione afferma:

- La protezione contro le perdite del sito StorageGRID sarà valida per tutta la durata di questa regola.
- Gli oggetti elaborati da questa regola non verranno eliminati da ILM.

Reference time ⓘ

Ingest time

Time period and placements

Sort by start date

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1

From Day 0

store forever

Store objects by replicating 1 copies at Site 1

and store objects by replicating 1 copies at Site 2

Add other type or location

Add another time period

Retention diagram

Replicated copy

Rule analysis:

- StorageGRID site-loss protection will apply for the duration of this rule.
- Objects processed by this rule will not be deleted by ILM.

Reference time: Ingest time

Day 0

Day 0 - forever

1 replicated copy - Site 1

1 replicated copy - Site 2

Duration Forever

Regola ILM 2 per l'esempio 1: profilo di codifica di cancellazione con corrispondenza del bucket

Questa regola ILM di esempio utilizza un profilo di codifica di cancellazione e un bucket S3 per determinare dove e per quanto tempo l'oggetto viene archiviato.

401

Definizione della regola	Valore di esempio
Pool di archiviazione con più siti	• Un pool di archiviazione su tre siti (siti 1, 2, 3) • Utilizzare lo schema di codifica di cancellazione 6+3
Nome della regola	S3 Bucket finance-records
Tempo di riferimento	Tempo di ingestione
Posizionamenti	Per gli oggetti nel bucket S3 denominato finance-records, creare una copia con codice di cancellazione nel pool specificato dal profilo di codifica di cancellazione. Conserva questa copia per sempre.

Time period and placements

Sort by start date

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1

From Day 0

store

forever

Store objects by

erasure coding

using

6+3 EC scheme at Sites 1, 2, 3

Add other type or location

Add another time period

Retention diagram

Erasure-coded (EC) copy

Rule analysis:

- StorageGRID site-loss protection will apply for the duration of this rule.
- Objects processed by this rule will not be deleted by ILM.

Reference time: Ingest time

Day 0

Day 0 - forever

EC 6+3 - Sites 1, 2, 3

Duration Forever

Politica ILM per esempio 1

Nella pratica, la maggior parte delle policy ILM sono semplici, anche se il sistema StorageGRID consente di progettare policy ILM sofisticate e complesse.

Una tipica policy ILM per una griglia multi-sito potrebbe includere regole ILM come le seguenti:

- Durante l'acquisizione, archivia tutti gli oggetti appartenenti al bucket S3 denominato `finance-records` in un pool di archiviazione che contiene tre siti. Utilizzare la codifica di cancellazione 6+3.
- Se un oggetto non corrisponde alla prima regola ILM, utilizzare la regola ILM predefinita del criterio, Due copie due data center, per archiviare una copia di tale oggetto nel Sito 1 e una copia nel Sito 2.

Proposed policy name

Object Storage Policy

Reason for change

example 1

Manage rules

1. Select the rules you want to add to the policy.
2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

Select rules

Rule order	Rule name	Filters
1	S3 Bucket finance-records	Tenant is Finance Bucket name is finance-records
Default	Two Copies Two Data Centers	—

Informazioni correlate

- ["Utilizzare le policy ILM"](#)
- ["Creare policy ILM"](#)

Esempio 2: regole e policy ILM per il filtraggio delle dimensioni degli oggetti EC

È possibile utilizzare le seguenti regole e policy di esempio come punti di partenza per definire una policy ILM che filtri in base alle dimensioni dell'oggetto per soddisfare i requisiti EC consigliati.



Le seguenti regole e policy ILM sono solo esempi. Esistono molti modi per configurare le regole ILM. Prima di attivare una nuova policy, simulala per verificare che funzioni come previsto per proteggere i contenuti dalla perdita.

Regola ILM 1 per l'esempio 2: utilizzare EC per oggetti maggiori di 1 MB

Questa regola ILM di esempio codifica gli oggetti di dimensioni superiori a 1 MB.



La codifica di cancellazione è più adatta per oggetti di dimensioni superiori a 1 MB. Non utilizzare la codifica di cancellazione per oggetti di dimensioni inferiori a 200 KB per evitare il sovraccarico dovuto alla gestione di frammenti molto piccoli con codifica di cancellazione.

Definizione della regola	Valore di esempio
Nome della regola	Solo oggetti EC > 1 MB
Tempo di riferimento	Tempo di ingestione
Filtro avanzato per la dimensione dell'oggetto	Dimensione dell'oggetto maggiore di 1 MB

Definizione della regola	Valore di esempio
Posizionamenti	Crea una copia con codice di cancellazione 2+1 utilizzando tre siti

Filter group 1
Objects with all of following metadata will be evaluated by this rule:

Object size
greater than
1
MB

Regola ILM 2 per esempio 2: Due copie replicate

Questa regola ILM di esempio crea due copie replicate e non filtra in base alle dimensioni dell'oggetto. Questa regola è la regola predefinita per la policy. Poiché la prima regola filtra tutti gli oggetti di dimensioni superiori a 1 MB, questa regola si applica solo agli oggetti di dimensioni pari o inferiori a 1 MB.

Definizione della regola	Valore di esempio
Nome della regola	Due copie replicate
Tempo di riferimento	Tempo di ingestione
Filtro avanzato per la dimensione dell'oggetto	Nessuno
Posizionamenti	Dal giorno 0 all'infinito, conserva una copia replicata nel sito 1 e una copia replicata nel sito 2.

Criterio ILM per esempio 2: utilizzare EC per oggetti maggiori di 1 MB

Questo esempio di policy ILM include due regole ILM:

- La prima regola codifica tutti gli oggetti di dimensioni superiori a 1 MB.
- La seconda regola ILM (predefinita) crea due copie replicate. Poiché gli oggetti di dimensioni superiori a 1 MB sono stati filtrati dalla regola 1, la regola 2 si applica solo agli oggetti di dimensioni pari o inferiori a 1 MB.

Esempio 3: Regole e policy ILM per una migliore protezione dei file immagine

È possibile utilizzare le seguenti regole e policy di esempio per garantire che le immagini di dimensioni superiori a 1 MB vengano codificate con cancellazione e che vengano realizzate due copie delle immagini più piccole.



Le seguenti regole e policy ILM sono solo esempi. Esistono molti modi per configurare le regole ILM. Prima di attivare una nuova policy, simulala per verificare che funzioni come previsto per proteggere i contenuti dalla perdita.

Regola ILM 1 per esempio 3: utilizzare EC per file immagine superiori a 1 MB

Questa regola ILM di esempio utilizza un filtro avanzato per cancellare il codice di tutti i file immagine di dimensioni superiori a 1 MB.



La codifica di cancellazione è più adatta per oggetti di dimensioni superiori a 1 MB. Non utilizzare la codifica di cancellazione per oggetti di dimensioni inferiori a 200 KB per evitare il sovraccarico dovuto alla gestione di frammenti molto piccoli con codifica di cancellazione.

Definizione della regola	Valore di esempio
Nome della regola	File immagine EC > 1 MB
Tempo di riferimento	Tempo di ingestione
Filtro avanzato per la dimensione dell'oggetto	Dimensione dell'oggetto maggiore di 1 MB
Filtri avanzati per la chiave	• Termina con .jpg • Termina con .png
Posizionamenti	Crea una copia con codice di cancellazione 2+1 utilizzando tre siti

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ✕

Object size ▼ greater than ▼ 1 ↕ MB ▼ ✕

and Key ▼ ends with ▼ .jpg ✕

or Filter group 2 Objects with all of following metadata will be evaluated by this rule: ✕

Object size ▼ greater than ▼ 1 ↕ MB ▼ ✕

and Key ▼ ends with ▼ .png ✕

Poiché questa regola è configurata come la prima regola del criterio, l'istruzione di posizionamento della codifica di cancellazione si applica solo ai file .jpg e .png di dimensioni superiori a 1 MB.

Regola ILM 2 per l'esempio 3: creare 2 copie replicate per tutti i file immagine rimanenti

Questa regola ILM di esempio utilizza un filtro avanzato per specificare che i file immagine più piccoli devono essere replicati. Poiché la prima regola del criterio ha già trovato corrispondenze con file immagine di dimensioni superiori a 1 MB, questa regola si applica ai file immagine di dimensioni pari o inferiori a 1 MB.

Definizione della regola	Valore di esempio
Nome della regola	2 copie per i file immagine

Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di ingestione
Filtri avanzati per la chiave	• Termina con .jpg • Termina con .png
Posizionamenti	Crea 2 copie replicate in due pool di archiviazione

Politica ILM per esempio 3: migliore protezione per i file immagine

Questo esempio di policy ILM include tre regole:

- La prima regola codifica tutti i file immagine di dimensioni superiori a 1 MB.
- La seconda regola crea due copie di tutti i file immagine rimanenti (ovvero immagini di dimensioni pari o inferiori a 1 MB).
- La regola predefinita si applica a tutti gli oggetti rimanenti (ovvero tutti i file non immagine).

Rule order	Rule name	Filters
1	EC image files > 1 MB	Object size is greater than 1 MB
2	2 copies for small images	Object size is less than or equal to 200 KB
Default	Default rule	—

Esempio 4: regole e policy ILM per oggetti con versione S3

Se disponi di un bucket S3 con il controllo delle versioni abilitato, puoi gestire le versioni degli oggetti non correnti includendo regole nella policy ILM che utilizzano "Tempo non corrente" come tempo di riferimento.



Se si specifica un periodo di conservazione limitato per gli oggetti, tali oggetti verranno eliminati definitivamente una volta raggiunto il periodo di tempo specificato. Assicuratevi di aver capito per quanto tempo gli oggetti verranno conservati.

Come mostra questo esempio, è possibile controllare la quantità di spazio di archiviazione utilizzato dagli oggetti sottoposti a controllo di versione utilizzando diverse istruzioni di posizionamento per le versioni non correnti degli oggetti.



Le seguenti regole e policy ILM sono solo esempi. Esistono molti modi per configurare le regole ILM. Prima di attivare una nuova policy, simulala per verificare che funzioni come previsto per proteggere i contenuti dalla perdita.



Per eseguire la simulazione dei criteri ILM su una versione non corrente di un oggetto, è necessario conoscere l'UUID o il CBID della versione dell'oggetto. Per trovare l'UUID e il CBID, utilizzare ["ricerca metadati oggetto"](#) mentre l'oggetto è ancora attuale.

Informazioni correlate

["Come vengono eliminati gli oggetti"](#)

Regola ILM 1 per esempio 4: Conservare tre copie per 10 anni

Questa regola ILM di esempio memorizza una copia di ciascun oggetto in tre siti per 10 anni.

Questa regola si applica a tutti gli oggetti, indipendentemente dal fatto che siano sottoposti a controllo di versione o meno.

Definizione della regola	Valore di esempio
Pool di stoccaggio	Tre pool di archiviazione, ciascuno composto da data center diversi, denominati Sito 1, Sito 2 e Sito 3.
Nome della regola	Tre copie dieci anni
Tempo di riferimento	Tempo di ingestione
Posizionamenti	Il giorno 0, conservare tre copie replicate per 10 anni (3.652 giorni), una nel sito 1, una nel sito 2 e una nel sito 3. Dopo 10 anni, eliminare tutte le copie dell'oggetto.

Regola ILM 2 per esempio 4: Salvare due copie delle versioni non correnti per 2 anni

Questa regola ILM di esempio memorizza due copie delle versioni non correnti di un oggetto con versione S3 per 2 anni.

Poiché la regola ILM 1 si applica a tutte le versioni dell'oggetto, è necessario creare un'altra regola per filtrare tutte le versioni non correnti.

Per creare una regola che utilizzi "Tempo non corrente" come orario di riferimento, seleziona **Sì** alla domanda "Applicare questa regola solo alle versioni precedenti degli oggetti (in bucket S3 con controllo delle versioni abilitato)?" nel passaggio 1 (Immetti dettagli) della procedura guidata Crea una regola ILM. Selezionando **Sì**, *Tempo non corrente* viene automaticamente selezionato come orario di riferimento e non è possibile selezionare un orario di riferimento diverso.

1

Enter details

2

Define placements

3

Select ingest behavior

Rule name

Older Object Versions: Two Copies Two Years

Description (optional)

Older versions only

Basic filters (optional)

Specify which tenant accounts and buckets this rule applies to.

Tenant accounts ?

Select tenant accounts

Bucket name ?

matches all

Apply this rule to older object versions only (in S3 buckets with versioning enabled)? ?

☐ No☒ Yes

In questo esempio, vengono archiviate solo due copie delle versioni non correnti, che verranno conservate per due anni.

Definizione della regola	Valore di esempio
Pool di archiviazione	Due pool di archiviazione, ciascuno in data center diversi, Sito 1 e Sito 2.
Nome della regola	Versioni non correnti: due copie due anni
Tempo di riferimento	Tempo non corrente Selezionato automaticamente quando si seleziona Sì alla domanda "Applicare questa regola solo alle versioni precedenti degli oggetti (in bucket S3 con controllo delle versioni abilitato)?" nella procedura guidata Crea una regola ILM.
Posizionamenti	Il giorno 0 relativo al tempo non corrente (ovvero a partire dal giorno in cui la versione dell'oggetto diventa la versione non corrente), conservare due copie replicate delle versioni dell'oggetto non corrente per 2 anni (730 giorni), una nel sito 1 e una nel sito 2. Dopo 2 anni, eliminare le versioni non correnti.

Criterio ILM per esempio 4: oggetti con versione S3

Se si desidera gestire le versioni precedenti di un oggetto in modo diverso rispetto alla versione corrente, le regole che utilizzano "Tempo non corrente" come orario di riferimento devono comparire nel criterio ILM prima delle regole che si applicano alla versione corrente dell'oggetto.

Una policy ILM per oggetti con versione S3 potrebbe includere regole ILM come le seguenti:

- Conservare tutte le versioni precedenti (non aggiornate) di ciascun oggetto per 2 anni, a partire dal giorno in cui la versione è diventata non aggiornata.



Le regole "Tempo non corrente" devono comparire nel criterio prima delle regole che si applicano alla versione corrente dell'oggetto. In caso contrario, le versioni degli oggetti non correnti non verranno mai abbinate dalla regola "Tempo non corrente".

- Al momento dell'ingestione, creare tre copie replicate e conservarne una copia in ciascuno dei tre siti. Conservare copie della versione corrente dell'oggetto per 10 anni.

Quando si simula la policy di esempio, ci si aspetterebbe che gli oggetti di prova vengano valutati come segue:

- Tutte le versioni non correnti degli oggetti verrebbero confrontate con la prima regola. Se una versione non corrente di un oggetto è più vecchia di 2 anni, ILM la elimina definitivamente (tutte le copie della versione non corrente vengono rimosse dalla griglia).
- La versione corrente dell'oggetto verrebbe abbinata alla seconda regola. Quando la versione corrente dell'oggetto è stata archiviata per 10 anni, il processo ILM aggiunge un marcatore di eliminazione come versione corrente dell'oggetto e rende la versione precedente dell'oggetto "non corrente". La prossima volta che si verifica la valutazione ILM, questa versione non corrente viene abbinata alla prima regola. Di conseguenza, la copia nel Sito 3 viene eliminata e le due copie nel Sito 1 e nel Sito 2 vengono conservate per altri 2 anni.

Esempio 5: regole e policy ILM per un comportamento di acquisizione rigoroso

È possibile utilizzare un filtro di posizione e il comportamento di acquisizione Rigoroso in una regola per impedire che gli oggetti vengano salvati in una posizione specifica del data center.

In questo esempio, un inquilino con sede a Parigi non vuole immagazzinare alcuni oggetti al di fuori dell'UE a causa di problemi normativi. Altri oggetti, compresi tutti gli oggetti provenienti da altri account tenant, possono essere archiviati nel data center di Parigi o in quello degli Stati Uniti.



Le seguenti regole e policy ILM sono solo esempi. Esistono molti modi per configurare le regole ILM. Prima di attivare una nuova policy, simulala per verificare che funzioni come previsto per proteggere i contenuti dalla perdita.

Informazioni correlate

- ["Opzioni di acquisizione"](#)
- ["Crea regola ILM: seleziona il comportamento di acquisizione"](#)

Regola ILM 1 per esempio 5: Ingestione rigorosa per garantire il data center di Parigi

Questa regola ILM di esempio utilizza il comportamento di ingestione Strict per garantire che gli oggetti salvati da un tenant con sede a Parigi nei bucket S3 con la regione impostata su eu-west-3 (Parigi) non vengano mai

archiviati nel data center statunitense.

Questa regola si applica agli oggetti che appartengono al tenant di Parigi e che hanno la regione del bucket S3 impostata su eu-west-3 (Parigi).

Definizione della regola	Valore di esempio
Conto inquilino	inquilino di Parigi
Filtro avanzato	Il vincolo di posizione è uguale a eu-west-3
Pool di stoccaggio	Sito 1 (Parigi)
Nome della regola	Rigoroso inserimento per garantire il data center di Parigi
Tempo di riferimento	Tempo di ingestione
Posizionamenti	Il giorno 0, conserva due copie replicate per sempre nel sito 1 (Parigi)
Comportamento di ingestione	Rigoroso. Utilizzare sempre i posizionamenti di questa regola durante l'acquisizione. L'acquisizione fallisce se non è possibile archiviare due copie dell'oggetto nel data center di Parigi.

Strict ingest to guarantee Paris data center

Compliant: Yes

Used in active policy: No

Used in proposed policy: No

Ingest behavior: Strict

Reference time: Ingest time

Clone

Edit

Remove

Filters

This rule applies if:

- Tenant is Paris tenant

And it only applies if objects have this metadata:

- Location constraint is eu-west-3

Time period and placements

Retention diagram

Placement instructions

Sort placements by

Time period

Storage pool

● Replicated copy

Rule analysis:

- StorageGRID site-loss protection will not apply from Day 0 - Forever.
- Objects processed by this rule will not be deleted by ILM.

Reference time: Ingest time

Ingest behavior: Strict

Day 0

Day 0 - forever

2 replicated copies - Site 1

Duration

Forever

410

Regola ILM 2 per esempio 5: Ingestione bilanciata per altri oggetti

Questa regola ILM di esempio utilizza il comportamento di acquisizione bilanciato per garantire un'efficienza ILM ottimale per tutti gli oggetti non corrispondenti alla prima regola. Verranno conservate due copie di tutti gli oggetti che soddisfano questa regola: una nel centro dati degli Stati Uniti e una nel centro dati di Parigi. Se la regola non può essere soddisfatta immediatamente, vengono conservate copie provvisorie in qualsiasi posizione disponibile.

Questa regola si applica agli oggetti che appartengono a qualsiasi tenant e a qualsiasi regione.

Definizione della regola	Valore di esempio
Conto inquilino	Ignorare
Filtro avanzato	<i>Non specificato</i>
Pool di stoccaggio	Sito 1 (Parigi) e Sito 2 (Stati Uniti)
Nome della regola	2 copie 2 data center
Tempo di riferimento	Tempo di ingestione
Posizionamenti	Il giorno 0, conserva due copie replicate per sempre in due data center
Comportamento di ingestione	Equilibrato. Se possibile, gli oggetti che corrispondono a questa regola vengono posizionati secondo le istruzioni di posizionamento della regola. In caso contrario, vengono effettuate copie provvisorie in qualsiasi luogo disponibile.

Politica ILM per l'esempio 5: combinazione di comportamenti di acquisizione

L'esempio di policy ILM include due regole con comportamenti di acquisizione diversi.

Una policy ILM che utilizza due diversi comportamenti di acquisizione potrebbe includere regole ILM come le seguenti:

- Archiviare gli oggetti che appartengono al tenant di Parigi e che hanno la regione del bucket S3 impostata su eu-west-3 (Parigi) solo nel data center di Parigi. L'acquisizione non riesce se il data center di Parigi non è disponibile.
- Archiviare tutti gli altri oggetti (inclusi quelli che appartengono al tenant di Parigi ma che hanno una regione bucket diversa) sia nel data center statunitense che in quello di Parigi. Se non è possibile soddisfare le istruzioni di posizionamento, effettuare copie provvisorie in qualsiasi luogo disponibile.

Quando si simula la policy di esempio, ci si aspetta che gli oggetti di prova vengano valutati come segue:

- Tutti gli oggetti che appartengono al tenant di Parigi e che hanno la regione del bucket S3 impostata su eu-west-3 vengono abbinati alla prima regola e vengono archiviati nel data center di Parigi. Poiché la prima regola utilizza l'acquisizione rigorosa, questi oggetti non vengono mai archiviati nel data center statunitense. Se i nodi di archiviazione nel data center di Parigi non sono disponibili, l'acquisizione fallisce.
- Tutti gli altri oggetti vengono abbinati dalla seconda regola, compresi gli oggetti che appartengono al tenant di Parigi e che non hanno la regione del bucket S3 impostata su eu-west-3. In ogni data center viene

salvata una copia di ogni oggetto. Tuttavia, poiché la seconda regola utilizza l'acquisizione bilanciata, se un data center non è disponibile, vengono salvate due copie provvisorie in qualsiasi posizione disponibile.

Esempio 6: Modificare una policy ILM

Se è necessario modificare la protezione dei dati o aggiungere nuovi siti, è possibile creare e attivare una nuova policy ILM.

Prima di modificare una policy, è necessario comprendere in che modo le modifiche ai posizionamenti ILM possono influire temporaneamente sulle prestazioni complessive di un sistema StorageGRID .

In questo esempio, è stato aggiunto un nuovo sito StorageGRID in un'espansione ed è necessario implementare una nuova policy ILM attiva per archiviare i dati nel nuovo sito. Per implementare una nuova politica attiva, prima **"creare una politica"** . Dopodiché, devi **"simulare"** poi **"attivare"** la nuova politica.



Le seguenti regole e policy ILM sono solo esempi. Esistono molti modi per configurare le regole ILM. Prima di attivare una nuova policy, simulala per verificare che funzioni come previsto per proteggere i contenuti dalla perdita.

Come la modifica di una policy ILM influisce sulle prestazioni

Quando si attiva una nuova policy ILM, le prestazioni del sistema StorageGRID potrebbero essere temporaneamente compromesse, soprattutto se le istruzioni di posizionamento nella nuova policy richiedono lo spostamento di molti oggetti esistenti in nuove posizioni.

Quando si attiva una nuova policy ILM, StorageGRID la utilizza per gestire tutti gli oggetti, compresi quelli esistenti e quelli appena acquisiti. Prima di attivare una nuova policy ILM, rivedere tutte le modifiche apportate al posizionamento degli oggetti replicati e con codice di cancellazione esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi temporanei di risorse quando i nuovi posizionamenti vengono valutati e implementati.

Per garantire che una nuova policy ILM non influisca sul posizionamento degli oggetti replicati e codificati per la cancellazione esistenti, è possibile **"creare una regola ILM con un filtro temporale di acquisizione"** . Ad esempio, **L'ora di ingestione è uguale o successiva <data e ora>**, in modo che la nuova regola si applichi solo agli oggetti ingeriti nella data e ora specificate o successivamente.

I tipi di modifiche ai criteri ILM che possono influire temporaneamente sulle prestazioni StorageGRID includono quanto segue:

- Applicazione di un profilo di codifica di cancellazione diverso agli oggetti con codifica di cancellazione esistenti.



StorageGRID considera ogni profilo di codifica di cancellazione come univoco e non riutilizza i frammenti di codifica di cancellazione quando viene utilizzato un nuovo profilo.

- Modifica del tipo di copie richieste per gli oggetti esistenti; ad esempio, convertendo una grande percentuale di oggetti replicati in oggetti con codice di cancellazione.
- Spostamento di copie di oggetti esistenti in una posizione completamente diversa; ad esempio, spostamento di un gran numero di oggetti da o verso un pool di archiviazione cloud o da o verso un sito remoto.

Criterio ILM attivo per esempio 6: Protezione dei dati in due siti

In questo esempio, la policy ILM attiva è stata inizialmente progettata per un sistema StorageGRID a due siti e utilizza due regole ILM.

Active policy

Policy history

Policy name:

Data Protection for Two Sites (2 rules)

Reason for change :

Data protection for two sites (using 2 rules)

Start date:

2022-10-11 10:37:11 MDT

Simulate

Policy rules

Retention diagram

Rule order ?	Rule name	Filters ?
1	One-Site Erasure Coding for Tenant A	Tenant is Tenant A
Default	Two-Site Replication for Other Tenants	—

In questa policy ILM, gli oggetti appartenenti al tenant A sono protetti tramite codifica di cancellazione 2+1 in un singolo sito, mentre gli oggetti appartenenti a tutti gli altri tenant sono protetti su due siti tramite replica a 2 copie.

Regola 1: Codifica di cancellazione in un unico sito per l'inquilino A

Definizione della regola	Valore di esempio
Nome della regola	Codifica di cancellazione in un unico sito per l'inquilino A
Conto inquilino	Inquilino A
Pool di archiviazione	Sito 1
Posizionamenti	Codifica di cancellazione 2+1 nel sito 1 dal giorno 0 all'infinito

Regola 2: Replicazione a due siti per altri tenant

Definizione della regola	Valore di esempio
Nome della regola	Replica a due siti per altri tenant
Conto inquilino	Ignorare
Pool di archiviazione	Sito 1 e Sito 2

Definizione della regola	Valore di esempio
Posizionamenti	Due copie replicate dal giorno 0 all'infinito: una copia nel Sito 1 e una copia nel Sito 2.

Politica ILM per esempio 6: Protezione dei dati in tre siti

In questo esempio, la policy ILM viene sostituita con una nuova policy per un sistema StorageGRID a tre siti.

Dopo aver eseguito un'espansione per aggiungere il nuovo sito, l'amministratore della griglia ha creato due nuovi pool di archiviazione: un pool di archiviazione per il sito 3 e un pool di archiviazione contenente tutti e tre i siti (diverso dal pool di archiviazione predefinito Tutti i nodi di archiviazione). Quindi, l'amministratore ha creato due nuove regole ILM e una nuova policy ILM, studiate per proteggere i dati in tutti e tre i siti.

Quando questa nuova policy ILM verrà attivata, gli oggetti appartenenti al Tenant A saranno protetti tramite codifica di cancellazione 2+1 in tre siti, mentre gli oggetti appartenenti ad altri tenant (e oggetti più piccoli appartenenti al Tenant A) saranno protetti in tre siti tramite replica a 3 copie.

Regola 1: Codifica di cancellazione a tre siti per l'inquilino A

Definizione della regola	Valore di esempio
Nome della regola	Codifica di cancellazione a tre siti per l'inquilino A
Conto inquilino	Inquilino A
Pool di archiviazione	Tutti e 3 i siti (include il sito 1, il sito 2 e il sito 3)
Posizionamenti	Codifica di cancellazione 2+1 in tutti e 3 i siti dal giorno 0 all'infinito

Regola 2: Replicazione a tre siti per altri tenant

Definizione della regola	Valore di esempio
Nome della regola	Replica a tre siti per altri tenant
Conto inquilino	Ignorare
Pool di archiviazione	Sito 1, Sito 2 e Sito 3
Posizionamenti	Tre copie replicate dal giorno 0 all'infinito: una copia nel Sito 1, una copia nel Sito 2 e una copia nel Sito 3.

Attivazione della politica ILM ad esempio 6

Quando si attiva una nuova policy ILM, gli oggetti esistenti potrebbero essere spostati in nuove posizioni oppure potrebbero essere create nuove copie degli oggetti esistenti, in base alle istruzioni di posizionamento contenute in eventuali regole nuove o aggiornate.



Gli errori in una policy ILM possono causare una perdita di dati irrecuperabile. Esaminare attentamente e simulare la policy prima di attivarla per confermare che funzionerà come previsto.



Quando si attiva una nuova policy ILM, StorageGRID la utilizza per gestire tutti gli oggetti, compresi quelli esistenti e quelli appena acquisiti. Prima di attivare una nuova policy ILM, rivedere tutte le modifiche apportate al posizionamento degli oggetti replicati e con codice di cancellazione esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi temporanei di risorse quando i nuovi posizionamenti vengono valutati e implementati.

Cosa succede quando cambiano le istruzioni di codifica di cancellazione

Nella policy ILM attualmente attiva per questo esempio, gli oggetti appartenenti al Tenant A sono protetti mediante la codifica di cancellazione 2+1 nel Sito 1. Nella nuova politica ILM, gli oggetti appartenenti al Tenant A saranno protetti mediante la codifica di cancellazione 2+1 nei siti 1, 2 e 3.

Quando viene attivata la nuova policy ILM, si verificano le seguenti operazioni ILM:

- I nuovi oggetti acquisiti dal Tenant A vengono suddivisi in due frammenti di dati e viene aggiunto un frammento di parità. Quindi, ciascuno dei tre frammenti viene conservato in un sito diverso.
- Gli oggetti esistenti appartenenti al Tenant A vengono rivalutati durante il processo di scansione ILM in corso. Poiché le istruzioni di posizionamento ILM utilizzano un nuovo profilo di codifica di cancellazione, vengono creati e distribuiti ai tre siti frammenti completamente nuovi con codifica di cancellazione.



I frammenti 2+1 esistenti nel Sito 1 non vengono riutilizzati. StorageGRID considera ogni profilo di codifica di cancellazione come univoco e non riutilizza i frammenti di codifica di cancellazione quando viene utilizzato un nuovo profilo.

Cosa succede quando cambiano le istruzioni di replicazione

Nella policy ILM attualmente attiva per questo esempio, gli oggetti appartenenti ad altri tenant vengono protetti mediante due copie replicate nei pool di archiviazione nei siti 1 e 2. Nella nuova policy ILM, gli oggetti appartenenti ad altri tenant saranno protetti mediante tre copie replicate in pool di archiviazione nei siti 1, 2 e 3.

Quando viene attivata la nuova policy ILM, si verificano le seguenti operazioni ILM:

- Quando un tenant diverso dal tenant A acquisisce un nuovo oggetto, StorageGRID ne crea tre copie e ne salva una in ogni sito.
- Gli oggetti esistenti appartenenti a questi altri inquilini vengono rivalutati durante il processo di scansione ILM in corso. Poiché le copie degli oggetti esistenti nel Sito 1 e nel Sito 2 continuano a soddisfare i requisiti di replicazione della nuova regola ILM, StorageGRID deve creare solo una nuova copia dell'oggetto per il Sito 3.

Impatto sulle prestazioni dell'attivazione di questa policy

Quando viene attivata la policy ILM in questo esempio, le prestazioni complessive del sistema StorageGRID saranno temporaneamente compromesse. Saranno necessari livelli di risorse di rete superiori al normale per creare nuovi frammenti con codice di cancellazione per gli oggetti esistenti del Tenant A e nuove copie replicate nel Sito 3 per gli oggetti esistenti degli altri tenant.

A seguito della modifica della policy ILM, le richieste di lettura e scrittura dei client potrebbero temporaneamente presentare latenze superiori al normale. Le latenze torneranno ai livelli normali dopo che le

istruzioni di posizionamento saranno state completamente implementate nella griglia.

Per evitare problemi di risorse durante l'attivazione di un nuovo criterio ILM, è possibile utilizzare il filtro avanzato Tempo di acquisizione in qualsiasi regola che potrebbe modificare la posizione di un gran numero di oggetti esistenti. Impostare il tempo di acquisizione su un valore maggiore o uguale al momento approssimativo in cui la nuova policy entrerà in vigore, per garantire che gli oggetti esistenti non vengano spostati inutilmente.



Contattare l'assistenza tecnica se è necessario rallentare o aumentare la velocità di elaborazione degli oggetti dopo una modifica della policy ILM.

Esempio 7: Politica ILM conforme per S3 Object Lock

È possibile utilizzare il bucket S3, le regole ILM e la policy ILM in questo esempio come punto di partenza quando si definisce una policy ILM per soddisfare i requisiti di protezione e conservazione degli oggetti nei bucket con S3 Object Lock abilitato.



Se hai utilizzato la funzionalità di conformità legacy nelle versioni precedenti StorageGRID , puoi utilizzare questo esempio anche per gestire eventuali bucket esistenti in cui è abilitata la funzionalità di conformità legacy.



Le seguenti regole e policy ILM sono solo esempi. Esistono molti modi per configurare le regole ILM. Prima di attivare una nuova policy, simulala per verificare che funzioni come previsto per proteggere i contenuti dalla perdita.

Informazioni correlate

- ["Gestisci gli oggetti con S3 Object Lock"](#)
- ["Creare una policy ILM"](#)

Esempio di bucket e oggetti per S3 Object Lock

In questo esempio, un account tenant S3 denominato Bank of ABC ha utilizzato Tenant Manager per creare un bucket con S3 Object Lock abilitato per archiviare i record bancari critici.

Definizione di bucket	Valore di esempio
Nome dell'account dell'inquilino	Banca ABC
Nome del bucket	registri bancari
Regione del bucket	us-east-1 (predefinito)

Ogni oggetto e versione dell'oggetto che viene aggiunto al bucket dei record bancari utilizzerà i seguenti valori per `retain-until-date` E `legal hold` impostazioni.

Impostazione per ogni oggetto	Valore di esempio
<code>retain-until-date</code>	"2030-12-30T23:59:59Z" (30 dicembre 2030) Ogni versione dell'oggetto ha la sua <code>retain-until-date</code> collocamento. Questa impostazione può essere aumentata, ma non diminuita.
<code>legal hold</code>	"OFF" (Non in vigore) È possibile applicare o rimuovere un blocco legale su qualsiasi versione dell'oggetto in qualsiasi momento durante il periodo di conservazione. Se un oggetto è sottoposto a una sospensione legale, l'oggetto non può essere eliminato anche se <code>retain-until-date</code> è stato raggiunto.

Regola ILM 1 per esempio di blocco oggetto S3: profilo di codifica di cancellazione con corrispondenza bucket

Questa regola ILM di esempio si applica solo al conto tenant S3 denominato Bank of ABC. Corrisponde a qualsiasi oggetto nel `bank-records` bucket e quindi utilizza la codifica di cancellazione per archiviare l'oggetto sui nodi di archiviazione in tre siti di data center utilizzando un profilo di codifica di cancellazione 6+3. Questa regola soddisfa i requisiti del bucket con S3 Object Lock abilitato: una copia viene conservata sui nodi di archiviazione dal giorno 0 all'infinito, utilizzando l'ora di ingestione come ora di riferimento.

Definizione della regola	Valore di esempio
Nome della regola	Regola conforme: Oggetti EC nel bucket dei registri bancari - Bank of ABC
Conto inquilino	Banca ABC
Nome del bucket	<code>bank-records</code>
Filtro avanzato	Dimensione oggetto (MB) maggiore di 1 Nota: questo filtro garantisce che la codifica di cancellazione non venga utilizzata per oggetti di dimensioni pari o inferiori a 1 MB.

Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di ingestione
Posizionamenti	Dal giorno 0 conservalo per sempre
Profilo di codifica di cancellazione	• Creare una copia con codice di cancellazione sui nodi di archiviazione in tre siti di data center • Utilizza lo schema di codifica di cancellazione 6+3

Esempio di regola ILM 2 per blocco oggetto S3: regola non conforme

Questa regola ILM di esempio memorizza inizialmente due copie replicate dell'oggetto sui nodi di archiviazione. Dopo un anno, ne memorizza una copia per sempre su un Cloud Storage Pool. Poiché questa regola utilizza un Cloud Storage Pool, non è conforme e non verrà applicata agli oggetti nei bucket con S3 Object Lock abilitato.

Definizione della regola	Valore di esempio
Nome della regola	Regola non conforme: utilizzare Cloud Storage Pool
Conti degli inquilini	Non specificato
Nome del bucket	Non specificato, ma si applicherà solo ai bucket in cui non è abilitato S3 Object Lock (o la funzionalità legacy Compliance).
Filtro avanzato	Non specificato

Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di ingestione
Posizionamenti	• Il giorno 0, conserva due copie replicate sui nodi di archiviazione nel Data Center 1 e nel Data Center 2 per 365 giorni • Dopo 1 anno, conserva una copia replicata in un Cloud Storage Pool per sempre

Regola ILM 3 per esempio di blocco oggetto S3: regola predefinita

Questa regola ILM di esempio copia i dati degli oggetti nei pool di archiviazione in due data center. Questa regola conforme è concepita per essere la regola predefinita nella policy ILM. Non include alcun filtro, non utilizza il tempo di riferimento non corrente e soddisfa i requisiti dei bucket con S3 Object Lock abilitato: due copie dell'oggetto vengono conservate sui nodi di archiviazione dal giorno 0 all'infinito, utilizzando Ingest come tempo di riferimento.

Definizione della regola	Valore di esempio
Nome della regola	Regola di conformità predefinita: due copie, due data center
Conto inquilino	Non specificato
Nome del bucket	Non specificato
Filtro avanzato	Non specificato

Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di ingestione

Definizione della regola	Valore di esempio
Posizionamenti	Dal giorno 0 all'infinito, conserva due copie replicate: una sui nodi di archiviazione nel Data Center 1 e una sui nodi di archiviazione nel Data Center 2.

Esempio di policy ILM conforme per S3 Object Lock

Per creare una policy ILM che protegga efficacemente tutti gli oggetti nel sistema, compresi quelli nei bucket con S3 Object Lock abilitato, è necessario selezionare le regole ILM che soddisfano i requisiti di archiviazione per tutti gli oggetti. Quindi, è necessario simulare e attivare la policy.

Aggiungere regole alla policy

In questo esempio, la policy ILM include tre regole ILM, nel seguente ordine:

1. Una regola conforme che utilizza la codifica di cancellazione per proteggere gli oggetti di dimensioni superiori a 1 MB in un bucket specifico con S3 Object Lock abilitato. Gli oggetti vengono archiviati sui nodi di archiviazione dal giorno 0 all'infinito.
2. Una regola non conforme che crea due copie replicate dell'oggetto sui nodi di archiviazione per un anno e poi sposta una copia dell'oggetto in un pool di archiviazione cloud per sempre. Questa regola non si applica ai bucket con S3 Object Lock abilitato perché utilizza un Cloud Storage Pool.
3. La regola di conformità predefinita che crea due copie replicate degli oggetti sui nodi di archiviazione dal giorno 0 all'infinito.

Simulare la politica

Dopo aver aggiunto regole alla policy, scelto una regola conforme predefinita e organizzato le altre regole, dovresti simulare la policy testando gli oggetti dal bucket con S3 Object Lock abilitato e da altri bucket. Ad esempio, quando si simula la policy di esempio, ci si aspetterebbe che gli oggetti di prova vengano valutati come segue:

- La prima regola corrisponderà solo agli oggetti di prova che sono maggiori di 1 MB nel bucket bank-records per il tenant Bank of ABC.
- La seconda regola corrisponderà a tutti gli oggetti in tutti i bucket non conformi per tutti gli altri account tenant.
- La regola predefinita corrisponderà a questi oggetti:
 - Oggetti di dimensioni pari o inferiori a 1 MB nel bucket bank-records per il tenant Bank of ABC.
 - Oggetti in qualsiasi altro bucket in cui è abilitato il blocco oggetti S3 per tutti gli altri account tenant.

Attiva la politica

Quando sei completamente soddisfatto che la nuova policy protegga i dati degli oggetti come previsto, puoi attivarla.

Esempio 8: Priorità per il ciclo di vita del bucket S3 e policy ILM

A seconda della configurazione del ciclo di vita, gli oggetti seguono le impostazioni di conservazione del ciclo di vita del bucket S3 o di un criterio ILM.

Esempio di ciclo di vita del bucket che ha la priorità sulla policy ILM

Politica ILM

- Regola basata sul riferimento temporale non corrente: il giorno 0, conserva X copie per 20 giorni
- Regola basata sul riferimento al momento dell'acquisizione (predefinita): il giorno 0, conserva X copie per 50 giorni

Ciclo di vita del bucket

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"Days": 100},  
"NoncurrentVersionExpiration": {"NoncurrentDays": 5}
```

Risultato

- Viene acquisito un oggetto denominato "docs/text". Corrisponde al filtro del ciclo di vita del bucket del prefisso "docs/".
 - Dopo 100 giorni viene creato un marcatore di eliminazione e "docs/text" diventa non corrente.
 - Dopo 5 giorni, per un totale di 105 giorni dall'acquisizione, "docs/text" viene eliminato.
 - Dopo 95 giorni, per un totale di 200 giorni dall'inserimento e 100 giorni dalla creazione del delete-marker, il delete-marker scaduto viene eliminato.
- Viene acquisito un oggetto denominato "video/film". Non corrisponde al filtro e utilizza il criterio di conservazione ILM.
 - Dopo 50 giorni viene creato un marcatore di eliminazione e "video/film" diventa non corrente.
 - Dopo 20 giorni, ovvero 70 giorni in totale dall'acquisizione, "video/film" viene eliminato.
 - Dopo 30 giorni, per un totale di 100 giorni dall'inserimento e 50 giorni dalla creazione del delete-marker, il delete-marker scaduto viene eliminato.

Esempio di ciclo di vita del bucket che mantiene implicitamente per sempre

Politica ILM

- Regola basata sul riferimento temporale non corrente: il giorno 0, conserva X copie per 20 giorni
- Regola basata sul riferimento al momento dell'acquisizione (predefinita): il giorno 0, conserva X copie per 50 giorni

Ciclo di vita del bucket

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"ExpiredObjectDeleteMarker":  
true}
```

Risultato

- Viene acquisito un oggetto denominato "docs/text". Corrisponde al filtro del ciclo di vita del bucket del prefisso "docs/".

IL `Expiration` l'azione si applica solo ai marcatori di eliminazione scaduti, il che implica il mantenimento di tutto il resto per sempre (a partire da "docs/").

I marcatori di eliminazione che iniziano con "docs/" vengono rimossi quando scadono.

- Viene acquisito un oggetto denominato "video/film". Non corrisponde al filtro e utilizza il criterio di conservazione ILM.
 - Dopo 50 giorni viene creato un marcatore di eliminazione e "video/film" diventa non corrente.

- Dopo 20 giorni, ovvero 70 giorni in totale dall'acquisizione, "video/film" viene eliminato.
- Dopo 30 giorni, per un totale di 100 giorni dall'inserimento e 50 giorni dalla creazione del delete-marker, il delete-marker scaduto viene eliminato.

Esempio di utilizzo del ciclo di vita del bucket per duplicare ILM e ripulire i marcatori di eliminazione scaduti

Politica ILM

- Regola basata sul riferimento temporale non corrente: il giorno 0, conserva X copie per 20 giorni
- Regola basata sul riferimento al momento dell'acquisizione (predefinita): il giorno 0, conserva X copie per sempre

Ciclo di vita del bucket

```
"Filter": {}, "Expiration": {"ExpiredObjectDeleteMarker": true},
"NoncurrentVersionExpiration": {"NoncurrentDays": 20}
```

Risultato

- La policy ILM viene duplicata nel ciclo di vita del bucket.
 - La regola "per sempre" della policy ILM è progettata per rimuovere manualmente gli oggetti e ripulire le versioni non correnti dopo 20 giorni. Di conseguenza, la regola ingest-time manterrà per sempre i marcatori di eliminazione scaduti.
 - Il ciclo di vita del bucket duplica il comportamento della policy ILM durante l'aggiunta "ExpiredObjectDeleteMarker": true, che rimuove i marcatori di eliminazione una volta scaduti
- Un oggetto viene ingerito. Nessun filtro significa che il ciclo di vita del bucket si applica a tutti gli oggetti e sostituisce le impostazioni di conservazione ILM.
 - Quando un tenant invia una richiesta di eliminazione di un oggetto, viene creato un marcatore di eliminazione e l'oggetto diventa non corrente.
 - Dopo 20 giorni, l'oggetto non corrente viene eliminato e il marcatore di eliminazione scade.
 - Poco dopo, il marcatore di eliminazione scaduto viene eliminato.

Rafforzamento del sistema

Considerazioni generali per il rafforzamento del sistema

Il rafforzamento del sistema è il processo di eliminazione del maggior numero possibile di rischi per la sicurezza da un sistema StorageGRID .

Durante l'installazione e la configurazione StorageGRID, utilizzare queste linee guida per soddisfare gli obiettivi di sicurezza prescritti in termini di riservatezza, integrità e disponibilità.

Dovresti già utilizzare le best practice standard del settore per il rafforzamento del sistema. Ad esempio, si utilizzano password complesse per StorageGRID, si utilizza HTTPS anziché HTTP e si abilita l'autenticazione basata su certificato, ove disponibile.

StorageGRID segue il ["Politica di gestione delle vulnerabilità NetApp"](#) . Le vulnerabilità segnalate vengono verificate e affrontate in base al processo di risposta agli incidenti di sicurezza del prodotto.

Quando si rafforza un sistema StorageGRID , tenere presente quanto segue:

- ***Quale delle tre reti StorageGRID * hai implementato?** Tutti i sistemi StorageGRID devono utilizzare la rete Grid, ma è possibile utilizzare anche la rete amministrativa, la rete client o entrambe. Ogni rete ha diverse considerazioni in materia di sicurezza.
- **Il tipo di piattaforme** utilizzate per i singoli nodi nel sistema StorageGRID . I nodi StorageGRID possono essere distribuiti su macchine virtuali VMware, all'interno di un motore di container su host Linux o come dispositivi hardware dedicati. Ogni tipo di piattaforma ha il suo insieme di best practice di rafforzamento.
- **Quanto sono affidabili gli account degli inquilini.** Se sei un fornitore di servizi con account tenant non attendibili, avrai problemi di sicurezza diversi rispetto a quando utilizzi solo tenant interni attendibili.
- **Quali requisiti e convenzioni di sicurezza** segue la tua organizzazione. Potrebbe essere necessario rispettare specifici requisiti normativi o aziendali.

Linee guida per il rafforzamento degli aggiornamenti software

Per difendersi dagli attacchi, è necessario mantenere aggiornati il sistema StorageGRID e i servizi correlati.

Aggiornamenti al software StorageGRID

Se possibile, è consigliabile aggiornare il software StorageGRID alla versione principale più recente o a quella precedente. Mantenere StorageGRID aggiornato aiuta a ridurre il tempo di attività delle vulnerabilità note e riduce la superficie complessiva di attacco. Inoltre, le versioni più recenti di StorageGRID spesso contengono funzionalità di rafforzamento della sicurezza non incluse nelle versioni precedenti.

Consultare il "[Strumento matrice di interoperabilità NetApp](#)" (IMT) per determinare quale versione del software StorageGRID dovresti utilizzare. Quando è necessario un hotfix, NetApp dà priorità alla creazione di aggiornamenti per le versioni più recenti. Alcune patch potrebbero non essere compatibili con le versioni precedenti.

- Per scaricare le versioni e gli hotfix più recenti StorageGRID , vai a "[Download NetApp : StorageGRID](#)" .
- Per aggiornare il software StorageGRID , vedere "[Istruzioni per l'aggiornamento](#)" .
- Per applicare un hotfix, vedere "[Procedura di hotfix di StorageGRID](#)" .

Aggiornamenti ai servizi esterni

I servizi esterni possono presentare vulnerabilità che influiscono indirettamente StorageGRID . È necessario assicurarsi che i servizi da cui dipende StorageGRID siano sempre aggiornati. Questi servizi includono LDAP, KMS (o server KMIP), DNS e NTP.

Per un elenco delle versioni supportate, vedere "[Strumento matrice di interoperabilità NetApp](#)" .

Aggiornamenti agli hypervisor

Se i nodi StorageGRID sono in esecuzione su VMware o su un altro hypervisor, è necessario assicurarsi che il software e il firmware dell'hypervisor siano aggiornati.

Per un elenco delle versioni supportate, vedere "[Strumento matrice di interoperabilità NetApp](#)" .

Aggiornamenti ai nodi Linux

Se i nodi StorageGRID utilizzano piattaforme host Linux, è necessario assicurarsi che gli aggiornamenti di sicurezza e del kernel vengano applicati al sistema operativo host. Inoltre, è necessario applicare gli aggiornamenti del firmware all'hardware vulnerabile quando questi aggiornamenti diventano disponibili.

Per un elenco delle versioni supportate, vedere ["Strumento matrice di interoperabilità NetApp"](#) .

Linee guida per il rafforzamento delle reti StorageGRID

Il sistema StorageGRID supporta fino a tre interfacce di rete per nodo della griglia, consentendo di configurare la rete per ogni singolo nodo della griglia in base ai requisiti di sicurezza e accesso.

Per informazioni dettagliate sulle reti StorageGRID , vedere ["Tipi di rete StorageGRID"](#) .

Linee guida per la rete Grid

È necessario configurare una rete Grid per tutto il traffico StorageGRID interno. Tutti i nodi della griglia sono sulla rete Grid e devono essere in grado di comunicare con tutti gli altri nodi.

Durante la configurazione della rete Grid, seguire queste linee guida:

- Assicurarsi che la rete sia protetta da client non attendibili, come quelli presenti su Internet.
- Se possibile, utilizzare la rete Grid esclusivamente per il traffico interno. Sia la rete amministrativa che la rete client presentano ulteriori restrizioni firewall che bloccano il traffico esterno verso i servizi interni. È supportato l'utilizzo della Grid Network per il traffico client esterno, ma questo utilizzo offre meno livelli di protezione.
- Se la distribuzione StorageGRID si estende su più data center, utilizzare una rete privata virtuale (VPN) o equivalente sulla rete Grid per fornire ulteriore protezione al traffico interno.
- Alcune procedure di manutenzione richiedono l'accesso Secure Shell (SSH) sulla porta 22 tra il nodo di amministrazione primario e tutti gli altri nodi della griglia. Utilizzare un firewall esterno per limitare l'accesso SSH ai client attendibili.

Linee guida per la rete di amministrazione

La rete di amministrazione viene in genere utilizzata per attività amministrative (dipendenti fidati che utilizzano Grid Manager o SSH) e per comunicare con altri servizi fidati quali LDAP, DNS, NTP o KMS (o server KMIP). Tuttavia, StorageGRID non impone questo utilizzo internamente.

Se si utilizza Admin Network, seguire queste linee guida:

- Bloccare tutte le porte di traffico interno sulla rete di amministrazione. Vedi il ["elenco delle porte interne"](#) .
- Se i client non attendibili riescono ad accedere alla rete di amministrazione, bloccare l'accesso a StorageGRID sulla rete di amministrazione con un firewall esterno.

Linee guida per la rete clienti

La rete client viene in genere utilizzata per i tenant e per comunicare con servizi esterni, come il servizio di replica CloudMirror o un altro servizio della piattaforma. Tuttavia, StorageGRID non impone questo utilizzo internamente.

Se si utilizza la rete client, seguire queste linee guida:

- Blocca tutte le porte di traffico interno sulla rete client. Vedi il ["elenco delle porte interne"](#) .
- Accetta il traffico client in entrata solo sugli endpoint configurati in modo esplicito. Vedi le informazioni su ["gestione dei controlli del firewall"](#) .

Linee guida per il rafforzamento dei nodi StorageGRID

I nodi StorageGRID possono essere distribuiti su macchine virtuali VMware, all'interno di un motore di container su host Linux o come dispositivi hardware dedicati. Ogni tipo di piattaforma e ogni tipo di nodo ha il suo insieme di best practice di rafforzamento.

Controllare l'accesso IPMI remoto a BMC

È possibile abilitare o disabilitare l'accesso IPMI remoto per tutti gli apparecchi che contengono un BMC. L'interfaccia IPMI remota consente l'accesso hardware di basso livello ai dispositivi StorageGRID a chiunque disponga di un account e di una password BMC. Se non è necessario l'accesso IPMI remoto al BMC, disabilitare questa opzione.

- Per controllare l'accesso IPMI remoto al BMC in Grid Manager, andare su **CONFIGURAZIONE > Sicurezza > Impostazioni di sicurezza > Appliance**:
 - Deselezionare la casella di controllo **Abilita accesso IPMI remoto** per disabilitare l'accesso IPMI al BMC.
 - Selezionare la casella di controllo **Abilita accesso IPMI remoto** per abilitare l'accesso IPMI al BMC.

Configurazione del firewall

Come parte del processo di rafforzamento del sistema, è necessario rivedere le configurazioni del firewall esterno e modificarle in modo che il traffico venga accettato solo dagli indirizzi IP e sulle porte da cui è strettamente necessario.

StorageGRID include un firewall interno su ciascun nodo che migliora la sicurezza della griglia consentendo di controllare l'accesso di rete al nodo. Dovresti ["gestire i controlli del firewall interno"](#) per impedire l'accesso alla rete su tutte le porte, eccetto quelle necessarie per la distribuzione specifica della griglia. Le modifiche alla configurazione apportate nella pagina di controllo del firewall vengono distribuite a ciascun nodo.

Nello specifico, puoi gestire queste aree:

- **Indirizzi privilegiati**: puoi consentire a determinati indirizzi IP o subnet di accedere alle porte chiuse dalle impostazioni nella scheda Gestisci accesso esterno.
- **Gestisci accesso esterno**: puoi chiudere le porte aperte per impostazione predefinita o riaprire quelle chiuse in precedenza.
- **Rete client non attendibile**: è possibile specificare se un nodo si fida del traffico in entrata dalla rete client, nonché delle porte aggiuntive che si desidera aprire quando è configurata la rete client non attendibile.

Sebbene questo firewall interno fornisca un ulteriore livello di protezione contro alcune minacce comuni, non elimina la necessità di un firewall esterno.

Per un elenco di tutte le porte interne ed esterne utilizzate da StorageGRID, vedere ["Riferimento porta di rete"](#).

Disabilitare i servizi non utilizzati

Per tutti i nodi StorageGRID, è necessario disabilitare o bloccare l'accesso ai servizi non utilizzati. Ad esempio, se non si prevede di utilizzare DHCP, utilizzare Grid Manager per chiudere la porta 68. Selezionare **CONFIGURAZIONE > Controllo firewall > Gestisci accesso esterno**. Quindi modifica l'interruttore di stato per la porta 68 da **Aperto** a **Chiuso**.

Virtualizzazione, container e hardware condiviso

Per tutti i nodi StorageGRID , evitare di eseguire StorageGRID sullo stesso hardware fisico di software non attendibile. Non dare per scontato che le protezioni dell'hypervisor impediscano al malware di accedere ai dati protetti StorageGRID se sia StorageGRID che il malware sono presenti sullo stesso hardware fisico. Ad esempio, gli attacchi Meltdown e Spectre sfruttano vulnerabilità critiche nei processori moderni e consentono ai programmi di rubare dati nella memoria dello stesso computer.

Proteggere i nodi durante l'installazione

Non consentire agli utenti non attendibili di accedere ai nodi StorageGRID tramite la rete durante l'installazione dei nodi. I nodi non sono completamente sicuri finché non vengono uniti alla griglia.

Linee guida per i nodi di amministrazione

I nodi amministrativi forniscono servizi di gestione quali configurazione del sistema, monitoraggio e registrazione. Quando accedi a Grid Manager o a Tenant Manager, ti stai connettendo a un nodo di amministrazione.

Seguire queste linee guida per proteggere i nodi amministrativi nel sistema StorageGRID :

- Proteggere tutti i nodi amministrativi da client non attendibili, come quelli presenti su Internet aperto. Assicurarsi che nessun client non attendibile possa accedere a nessun nodo di amministrazione sulla rete Grid, sulla rete di amministrazione o sulla rete client.
- I gruppi StorageGRID controllano l'accesso alle funzionalità Grid Manager e Tenant Manager. Concedi a ciascun gruppo di utenti le autorizzazioni minime richieste per il loro ruolo e utilizza la modalità di accesso di sola lettura per impedire agli utenti di modificare la configurazione.
- Quando si utilizzano endpoint del bilanciamento del carico StorageGRID , utilizzare nodi gateway anziché nodi amministrativi per il traffico client non attendibile.
- Se hai tenant non attendibili, non consentire loro di accedere direttamente a Tenant Manager o all'API Tenant Management. In alternativa, fai in modo che tutti gli inquilini non attendibili utilizzino un portale per gli inquilini o un sistema di gestione degli inquilini esterno, che interagisca con l'API di gestione degli inquilini.
- Facoltativamente, utilizzare un proxy di amministrazione per un maggiore controllo sulla comunicazione AutoSupport dai nodi di amministrazione al supporto NetApp . Vedi i passaggi per ["creazione di un proxy amministratore"](#) .
- Facoltativamente, utilizzare le porte riservate 8443 e 9443 per separare le comunicazioni tra Grid Manager e Tenant Manager. Per una maggiore protezione, bloccare la porta condivisa 443 e limitare le richieste dei tenant alla porta 9443.
- Facoltativamente, utilizzare nodi amministrativi separati per gli amministratori della griglia e gli utenti tenant.

Per maggiori informazioni, consultare le istruzioni per ["amministrazione di StorageGRID"](#) .

Linee guida per i nodi di archiviazione

I nodi di archiviazione gestiscono e archiviano dati e metadati degli oggetti. Seguire queste linee guida per proteggere i nodi di archiviazione nel sistema StorageGRID .

- Non consentire ai client non attendibili di connettersi direttamente ai nodi di archiviazione. Utilizzare un endpoint di bilanciamento del carico servito da un nodo gateway o da un bilanciamento del carico di terze parti.

- Non abilitare i servizi in uscita per i tenant non attendibili. Ad esempio, quando si crea un account per un tenant non attendibile, non consentire al tenant di utilizzare la propria origine identità e non consentire l'utilizzo dei servizi della piattaforma. Vedi i passaggi per ["creazione di un account inquilino"](#) .
- Utilizzare un bilanciatore del carico di terze parti per il traffico client non attendibile. Il bilanciamento del carico di terze parti offre maggiore controllo e ulteriori livelli di protezione contro gli attacchi.
- Facoltativamente, utilizzare un proxy di archiviazione per un maggiore controllo sui pool di archiviazione cloud e sulla comunicazione dei servizi della piattaforma dai nodi di archiviazione ai servizi esterni. Vedi i passaggi per ["creazione di un proxy di archiviazione"](#) .
- Facoltativamente, è possibile connettersi ai servizi esterni tramite la rete client. Quindi, selezionare **CONFIGURAZIONE > Sicurezza > Controllo firewall > Reti client non attendibili** e indicare che la rete client sul nodo di archiviazione non è attendibile. Il nodo di archiviazione non accetta più traffico in entrata sulla rete client, ma continua a consentire richieste in uscita per i servizi della piattaforma.

Linee guida per i nodi gateway

I nodi gateway forniscono un'interfaccia di bilanciamento del carico opzionale che le applicazioni client possono utilizzare per connettersi a StorageGRID. Seguire queste linee guida per proteggere tutti i nodi gateway nel sistema StorageGRID :

- Configurare e utilizzare gli endpoint del bilanciatore del carico. Vedere ["Considerazioni sul bilanciamento del carico"](#) .
- Utilizzare un bilanciatore del carico di terze parti tra il client e il nodo gateway o i nodi di archiviazione per il traffico client non attendibile. Il bilanciamento del carico di terze parti offre maggiore controllo e ulteriori livelli di protezione contro gli attacchi. Se si utilizza un bilanciatore del carico di terze parti, è comunque possibile configurare il traffico di rete in modo che passi attraverso un endpoint del bilanciatore del carico interno o venga inviato direttamente ai nodi di archiviazione.
- Se si utilizzano endpoint di bilanciamento del carico, è possibile fare in modo che i client si connettano tramite la rete client. Quindi, selezionare **CONFIGURAZIONE > Sicurezza > Controllo firewall > Reti client non attendibili** e indicare che la rete client sul nodo gateway non è attendibile. Il nodo gateway accetta solo il traffico in entrata sulle porte configurate esplicitamente come endpoint del bilanciatore del carico.

Linee guida per i nodi degli apparecchi hardware

Gli apparecchi hardware StorageGRID sono progettati specificamente per l'uso in un sistema StorageGRID . Alcuni dispositivi possono essere utilizzati come nodi di archiviazione. Altri dispositivi possono essere utilizzati come nodi amministrativi o nodi gateway. È possibile combinare nodi appliance con nodi basati su software oppure implementare griglie completamente progettate per tutti gli appliance.

Seguire queste linee guida per proteggere tutti i nodi degli apparecchi hardware nel sistema StorageGRID :

- Se l'appliance utilizza SANtricity System Manager per la gestione del controller di archiviazione, impedire ai client non attendibili di accedere a SANtricity System Manager tramite la rete.
- Se l'appliance è dotata di un controller di gestione della scheda base (BMC), tenere presente che la porta di gestione BMC consente l'accesso hardware di basso livello. Collegare la porta di gestione BMC solo a una rete di gestione interna sicura e affidabile. Se non è disponibile alcuna rete di questo tipo, lasciare la porta di gestione BMC scollegata o bloccata, a meno che il supporto tecnico non richieda una connessione BMC .
- Se l'appliance supporta la gestione remota dell'hardware del controller tramite Ethernet utilizzando lo standard Intelligent Platform Management Interface (IPMI), bloccare il traffico non attendibile sulla porta 623.



È possibile abilitare o disabilitare l'accesso IPMI remoto per tutti gli apparecchi che contengono un BMC. L'interfaccia IPMI remota consente l'accesso hardware di basso livello ai dispositivi StorageGRID a chiunque disponga di un account e di una password BMC. Se non è necessario l'accesso IPMI remoto al BMC, disabilitare questa opzione utilizzando uno dei seguenti metodi:

- + In Grid Manager, andare su **CONFIGURAZIONE > Sicurezza > Impostazioni di sicurezza > Appliance** e deselezionare la casella di controllo **Abilita accesso IPMI remoto**.
- + Nell'API di gestione della griglia, utilizzare l'endpoint privato: `PUT /private/bmc`.

- Per i modelli di appliance contenenti unità SED, FDE o FIPS NL-SAS gestite con SANtricity System Manager, ["abilitare e configurare SANtricity Drive Security"](#).
- Per i modelli di appliance contenenti SSD SED o FIPS NVMe gestiti tramite StorageGRID Appliance Installer e Grid Manager, ["abilitare e configurare la crittografia dell'unità StorageGRID"](#).
- Per gli apparecchi senza unità SED, FDE o FIPS, abilitare e configurare la crittografia del nodo software StorageGRID ["utilizzando un server di gestione delle chiavi \(KMS\)"](#).

Linee guida per il rafforzamento di TLS e SSH

È necessario sostituire i certificati predefiniti creati durante l'installazione e selezionare la policy di sicurezza appropriata per le connessioni TLS e SSH.

Linee guida per il rafforzamento dei certificati

Dovresti sostituire i certificati predefiniti creati durante l'installazione con i tuoi certificati personalizzati.

Per molte organizzazioni, il certificato digitale autofirmato per l'accesso web a StorageGRID non è conforme alle policy di sicurezza delle informazioni. Nei sistemi di produzione, è necessario installare un certificato digitale firmato da una CA da utilizzare per l'autenticazione StorageGRID.

Nello specifico, dovresti utilizzare certificati server personalizzati anziché questi certificati predefiniti:

- **Certificato dell'interfaccia di gestione:** utilizzato per proteggere l'accesso a Grid Manager, Tenant Manager, Grid Management API e Tenant Management API.
- **Certificato API S3:** utilizzato per proteggere l'accesso ai nodi di archiviazione e ai nodi gateway, che le applicazioni client S3 utilizzano per caricare e scaricare i dati degli oggetti.

Vedere ["Gestire i certificati di sicurezza"](#) per dettagli e istruzioni.



StorageGRID gestisce separatamente i certificati utilizzati per gli endpoint del bilanciamento del carico. Per configurare i certificati del bilanciamento del carico, vedere ["Configurare gli endpoint del bilanciamento del carico"](#).

Quando si utilizzano certificati server personalizzati, seguire queste linee guida:

- I certificati dovrebbero avere un `subjectAltName` che corrisponde alle voci DNS per StorageGRID. Per i dettagli, vedere la sezione 4.2.1.6, "Nome alternativo dell'oggetto", in ["RFC 5280: Certificato PKIX e profilo CRL"](#).
- Se possibile, evitare l'uso di certificati jolly. Un'eccezione a questa linea guida è il certificato per un endpoint in stile host virtuale S3, che richiede l'uso di un carattere jolly se i nomi dei bucket non sono noti in anticipo.
- Quando è necessario utilizzare caratteri jolly nei certificati, è opportuno adottare misure aggiuntive per

ridurre i rischi. Utilizzare un modello jolly come `*.s3.example.com` e non usare il `s3.example.com` suffisso per altre applicazioni. Questo modello funziona anche con l'accesso S3 in stile percorso, come `dc1-s1.s3.example.com/mybucket`.

- Imposta tempi di scadenza dei certificati brevi (ad esempio, 2 mesi) e utilizza l'API Grid Management per automatizzare la rotazione dei certificati. Ciò è particolarmente importante per i certificati jolly.

Inoltre, i client devono utilizzare un controllo rigoroso del nome host quando comunicano con StorageGRID.

Linee guida per il rafforzamento della politica TLS e SSH

È possibile selezionare una policy di sicurezza per determinare quali protocolli e cifrari vengono utilizzati per stabilire connessioni TLS sicure con le applicazioni client e connessioni SSH sicure con i servizi StorageGRID interni.

La policy di sicurezza controlla il modo in cui TLS e SSH crittografano i dati in movimento. Come buona pratica, dovresti disabilitare le opzioni di crittografia non necessarie per la compatibilità dell'applicazione. Utilizzare il criterio Modern predefinito, a meno che il sistema non debba essere conforme ai Common Criteria o non sia necessario utilizzare altri cifrari.

Vedere ["Gestire la politica TLS e SSH"](#) per dettagli e istruzioni.

Altre linee guida per il rafforzamento

Oltre a seguire le linee guida di rafforzamento per le reti e i nodi StorageGRID, è necessario seguire anche le linee guida di rafforzamento per altre aree del sistema StorageGRID.

Password di installazione temporanea

Per proteggere il sistema StorageGRID durante l'installazione, impostare una password nella pagina della password temporanea del programma di installazione nell'interfaccia utente di installazione StorageGRID o nell'API di installazione. Se impostata, questa password si applica a tutti i metodi di installazione StorageGRID, inclusa l'interfaccia utente, l'API di installazione e `configure-storagegrid.py` sceneggiatura.

Per maggiori informazioni, fare riferimento a:

- ["Installa StorageGRID su Red Hat Enterprise Linux"](#)
- ["Installa StorageGRID su Ubuntu o Debian"](#)
- ["Installa StorageGRID su VMware"](#)
- ["Installare l'appliance StorageGRID"](#)

Registri e messaggi di controllo

Proteggere sempre in modo sicuro i registri StorageGRID e l'output dei messaggi di controllo. I registri e i messaggi di controllo StorageGRID forniscono informazioni preziose dal punto di vista del supporto e della disponibilità del sistema. Inoltre, le informazioni e i dettagli contenuti nei log StorageGRID e nell'output dei messaggi di controllo sono generalmente di natura sensibile.

Configurare StorageGRID per inviare eventi di sicurezza a un server syslog esterno. Se si utilizza l'esportazione syslog, selezionare TLS e RELP/TLS per i protocolli di trasporto.

Vedi il ["Riferimento ai file di registro"](#) per ulteriori informazioni sui log StorageGRID. Vedere ["Messaggi di](#)

[controllo](#)" per ulteriori informazioni sui messaggi di controllo StorageGRID .

AutoSupport NetApp

La funzionalità AutoSupport di StorageGRID consente di monitorare in modo proattivo lo stato del sistema e di inviare automaticamente pacchetti al sito di supporto NetApp , al team di supporto interno della tua organizzazione o a un partner di supporto. Per impostazione predefinita, l'invio di pacchetti AutoSupport a NetApp è abilitato quando StorageGRID viene configurato per la prima volta.

La funzione AutoSupport può essere disattivata. Tuttavia, NetApp consiglia di abilitarlo perché AutoSupport aiuta ad accelerare l'identificazione e la risoluzione dei problemi nel caso in cui si verifichino nel sistema StorageGRID .

AutoSupport supporta HTTPS, HTTP e SMTP per i protocolli di trasporto. Data la natura sensibile dei pacchetti AutoSupport , NetApp consiglia vivamente di utilizzare HTTPS come protocollo di trasporto predefinito per l'invio dei pacchetti AutoSupport a NetApp.

Condivisione delle risorse tra origini (CORS)

È possibile configurare la condivisione delle risorse tra origini (CORS) per un bucket S3 se si desidera che il bucket e gli oggetti in esso contenuti siano accessibili alle applicazioni Web in altri domini. In generale, non abilitare CORS a meno che non sia necessario. Se CORS è richiesto, limitarlo alle origini attendibili.

Vedi i passaggi per "[configurazione della condivisione delle risorse tra origini \(CORS\)](#)" .

Dispositivi di sicurezza esterni

Una soluzione di rafforzamento completa deve tenere conto dei meccanismi di sicurezza esterni a StorageGRID. L'utilizzo di dispositivi infrastrutturali aggiuntivi per filtrare e limitare l'accesso a StorageGRID è un modo efficace per stabilire e mantenere un rigoroso livello di sicurezza. Questi dispositivi di sicurezza esterni includono firewall, sistemi di prevenzione delle intrusioni (IPS) e altri dispositivi di sicurezza.

Per il traffico client non attendibile si consiglia l'uso di un bilanciatore del carico di terze parti. Il bilanciamento del carico di terze parti offre maggiore controllo e ulteriori livelli di protezione contro gli attacchi.

Mitigazione del ransomware

Aiuta a proteggere i dati dei tuoi oggetti dagli attacchi ransomware seguendo i consigli in "[Difesa dal ransomware con StorageGRID](#)" .

Configurare StorageGRID per FabricPool

Configurare StorageGRID per FabricPool

Se si utilizza il software NetApp ONTAP , è possibile utilizzare NetApp FabricPool per suddividere i dati inattivi in un sistema di archiviazione di oggetti NetApp StorageGRID .

Utilizzare queste istruzioni per:

- Scopri le considerazioni e le best practice per la configurazione di StorageGRID per un carico di lavoro FabricPool .
- Scopri come configurare un sistema di archiviazione di oggetti StorageGRID per l'utilizzo con FabricPool.

- Scopri come fornire i valori richiesti a ONTAP quando colleghi StorageGRID come livello cloud FabricPool .

Guida rapida per la configurazione di StorageGRID per FabricPool

1

Pianifica la tua configurazione

- Decidi quale criterio di suddivisione in livelli del volume FabricPool utilizzerai per suddividere in livelli i dati ONTAP inattivi in StorageGRID.
- Pianifica e installa un sistema StorageGRID per soddisfare le tue esigenze di capacità di archiviazione e prestazioni.
- Acquisire familiarità con il software di sistema StorageGRID , incluso il ["Responsabile della griglia"](#) e il ["Responsabile degli inquilini"](#) .
- Esaminare le best practice di FabricPool per ["gruppi HA"](#) , ["bilanciamento del carico"](#) , ["ILM"](#) , E ["Di più"](#) .
- Consultare queste risorse aggiuntive, che forniscono dettagli sull'utilizzo e la configurazione ONTAP e FabricPool:

["TR-4598: Migliori pratiche FabricPool in ONTAP"](#)

["Documentazione ONTAP per FabricPool"](#)

2

Eeguire le attività prerequisito

Ottieni il ["informazioni necessarie per collegare StorageGRID come livello cloud"](#) , tra cui:

- indirizzi IP
- Nomi di dominio
- Certificato SSL

Facoltativamente, configurare ["federazione di identità"](#) E ["accesso unico"](#) .

3

Configurare le impostazioni StorageGRID

Utilizzare StorageGRID per ottenere i valori di cui ONTAP ha bisogno per connettersi alla rete.

Utilizzando il ["Procedura guidata di configurazione FabricPool"](#) è il metodo consigliato e più veloce per configurare tutti gli elementi, ma è anche possibile configurare manualmente ogni entità, se necessario.

4

Configurare ONTAP e DNS

Utilizzare ONTAP per ["aggiungere un livello cloud"](#) che utilizza i valori StorageGRID . Poi, ["configurare le voci DNS"](#) per associare gli indirizzi IP a qualsiasi nome di dominio che intendi utilizzare.

5

Monitorare e gestire

Quando il sistema è attivo e funzionante, esegui attività continue in ONTAP e StorageGRID per gestire e monitorare la suddivisione in livelli dei dati FabricPool nel tempo.

Che cos'è FabricPool?

FabricPool è una soluzione di storage ibrida ONTAP che utilizza un aggregato flash ad alte prestazioni come livello di prestazioni e un archivio di oggetti come livello cloud. Utilizzando aggregati abilitati per FabricPool è possibile ridurre i costi di archiviazione senza compromettere prestazioni, efficienza o protezione.

FabricPool associa un livello cloud (un archivio di oggetti esterno, come StorageGRID) a un livello locale (un aggregato di archiviazione ONTAP) per creare una raccolta composita di dischi. I volumi all'interno di FabricPool possono quindi sfruttare la suddivisione in livelli mantenendo i dati attivi (hot) su un archivio ad alte prestazioni (il livello locale) e disattivando i dati (cold) nell'archivio oggetti esterno (il livello cloud).

Non sono necessarie modifiche architettoniche e puoi continuare a gestire i tuoi dati e l'ambiente applicativo dal sistema di archiviazione centrale ONTAP.

Che cos'è StorageGRID?

NetApp StorageGRID è un'architettura di storage che gestisce i dati come oggetti, a differenza di altre architetture di storage come l'archiviazione di file o di blocchi. Gli oggetti vengono conservati all'interno di un singolo contenitore (ad esempio un bucket) e non sono annidati come file all'interno di una directory all'interno di altre directory. Sebbene l'archiviazione di oggetti offra generalmente prestazioni inferiori rispetto all'archiviazione di file o blocchi, è significativamente più scalabile. I bucket StorageGRID possono contenere petabyte di dati e miliardi di oggetti.

Perché utilizzare StorageGRID come livello cloud FabricPool ?

FabricPool può suddividere i dati ONTAP in livelli per diversi provider di archiviazione di oggetti, tra cui StorageGRID. A differenza dei cloud pubblici che potrebbero impostare un numero massimo di operazioni di input/output supportate al secondo (IOPS) a livello di bucket o contenitore, le prestazioni StorageGRID variano in base al numero di nodi in un sistema. Utilizzando StorageGRID come livello cloud FabricPool puoi conservare i tuoi dati inattivi nel tuo cloud privato, per ottenere le massime prestazioni e il controllo completo sui tuoi dati.

Inoltre, non è richiesta una licenza FabricPool quando si utilizza StorageGRID come livello cloud.

Informazioni necessarie per collegare StorageGRID come livello cloud

Prima di poter collegare StorageGRID come livello cloud per FabricPool, è necessario eseguire i passaggi di configurazione in StorageGRID e ottenere determinati valori da utilizzare in ONTAP.

Di quali valori ho bisogno?

Nella tabella seguente vengono mostrati i valori che è necessario configurare in StorageGRID e come tali valori vengono utilizzati da ONTAP e dal server DNS.

Valore	Dove è configurato il valore	Dove viene utilizzato il valore
Indirizzi IP virtuali (VIP)	StorageGRID > Gruppo HA	voce DNS
Porta	StorageGRID > Endpoint del bilanciatore del carico	ONTAP System Manager > Aggiungi livello cloud

Valore	Dove è configurato il valore	Dove viene utilizzato il valore
Certificato SSL	StorageGRID > Endpoint del bilanciatore del carico	ONTAP System Manager > Aggiungi livello cloud
Nome del server (FQDN)	StorageGRID > Endpoint del bilanciatore del carico	voce DNS
ID chiave di accesso e chiave di accesso segreta	StorageGRID > Tenant e bucket	ONTAP System Manager > Aggiungi livello cloud
Nome del bucket/contenitore	StorageGRID > Tenant e bucket	ONTAP System Manager > Aggiungi livello cloud

Come posso ottenere questi valori?

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

- Utilizzare il ["Procedura guidata di configurazione FabricPool"](#) . La procedura guidata di configurazione FabricPool consente di configurare rapidamente i valori richiesti in StorageGRID e genera un file che è possibile utilizzare per configurare ONTAP System Manager. La procedura guidata ti guida attraverso i passaggi necessari e ti aiuta a verificare che le tue impostazioni siano conformi alle best practice StorageGRID e FabricPool .
- Configurare manualmente ogni elemento. Quindi, immettere i valori in ONTAP System Manager o in ONTAP CLI. Segui questi passaggi:
 - a. ["Configurare un gruppo ad alta disponibilità \(HA\) per FabricPool"](#) .
 - b. ["Creare un endpoint del bilanciatore del carico per FabricPool"](#) .
 - c. ["Crea un account tenant per FabricPool"](#) .
 - d. Sign in all'account tenant e ["creare il bucket e le chiavi di accesso per l'utente root"](#) .
 - e. Crea una regola ILM per i dati FabricPool e aggiungila ai tuoi criteri ILM attivi. Vedere ["Configurare ILM per i dati FabricPool"](#) .
 - f. Facoltativamente, ["creare una politica di classificazione del traffico per FabricPool"](#) .

Utilizzare la procedura guidata di configurazione FabricPool

Utilizzare la procedura guidata di configurazione FabricPool : considerazioni e requisiti

È possibile utilizzare la procedura guidata di configurazione FabricPool per configurare StorageGRID come sistema di archiviazione degli oggetti per un livello cloud FabricPool . Dopo aver completato la procedura guidata di configurazione, è possibile immettere i dettagli richiesti in ONTAP System Manager.

Quando utilizzare la procedura guidata di configurazione FabricPool

La procedura guidata di configurazione FabricPool ti guida attraverso ogni fase della configurazione di StorageGRID per l'utilizzo con FabricPool e configura automaticamente determinate entità, come ILM e criteri di classificazione del traffico. Per completare la procedura guidata, è necessario scaricare un file che è

possibile utilizzare per immettere valori in ONTAP System Manager. Utilizza la procedura guidata per configurare il sistema più rapidamente e per assicurarti che le impostazioni siano conformi alle best practice StorageGRID e FabricPool .

Supponendo di disporre dell'autorizzazione di accesso Root, è possibile completare la procedura guidata di configurazione FabricPool quando si inizia a utilizzare StorageGRID Grid Manager oppure è possibile accedere e completare la procedura guidata in qualsiasi momento successivo. A seconda delle esigenze, è anche possibile configurare manualmente alcuni o tutti gli elementi richiesti e quindi utilizzare la procedura guidata per assemblare i valori di cui ONTAP ha bisogno in un unico file.



Utilizzare la procedura guidata di configurazione FabricPool a meno che non si abbiano requisiti particolari o che l'implementazione richieda una personalizzazione significativa.

Prima di utilizzare la procedura guidata

Conferma di aver completato questi passaggi preliminari.

Esaminare le migliori pratiche

- Hai una comprensione generale del ["informazioni necessarie per collegare StorageGRID come livello cloud"](#) .
- Hai esaminato le best practice FabricPool per:
 - ["Gruppi ad alta disponibilità \(HA\)"](#)
 - ["Bilanciamento del carico"](#)
 - ["Regole e politica ILM"](#)

Ottenere indirizzi IP e configurare le interfacce VLAN

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

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

Configurare la federazione delle identità e SSO

Se intendi utilizzare la federazione delle identità o l'accesso singolo (SSO) per il tuo sistema StorageGRID , hai abilitato queste funzionalità. Si sa anche quale gruppo federato dovrebbe avere accesso root per l'account tenant che ONTAP utilizzerà. Vedere ["Utilizzare la federazione delle identità"](#) E ["Configurare l'accesso singolo"](#) .

Ottieni e configura i nomi di dominio

- Sai quale nome di dominio completo (FQDN) utilizzare per StorageGRID. Le voci del server dei nomi di dominio (DNS) mapperanno questo FQDN agli indirizzi IP virtuali (VIP) del gruppo HA creato tramite la procedura guidata. Vedere ["Configurare il server DNS"](#) .
- Se si prevede di utilizzare richieste in stile host virtuale S3, è necessario ["nomi di dominio endpoint S3 configurati"](#) . Per impostazione predefinita, ONTAP utilizza URL in stile percorso, ma si consiglia di utilizzare richieste in stile virtual hosted.

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

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

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

Confermare la configurazione del pool di archiviazione ILM

se inizialmente hai installato StorageGRID 11.6 o una versione precedente, hai configurato il pool di archiviazione che utilizzerai. In generale, dovresti creare un pool di archiviazione per ogni sito StorageGRID che utilizzerai per archiviare i dati ONTAP .



Questo prerequisito non si applica se inizialmente è stato installato StorageGRID 11.7 o 11.8. Quando si installa inizialmente una di queste versioni, vengono creati automaticamente dei pool di archiviazione per ogni sito.

Relazione tra ONTAP e il livello cloud StorageGRID

La procedura guidata FabricPool ti guida attraverso il processo di creazione di un singolo livello cloud StorageGRID che include un tenant StorageGRID , un set di chiavi di accesso e un bucket StorageGRID . È possibile collegare questo livello cloud StorageGRID a uno o più livelli locali ONTAP .

La prassi migliore in generale è quella di collegare un singolo livello cloud a più livelli locali in un cluster. Tuttavia, a seconda delle esigenze, potresti voler utilizzare più di un bucket o addirittura più di un tenant StorageGRID per i livelli locali in un singolo cluster. L'utilizzo di bucket e tenant diversi consente di isolare i dati e l'accesso ai dati tra i livelli locali ONTAP , ma è un po' più complesso da configurare e gestire.

NetApp sconsiglia di collegare un singolo livello cloud a livelli locali in più cluster.



Per le best practice per l'utilizzo di StorageGRID con NetApp MetroCluster™ e FabricPool Mirror, vedere ["TR-4598: Migliori pratiche FabricPool in ONTAP"](#) .

Facoltativo: utilizzare un bucket diverso per ogni livello locale

Per utilizzare più di un bucket per i livelli locali in un cluster ONTAP , aggiungere più di un livello cloud StorageGRID in ONTAP. Ogni livello cloud condivide lo stesso gruppo HA, endpoint del bilanciatore del carico, tenant e chiavi di accesso, ma utilizza un contenitore diverso (bucket StorageGRID). Seguire questi passaggi generali:

1. Da StorageGRID Grid Manager, completare la procedura guidata di configurazione FabricPool per il primo livello cloud.
2. Da ONTAP System Manager, aggiungi un livello cloud e utilizza il file scaricato da StorageGRID per fornire i valori richiesti.
3. Da StorageGRID Tenant Manager, accedi al tenant creato dalla procedura guidata e crea un secondo bucket.
4. Completare nuovamente la procedura guidata FabricPool . Selezionare il gruppo HA esistente, l'endpoint del bilanciatore del carico e il tenant. Quindi, seleziona il nuovo bucket che hai creato manualmente. Crea una nuova regola ILM per il nuovo bucket e attiva un criterio ILM per includere tale regola.
5. Da ONTAP, aggiungi un secondo livello cloud ma fornisci il nome del nuovo bucket.

Facoltativo: utilizzare un tenant e un bucket diversi per ogni livello locale

Per utilizzare più di un tenant e diversi set di chiavi di accesso per i livelli locali in un cluster ONTAP , aggiungere più di un livello cloud StorageGRID in ONTAP. Ogni livello cloud condivide lo stesso gruppo HA, lo stesso endpoint del bilanciatore del carico, ma utilizza un tenant, chiavi di accesso e un contenitore (bucket StorageGRID) diversi. Seguire questi passaggi generali:

1. Da StorageGRID Grid Manager, completare la procedura guidata di configurazione FabricPool per il primo livello cloud.
2. Da ONTAP System Manager, aggiungi un livello cloud e utilizza il file scaricato da StorageGRID per fornire i valori richiesti.
3. Completare nuovamente la procedura guidata FabricPool . Selezionare il gruppo HA esistente e l'endpoint del bilanciatore del carico. Crea un nuovo tenant e un nuovo bucket. Crea una nuova regola ILM per il nuovo bucket e attiva un criterio ILM per includere tale regola.
4. Da ONTAP, aggiungi un secondo livello cloud, ma fornisci la nuova chiave di accesso, la chiave segreta e il nome del bucket.

Accedi e completa la procedura guidata di configurazione FabricPool

È possibile utilizzare la procedura guidata di configurazione FabricPool per configurare StorageGRID come sistema di archiviazione degli oggetti per un livello cloud FabricPool .

Prima di iniziare

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



Se si desidera configurare StorageGRID per l'utilizzo con qualsiasi altra applicazione client S3, andare a "[Utilizzare la procedura guidata di configurazione S3](#)" .

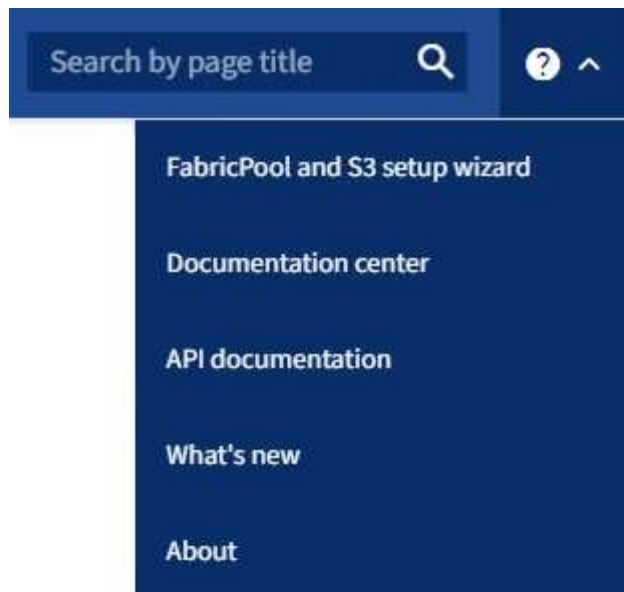
- Tu hai il "[Permesso di accesso root](#)" .

Accedi alla procedura guidata

È possibile completare la procedura guidata di configurazione FabricPool quando si inizia a utilizzare StorageGRID Grid Manager oppure è possibile accedere e completare la procedura guidata in qualsiasi momento successivo.

Passi

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



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

Viene visualizzato **Passaggio 1 di 9: Configura gruppo HA**.

Passaggio 1 di 9: configurare il gruppo HA

Un gruppo ad alta disponibilità (HA) è una raccolta di nodi, ciascuno dei quali contiene il servizio StorageGRID Load Balancer. Un gruppo HA può contenere nodi gateway, nodi amministrativi o entrambi.

È possibile utilizzare un gruppo HA per mantenere disponibili le connessioni dati FabricPool . Un gruppo HA utilizza indirizzi IP virtuali (VIP) per fornire un accesso altamente disponibile al servizio Load Balancer. Se l'interfaccia attiva nel gruppo HA fallisce, un'interfaccia di backup può gestire il carico di lavoro con un impatto minimo sulle operazioni FabricPool

Per i dettagli su questa attività, vedere "[Gestire gruppi ad alta disponibilità](#)" E "[Procedure consigliate per i gruppi ad alta disponibilità](#)".

Passi

1. Se si prevede di utilizzare un bilanciatore del carico esterno, non è necessario creare un gruppo HA. Seleziona **Salta questo passaggio** e vai a [Passaggio 2 di 9: configurare l'endpoint del bilanciatore del carico](#) .
2. Per utilizzare il bilanciatore del carico StorageGRID , creare un nuovo gruppo HA o utilizzare un gruppo HA esistente.

Crea gruppo HA

- a. Per creare un nuovo gruppo HA, seleziona **Crea gruppo HA**.
- b. Per la fase **Inserisci dettagli**, compila i seguenti campi.

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

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

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

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

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

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

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

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

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

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

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

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

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

Utilizzare il gruppo HA esistente

a. Per utilizzare un gruppo HA esistente, seleziona il nome del gruppo HA dall'elenco a discesa **Seleziona un gruppo HA**.

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

Passaggio 2 di 9: configurare l'endpoint del bilanciatore del carico

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

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

Per i dettagli su questa attività, vedere la sezione generale ["considerazioni per il bilanciamento del carico"](#) e il ["best practice per il bilanciamento del carico per FabricPool"](#) .

Passi

1. Selezionare o creare un endpoint del bilanciatore del carico StorageGRID oppure utilizzare un bilanciatore del carico esterno.

Crea endpoint

- a. Selezionare **Crea endpoint**.
- b. Per il passaggio **Inserisci i dettagli dell'endpoint**, compila i seguenti campi.

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint.
Porta	La porta StorageGRID che si desidera utilizzare per il bilanciamento del carico. Per impostazione predefinita, questo campo è impostato su 10433 per il primo endpoint creato, ma è possibile immettere qualsiasi porta esterna non utilizzata. Se si immette 80 o 443, l'endpoint viene configurato solo sui nodi gateway, perché queste porte sono riservate sui nodi amministrativi. Nota: non sono consentite le porte utilizzate da altri servizi di rete. Vedi il "Riferimento porta di rete".
Tipo di cliente	Deve essere S3 .
Protocollo di rete	Selezionare HTTPS. Nota: la comunicazione con StorageGRID senza crittografia TLS è supportata ma non consigliata.

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

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

Modalità	Descrizione
Tipo di nodo	In base al tipo di nodo selezionato, i client devono utilizzare l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di amministrazione oppure l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo gateway per accedere a questo endpoint.

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

Campo	Descrizione
Consenti tutti i tenant (predefinito)	Tutti gli account tenant possono utilizzare questo endpoint per accedere ai propri bucket. Consenti tutti i tenant è quasi sempre l'opzione appropriata per l'endpoint del bilanciatore del carico utilizzato per FabricPool. È necessario selezionare questa opzione se si utilizza la procedura guidata di configurazione FabricPool per un nuovo sistema StorageGRID e non è ancora stato creato alcun account tenant.
Consenti inquilini selezionati	Solo gli account tenant selezionati possono utilizzare questo endpoint per accedere ai propri bucket.
Blocca gli inquilini selezionati	Gli account tenant selezionati non possono utilizzare questo endpoint per accedere ai propri bucket. Tutti gli altri tenant possono utilizzare questo endpoint.

e. Per il passaggio **Allega certificato**, seleziona una delle seguenti opzioni:

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

f. Selezionare **Fine** per tornare alla procedura guidata di configurazione FabricPool .

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



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

Utilizzare l'endpoint del bilanciatore del carico esistente

- a. Selezionare il nome di un endpoint esistente dall'elenco a discesa **Seleziona un endpoint del bilanciatore del carico**.
- b. Selezionare **Continua** per passare alla fase tenant e bucket.

Utilizzare un bilanciatore di carico esterno

- a. Compilare i seguenti campi per il bilanciatore del carico esterno.

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

- b. Selezionare **Continua** per passare alla fase tenant e bucket.

Fase 3 di 9: Inquilino e bucket

Un tenant è un'entità che può utilizzare le applicazioni S3 per archiviare e recuperare oggetti in StorageGRID. Ogni tenant ha i propri utenti, chiavi di accesso, bucket, oggetti e un set specifico di funzionalità. È necessario creare un tenant StorageGRID prima di poter creare il bucket che verrà utilizzato FabricPool .

Un bucket è un contenitore utilizzato per archiviare gli oggetti e i metadati degli oggetti di un tenant. Sebbene alcuni tenant possano avere molti bucket, la procedura guidata consente di creare o selezionare solo un tenant e un bucket alla volta. In seguito potrai utilizzare Tenant Manager per aggiungere altri bucket di cui hai bisogno.

È possibile creare un nuovo tenant e un nuovo bucket da utilizzare in FabricPool oppure selezionare un tenant e un bucket esistenti. Se si crea un nuovo tenant, il sistema crea automaticamente l'ID della chiave di accesso e la chiave di accesso segreta per l'utente root del tenant.

Per i dettagli su questa attività, vedere ["Crea un account tenant per FabricPool"](#) E ["Crea un bucket S3 e ottieni una chiave di accesso"](#) .

Passi

Crea un nuovo tenant e un nuovo bucket oppure seleziona un tenant esistente.

Nuovo inquilino e secchio

1. Per creare un nuovo tenant e un nuovo bucket, immettere un **Nome tenant**. Ad esempio, `FabricPool tenant`.
2. Definisci l'accesso root per l'account tenant, in base all'utilizzo o meno da parte del sistema StorageGRID "federazione di identità", "accesso unico (SSO)", o entrambi.

Opzione	Fai questo
Se la federazione delle identità non è abilitata	Specificare la password da utilizzare quando si accede al tenant come utente root locale.
Se la federazione delle identità è abilitata	a. Selezionare un gruppo federato esistente per ottenere l'autorizzazione di accesso Root per il tenant. b. Facoltativamente, specificare la password da utilizzare quando si accede al tenant come utente root locale.
Se sono abilitati sia la federazione delle identità che il Single Sign-On (SSO)	Selezionare un gruppo federato esistente per ottenere l'autorizzazione di accesso Root per il tenant. Nessun utente locale può effettuare l'accesso.

3. Per **Nome bucket**, immettere il nome del bucket che FabricPool utilizzerà per archiviare i dati ONTAP. Ad esempio, `fabricpool-bucket`.



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

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

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

5. Selezionare **Crea e continua** per creare il tenant e il bucket e per passare alla fase di download dei dati

Seleziona inquilino e bucket

L'account tenant esistente deve avere almeno un bucket in cui non è abilitato il controllo delle versioni. Non è possibile selezionare un account tenant esistente se non esiste alcun bucket per quel tenant.

1. Selezionare il tenant esistente dall'elenco a discesa **Nome del tenant**.
2. Selezionare il bucket esistente dall'elenco a discesa **Nome bucket**.

FabricPool non supporta il controllo delle versioni degli oggetti, pertanto i bucket in cui il controllo delle versioni è abilitato non vengono visualizzati.



Non selezionare un bucket in cui è abilitato S3 Object Lock per l'utilizzo con FabricPool.

3. Selezionare **Continua** per passare alla fase di download dei dati.

Passaggio 4 di 9: Scarica le impostazioni ONTAP

Durante questa fase, scaricherai un file che potrai utilizzare per immettere valori in ONTAP System Manager.

Passi

1. Facoltativamente, seleziona l'icona di copia () per copiare sia l'ID della chiave di accesso che la chiave di accesso segreta negli appunti.

Questi valori sono inclusi nel file scaricato, ma potresti volerli salvare separatamente.

2. Selezionare ***Scarica impostazioni ONTAP *** per scaricare un file di testo contenente i valori immessi finora.

IL `ONTAP_FabricPool_settings_bucketname.txt` Il file include le informazioni necessarie per configurare StorageGRID come sistema di archiviazione degli oggetti per un livello cloud FabricPool , tra cui:

- Dettagli sulla connessione del bilanciatore del carico, inclusi il nome del server (FQDN), la porta e il certificato
- Nome del bucket
- ID chiave di accesso e chiave di accesso segreta per l'utente root dell'account tenant

3. Salvare le chiavi copiate e il file scaricato in un luogo sicuro.



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

4. Seleziona la casella di controllo per confermare di aver scaricato o copiato l'ID della chiave di accesso e la chiave di accesso segreta.
5. Selezionare **Continua** per passare al passaggio relativo al pool di archiviazione ILM.

Passaggio 5 di 9: selezionare un pool di archiviazione

Un pool di archiviazione è un gruppo di nodi di archiviazione. Quando si seleziona un pool di archiviazione, si determinano quali nodi StorageGRID utilizzerà per archiviare i dati suddivisi in livelli da ONTAP.

Per i dettagli su questo passaggio, vedere ["Creare un pool di archiviazione"](#) .

Passi

1. Dall'elenco a discesa **Sito**, seleziona il sito StorageGRID che desideri utilizzare per i dati suddivisi in livelli da ONTAP.
2. Dall'elenco a discesa **Pool di archiviazione**, selezionare il pool di archiviazione per quel sito.

Il pool di archiviazione per un sito include tutti i nodi di archiviazione presenti in quel sito.

3. Selezionare **Continua** per passare alla fase della regola ILM.

Passaggio 6 di 9: rivedere la regola ILM per FabricPool

Le regole di gestione del ciclo di vita delle informazioni (ILM) controllano il posizionamento, la durata e il comportamento di acquisizione di tutti gli oggetti nel sistema StorageGRID .

La procedura guidata di configurazione FabricPool crea automaticamente la regola ILM consigliata per l'utilizzo FabricPool . Questa regola si applica solo al bucket specificato. Utilizza la codifica di cancellazione 2+1 in un singolo sito per memorizzare i dati suddivisi in livelli da ONTAP.

Per i dettagli su questo passaggio, vedere ["Crea regola ILM"](#) E ["Procedure consigliate per l'utilizzo di ILM con i dati FabricPool"](#) .

Passi

1. Rivedi i dettagli della regola.

Campo	Descrizione
Nome della regola	Generato automaticamente e non può essere modificato
Descrizione	Generato automaticamente e non può essere modificato
Filtro	Il nome del bucket Questa regola si applica solo agli oggetti salvati nel bucket specificato.
Tempo di riferimento	Tempo di ingestione Le istruzioni di posizionamento iniziano quando gli oggetti vengono salvati inizialmente nel bucket.
Istruzioni per il posizionamento	Utilizzare la codifica di cancellazione 2+1

2. Ordinare il diagramma di conservazione in base a **Periodo di tempo** e **Pool di archiviazione** per confermare le istruzioni di posizionamento.
 - Il **periodo di tempo** per la regola è **Giorno 0 - per sempre**. **Giorno 0** significa che la regola viene applicata quando i dati vengono suddivisi in livelli da ONTAP. **Per sempre** significa che StorageGRID ILM non eliminerà i dati che sono stati suddivisi in livelli da ONTAP.
 - Il **pool di archiviazione** per la regola è il pool di archiviazione selezionato. **EC 2+1** significa che i dati verranno memorizzati utilizzando la codifica di cancellazione 2+1. Ogni oggetto verrà salvato come due frammenti di dati e un frammento di parità. I tre frammenti per ciascun oggetto verranno salvati in diversi nodi di archiviazione in un unico sito.
3. Selezionare **Crea e continua** per creare questa regola e passare alla fase relativa alla policy ILM.

Passaggio 7 di 9: rivedere e attivare la policy ILM

Dopo che la procedura guidata di configurazione FabricPool ha creato la regola ILM per l'utilizzo FabricPool , crea un criterio ILM. È necessario simulare e rivedere attentamente questa politica prima di attivarla.

Per i dettagli su questo passaggio, vedere ["Crea policy ILM"](#) E ["Procedure consigliate per l'utilizzo di ILM con i dati FabricPool"](#) .



Quando si attiva una nuova policy ILM, StorageGRID utilizza tale policy per gestire il posizionamento, la durata e la protezione dei dati di tutti gli oggetti nella griglia, inclusi gli oggetti esistenti e quelli appena acquisiti. In alcuni casi, l'attivazione di una nuova policy può comportare lo spostamento di oggetti esistenti in nuove posizioni.



Per evitare la perdita di dati, non utilizzare una regola ILM che farà scadere o eliminerà i dati del livello cloud FabricPool. Impostare il periodo di conservazione su **per sempre** per garantire che gli oggetti FabricPool non vengano eliminati da StorageGRID ILM.

Passi

1. Facoltativamente, aggiornare il **Nome criterio** generato dal sistema. Per impostazione predefinita, il sistema aggiunge "+ FabricPool" al nome della policy attiva o inattiva, ma è possibile specificare un nome personalizzato.
2. Esaminare l'elenco delle regole nella policy inattiva.
 - Se la griglia non dispone di un criterio ILM inattivo, la procedura guidata crea un criterio inattivo clonando il criterio attivo e aggiungendo la nuova regola in alto.
 - Se la griglia ha già un criterio ILM inattivo e tale criterio utilizza le stesse regole e lo stesso ordine del criterio ILM attivo, la procedura guidata aggiunge la nuova regola all'inizio del criterio inattivo.
 - Se la policy inattiva contiene regole diverse o un ordine diverso rispetto alla policy attiva, la procedura guidata crea una nuova policy inattiva clonando la policy attiva e aggiungendo la nuova regola in alto.
3. Rivedere l'ordine delle regole nella nuova policy inattiva.

Poiché la regola FabricPool è la prima regola, tutti gli oggetti nel bucket FabricPool vengono posizionati prima che vengano valutate le altre regole nel criterio. Gli oggetti in qualsiasi altro bucket vengono inseriti dalle regole successive nella policy.

4. Esaminare il diagramma di conservazione per scoprire come verranno conservati i diversi oggetti.
 - a. Selezionare **Espandi tutto** per visualizzare un diagramma di conservazione per ciascuna regola nel criterio inattivo.
 - b. Selezionare **Periodo di tempo** e **Pool di archiviazione** per esaminare il diagramma di conservazione. Verificare che tutte le regole applicate al bucket o al tenant FabricPool conservino gli oggetti **per sempre**.
5. Dopo aver esaminato la policy inattiva, seleziona **Attiva e continua** per attivare la policy e passare alla fase di classificazione del traffico.



Gli errori in una policy ILM possono causare una perdita irreparabile di dati. Prima di attivarla, leggere attentamente la policy.

Passaggio 8 di 9: creare una policy di classificazione del traffico

Come opzione, la procedura guidata di configurazione FabricPool può creare un criterio di classificazione del traffico che è possibile utilizzare per monitorare il carico di lavoro FabricPool. Il criterio creato dal sistema utilizza una regola di corrispondenza per identificare tutto il traffico di rete correlato al bucket creato. Questa policy monitora solo il traffico; non limita il traffico per FabricPool o altri client.

Per i dettagli su questo passaggio, vedere ["Creare una policy di classificazione del traffico per FabricPool"](#).

Passi

1. Rivedi la politica.

2. Se si desidera creare questa policy di classificazione del traffico, selezionare **Crea e continua**.

Non appena FabricPool inizia a suddividere i dati in livelli per StorageGRID, è possibile accedere alla pagina Criteri di classificazione del traffico per visualizzare le metriche del traffico di rete per questo criterio. In seguito, è anche possibile aggiungere regole per limitare altri carichi di lavoro e garantire che il carico di lavoro FabricPool disponga della maggior parte della larghezza di banda.

3. Altrimenti, seleziona **Salta questo passaggio**.

Fase 9 di 9: Riepilogo della revisione

Il riepilogo fornisce dettagli sugli elementi configurati, tra cui il nome del bilanciatore del carico, del tenant e del bucket, la policy di classificazione del traffico e la policy ILM attiva.

Passi

1. Rivedi il riepilogo.
2. Selezionare **Fine**.

Prossimi passi

Dopo aver completato la procedura guidata FabricPool, eseguire questi passaggi aggiuntivi.

Passi

1. Vai a ["Configurare ONTAP System Manager"](#) per immettere i valori salvati e completare il lato ONTAP della connessione. È necessario aggiungere StorageGRID come livello cloud, collegare il livello cloud a un livello locale per creare un FabricPool e impostare i criteri di suddivisione in livelli del volume.
2. Vai a ["Configurare il server DNS"](#) e assicurati che il DNS includa un record per associare il nome del server StorageGRID (nome di dominio completo) a ciascun indirizzo IP StorageGRID che utilizzerai.
3. Vai a ["Altre best practice per StorageGRID e FabricPool"](#) per apprendere le best practice per i log di controllo StorageGRID e altre opzioni di configurazione globali.

Configurare StorageGRID manualmente

Creare un gruppo ad alta disponibilità (HA) per FabricPool

Quando si configura StorageGRID per l'utilizzo con FabricPool, è possibile creare facoltativamente uno o più gruppi ad alta disponibilità (HA). Un gruppo HA è una raccolta di nodi, ognuno dei quali contiene il servizio StorageGRID Load Balancer. Un gruppo HA può contenere nodi gateway, nodi amministrativi o entrambi.

È possibile utilizzare un gruppo HA per mantenere disponibili le connessioni dati FabricPool. Un gruppo HA utilizza indirizzi IP virtuali (VIP) per fornire un accesso altamente disponibile al servizio Load Balancer. Se l'interfaccia attiva nel gruppo HA fallisce, un'interfaccia di backup può gestire il carico di lavoro con un impatto minimo sulle operazioni FabricPool.

Per i dettagli su questa attività, vedere ["Gestire gruppi ad alta disponibilità"](#). Per utilizzare la procedura guidata di configurazione FabricPool per completare questa attività, andare a ["Accedi e completa la procedura guidata di configurazione FabricPool"](#).

Prima di iniziare

- Hai esaminato il ["best practice per gruppi ad alta disponibilità"](#).

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Permesso di accesso root"](#) .
- Se si prevede di utilizzare una VLAN, è stata creata l'interfaccia VLAN. Vedere ["Configurare le interfacce VLAN"](#) .

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Gruppi ad alta disponibilità**.
2. Seleziona **Crea**.
3. Per la fase **Inserisci dettagli**, compila i seguenti campi.

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

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

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

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

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

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

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

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

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

Campo	Descrizione
CIDR di sottorete	L'indirizzo della subnet VIP in notazione CIDR: un indirizzo IPv4 seguito da una barra e dalla lunghezza della subnet (0-32). L'indirizzo di rete non deve avere alcun bit host impostato. Ad esempio, 192.16.0.0/22 .

Campo	Descrizione
Indirizzo IP del gateway (facoltativo)	Opzionale. Se gli indirizzi IP ONTAP utilizzati per accedere a StorageGRID non si trovano sulla stessa subnet degli indirizzi VIP StorageGRID , immettere l'indirizzo IP del gateway locale VIP StorageGRID . L'indirizzo IP del gateway locale deve essere all'interno della subnet VIP.
Indirizzo IP virtuale	Inserire almeno uno e non più di dieci indirizzi VIP per l'interfaccia attiva nel gruppo HA. Tutti gli indirizzi VIP devono trovarsi all'interno della subnet VIP. Almeno un indirizzo deve essere IPv4. Facoltativamente, è possibile specificare indirizzi IPv4 e IPv6 aggiuntivi.

7. Selezionare **Crea gruppo HA** e quindi selezionare **Fine**.

Creare un endpoint del bilanciatore del carico per FabricPool

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

Quando si configura StorageGRID per l'utilizzo con FabricPool, è necessario configurare un endpoint del bilanciatore del carico e caricare o generare un certificato dell'endpoint del bilanciatore del carico, che viene utilizzato per proteggere la connessione tra ONTAP e StorageGRID.

Per utilizzare la procedura guidata di configurazione FabricPool per completare questa attività, andare a ["Accedi e completa la procedura guidata di configurazione FabricPool"](#) .

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Permesso di accesso root"](#) .
- Hai esaminato il generale ["considerazioni per il bilanciamento del carico"](#) così come il ["best practice per il bilanciamento del carico per FabricPool"](#) .

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Endpoint del bilanciatore del carico**.
2. Seleziona **Crea**.
3. Per il passaggio **Inserisci i dettagli dell'endpoint**, compila i seguenti campi.

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint.

Campo	Descrizione
Porta	La porta StorageGRID che si desidera utilizzare per il bilanciamento del carico. Per impostazione predefinita, questo campo è impostato su 10433 per il primo endpoint creato, ma è possibile immettere qualsiasi porta esterna non utilizzata. Se si immette 80 o 443, l'endpoint viene configurato solo sui nodi gateway. Queste porte sono riservate sui nodi amministrativi. Nota: non sono consentite le porte utilizzate da altri servizi di rete. Vedi il "Riferimento porta di rete". Fornirai questo numero a ONTAP quando collegherai StorageGRID come livello cloud FabricPool.
Tipo di cliente	Selezionare S3 .
Protocollo di rete	Selezionare HTTPS. Nota: la comunicazione con StorageGRID senza crittografia TLS è supportata ma non consigliata.

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

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

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

Campo	Descrizione
Consenti tutti i tenant (predefinito)	Tutti gli account tenant possono utilizzare questo endpoint per accedere ai propri bucket. Consenti tutti i tenant è quasi sempre l'opzione appropriata per l'endpoint del bilanciamento del carico utilizzato per FabricPool. È necessario selezionare questa opzione se non è ancora stato creato alcun account tenant.
Consenti inquilini selezionati	Solo gli account tenant selezionati possono utilizzare questo endpoint per accedere ai propri bucket.
Blocca gli inquilini selezionati	Gli account tenant selezionati non possono utilizzare questo endpoint per accedere ai propri bucket. Tutti gli altri tenant possono utilizzare questo endpoint.

6. Per il passaggio **Allega certificato**, seleziona una delle seguenti opzioni:

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

7. Seleziona **Crea**.



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

Crea un account tenant per FabricPool

Per utilizzare FabricPool è necessario creare un account tenant in Grid Manager.

Gli account tenant consentono alle applicazioni client di archiviare e recuperare oggetti su StorageGRID. Ogni account tenant ha il proprio ID account, gruppi e utenti autorizzati, bucket e oggetti.

Per i dettagli su questa attività, vedere ["Crea un account inquilino"](#) . Per utilizzare la procedura guidata di configurazione FabricPool per completare questa attività, andare a ["Accedi e completa la procedura guidata di configurazione FabricPool"](#) .

Prima di iniziare

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

Passi

1. Selezionare **INQUILINI**.
2. Seleziona **Crea**.
3. Per i passaggi Inserisci dettagli, inserisci le seguenti informazioni.

Campo	Descrizione
Nome	Un nome per l'account del tenant. I nomi degli inquilini non devono essere univoci. Quando viene creato l'account tenant, questo riceve un ID account numerico univoco.
Descrizione (facoltativa)	Una descrizione che aiuti a identificare l'inquilino.
Tipo di cliente	Deve essere S3 per FabricPool.
Quota di archiviazione (facoltativa)	Lasciare vuoto questo campo per FabricPool.

4. Per il passaggio Seleziona autorizzazioni:

- a. Non selezionare **Consenti servizi di piattaforma**.

In genere, i tenant FabricPool non hanno bisogno di utilizzare servizi di piattaforma, come la replica di CloudMirror.

- b. Facoltativamente, seleziona **Usa la tua fonte di identità**.

- c. Non selezionare **Consenti selezione S3**.

In genere, i tenant FabricPool non hanno bisogno di utilizzare S3 Select.

- d. Facoltativamente, seleziona **Usa connessione federazione griglia** per consentire al tenant di utilizzare una ["collegamento della federazione di rete"](#) per la clonazione dell'account e la replica tra griglie. Quindi, seleziona la connessione di federazione della griglia da utilizzare.

5. Per il passaggio Definisci accesso root, specificare quale utente avrà l'autorizzazione di accesso root iniziale per l'account tenant, in base al fatto che il sistema StorageGRID utilizzi ["federazione di identità"](#) , ["accesso unico \(SSO\)"](#) , o entrambi.

Opzione	Fai questo
Se la federazione delle identità non è abilitata	Specificare la password da utilizzare quando si accede al tenant come utente root locale.
Se la federazione delle identità è abilitata	a. Selezionare un gruppo federato esistente per ottenere l'autorizzazione di accesso Root per il tenant. b. Facoltativamente, specificare la password da utilizzare quando si accede al tenant come utente root locale.

Opzione	Fai questo
Se sono abilitati sia la federazione delle identità che il Single Sign-On (SSO)	Selezionare un gruppo federato esistente per ottenere l'autorizzazione di accesso Root per il tenant. Nessun utente locale può effettuare l'accesso.

6. Selezionare **Crea tenant**.

Crea un bucket S3 e ottieni le chiavi di accesso

Prima di utilizzare StorageGRID con un carico di lavoro FabricPool , è necessario creare un bucket S3 per i dati FabricPool . È inoltre necessario ottenere una chiave di accesso e una chiave di accesso segreta per l'account tenant che verrà utilizzato per FabricPool.

Per i dettagli su questa attività, vedere ["Crea bucket S3"](#) E ["Crea le tue chiavi di accesso S3"](#) . Per utilizzare la procedura guidata di configurazione FabricPool per completare questa attività, andare a ["Accedi e completa la procedura guidata di configurazione FabricPool"](#) .

Prima di iniziare

- Hai creato un account tenant per l'utilizzo FabricPool .
- Hai accesso Root all'account tenant.

Passi

1. Sign in a Tenant Manager.

Puoi procedere in uno dei seguenti modi:

- Dalla pagina Account tenant in Grid Manager, seleziona il link * Sign in* per il tenant e inserisci le tue credenziali.
- Inserisci l'URL dell'account tenant in un browser Web e inserisci le tue credenziali.

2. Crea un bucket S3 per i dati FabricPool .

È necessario creare un bucket univoco per ogni cluster ONTAP che si intende utilizzare.

- Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (S3) > Bucket**.
- Seleziona **Crea bucket**.
- Immettere il nome del bucket StorageGRID che si desidera utilizzare con FabricPool. Ad esempio, `fabricpool-bucket` .



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

d. Seleziona la regione per questo bucket.

Per impostazione predefinita, tutti i bucket vengono creati in `us-east-1` regione.

e. Selezionare **Continua**.

f. Seleziona **Crea bucket**.



Non selezionare **Abilita controllo delle versioni degli oggetti** per il bucket FabricPool . Allo stesso modo, non modificare un bucket FabricPool per utilizzare **Disponibile** o una coerenza non predefinita. La coerenza consigliata per i bucket FabricPool è **Read-after-new-write**, che è la coerenza predefinita per un nuovo bucket.

3. Creare una chiave di accesso e una chiave di accesso segreta.

- Selezionare **ARCHIVIAZIONE (S3) > Le mie chiavi di accesso**.
- Seleziona **Crea chiave**.
- Seleziona **Crea chiave di accesso**.
- Copiare l'ID della chiave di accesso e la chiave di accesso segreta in un luogo sicuro oppure selezionare **Scarica .csv** per salvare un file di foglio di calcolo contenente l'ID della chiave di accesso e la chiave di accesso segreta.

Questi valori verranno immessi in ONTAP quando si configura StorageGRID come livello cloud FabricPool .



Se in futuro si genera una nuova chiave di accesso e una chiave di accesso segreta in StorageGRID , immettere le nuove chiavi in ONTAP prima di eliminare i vecchi valori da StorageGRID. In caso contrario, ONTAP potrebbe perdere temporaneamente l'accesso a StorageGRID.

Configurare ILM per i dati FabricPool

È possibile utilizzare questo semplice esempio di policy come punto di partenza per le proprie regole e policy ILM.

In questo esempio si presuppone che si stiano progettando le regole ILM e una policy ILM per un sistema StorageGRID dotato di quattro nodi di archiviazione in un unico data center a Denver, Colorado. I dati FabricPool in questo esempio utilizzano un bucket denominato `fabricpool-bucket` .



Le seguenti regole e policy ILM sono solo esempi. Esistono molti modi per configurare le regole ILM. Prima di attivare una nuova policy, simulala per verificare che funzioni come previsto per proteggere i contenuti dalla perdita. Per saperne di più, vedere ["Gestire gli oggetti con ILM"](#) .



Per evitare la perdita di dati, non utilizzare una regola ILM che farà scadere o eliminerà i dati del livello cloud FabricPool . Impostare il periodo di conservazione su **per sempre** per garantire che gli oggetti FabricPool non vengano eliminati da StorageGRID ILM.

Prima di iniziare

- Hai esaminato il ["best practice per l'utilizzo di ILM con dati FabricPool"](#) .
- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Autorizzazione di accesso ILM o Root"](#) .
- Se hai eseguito l'aggiornamento a StorageGRID 11.9 da una versione precedente StorageGRID , hai configurato il pool di archiviazione che utilizzerai. In generale, dovresti creare un pool di archiviazione per ogni sito StorageGRID che utilizzerai per archiviare i dati.



Questo prerequisito non si applica se inizialmente è stato installato StorageGRID 11.7 o 11.8. Quando si installa inizialmente una di queste versioni, vengono creati automaticamente dei pool di archiviazione per ogni sito.

Passi

1. Creare una regola ILM che si applica solo ai dati in `fabricpool-bucket`. Questa regola di esempio crea copie con codice di cancellazione.

Definizione della regola	Valore di esempio
Nome della regola	Codifica di cancellazione 2 + 1 per i dati FabricPool
Nome del bucket	<code>fabricpool-bucket</code> È anche possibile filtrare in base all'account tenant FabricPool .
Filtri avanzati	Dimensione dell'oggetto superiore a 0,2 MB. Nota: FabricPool scrive solo oggetti da 4 MB, ma è necessario aggiungere un filtro per le dimensioni degli oggetti perché questa regola utilizza la codifica di cancellazione.
Tempo di riferimento	Tempo di ingestione
Periodo di tempo e collocamenti	Dal giorno 0 conservalo per sempre Memorizzare gli oggetti tramite codifica di cancellazione utilizzando lo schema EC 2+1 a Denver e conservare tali oggetti in StorageGRID per sempre.  Per evitare la perdita di dati, non utilizzare una regola ILM che farà scadere o eliminerà i dati del livello cloud FabricPool .
Comportamento di ingestione	Equilibrato

2. Crea una regola ILM predefinita che creerà due copie replicate di tutti gli oggetti non corrispondenti alla prima regola. Non selezionare un filtro di base (account tenant o nome bucket) né filtri avanzati.

Definizione della regola	Valore di esempio
Nome della regola	Due copie replicate
Nome del bucket	<i>nessuno</i>
Filtri avanzati	<i>nessuno</i>
Tempo di riferimento	Tempo di ingestione

Definizione della regola	Valore di esempio
Periodo di tempo e collocamenti	Dal giorno 0 conservalo per sempre Conserva gli oggetti replicandone 2 copie a Denver.
Comportamento di ingestione	Equilibrato

3. Creare una policy ILM e selezionare le due regole. Poiché la regola di replica non utilizza alcun filtro, può essere la regola predefinita (ultima) per il criterio.
4. Inserire gli oggetti di prova nella griglia.
5. Simulare la policy con gli oggetti di prova per verificarne il comportamento.
6. Attiva la policy.

Quando questa policy è attivata, StorageGRID posiziona i dati degli oggetti come segue:

- I dati suddivisi in livelli da FabricPool in `fabricpool-bucket` verrà codificato con cancellazione utilizzando lo schema di codifica 2+1. Due frammenti di dati e un frammento di parità verranno posizionati su tre nodi di archiviazione diversi.
- Tutti gli oggetti in tutti gli altri bucket verranno replicati. Verranno create due copie e posizionate su due nodi di archiviazione diversi.
- Le copie verranno conservate in StorageGRID per sempre. StorageGRID ILM non eliminerà questi oggetti.

Creare una policy di classificazione del traffico per FabricPool

Facoltativamente, è possibile progettare una policy di classificazione del traffico StorageGRID per ottimizzare la qualità del servizio per il carico di lavoro FabricPool .

Per i dettagli su questa attività, vedere ["Gestire le policy di classificazione del traffico"](#) . Per utilizzare la procedura guidata di configurazione FabricPool per completare questa attività, andare a ["Accedi e completa la procedura guidata di configurazione FabricPool"](#) .

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#) .
- Tu hai il ["Permesso di accesso root"](#) .

Informazioni su questo compito

Le best practice per la creazione di una policy di classificazione del traffico per FabricPool dipendono dal carico di lavoro, come segue:

- Se si prevede di suddividere i dati del carico di lavoro primario FabricPool in livelli su StorageGRID, è necessario assicurarsi che il carico di lavoro FabricPool disponga della maggior parte della larghezza di banda. È possibile creare una policy di classificazione del traffico per limitare tutti gli altri carichi di lavoro.



In generale, è più importante dare priorità alle operazioni di lettura FabricPool rispetto alle operazioni di scrittura.

Ad esempio, se altri client S3 utilizzano questo sistema StorageGRID , è necessario creare una policy di classificazione del traffico. È possibile limitare il traffico di rete per gli altri bucket, tenant, subnet IP o

endpoint del bilanciatore del carico.

- In genere, non dovresti imporre limiti alla qualità del servizio su alcun carico di lavoro FabricPool ; dovresti limitare solo gli altri carichi di lavoro.
- I limiti imposti ad altri carichi di lavoro dovrebbero tenere conto del comportamento di tali carichi di lavoro. I limiti imposti varieranno anche in base alle dimensioni e alle capacità della rete e al livello di utilizzo previsto.

Passi

1. Selezionare **CONFIGURAZIONE > Rete > Classificazione del traffico**.
2. Seleziona **Crea**.
3. Inserisci un nome e una descrizione (facoltativa) per la policy e seleziona **Continua**.
4. Per il passaggio Aggiungi regole di corrispondenza, aggiungere almeno una regola.
 - a. Seleziona **Aggiungi regola**
 - b. Per Tipo, seleziona **Endpoint del bilanciatore del carico** e seleziona l'endpoint del bilanciatore del carico creato per FabricPool.

È anche possibile selezionare l'account tenant o il bucket FabricPool .
 - c. Se si desidera che questa policy del traffico limiti il traffico per gli altri endpoint, selezionare **Corrispondenza inversa**.
5. Facoltativamente, aggiungi uno o più limiti per controllare il traffico di rete a cui corrisponde la regola.



StorageGRID raccoglie le metriche anche se non si aggiungono limiti, in modo da poter comprendere le tendenze del traffico.

- a. Seleziona **Aggiungi un limite**.
 - b. Seleziona il tipo di traffico che vuoi limitare e il limite da applicare.
6. Selezionare **Continua**.
 7. Leggere e rivedere la politica di classificazione del traffico. Utilizzare il pulsante **Precedente** per tornare indietro e apportare le modifiche desiderate. Quando sei soddisfatto della policy, seleziona **Salva e continua**.

Dopo aver finito

["Visualizza le metriche del traffico di rete"](#) per verificare che le norme rispettino i limiti di traffico previsti.

Configurare ONTAP System Manager

Dopo aver ottenuto le informazioni StorageGRID richieste, puoi andare su ONTAP per aggiungere StorageGRID come livello cloud.

Prima di iniziare

- Se hai completato la procedura guidata di configurazione FabricPool , hai `ONTAP_FabricPool_settings_bucketname.txt` file che hai scaricato.
- Se hai configurato StorageGRID manualmente, disponi del nome di dominio completo (FQDN) che stai utilizzando per StorageGRID o dell'indirizzo IP virtuale (VIP) per il gruppo StorageGRID HA, del numero di porta per l'endpoint del bilanciatore del carico, del certificato del bilanciatore del carico, dell'ID della chiave di accesso e della chiave segreta per l'utente root dell'account tenant e del nome del bucket che ONTAP

utilizzerà in quel tenant.

Access ONTAP System Manager

Queste istruzioni descrivono come utilizzare ONTAP System Manager per aggiungere StorageGRID come livello cloud. È possibile completare la stessa configurazione utilizzando ONTAP CLI. Per le istruzioni, vai a ["Documentazione ONTAP per FabricPool"](#) .

Passi

1. Accedi a System Manager per il cluster ONTAP che desideri suddividere in livelli su StorageGRID.
2. Sign in come amministratore per il cluster.
3. Vai a **ARCHIVIAZIONE > Livelli > Aggiungi livello cloud**.
4. Selezionare * StorageGRID* dall'elenco dei provider di archiviazione oggetti.

Inserisci i valori StorageGRID

Vedere ["Documentazione ONTAP per FabricPool"](#) per maggiori informazioni.

Passi

1. Completa il modulo Aggiungi livello cloud, utilizzando `ONTAP_FabricPool_settings_bucketname.txt` file o i valori ottenuti manualmente.

Campo	Descrizione
Nome	Inserisci un nome univoco per questo livello cloud. È possibile accettare il valore predefinito.
Stile URL	Se tu "nomi di dominio endpoint S3 configurati" , seleziona URL in stile ospitato virtuale. Path-Style URL è l'impostazione predefinita per ONTAP, ma per StorageGRID si consiglia di utilizzare richieste in stile virtual hosted. È necessario utilizzare URL stile percorso se si fornisce un indirizzo IP anziché un nome di dominio per il campo Nome server (FQDN).
Nome del server (FQDN)	Immettere il nome di dominio completo (FQDN) utilizzato per StorageGRID o l'indirizzo IP virtuale (VIP) per il gruppo StorageGRID HA. Ad esempio, <code>s3.storagegrid.company.com</code> . Notare quanto segue: • L'indirizzo IP o il nome di dominio specificato qui deve corrispondere al certificato caricato o generato per l'endpoint del bilanciatore del carico StorageGRID . • Se si fornisce un nome di dominio, il record DNS deve essere mappato su ciascun indirizzo IP che si utilizzerà per connettersi a StorageGRID. Vedere "Configurare il server DNS" .
SSL	Abilitato (predefinito).

Campo	Descrizione
Certificato di archiviazione degli oggetti	Incolla il certificato PEM che stai utilizzando per l'endpoint del bilanciatore del carico StorageGRID , inclusi: -----BEGIN CERTIFICATE----- E -----END CERTIFICATE----- . Nota: se una CA intermedia ha emesso il certificato StorageGRID , è necessario fornire il certificato della CA intermedia. Se il certificato StorageGRID è stato emesso direttamente dalla CA radice, è necessario fornire il certificato della CA radice.
Porta	Immettere la porta utilizzata dall'endpoint del bilanciatore del carico StorageGRID . ONTAP utilizzerà questa porta quando si conatterà a StorageGRID. Ad esempio, 10433.
Chiave di accesso e chiave segreta	Immettere l'ID della chiave di accesso e la chiave di accesso segreta per l'utente root dell'account tenant StorageGRID . Suggerimento: se in futuro si genera una nuova chiave di accesso e una chiave di accesso segreta in StorageGRID , immettere le nuove chiavi in ONTAP prima di eliminare i vecchi valori da StorageGRID. In caso contrario, ONTAP potrebbe perdere temporaneamente l'accesso a StorageGRID.
Nome del contenitore	Inserisci il nome del bucket StorageGRID creato per l'utilizzo con questo livello ONTAP .

2. Completare la configurazione finale FabricPool in ONTAP.

- Collegare uno o più aggregati al livello cloud.
- Facoltativamente, creare una politica di suddivisione in livelli del volume.

Configurare il server DNS

Dopo aver configurato i gruppi ad alta disponibilità, gli endpoint del bilanciatore del carico e i nomi di dominio degli endpoint S3, è necessario assicurarsi che il DNS includa le voci necessarie per StorageGRID. È necessario includere una voce DNS per ogni nome nel certificato di sicurezza e per ogni indirizzo IP che si desidera utilizzare.

Vedere ["Considerazioni sul bilanciamento del carico"](#) .

Voci DNS per il nome del server StorageGRID

Aggiungere voci DNS per associare il nome del server StorageGRID (nome di dominio completo) a ciascun indirizzo IP StorageGRID che verrà utilizzato. Gli indirizzi IP immessi nel DNS dipendono dall'utilizzo o meno di un gruppo HA di nodi di bilanciamento del carico:

- Se è stato configurato un gruppo HA, ONTAP si conatterà agli indirizzi IP virtuali di quel gruppo HA.
- Se non si utilizza un gruppo HA, ONTAP può conatterci al servizio StorageGRID Load Balancer utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministrativo.
- Se il nome del server si risolve in più di un indirizzo IP, ONTAP stabilisce connessioni client con tutti gli

indirizzi IP (fino a un massimo di 16 indirizzi IP). Gli indirizzi IP vengono rilevati tramite un metodo round-robin quando vengono stabilite le connessioni.

Voci DNS per richieste in stile ospitato virtuale

Se hai definito ["Nomi di dominio endpoint S3"](#) e utilizzerai richieste in stile virtual hosted, aggiungerai voci DNS per tutti i nomi di dominio degli endpoint S3 richiesti, inclusi eventuali nomi jolly.

Le migliori pratiche StorageGRID per FabricPool

Procedure consigliate per i gruppi ad alta disponibilità (HA)

Prima di collegare StorageGRID come livello cloud FabricPool , informati sui gruppi ad alta disponibilità (HA) StorageGRID e rivedi le best practice per l'utilizzo dei gruppi HA con FabricPool.

Che cos'è un gruppo HA?

Un gruppo ad alta disponibilità (HA) è una raccolta di interfacce provenienti da più nodi gateway StorageGRID , nodi amministrativi o entrambi. Un gruppo HA aiuta a mantenere disponibili le connessioni dati dei client. Se l'interfaccia attiva nel gruppo HA fallisce, un'interfaccia di backup può gestire il carico di lavoro con un impatto minimo sulle operazioni FabricPool .

Ogni gruppo HA fornisce un accesso altamente disponibile ai servizi condivisi sui nodi associati. Ad esempio, un gruppo HA costituito da interfacce solo sui nodi gateway o sia sui nodi amministrativi che sui nodi gateway fornisce un accesso altamente disponibile al servizio Load Balancer condiviso.

Per saperne di più sui gruppi ad alta disponibilità, vedere ["Gestire gruppi ad alta disponibilità \(HA\)"](#) .

Utilizzo di gruppi HA

Le procedure consigliate per la creazione di un gruppo StorageGRID HA per FabricPool dipendono dal carico di lavoro.

- Se si prevede di utilizzare FabricPool con i dati del carico di lavoro primario, è necessario creare un gruppo HA che includa almeno due nodi di bilanciamento del carico per evitare interruzioni nel recupero dei dati.
- Se si prevede di utilizzare la politica di suddivisione in livelli del volume basata solo su snapshot FabricPool o livelli di prestazioni locali non primari (ad esempio, posizioni di disaster recovery o destinazioni NetApp SnapMirror), è possibile configurare un gruppo HA con un solo nodo.

Queste istruzioni descrivono come impostare un gruppo HA per HA Active-Backup (un nodo è attivo e l'altro è di backup). Tuttavia, potresti preferire utilizzare DNS Round Robin o Active-Active HA. Per conoscere i vantaggi di queste altre configurazioni HA, vedere ["Opzioni di configurazione per i gruppi HA"](#) .

Best practice per il bilanciamento del carico per FabricPool

Prima di collegare StorageGRID come livello cloud FabricPool , rivedere le best practice per l'utilizzo dei bilanciatori del carico con FabricPool.

Per informazioni generali sul bilanciatore del carico StorageGRID e sul certificato del bilanciatore del carico, vedere ["Considerazioni sul bilanciamento del carico"](#) .

Procedure consigliate per l'accesso del tenant all'endpoint del bilanciatore del carico utilizzato per FabricPool

È possibile controllare quali tenant possono utilizzare uno specifico endpoint del bilanciatore del carico per accedere ai propri bucket. È possibile consentire l'accesso a tutti gli inquilini, ad alcuni o bloccarne alcuni. Quando si crea un endpoint di bilanciamento del carico per l'utilizzo FabricPool, selezionare **Consenti tutti i tenant**. ONTAP crittografa i dati inseriti nei bucket StorageGRID, pertanto questo livello di sicurezza aggiuntivo garantirebbe poca sicurezza aggiuntiva.

Buone pratiche per il certificato di sicurezza

Quando si crea un endpoint del bilanciatore del carico StorageGRID per l'utilizzo in FabricPool, si fornisce il certificato di sicurezza che consentirà a ONTAP di autenticarsi con StorageGRID.

Nella maggior parte dei casi, la connessione tra ONTAP e StorageGRID dovrebbe utilizzare la crittografia Transport Layer Security (TLS). L'utilizzo di FabricPool senza crittografia TLS è supportato ma non consigliato. Quando si seleziona il protocollo di rete per l'endpoint del bilanciatore del carico StorageGRID, selezionare **HTTPS**. Quindi fornire il certificato di sicurezza che consentirà a ONTAP di autenticarsi con StorageGRID.

Per saperne di più sul certificato del server per un endpoint di bilanciamento del carico:

- ["Gestire i certificati di sicurezza"](#)
- ["Considerazioni sul bilanciamento del carico"](#)
- ["Linee guida per il rafforzamento dei certificati del server"](#)

Aggiungi certificato a ONTAP

Quando si aggiunge StorageGRID come livello cloud FabricPool, è necessario installare lo stesso certificato sul cluster ONTAP, inclusi i certificati radice e tutti i certificati dell'autorità di certificazione (CA) subordinata.

Gestisci la scadenza del certificato



Se il certificato utilizzato per proteggere la connessione tra ONTAP e StorageGRID scade, FabricPool smetterà temporaneamente di funzionare e ONTAP perderà temporaneamente l'accesso ai dati suddivisi in livelli su StorageGRID.

Per evitare problemi di scadenza dei certificati, seguire queste best practice:

- Monitorare attentamente tutti gli avvisi che segnalano l'avvicinarsi della data di scadenza dei certificati, come gli avvisi **Scadenza del certificato dell'endpoint del bilanciatore del carico** e **Scadenza del certificato del server globale per l'API S3**.
- Mantenere sempre sincronizzate le versioni StorageGRID e ONTAP del certificato. Se si sostituisce o si rinnova il certificato utilizzato per un endpoint del bilanciatore del carico, è necessario sostituire o rinnovare il certificato equivalente utilizzato da ONTAP per il livello cloud.
- Utilizzare un certificato CA firmato pubblicamente. Se si utilizza un certificato firmato da una CA, è possibile utilizzare l'API Grid Management per automatizzare la rotazione dei certificati. Ciò consente di sostituire i certificati prossimi alla scadenza senza interruzioni.
- Se hai generato un certificato StorageGRID autofirmato e tale certificato sta per scadere, devi sostituirlo manualmente sia in StorageGRID che in ONTAP prima che scada il certificato esistente. Se un certificato autofirmato è già scaduto, disattivare la convalida del certificato in ONTAP per evitare la perdita di accesso.

Vedere ["Knowledge Base NetApp : come configurare un nuovo certificato server autofirmato StorageGRID"](#)

su una distribuzione ONTAP FabricPool esistente" per istruzioni.

Procedure consigliate per l'utilizzo di ILM con i dati FabricPool

Se si utilizza FabricPool per suddividere i dati in livelli per StorageGRID, è necessario comprendere i requisiti per l'utilizzo della gestione del ciclo di vita delle informazioni (ILM) StorageGRID con i dati FabricPool .



FabricPool non ha alcuna conoscenza delle regole o delle policy ILM StorageGRID . Se la policy StorageGRID ILM non è configurata correttamente, si può verificare una perdita di dati. Per informazioni dettagliate, vedere ["Utilizzare le regole ILM per gestire gli oggetti"](#) E ["Creare policy ILM"](#) .

Linee guida per l'utilizzo di ILM con FabricPool

Quando si utilizza la procedura guidata di configurazione FabricPool , questa crea automaticamente una nuova regola ILM per ogni bucket S3 creato e aggiunge tale regola a un criterio inattivo. Ti verrà chiesto di attivare la policy. La regola creata automaticamente segue le best practice consigliate: utilizza la codifica di cancellazione 2+1 in un singolo sito.

Se si configura StorageGRID manualmente anziché utilizzare la procedura guidata di configurazione FabricPool , consultare queste linee guida per assicurarsi che le regole e i criteri ILM siano adatti ai dati FabricPool e ai requisiti aziendali. Potrebbe essere necessario creare nuove regole e aggiornare le policy ILM attive per soddisfare queste linee guida.

- È possibile utilizzare qualsiasi combinazione di regole di replicazione e di codifica di cancellazione per proteggere i dati del livello cloud.

La migliore pratica consigliata è quella di utilizzare la codifica di cancellazione 2+1 all'interno di un sito per una protezione dei dati conveniente. La codifica di cancellazione utilizza più CPU, ma offre una capacità di archiviazione notevolmente inferiore rispetto alla replicazione. Gli schemi 4+1 e 6+1 utilizzano meno capacità rispetto allo schema 2+1. Tuttavia, gli schemi 4+1 e 6+1 sono meno flessibili se è necessario aggiungere nodi di archiviazione durante l'espansione della griglia. Per maggiori dettagli, vedere ["Aggiungere capacità di archiviazione per oggetti con codice di cancellazione"](#) .

- Ogni regola applicata ai dati FabricPool deve utilizzare la codifica di cancellazione oppure deve creare almeno due copie replicate.



Una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo espone i dati al rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, tale oggetto viene perso se un nodo di archiviazione si guasta o presenta un errore significativo. Inoltre, durante le procedure di manutenzione, come gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

- Se hai bisogno di ["rimuovere i dati FabricPool da StorageGRID"](#) , utilizzare ONTAP per recuperare tutti i dati per il volume FabricPool e promuoverlo al livello di prestazioni.



Per evitare la perdita di dati, non utilizzare una regola ILM che farà scadere o eliminerà i dati del livello cloud FabricPool . Impostare il periodo di conservazione in ogni regola ILM su **per sempre** per garantire che gli oggetti FabricPool non vengano eliminati da StorageGRID ILM.

- Non creare regole che sposteranno i dati del livello cloud FabricPool dal bucket a un'altra posizione. Non è

possibile utilizzare un Cloud Storage Pool per spostare i dati FabricPool in un altro archivio oggetti.



L'utilizzo di Cloud Storage Pool con FabricPool non è supportato a causa della latenza aggiuntiva necessaria per recuperare un oggetto dalla destinazione di Cloud Storage Pool.

- A partire da ONTAP 9.8, è possibile creare facoltativamente tag di oggetti per facilitare la classificazione e l'ordinamento dei dati a livelli, semplificandone la gestione. Ad esempio, è possibile impostare i tag solo sui volumi FabricPool collegati a StorageGRID. Quindi, quando si creano regole ILM in StorageGRID, è possibile utilizzare il filtro avanzato Object Tag per selezionare e posizionare questi dati.

Altre best practice per StorageGRID e FabricPool

Quando si configura un sistema StorageGRID per l'utilizzo con FabricPool, potrebbe essere necessario modificare altre opzioni StorageGRID. Prima di modificare un'impostazione globale, valutare l'impatto della modifica sulle altre applicazioni S3.

Destinazioni dei messaggi di controllo e dei registri

I carichi di lavoro FabricPool presentano spesso un elevato tasso di operazioni di lettura, che può generare un volume elevato di messaggi di audit.

- Se non è necessario un record delle operazioni di lettura del client per FabricPool o qualsiasi altra applicazione S3, è possibile passare facoltativamente a **CONFIGURAZIONE > Monitoraggio > Server di audit e syslog**. Modificare l'impostazione **Letture client** su **Errore** per ridurre il numero di messaggi di controllo registrati nel registro di controllo. Vedere ["Configurare i messaggi di controllo e le destinazioni dei registri"](#) per i dettagli.
- Se si dispone di una griglia di grandi dimensioni, si utilizzano più tipi di applicazioni S3 o si desidera conservare tutti i dati di audit, configurare un server syslog esterno e salvare le informazioni di audit in remoto. L'utilizzo di un server esterno riduce al minimo l'impatto sulle prestazioni della registrazione dei messaggi di controllo senza ridurre la completezza dei dati di controllo. Vedere ["Considerazioni per il server syslog esterno"](#) per i dettagli.

Crittografia degli oggetti

Durante la configurazione di StorageGRID, è possibile abilitare facoltativamente ["opzione globale per la crittografia degli oggetti memorizzati"](#) se è richiesta la crittografia dei dati per altri client StorageGRID. I dati suddivisi in livelli da FabricPool a StorageGRID sono già crittografati, pertanto non è necessario abilitare l'impostazione StorageGRID. Le chiavi di crittografia lato client sono di proprietà di ONTAP.

Compressione degli oggetti

Quando si configura StorageGRID, non abilitare ["opzione globale per comprimere gli oggetti memorizzati"](#). I dati suddivisi in livelli da FabricPool a StorageGRID sono già compressi. L'utilizzo dell'opzione StorageGRID non ridurrà ulteriormente le dimensioni di un oggetto.

Consistenza del secchio

Per i bucket FabricPool, la coerenza consigliata è **Read-after-new-write**, che è la coerenza predefinita per un nuovo bucket. Non modificare i bucket FabricPool per utilizzare **Disponibile** o **Strong-site**.

Struttura a FabricPool

Se un nodo StorageGRID utilizza storage assegnato da un sistema NetApp ONTAP, verificare che il volume

non abbia un criterio di suddivisione in livelli FabricPool abilitato. Ad esempio, se un nodo StorageGRID è in esecuzione su un host VMware, assicurarsi che il volume che supporta il datastore per il nodo StorageGRID non abbia un criterio di suddivisione in livelli FabricPool abilitato. La disattivazione della suddivisione in livelli FabricPool per i volumi utilizzati con i nodi StorageGRID semplifica la risoluzione dei problemi e le operazioni di archiviazione.



Non utilizzare mai FabricPool per riportare i dati relativi a StorageGRID a StorageGRID stesso. Il riordino dei dati StorageGRID su StorageGRID aumenta la complessità operativa e la risoluzione dei problemi.

Rimuovere i dati FabricPool da StorageGRID

Se è necessario rimuovere i dati FabricPool attualmente archiviati in StorageGRID, è necessario utilizzare ONTAP per recuperare tutti i dati per il volume FabricPool e promuoverli al livello di prestazioni.

Prima di iniziare

- Hai esaminato le istruzioni e le considerazioni in ["Promuovi i dati al livello di prestazioni"](#) .
- Stai utilizzando ONTAP 9.8 o versione successiva.
- Stai utilizzando un ["browser web supportato"](#) .
- Appartieni a un gruppo di utenti StorageGRID per l'account tenant FabricPool che ha ["Gestisci tutti i bucket o l'autorizzazione di accesso Root"](#) .

Informazioni su questo compito

Queste istruzioni spiegano come spostare i dati da StorageGRID a FabricPool. Questa procedura viene eseguita utilizzando ONTAP e StorageGRID Tenant Manager.

Passi

1. Da ONTAP, emettere il `volume modify` comando.

Impostato `tiering-policy` A `none` per fermare la nuova suddivisione in livelli e impostare `cloud-retrieval-policy` A `promote` per restituire tutti i dati precedentemente suddivisi in livelli su StorageGRID.

Vedere ["Promuovi tutti i dati da un volume FabricPool al livello di prestazioni"](#) .

2. Attendere il completamento dell'operazione.

Puoi usare il `volume object-store` comando con il `tiering` opzione per ["verificare lo stato della promozione del livello di performance"](#) .

3. Una volta completata l'operazione di promozione, accedi a StorageGRID Tenant Manager per l'account tenant FabricPool .
4. Selezionare **Visualizza bucket** dalla dashboard oppure selezionare **ARCHIVIAZIONE (S3) > Bucket**.
5. Verificare che il bucket FabricPool sia ora vuoto.
6. Se il secchio è vuoto, ["elimina il bucket"](#) .

Dopo aver finito

Quando si elimina il bucket, la suddivisione in livelli da FabricPool a StorageGRID non può più continuare.

Tuttavia, poiché il livello locale è ancora collegato al livello cloud StorageGRID , ONTAP System Manager restituirà messaggi di errore che indicano che il bucket non è accessibile.

Per evitare questi messaggi di errore, procedere in uno dei seguenti modi:

- Utilizzare FabricPool Mirror per collegare un livello cloud diverso all'aggregato.
- Spostare i dati dall'aggregato FabricPool a un aggregato non FabricPool , quindi eliminare l'aggregato non utilizzato.

Vedi il "[Documentazione ONTAP per FabricPool](#)" per istruzioni.

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.